

# Detekcia útočníkov a anomálii v sieti

Bc. Tomáš Mišutka

---

Diplomová práce  
2022



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

## Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení: **Bc. Tomáš Míšutka**  
Osobní číslo: **A20192**  
Adresa: **Hrabové 306, Bytča, 01401 Bytča, Slovenská republika**  
  
Téma práce: **Detekce útočníků a anomálií v síti**  
Téma práce anglicky: **Detection of attackers and anomalies in the network**  
  
Vedoucí práce: **Ing. David Malaník, Ph.D.**  
**Ústav informatiky a umělé inteligence**

### Zásady pro vypracování:

1. Zpracujte mapu sítě a stanovte její kritické body.
2. Specifikujte možné hrozby pro Vámi zabezpečovanou síť.
3. Navrhněte prvky pro detekci zranitelností v dané infrastruktuře.
4. Navrhněte prvky pro monitoring provozu infrastruktury.
5. Proveďte implementaci Vašeho řešení v testovacím segmentu sítě.
6. Ověřte detekční možnosti a možnosti monitoringu na testovacím provozu.

### Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
2. WU, Chwan-Hwa a J. David IRWIN. \_Introduction to computer networks and cybersecurity\_. Boca Raton: CRC Press, c2013, xxxix, 1336 s. ISBN 9781466572133.
3. SELECKÝ, Matěj. \_Penetrační testy a exploitace\_. Brno: Computer Press, 2012, 303 s. ISBN 9788025137529.
4. STALLINGS, William a Lawrie BROWN. \_Computer security: principles and practice\_. Fourth edition. Chennai: Pearson, [2020], 800 atm. ISBN 978-93-534-3886-9.
5. PHAN HAI, Phu Nguyen, Hoa NGUYEN HONG, Bao Bui QUOC a Trang HOANG. A Comparative Research on VPN Technologies on Operating System for Routers. \_2021 International Conference on Advanced Technologies for Communications (ATC). Advanced Technologies for Communications (ATC), 2021 International Conference on\_. [online]. 2021, , 89-93 [cit. 2021-11-30]. ISBN 9781665433792. ISSN 21621039. Dostupné z: doi:10.1109/ATC52653.2021.9598334
6. XU, Zhiwei a Jie NI. Research on network security of VPN technology. \_2020 International Conference on Information Science and Education (ICISE-IE). Information Science and Education (ICISE-IE), 2020 International Conference on, ICISE-IE\_. [online]. 2020, , 539-542 [cit. 2021-11-30]. ISBN 9781665422611. ISSN edsee.IEEE Conferenc. Dostupné z: doi:10.1109/ICISE51755.2020.00121
7. TRAORÉ, Issa, Ahmed AWAD a Isaac WOUNGANG. \_Information security practices: emerging threats and perspectives\_. Cham, Switzerland: Springer, [2017], 1 online resource. Dostupné z: doi:9783319489476

Podpis studenta:

Datum:

Podpis vedoucího práce:

Datum:

### **Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen přípouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Hrabovom, dňa 23.05.2022

Tomáš Mišutka, v. r.  
podpis diplomanta

## **ABSTRAKT**

V súčasnej dobe, v ktorej pribieha kybernetická vojna, je potrebné sledovať sieťovú aktivitu viac, ako kedykoľvek predtým. Efektívny spôsob sledovania sieťovej prevádzky je nutné spojiť aj s ďalšími metódami, akými sú hľadanie zraniteľností a monitorovanie prevádzky v reálnom čase. V prípade úspešne klasifikovaného útoku vieme omnoho rýchlejšie zareagovať na vzniknutý incident, a tým predísť obrovským škodám.

Kľúčové slová: zraniteľnosť, infraštruktúra, monitoring, AlienVault OSSIM, Zabbix

## **ABSTRACT**

At time of cyber war, network activity needs to be monitored more than ever before. An effective way to monitor network traffic must also be combined with other methods, such as vulnerability detection and real-time traffic monitoring. In the case of a successfully classified attack, we can respond to the incident much more quickly, thus preventing huge damage.

Keywords: vulnerability, infrastructure, monitoring, AlienVault OSSIM, Zabbix

## Podakovanie

Týmto spôsobom sa chcem poďakovať môjmu vedúcemu tejto práce, pánovi Ing. Davidovi Malaníkovi, Ph.D. za jeho odborné rady, pomoc, ochotu a usmernenie pri vypracovaní tejto diplomovej práce. Za podporu, pochopenie a ústretovosť chcem vyjadriť veľkú vďaku aj celej svojej rodine.

Prehlasujem, že odovzdaná verzia diplomovej práce a elektronická verzia, ktorá bola nahratá do IS/STAG sú totožné.

# Obsah

ÚVOD .....	10
1. CIELE DIPLOMOVEJ PRÁCE .....	12
2. TOPOLOGIA SIETE A JEJ KRITICKÉ BODY .....	14
2.1 Časté zraniteľnosti siete .....	14
2.1.1 Fyzické zraniteľnosti.....	15
2.1.2 Nefyzické zraniteľnosti.....	15
2.1.3 Typy sieťových zraniteľností .....	15
2.2 Topológia siete .....	16
2.2.1 Segmenty siete a ich adresný rozsah.....	17
2.2.2 Adresné rozsahy sietí .....	18
3. SÚČASNÉ HROZBY A TRENDY MALVÉRU.....	19
3.1 Ransomware .....	21
3.1.1 Popis malvéru.....	21
3.1.2 Šírenie malvéru .....	22
3.1.3 Nedávne útoky ransomwaru .....	26
3.2 Novinky z vojnového konfliktu na Ukrajine.....	28
3.2.1 HermeticWiper.....	29
3.2.2 IsaacWiper .....	29
3.2.3 CaddyWipper .....	30
3.2.4 HermeticWizzard .....	30
3.3 Dopad na našu infraštruktúru .....	31
4. DETEKCIA ZRANITEĽNOSTÍ .....	33
4.1 AlienVault OSSIM.....	33
4.1.1 Základný popis.....	33
4.1.2 Možnosti nástroja.....	34
4.1.3 Test skenera hľadaním zraniteľností.....	36

4.2	Greenbone .....	37
4.2.1	Základný popis.....	38
4.2.2	Možnosti nástroja.....	38
4.2.3	Test skenera hľadáním zraniteľností.....	41
4.3	Nessus.....	42
4.3.1	Základný popis.....	42
4.3.2	Možnosti nástroja.....	43
4.3.3	Test skenera hľadáním zraniteľností.....	44
4.4	Výber nástroja na ďalšie použitie.....	45
5.	PREVÁDZKOVÝ MONITORING.....	47
5.1	Nagios.....	47
5.1.1	Základný popis.....	47
5.1.2	Možnosti nástroja.....	48
5.2	Zabbix.....	51
5.2.1	Základný popis.....	51
5.2.2	Možnosti nástroja.....	53
5.3	Výber nástroja na ďalšie použitie.....	57
6.	TESTOVACIA INFRAŠTRUKTÚRA .....	60
7.	PRÍPRAVA NÁSTROJOV .....	62
7.1	Inštalácia nástroja AlienVault OSSIM.....	62
7.1.1	Systémové prostriedky.....	62
7.1.2	Inštalácia .....	63
7.1.3	Dokončenie inštalácie grafickým zohraním.....	64
7.1.4	Úprava sieťovej konfigurácie v spoločnosti .....	65
7.2	Inštalácia nástroja Zabbix.....	66
7.2.1	Systémové prostriedky.....	66
7.2.2	Inštalácia .....	67

7.2.3	Zmena predvolených prihlasovacích údajov .....	68
7.2.4	Úprava sieťovej konfigurácie v spoločnosti .....	69
7.3	Export, overenie inštalácie a nasadenie nástrojov v spoločnosti .....	69
7.3.1	Overenie inštalácie .....	70
7.3.2	Nasadenie nástrojov v testovacej infraštruktúre .....	70
8.	IMPLEMENTÁCIA RIEŠENIA .....	71
8.1	AlienVault OSSIM .....	71
8.1.1	Konfigurácia siete .....	72
8.1.2	Assety a grupy .....	72
8.1.3	HIDS agenti .....	74
8.1.4	Aplikácia pluginov .....	78
8.1.5	Vzdialené logy .....	78
8.1.6	Dostupnosť zariadení a služieb .....	81
8.1.7	Email Relay .....	83
8.1.8	Pravidelné prehľadávanie siete .....	87
8.1.9	Hľadanie zraniteľností v sieti .....	88
8.1.10	NetFlow .....	90
8.1.11	Konfigurácia direktívy proti útoku skenovaním portov .....	94
8.2	Zabbix .....	95
8.2.1	Import šablón .....	95
8.2.2	MIKROTIK router .....	96
8.2.3	MIKROTIK switch .....	98
8.2.4	Synology NAS .....	99
8.2.5	Tlačiareň Xerox .....	101
8.2.6	Vmware ESXi .....	102
8.2.7	Nastavenie emailov .....	104
8.2.8	Kontrola dostupnosti zariadení .....	107



8.2.9	Vlastný trigger .....	109
9.	OVERENIE IMPLEMENTÁCIE .....	114
9.1	Overenie detekcie zraniteľností .....	115
9.1.1	Skenovanie portov - nmap .....	115
9.1.2	Útok hrubou silou – brute-force .....	116
9.1.3	Výsledky hľadania zraniteľností .....	121
9.1.4	Overenie emailových notifikácií .....	126
9.2	Overenie monitoringu nástrojom zabbix .....	127
9.2.1	Signalizácia problémov .....	127
9.2.2	Získavanie dát zo zariadení .....	128
9.2.3	Notifikácia o nedostupnosti .....	129
9.2.4	Overenie funkčnosti triggeru .....	130
10.	VYHODNOTENIE RIEŠENIA .....	132
	ZÁVER .....	133
	ZOZNAM POUŽITEJ LITERATÚRY .....	134
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK .....	138
	ZOZNAM OBRÁZKOV .....	140
	ZOZNAM TABULIEK .....	145
	ZOZNAM PRÍLOH .....	146

## ÚVOD

Vývoj a inovácie informačných technológií rastú tak rýchlo, ako aj stále nové a sofistikované hackerské útoky. Tieto technológie sa dotýkajú aj nás všetkých, čo vytvára pre útočníkov veľmi atraktívne prostredie. Dáta, ktoré môžu útočníci získať môžu častokrát veľmi ovplyvniť náš pracovný, ale aj súkromný život.

Hlavne v pracovnom živote je potrebné stále investovať do nových, a modernejších technológií, ktoré držia akýsi cyklus medzi stále sofistikovanejšími útokmi hackerov a bezpečnostnými technológiami. Byť dobre pripravený na útok nemôžeme byť nikdy, avšak môžeme aspoň znížiť riziko jeho úspechu. Minimálne ho môžeme útočníkovi aspoň znepříjemniť.

Jedným z podstatných faktorov zastavenia, alebo aspoň spomalenia útoku, je jeho včasná a správna klasifikácia. Preto by sa mal stále viac zvyšovať dôraz a sieťové zabezpečenie s dostatočným sieťovým monitoringom a hľadaním anomálií.

Práca obsahuje niekoľko tzv. anglicizmov, ktoré jasnejšie popisujú prvok alebo výraz v porovnaní so slovenským prekladom.

# **I. TEORETICKÁ ČASŤ**

## 1. CIELE DIPLOMOVEJ PRÁCE

Cieľom tejto diplomovej práce je analyzovať mapu siete, stanoviť jej kritické body a navrhnúť a implementovať konkrétny systém na monitorovanie infraštruktúry, ktorá obsahuje približne 250 zariadení. Práca obsahuje zoznámenie sa s možnosťami dostupných nástrojov na detekciu útočníkov a anomálií v sieti s použitím sieťového monitoringu. Cieľom bude zabezpečiť infraštruktúru pred útokmi ako z vnútornej, tak aj z vonkajšej siete a celé riešenie na záver otestovať v testovacom segmente infraštruktúry spoločnosti.

V teoretickej časti sme sa zamerali na sieťovú infraštruktúru, kde sme vytvorili mapu siete spoločnosti, v ktorej sme stanovili jej kritické body, a podľa aktuálnych hrozieb a trendov sme upozornili na aktuálne bezpečnostné hrozby.

Zároveň sme sa zamerali na aktuálne hrozby a trendy malvéru, ktoré dnes predstavujú bezpečnostné riziko každej infraštruktúry. Bližšie sme popísali problematiku, ktorú so sebou prináša malvér typu ransomware, akú podobu môže byť, čo je jeho úlohou, ako sa šíri v sieti či ako sa do cieľovej infraštruktúry dostane.

Zároveň sme informovali o niekoľkých známych útokoch z Česko-slovenského kyberpriestoru, napríklad útok na Národnú knižnicu ČR alebo Fakultnú nemocnicu v Brne a ďalšie 2 útoky. Z nich sme mali možnosť vidieť, aký môže mať tento malvér dopad na akúkoľvek infraštruktúru. V krátkosti sme sa zamerali aj na novinky z aktuálnej kybernetickej vojny, ktorá vypukla ihneď po vzniku vojenského konfliktu na Ukrajine. Objavilo sa tam niekoľko nových deštruktívnych malvérov, ktorú majú veľmi podobnú úlohu ako ransomware s tým rozdielom, že jeho cieľom nie je dáta šifrovať, ale priamo ich zničiť či poškodiť systémové súbory a znefunkčniť systém.

V ďalších kapitolách teoretickej časti sme spravili výber potencionálne vhodných nástrojov na detekciu zraniteľností a anomálií v sieti a ich vzájomné porovnanie medzi sebou. V každom porovnaní sme sa zamerali na pozitívne, ale aj negatívne vlastnosti daného nástroja. Medzi vybranými nástrojmi nesmel chýbať softvér, akým je AlienVault OSSIM, Greenbone OpenVAS či linuxovým Nessus. Všetky tieto nástroje sú voľne k použitiu, tzv. open-source, takže k nim nebolo treba dodať žiadnu licenciu, aj keď vývojári týchto nástrojov ponúkajú aj rozšírenú verziu s licenciou.

Rovnakým spôsobom sme sa zamerali aj na výber a porovnanie nástrojov na prevádzkový monitoring siete. Za potencionálne vhodných kandidátov sme zvolili nástroj Zabbix a Nagios. V krátkosti sme sa s nástrojmi zoznámili vo vlastnej testovacej infraštruktúre.

V praktickej časti sme implementovali riešenie podľa požiadaviek externej spoločnosti, kde bolo potrebné sa zamerať na detekciu útočníkov, klasifikáciu a analýzu anomálii v sieti, a celé riešenie sme vyvíjali, a implementovali v testovacej segmente spoločnosti. Tá obsahovala potrebné zariadenia vrátane klonov zariadení z reálnej prevádzky.

Úlohou bolo klasifikovať útoky a oznámiť o tejto udalosti administrátora. Nasadenie vytvoreného riešenia do produkcie bolo vykonané vo vlastnej réžií sieťovým administrátorom spoločnosti podľa konfigurácie tejto práce.

## 2. TOPOLOGIA SIETE A JEJ KRITICKÉ BODY

Mapa siete alias sieťová infraštruktúra sú výrazy, ktoré sú v tejto diplomovej práci veľmi často spomínané, preto je na úvod dôležité objasniť, čo sa pod týmto slovným spojením z nášho hľadiska myslí, a aké zraniteľnosti sa v sieťach bežne vyskytujú.

Sieťovú infraštruktúru tvoria všetky zariadenia, ktoré sú pripojené do siete a umožňujú pripojenie na internet, správu, obchodné operácie či externú alebo internú komunikáciu. Zariadenia si predstavujeme ako výpočtovú techniku, ktorá zabezpečuje komunikáciu medzi používateľmi, službami, aplikáciami či procesmi. Zariadením môže byť v dnešnej dobe prakticky čokoľvek, od najsofistikovanejších a najmodernejších serverov až po jednoduché jednoúčelové sieťové prvky alebo zariadenia [1].

Problém však nastáva, keď sa pozrieme na oblasť bezpečnosti v našej sieťovej infraštruktúre, kde nastávajú možné hrozby. Kybernetická bezpečnosť je stále viac aktuálnou témou tohto obdobia, na ktorú sa kladie čoraz väčší dôraz.

V Českej republike je definovaný zákon číslo 205/2017 Sb., ktorý upravuje zákon číslo 181/2014 Sb. o kybernetickej bezpečnosti a bol vydaný Národným úradom pre kybernetickú a informačnú bezpečnosť (NÚKIB) Českej republiky, ktorý upravuje zaistenie bezpečnosti sietí elektronických komunikácií a informačných systémov [2].

Na Slovensku nadobudol zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti účinnosť 1. apríla 2018, ktorý definoval Národný bezpečnostný úrad (NBÚ) a ten komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti a uvádza základné bezpečnostné požiadavky a opatrenia, ktoré sú dôležité pre ochranu komunikačných a riadiacich systémov. Aj keď znenie týchto zákonov v oboch štátoch znie veľmi podobne, je tam dosť rozdielov, kde popis či analýza týchto rozdielov nie sú cieľom tejto práce [3].

### 2.1 Časté zraniteľnosti siete

Zraniteľnosť infraštruktúry je slabina alebo chyba v softvéri, v hardvéri prípadne v ďalších procesoch, v ktorých sa nachádza bezpečnostná chyba, čo vedie k možnému narušeniu bezpečnosti dát a prevádzky siete. Zraniteľnosti existujú ako fyzické, tak aj nefyzické [4].

### 2.1.1 Fyzické zraniteľnosti

Fyzická zraniteľnosť siete poukazuje na dôležitosť správneho uloženia serveru a ďalších prvkov kritickej infraštruktúry do uzamykateľného racku so zámkom pomocou klasického kľúčového zámku alebo zámku s vyžiadaním si prístupového kódu. Dôvodom sú dôležité a citlivé informácie, akými sú náležité právne dokumenty či obchodné tajomstvá, ale aj poskytovanie web-hostingu a mnohé ďalšie. Ďalším odporúčením je zaviesť prísne fyzické bezpečnostné kontroly na vstupe do dátového centra, napríklad zavedením biometrických skenerov alebo prístupových kariet, čím sa eliminuje riziko fyzického prístupu neoprávnených osôb k zariadeniam [4].

### 2.1.2 Nefyzické zraniteľnosti

Tento typ zraniteľnosti sa týka všetkého, čo súvisí so zabezpečením prístupu k údajom a ďalším softvérom. Môžu to byť práve neaktualizované OS, ktoré sú ľahko infikovateľné na novo-vznikajúce hrozby a cez toto jedno zariadenie sa môže veľmi jednoducho infikovať potenciálne aj celá sieť. Medzi nefyzické zraniteľnosti sa radí aj zlyhanie ľudského faktoru napríklad pri phishingových útokoch [4].

### 2.1.3 Typy sieťových zraniteľností

Sieťové zraniteľnosti vystupujú v rôznych formách, avšak najčastejšie sa prejavujú ako:

- Malvér – alebo škodlivý softvér, akým je Trojan, vírus alebo červ, ktoré sa inštalujú na serveri alebo na používateľské počítače a zariadenia
- Sociálne inžinierstvo – snaží sa zatlačiť na slabú stránku, akým je ľudský faktor, ktorým sa snaží získať prihlasovacie údaje alebo infiltrovať sa do systému
- Zastaralé systémy a softvér – veľmi častým úspechom kybernetických útokov je práve zastaranosť a neaktuálnosť softvéru a systémov, vďaka ktorým je možné infiltrovať malvér do celej siete
- Zlá konfigurácia systémov a nástrojov – ďalšia kritická zraniteľnosť, ktorá však nie je zapríčinená samotným zlyhaním systému, ale iba nevhodnou, či nedostatočnou konfiguráciou [5].

Túto podkapitolu nebudeme ďalej a hlbšie rozvíjať, pretože popis typov malvéru je detailnejšie popísaný v ďalších kapitolách tejto práce. Cieľom je len priblíženie a oboznámenie čitateľa o najbežnejších zraniteľnostiach v sieťovej infraštruktúre, na ktoré chceme ešte pred

vytvorením topológie siete poukázať. Neskôr počas návrhu riešenia tieto súvislosti musíme zobrať do úvahy a budeme musieť s nimi počítať. Ďalším cieľom je analyzovať aktuálne trendy malvéru, aké udalosti vznikli dôsledkom nasadenia malvéru a aké hrozby sa v súčasnej dobe objavujú. Na túto problematiku sa zameriavame v ďalšej kapitole tejto práce.

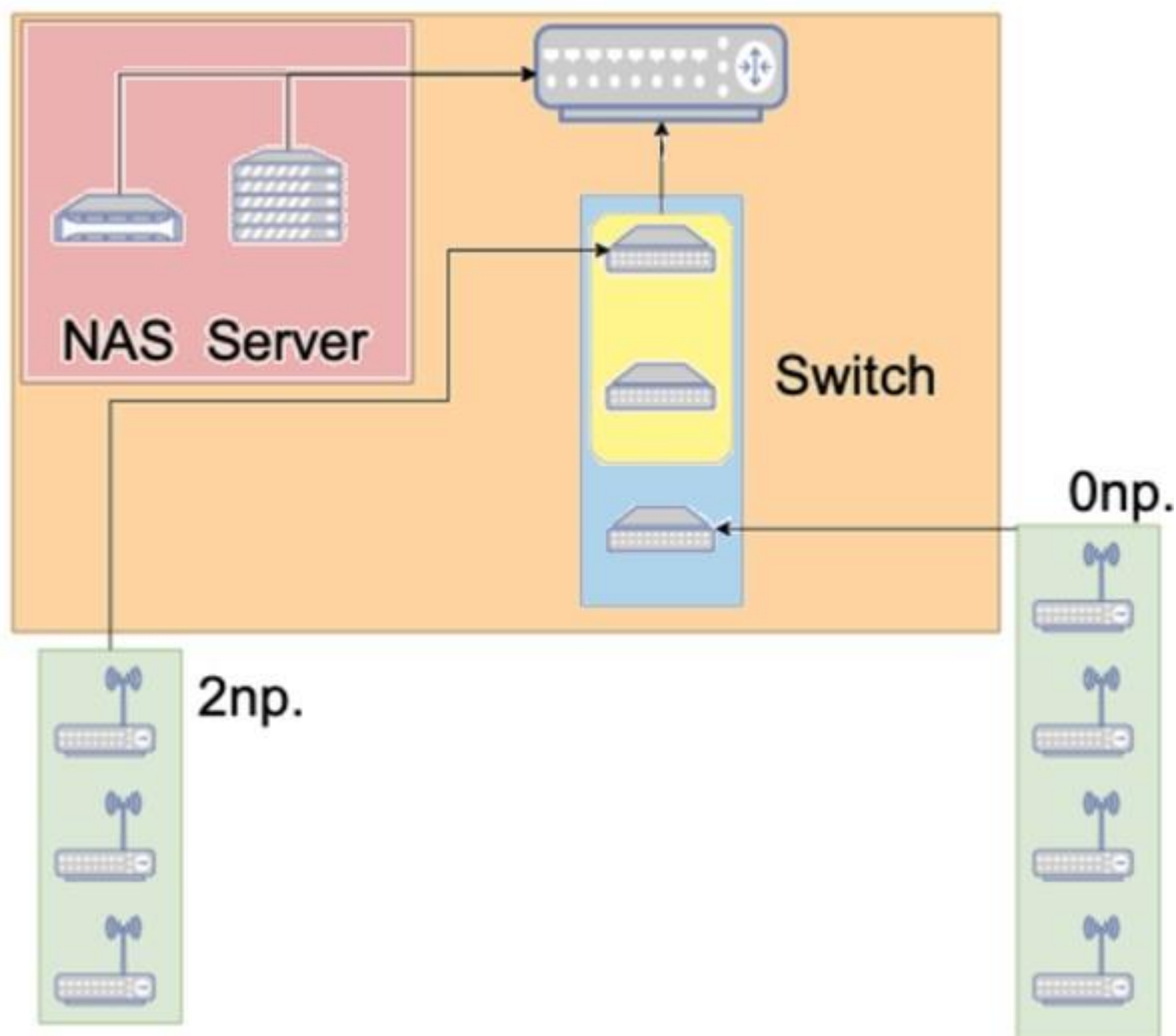
## 2.2 Topológia siete

V tejto podkapitole sa zameriame na zostavenie a detailný popis infraštruktúry, ktorú sme vytvorili v spolupráci s externou spoločnosťou. Cieľom bude analyzovať kritickú a primárnu časť infraštruktúry a nasadiť riešenie, ktoré zlepší monitorovanie a hľadanie anomálií v sieti. Z bezpečnostných dôvodov a preventívnych opatrení nám nebol umožnený prístup do živej prevádzky spoločnosti a vykonať skenovanie zariadení v našej réžií.

Infraštruktúra je rozdelená na tri základné segmenty, ktoré sú bližšie popísané v tejto podkapitole. Segmenty siete sú rozdelené nasledovne:

- Kritická infraštruktúra (červenou farbou)
- Primárny segment siete (oranžovou farbou)
- Sekundárny segment siete (zelenou farbou)





Obrázok 2.1 Infraštruktúra spoločnosti, zdroj vlastný

V kritickej infraštruktúre sa nachádza niekoľko kritických prvkov, medzi ktoré patrí z nášho pohľadu hlavne NAS server, ktorý si získa našu hlavnú pozornosť. Ďalším dôležitým prvkom bude centrálny router a niekoľko switchov, ktoré sú umiestnené v primárnom segmente infraštruktúry, a naším hlavným cieľom bude zamerať sa na detekciu zraniteľností a prevádzkový monitoring v kombinácii s hľadaním anomálií.

### 2.2.1 Segmenty siete a ich adresný rozsah

Adresné rozsahy, sieťové pravidlá a politika sú rozdelené podľa segmentov, ktoré sme zdefinovali vyššie a sú od seba navzájom oddelené. Každý segment má určené striktné pravidlá, kto s kým, a kam môže daná sieť komunikovať.

V kritickom segmente sa nachádza sieť *Management*, čo je servisná sieť, ktorá zabezpečuje management všetkých ďalších segmentov a pre všetkých používateľov, a zvyšné

segmenty je skrytá. Pripojenie umožňuje iba znalosť SSID a hesla. Do tejto siete sú zaradené aj aktívne a pasívne prvky z primárneho, ale aj sekundárneho segmentu.

Ďalšie siete sa nachádzajú v sekundárnej časti infraštruktúry, ktoré oddeľujú hlavne zariadenia hostí a návštevy od svojich vlastných zamestnancov. Sieť, ktorá je vyhradená pre návštevy má názov *Hosts* a má pridelený maximálny počet zariadení na cca 150 zariadení. Zvyšné 2 siete majú názov *Employees* a *EmplOwn*.

V sieti *Employees* sa nachádzajú len zariadenia z internej siete, do ktorej sa dostanú zamestnanci len z priestorov kancelárie alebo pomocou VPN pripojenia s potrebnou autentifikáciou. Do tejto siete sa môžu zároveň pripojiť iba firmou vybrané a schválené zariadenia.

Poslednou sieťou segmentu je sieť s názvom *EmplOwn*, do ktorej dostanú prístup súkromné zariadenia zamestnancov a pripojiť sa môžu taktiež len splnením potrebnej autentifikácie. Táto sieť v porovnaní s predchádzajúcou, nemá prístup do internej siete ale len na internet.

### 2.2.2 Adresné rozsahy sietí

Adresný rozsah v kritickej časti a primárnom segmente siete je *192.168.4.0/24*. Tento adresný priestor je vyhradený pre zariadenia, ktoré sa nachádzajú v sieti *Management* a *Employees*.

Druhým adresným rozsahom je *192.168.5.0/24* a do tejto siete sú priradené zariadenia zo sietí *Hosts* a *EmplOwn*.

### 3. SÚČASNÉ HROZBY A TRENDY MALVÉRU

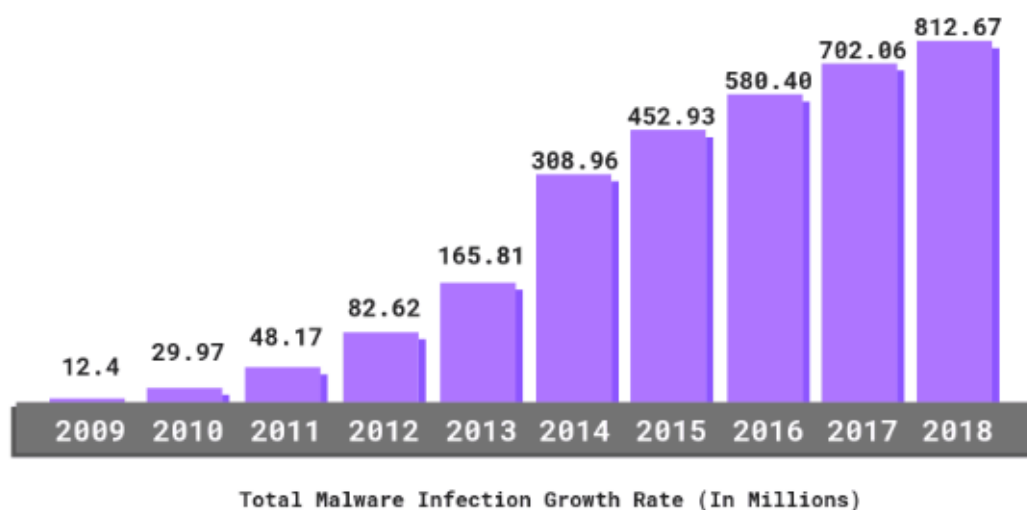
Malvér je akýkoľvek škodlivý program vytvorený s cieľom znefunkčniť alebo ovládnuť počítačový systém, prípadne vytvoriť aspoň určitý zmätok v systéme. Jeho podoba sa neustále mení a denne sa objavuje niekoľko desiatkov, či dokonca stovák nových spôsobov a variantov, aký môže malvér mať, čo vytvára veľký nátlak na odborníkov z oblasti bezpečnosti. Tento nátlak sa však premietol aj do technológie či novších a bezpečnejších systémov, čo medzi hackermi a bezpečnostnými odborníkmi vytvára akýsi neustále sa vyvíjajúci ekosystém.

Napriek všetkým odporúčaniam a zavedeným opatreniam proti malvéru hackeri stále hľadajú nové spôsoby prelomenia a infiltráciu systému, najmä ak sa jedná o nemalé peniaze. Aktuálne v roku 2022 sa však zdá, že hackeri začínajú meniť svoje taktiky tak, že vytvárajú stále nové, ešte neobjavené spôsoby v porovnaní s tými známymi, ale nedostatočne zabezpečenými. Aktuálne trendy a dáta poukazujú na to, že hackeri presúvajú svoje úsilie zamerané na infiltráciu do infraštruktúry prostredníctvom zraniteľností v IoT zariadeniach alebo prostredníctvom infikovanej prílohy alebo podvodného linku phishingovým útokom.

V roku 2020 po skúsenostiach spoločností a firiem vyšlo, že až v 61% prípadov sa aktivita malvéru začala šíriť práve od jedného zamestnanca k druhému dôsledkom phishingového útoku. V roku 2021 táto hodnota dokonca stúpila až na hodnotu 74%. Nárast šírenia malvéru práve od jedného zamestnanca k druhému môže mať hneď niekoľko dôvodov, je to však spojené najmä s tým, že ľudia začali pracovať viac z domu v porovnaní s obdobím pred pandémiou covid-19 [6].

Existuje niekoľko typov malvéru, ako sú počítačové vírusy, trojské kone, spyware, ransomware, adware, červy, file-less malvér alebo hybridné útoky. Posledné útoky sa stávajú stále viac sofistikované práve využívaním strojového učenia či umelou inteligenciou, dokonca aj v cielených phishingových kampaniach, čo je šírenie malvéru prostredníctvom emailov s cieľenými obeťami.

Celková aktivita kybernetických útokov rástla a stále rastie doslova o niekoľko miliónov vzoriek ročne, čo môžeme vidieť aj v nasledujúcom grafe 3.1. V grafe môžeme pozorovať nárast v priebehu 10 rokov do roku 2018 o takmer 800 miliónov vzoriek malvéru za rok v porovnaní s rokom 2009.



Obrázok 3.1 Nárast malvéru počas obdobia od roku 2009 až 2018, zdroj [7]

Z toho je nárast o 92% útokov viac, ktoré boli doručené práve emailovou komunikáciou. Rovnako je na vzostupe aj počet nových variantov pre mobilné zariadenia, čo v roku 2018 znamenalo nárast o 54%.

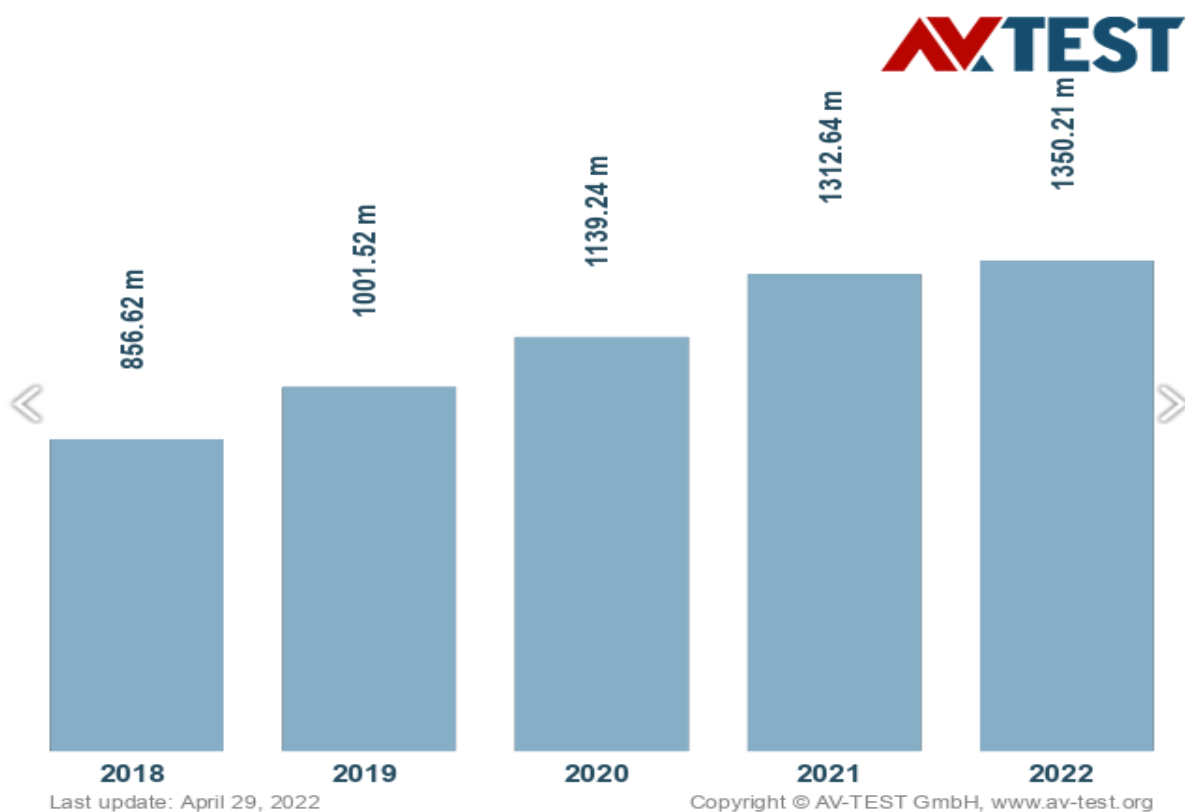
Najčastejšie sa mobilný malvér šíri prostredníctvom aplikácii tretích strán, čo je v prepočte nárast až o 99%. Príkladom je malvérová aplikácia *Trojan-Banker.AndroidOS.Asacub*, ktorá napadla viac ako 250 tisíc unikátnych používateľov. Štatistika zároveň ukazuje, že až 98% mobilného malvéru sa zameriava na zariadenia s OS Android.

Za posledné obdobie vzrástol aj malvér cielený na zariadenia od spoločnosti Apple a jeho MacOS, a to konkrétne o 165%.

Aktivita trojského koňa bola zaznamenaná až v 51.45% prípadov spomedzi všetkých malvérov. Popularitu naberá v poslednom období najmä malvér typu ransomware, ktorý bol objavený až v 7 z 10 vzorkách malvérov. V roku 2018 sa každý deň vyprodukovalo v priemere 230 tisíc nových vzoriek malvéru, a tak sa dalo predpokladať, že tento počet bude ešte stále rásť [7].

Aktuálne sa nachádzame na hodnote okolo 450 tisíc nových vzoriek malvéru a neželaných aplikácií za deň. Mnohé nové vzorky malvérov sú aktívne len krátku dobu, a len malá čiastka z nich je aktívna dlhšie časové obdobie. Na nasledujúcom grafe 3.2 je zobrazená aktuálna hodnota nových vzoriek malvéru za posledných 5 rokov, údaje sú vyčíslené v miliónoch [8].

## Total malware



Obrázok 3.2 Aktuálne hodnoty vzoriek malvérov za posledných 5 rokov, zdroj [8]

### 3.1 Ransomware

V tejto podkapitole sa zameriavame na malvér typu ransomware, ktorého aktivita sa zaznamenáva čoraz častejšie, čo predstavuje pre nás, a aj našu infraštruktúru potencionálne vysoké riziko ohrozenia. Výstupom bude popis malvéru, spôsob jeho šírenia, možné ekonomické dopady a zároveň si popíšeme aj niekoľko známych útokov z nášho blízkeho okolia, ktoré sa udiali v neďalekej minulosti.

#### 3.1.1 Popis malvéru

Ransomware je typ malvéru, ktorý infikuje zariadenie a dokáže ho kompletne uzamknúť, prípadne zašifrovať cielený obsah alebo diskovú partíciu. Majiteľovi zariadenia sa zobrazia presné inštrukcie na zaplatenie výkupného. Hackeri pritom sľubujú bez akejkoľvek právnej či neprávnej záruky, že po zaplatení výkupného obnovia prístup k zašifrovaným dátam alebo zariadeniam.

Úspešný útok ransomware je ľahko rozpoznateľný na napadnutom zariadení, pretože vo väčšine prípadov je táto skutočnosť zobrazená priamo na obrazovke monitoru po zapnutí zariadenia [9].

Existuje hneď viacero druhov a techník tohto šifrovacieho malvéru:

- **Diskcoder ransomware** – táto technika spôsobí zašifrovanie celého disku a zakáže používateľovi prístup k OS
- **Screen locker** – táto technika zablokuje prístup k obrazovke zariadenia
- **Crypto-ransomware** – šifruje dáta, ktoré sú uložené na disku v zariadení obete
- **PIN locker** – táto technika je zameraná na mobilné zariadenia s OS Android, ktorej úlohou je zmeniť prístupové kódy do zariadenia alebo aplikácii [9]

Ransomware pri svojej protizákonnej činnosti používa asymetrické šifrovanie. Ide o kryptografiu, ktorá používa kľúčový pár na šifrovanie a na dešifrovanie dát. Tento pár sa skladá z verejného a privátneho kľúča, ktoré sú jedinečne vygenerované útočníkom pre svoju obeť, pričom privátny kľúč slúži na dešifrovanie dát. Tieto privátne kľúče obetí sú uložené na tzv. C&C serveroch, ktoré hackeri po zaplatení výkupného sprístupnia svojej obeti. Z vyhodnotenia nedávnych kampaní typu ransomware môžeme konštatovať, že v skutočnosti nie vždy je tomu tak.

Tento malvér, ako aj ďalšie typy malvérov, sú distribuované hlavne prostredníctvom emailových spamových kampaní alebo cielených útokov. Po úspešnom spustení malvéru v zariadení sa aktivuje škodlivá časť kódu, ktorá vystupuje v systéme ako binárny súbor. Tento súbor následne vyhľadáva, a potom šifruje všetky cenné súbory, ako sú dokumenty vo formáte .doc, .docx a rôzne iné formáty reprezentujúce textový súbor. Ďalej sa zameriava na obrázky, databázy, a ďalšie iné. Ransomware tiež hľadá ďalšie zraniteľnosti zariadenia, ktorými by bolo možné rozšírenie do iných systémov, a možno aj do celej siete v organizácii [10].

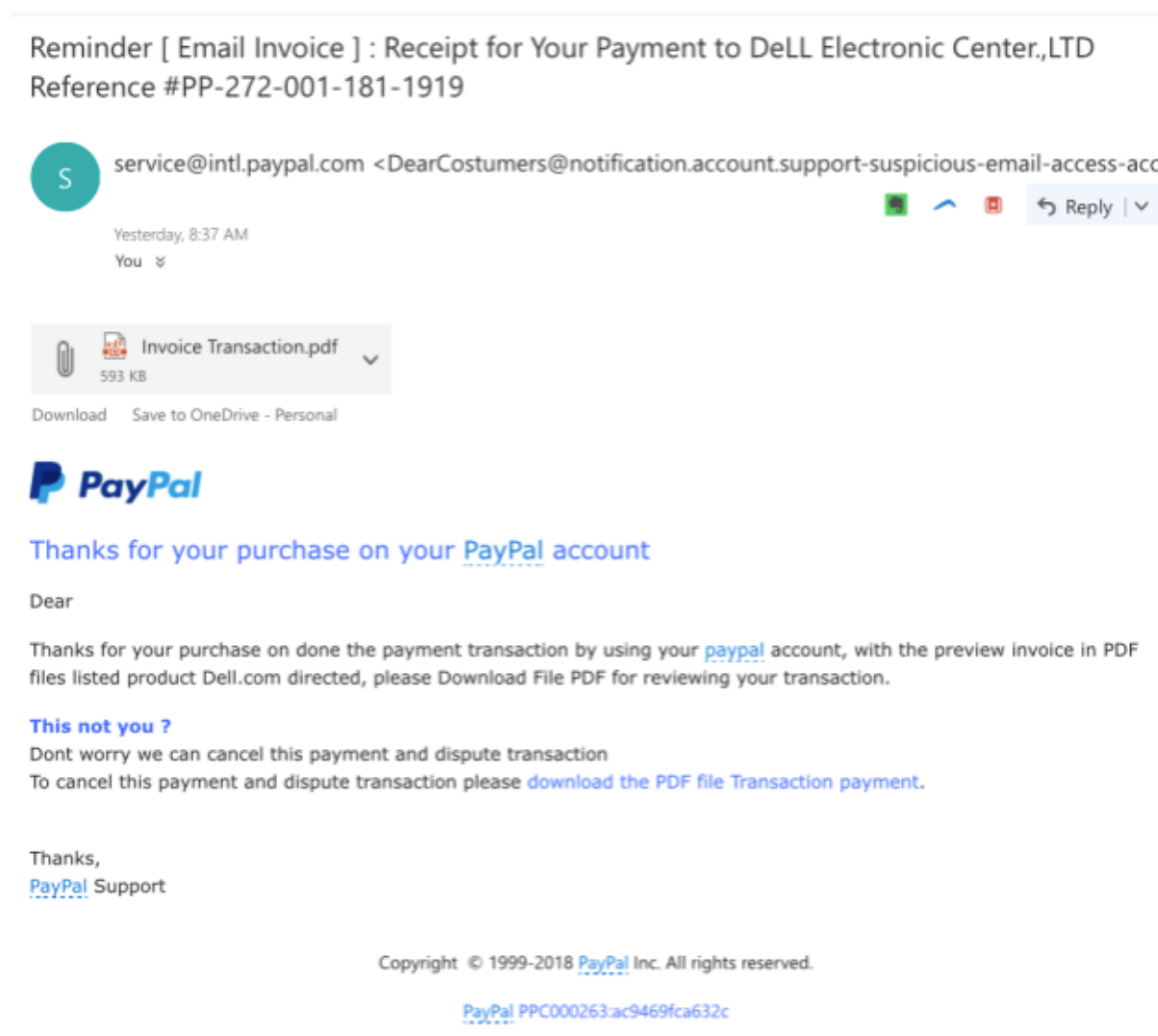
### 3.1.2 Šírenie malvéru

#### Emaily - phishing

Ako bolo spomenuté viackrát v tejto práci, aktuálnym trendom šírenia malvérov je najmä správne použité a na mieru prispôsobené sociálne inžinierstvo. Nie to tomu inak ani v prípade malvéru ransomware, ktorý motivuje prijímateľa emailu otvoriť, stiahnuť alebo inštalovať

škodlivú prílohu. Príloha je často v súborovom formáte PDF, tabuľkový súbor, dokumenty programu Microsoft Word alebo ZIP.

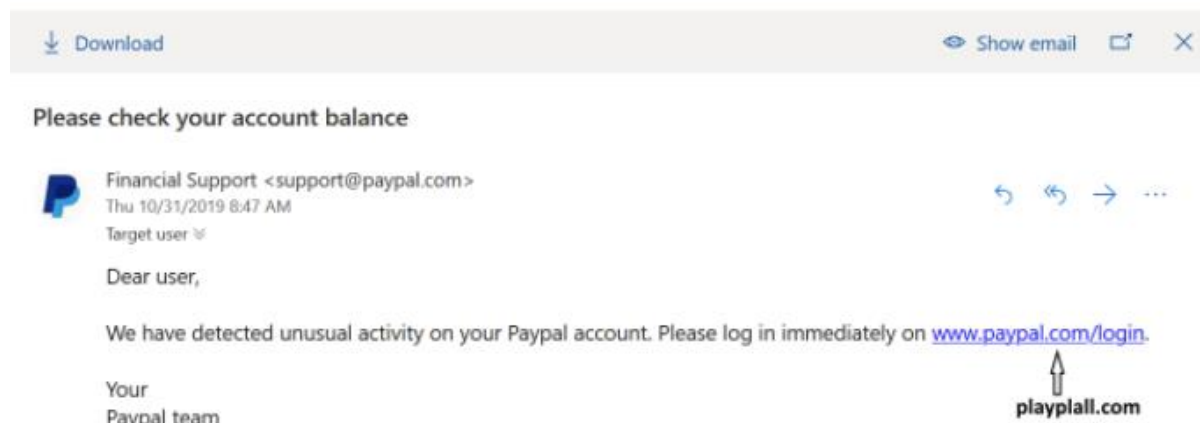
Keď používateľ na zariadení otvorí infikovanú prílohu, ransomware sa ihneď pokúsi preniknúť do systému a okamžite začať s činnosťou, avšak to nie je vždy pravidlom. Hlavným cieľom je úspešne nasadiť škodlivý kód na zariadenie. Štruktúra a forma malvéru často závisí aj od cieľa, kam bude smerovaný. Preto hackeri často robia obrovský výskum a experimentujú, aby bolo ich sociálne inžinierstvo v emailoch čo najdôveryhodnejšie. Pretože čím dôveryhodnejší email obdrží riaditeľ, vedúci pracovník alebo ktokoľvek ďalší s adminovskými právami, tým prichádza väčšia šanca na úspech [11].



Obrázok 3.3 Ukážka infikovanej prílohy s využitím platobnej brány PayPal, zdroj: [12]

## Falošné URL adresy

Novinkou nie sú ani škodlivé URL adresy šírené prostredníctvom emailov a sociálnych sietí. V druhej polovici roku 2019 bolo takmer každé štvrté šírenie malvéru typu ransomware prostredníctvom phishingu s falošnou URL adresou. Hlavným cieľom je prinútiť svoju obeť konať okamžite a s naliehavosťou kliknúť na falošný odkaz. Po kliknutí na odkaz sa spustí stiahnutie malvéru, ktorý postupne začne prenikať cez systém a šifrovať dáta [13].



Obrázok 3.4 Falošná URL adresa, kde útočník vyzýva svoju obeť na okamžité prihlásenie sa do platobnej brány PayPal, zdroj: [14]

## RDP protokol

RDP je komunikačný protokol, ktorý umožňuje pripojenie na ďalší počítač prostredníctvom sieťového pripojenia. Aj toto je veľmi častá cesta prieniku malvéru do infraštruktúry. Príkladom malvéru ransomware, ktorý sa šíril práve prostredníctvom tohto protokolu, boli napríklad SamSam, Dharma, GandGrab a mnohé ďalšie.

Predvolený sieťový port tohto protokolu je 3389. Hackeri to využívajú tak, že najskôr použijú rôzne skenery portov na odhalenie počítačov, ktoré majú dostupné porty priamo z celého internetu. Potom sa pokúsia preniknúť do systému využitím akejkoľvek bezpečnostnej chyby alebo použitím brute-force útoku na získanie prihlasovacích údajov.

Akonáhle útočník získa prístup k zariadeniu, môžeme sa začať správať, akoby mu dané zariadenie patrilo. Zvyčajne začne vypnutím antivírusových a iných bezpečnostných riešení, zmazanie dostupných záloh zariadenia a následne prichádza nasadenie malvéru. Občas hackeri inštalujú do zariadenia aj zadné vrátka, ktoré by mohli v budúcnosti použiť [13].

## Malvertising

Toto je spôsob, pri ktorom hackeri skrývajú škodlivý kód do legítimných online reklamných agentúr a sietí. Reklama je zvyčajne dostatočne agresívna a prispôbená na to, aby svoju



obet' prinútila na ňu kliknúť a tá ich presmeruje na falošné webové stránky. Týmto útokom bolo umožnené sa zacieliť aj na používateľov známych a vysoko uznávaných spoločností, ako sú *The New York Times*, *The London Stock Exchange* či *Spotify*, ktoré boli vtiahnuté do tejto kampane.

Ekosystém reklám online je veľmi komplexná sieť, ktorá zahŕňa vlastníkov stránky, reklamné servery, zámenu reklám či údaje o sieťach, kam sa ma obsah doručiť. Po kliknutí na reklamu dôjde k niekoľkým presmerovaniam medzi servermi, čo umožňuje útočníkom schovať malvér na miesta, ktoré sú len veľmi ťažko predvídateľné [15].

### USB kľúč

Ďalšou cestou, ako je možné prepašovať malvér do cieľovej infraštruktúry je stále vhodne podsunuté USB zariadenie. V roku 2016 to bolo také kritické, že Austrálska polícia vydala pre občanov a spoločnosti varovanie, že v poštových schránkach sa začali objavovať infikované USB kľúče. Tieto jednotky predstierali, že sa v nich nachádzajú propagačné kupóny k aplikácií Netflix a po otvorení sa nič netušiaciej obeti zašifrovalo zariadenie.

Niektoré vzorky malvéru mali dokonca schopnosť sa replikovať na ďalšie USB kľúče a iné vymeniteľné médiá, ktoré sa skrývali v skrytých súboroch. To umožnilo ešte lepšie šírenie sa pomocou vymeniteľných médií na ďalšie počítače, do ktorých sa médium pripojilo [16].

### Pirátsky softvér

Nakoniec ďalším, no určite nie posledným, je šírenie tohto malvéru prostredníctvom tzv. pirátskeho softvéru alebo cez tzv. crack verzie oficiálnych programov. Tieto programy prichádzajú s mnohými neželanými darčekom, ktoré môžu obsahovať ransomware rovnako ako aj ďalšie varianty malvéru alebo adware. Tieto neoficiálne verzie nielen že nepriamo zvyšujú riziko infekcie ransomwarom, ale aj nedostávajú potrebné aktualizácie, ktoré by práve útočníci mohli využiť.

V roku máji 2021 ransomware úspešne prenikol do jednej z nemenovaných európskych laboratórií, ktorá sa zaoberala výskumom nového vírusu COVID-19. Toto laboratórium malo blízke partnerstvá a vzájomnú spoluprácu s univerzitami, čo umožnilo študentom pripojiť sa k internej sieti laboratória. Jeden zo študentov si stiahol neoficiálnu verziu softvéru, ktorý používali na prácu aj predtým, avšak licencia stála niekoľko stoviek dolárov za rok. Študent teda stiahol pirátsky softvér a spustil ho na zariadení s OS Windows, a tým zaviedol malvér do celej siete výskumného centra [17].

### 3.1.3 Nedávne útoky ransomwaru

V tejto časti si objasníme niekoľko útokov ransomwaru z nedávnej minulosti, ktoré prebehli na našom území v Českej a Slovenskej republike. Medzi útokmi nesmie chýbať útok na Fakultnú nemocnicu v Brne, magistrát mesta Olomouc, Národná knižnica ČR či útok na slovenskú televíznu stanicu Senzi.

#### Fakultná nemocnica v Brne

Útok na Fakultnú nemocnicu v Brne nastal okolo 02:00 hodiny v noci 13.03.2020. Nebol to však ojedinelý útok na zdravotnícke zariadenia v Českej republike. Odložené boli všetky plánované operácie a akútnych pacientov boli nútení previesť do okolitých krajských nemocníc a iných nemocníc v Brne. Základná prevádzka nemocnice však okolo 10:00 hod. bola obnovená.

Funkčné zostali laboratória, hematológia, diagnostika, rádiologické systémy, avšak nebolo možné z týchto oddelení dáta prenášať do databázového systému. Základná prevádzka nemocnice pozostávala z vypisovania receptov na papier, obnovilo sa písanie a písacích strojoch a podobne. Vyšetrenia prebiehali štandardným spôsobom, aj keď lekári nemali prístup k údajom pacienta a databáze.

Okrem fakultnej nemocnice bola zasiahnutá aj detská nemocnica a pôrodnica v centre mesta. Na vyšetrovaní sa ihneď okrem polície začal podieľať aj NÚKIB [18].

Niekoľko hodín bol nefunkčný web nemocnice a neprístupný bol aj internetový objednávací systém na darovanie krvi. Napadnuté boli aj niektoré administratívne, ale aj ekonomické dáta. Časť z nich sa ale podarilo obnoviť prostredníctvom histórie z emailovej komunikácie [19].

Napadnuté boli aplikačné servery s OS Windows, zašifrovaný bol VIS SharePoint Online, ktorý spôsobil stratu 6 ročného vývoja aplikácii, ktoré podporovali informovanosť a pracovný proces. Ďalej boli zašifrované zariadenia, ktoré sa len pripravovali do prevádzky, a ďalšie neštandardne prevádzkované a nezabezpečené systémy či úložiská, ktoré boli ešte stále v správe dodávateľov. Útočníkom sa nepodarilo zašifrovať dostatočne zabezpečené zálohy dát pacientov a primárnych databáz.

Obnova Fakultnej nemocnice trvala rádovo niekoľko týždňov, len prvých 14 dní potrebovali takmer všetci zamestnanci IT oddelenia nemocnice na obnovu infraštruktúry a dátového centra s spolupráci s NÚKIB. Podarilo sa im na core switche zlepšiť segmentáciu siete a nasadili sa aj chýbajúce ACL. Ďalší 1 až 3 mesiace potrebovali na obnovu primárnych systémov a 4 až 6 týždňov zabral čas s výmenou asi 2500 HDD, inštaláciou systému a jeho konfigurácie

s ďalším potrebným softvérom na prácu. Až po období jedného roka od incidentu sa podarilo vo Fakultnej nemocnici nasaďiť hraničný firewall a pripojiť celú infraštruktúru na SOC. Antivírusovú ochranu na všetky koncové zariadenia sú v riešení doteraz [20].

### **Magistrát mesta Olomouc**

Rozsiahle kybernetické útoky zasiahli v apríli 2021 aj magistrát mesta Olomouc. Zasiahnutá bola celá dátová sieť a z bezpečnostných dôvodov boli odpojené jednotlivé systémy. Nasledovalo odstavenie webu, presunutie databázy, nastavenie novej ochrany a obnovenie webu [21].

Napadnuté a zašifrované boli centrálné servery malvérom typu ransomware, konkrétne Avaddon a útočníci požadovali výkupné za dešifrovanie systémov v hodnote 100 tisíc dolárov v kryptomenách, čo je v prepočte 2.1 milióna českých korún. Po odmietnutí zaplatiť výkupné prišlo po dvoch týždňoch k ďalšiemu útoku, tento raz mal útok charakter DDoS, avšak tento útok bol úspešne odvrátený. Sieť magistrátu bola odstavená približne na mesiac, kedy boli odstavené aj služobné emaily pracovníkov. Nefunkčný bol dokonca aj systém na platenie parkovného prostredníctvom SMS alebo mobilnej aplikácie. Hackerov sa doteraz nepodarilo identifikovať a obviniť [22].

Hackeri sa dostali do systémov prostredníctvom jedného prvku, ktorý obsahoval kritickú chybu v softvéri a zároveň bol v internete verejne dostupný. Cez tento prvok boli použité ďalšie techniky na krádež hesiel vrátane toho administrátorského. Dáta, ktoré obsahovali kontaktné údaje z platieb za komunálny odpad či kontaktné údaje pracovníkov magistrátu, boli neskôr aj zverejnené, dôvodom bolo nezapletenie výkupného [23].

### **Národná knižnica ČR**

Národná knižnica ČR sídliaca v Prahe sa stala 18.05.2021 terčom kybernetického útoku. Po zistení útoku bola knižnica ihneď pre verejnosť uzavretá a nedostupné boli aj online služby, ktoré knižnica poskytovala. V tejto organizácii bolo registrovaných okolo 30 tisíc čitateľov a knižnica sa radí medzi najstaršie české verejné knižnice. Zároveň spravuje najväčší knižný fond v Česku. Fond spravuje viac ako 6 miliónov dokumentov historickej i novodobej literatúry a ročne pribudne do zbierky zhruba 70 tisíc titulov [24].

Útok bol zaznamenaný jedným z pracovníkov pre podporu koncových zariadení, keď sa pokúšal o štandardnú kontrolu zariadení a ich aktualizáciu pomocou konzoly antivírusového programu. Tá bola však nedostupná. Pri základnej diagnostike systému a stavu ďalších zariadení

bolo zistené zašifrovanie serveru. Neskôr sa zistilo, že na napadnutých zariadeniach došlo k prihláseniu pomocou údajov doménového administrátora.

Pri ďalšej analýze sa zistilo, že niekoľko zamestnancov knižnice reagovalo na emailové výzvy o obnovu hesla do systému Windows, ktoré boli doručené z adresy pracovníka Slovenského hydrometeorologického ústavu, ktorý s národnou knižnicou úzko spolupracuje. Následne bol tento ústav kontaktovaný a ten potvrdil narušenie bezpečnosti aj na jeho strane. Zasiiahnuté boli systémy s OS Windows, systémy na platforme LINUX poškodené neboli.

Útok bol vedený pravdepodobne z Ruska prostredníctvom prieniku cez VPN knižnice a útok bol vedený proti portom 445 a 3389. Po získaní prihlasovacích údajov cez dôkladný phishingový útok sa hacker začal prihlasovať na pracovné stanice a servery, kde vypol antivírový systém a spúšťal na nich ransomware. Obnova infraštruktúry, systémov a následná modernizácie topológie a technológií trvala niekoľko týždňov [25].

### Televízia Senzi

Výnimku v kyberpriestore nedostáva ani Slovenská republika, ktorá čelí taktiež masívnym kybernetickým útokom. Populárnu slovenskú televíziu zasiahol v piatok 20. novembra 2020 hackerský útok typu ransomware.

Časť vysielania sa podarila obnoviť už po 24 hodinách vytvorením nového vysunutého pracoviska s novou technikou a v inej lokalite. Časť programovej štruktúry či grafiky bola zašifrovaná. Zašifrované boli všetky počítače vrátane záloh, čo znemožnilo obnovu systémov a museli sa hľadať iné alternatívy, napríklad prostredníctvom externých spoločností. Spoločnosť, ktorá vlastnila televíznu stanicu však na zaplatenie výkupného nepristúpila a podala trestné oznámenie. Spôsobené škody zverejnené neboli [26].

## 3.2 Novinky z vojnového konfliktu na Ukrajine

Novinky z oblasti malvéru, ktoré sa začali objavovať tesne pred vojnovým konfliktom Ruskej federácie a Ukrajiny, čoho dôsledkom je aktuálne prebiehajúca kybernetická vojna, ktorá zachytáva neustály vývoj praktík v hackerskej činnosti. Od začiatku roka 2022 odborníci v oblasti bezpečnosti identifikovali už niekoľko nových typov malvéru, ktoré sú určené na likvidáciu dát, známe ako wipre. Niektoré z nich objavila Slovenská spoločnosť ESET, pred začiatkom Ruskej vojenskej ofenzívy na Ukrajinu a ďalšie počas nej. Podľa spoločnosti ESET boli zasiiahnuté najmä veľké organizácie a kritická infraštruktúra Ukrajiny a v spolupráci s expertmi z tímu Symantec v spravodajstve o hrozbách uviedli, že nové druhy malvéru zasiahli aj

ukrajinských vládnych dodávateľov pochádzajúcich z Lotyšska a Litvy a ďalšie ukrajinské finančné inštitúcie [27].

### 3.2.1 HermeticWiper

Tento malvér sa objavil niekoľko hodín pred začiatkom invázie, kedy ukrajinské vládne inštitúcie a bankový sektor bol zahľtený mohutnými DoS a DDoS útokmi, ktorý vyradili z prevádzky niekoľko webových portálov. Po týchto útokoch bol zaznamenaný tento wiper na stovkách zariadení. ESET nazval tento nový malvér podľa odcudzeného digitálneho certifikátu od spoločnosti *Hermetica Digital Ltd.*

Tento malvér bol navrhnutý na prienik do zariadení s OS Windows, ktorý mal schopnosť obísť jeho bezpečnostné nástroje a tak získať práva na zápis do mnohých nízko-úrovňových dátových štruktúr na disku. 32-bitový windowsový spúšťač súbor s ikonou darčeku, ktorý mal názov *cl.exe* musel byť spustený s administrátorskými právami na to, aby dosiahol úspech. Po spustení malvéru sa disk začal fragmentovať. Už počas behu malvéru niektoré aplikácie systému prestali pracovať, pretože malvér prepisoval časť disku náhodnými dátami tak, aby po reštarte OS Windows nebol viac dostupný [28].

Okrem toho hackeri sa zamerali aj na fragmentáciu súborov na disku s cieľom prepísať ich, aby nebola možná obnova dát. Pri analýze a prieskume tohto malvéru sa zistilo, že v tejto kampani boli zapracované aj ďalšie komponenty, ktoré majú znaky červa a typického ransomvéru [29].

ESET poukázal na skutočnosť, že komponentom malvéru bol červ známy ako *HermeticWizzard*, ktorý sa použil na šírenie malvéru *HermeticWipper* v lokálnej sieti [30].

### 3.2.2 IsaacWiper

Tento nový malvér zasiahol najmenej 1 ukrajinskú vládnu spoločnosť v deň začiatku invázie. Časové otlčky tohto malvéru však siahajú ešte do októbra minulého roku 2021, čo znamená že útok sa pripravoval už mesiace predtým. Podľa odborníkov zo spoločnosti ESET mohol byť malvér nasadený aj v predchádzajúcich operáciách, ale nemusel byť zachytený. Nová verzia tohto malvéru prišla na druhý deň invázie, teda 25.02.2022, ktorý obsahoval nasadenie logov na debugging, čo môže nasvedčovať tomu, že predchádzajúce útoky nemuseli byť úspešné. Stringové výpisy do konzoly umožňovali developerom pochopiť, čo sa na infikovaných zariadeniach aktuálne deje.

IsaacWiper patrí do rodiny deštruktívnych malvérov pre OS Windows, ktorý prepisuje všetky fyzické i logické diskové zväzky v počítači. Cieľom hackerov je zničenie dát na zariadeniach svojich obetí a spraviť systémy tak, aby neumožnili znovu bootovať a prinútiť obeť preinštalovať systém. Tento wiper prechádza všetky systémové súbory a prepisuje ich, čo je podobné správanie ako u ransomvéru, ale v tomto prípade nie je potrebný žiadny dešifrovací kľúč [31].

### 3.2.3 CaddyWipper

Ruská invázia pokračuje a CaddyWipper už je tretí nový malvér počas invázie a štvrtý v poradí, ktorý zasahuje Ukrajinskú infraštruktúru mazaním dát. Tento malvér bol zachytený po prvýkrát 14.03.2022, keď mazal používateľské dáta, informácie o partíciách z pripojených zväzkov.

Malvér je cielený na počítače a servery, ktoré zohrávajú rolu doménového radiča v sieti. Počítače, ktoré nesplňujú túto nutnú požiadavku doménového radiča poškodené nebudú a malvér svoju aktivitu ukončuje. Ak sa cieľové zariadenie identifikuje ako doménový radič, Caddy začne mazanie v adresároch „C:\\Users“, s cieľom nepoškodiť systémovú časť, predtým ako sa spustí kompletne mazanie dát. Následne sa začnú prehľadávať a postupne ničiť diskové oddiely od D:\\ až po Z:\\. Ak bol malvér spustený s administrátorskými právami, premaže sa kompletne aj fyzická časť disku na absolútne znefunkčnenie OS.

Malvér poškodzuje každý možný súbor, na ktorý narazí, avšak prepíše jeho časť od začiatku súboru do veľkosti maximálne 10 MB kvôli jeho optimalizácií a výkonnosti. Caddy sa môže spustiť ako s administrátorskými právami, tak aj bez nich. No v oboch prípadoch spôsobuje škody, ktoré značne poškodzujú systém alebo menia dáta bezcennými [32].

### 3.2.4 HermeticWizzard

Tento malvér do rodiny malvéru typu červ, ktorý bol nasadený na Ukrajinské ciele okolo obeda deň pred inváziou. Vystupoval vo forme DLL súboru, naprogramovaný v jazyku C++, ktorý exportuje funkcie *dllIntall*, *DllRegisterServer* a *DllUnregisterServer* a celý súbor má názov *Wizzard.dll*.

Obsahuje tri zdroje, ktoré sú šifrované ako súbory PE:

- Vzorka *HermeticWipera* (912342F1C840A42F6B74132F8A7C4FFE7D40FB77)
- Súbor *exec\_32.dll* zodpovedný za šírenie na počítače v lokálnej sieti cez WMI (6B5958BFABFE7C731193ADB96880B225C8505B73)

- *romance.dll* zodpovedný za šírenie na počítače v lokálnej sieti prostredníctvom SMB

Tieto tri zdroje sú šifrované reverznou slučkou XOR a každé 4 bajty sú šifrované predchádzajúcimi 4 bajtmi a prvý blok je šifrovaný pevnou hodnotou *0x4A29B1A3*.

Následne sa spustí príkazový riadok a začne sa skúmať lokálne sieť hľadaním ďalších zariadení v podobe IP adries. Po skenovaní siete sa pokúsi vytvoriť nové TCP pripojenie na porty 20, 21, 22, 80, 135, 137, 139, 443 a 445 v náhodnom poradí. Na disk dostupných zariadení v sieti nasadí tzv. WMI spreader, pomocou ktorého sa vytvorí nová relácia v príkazovom riadku s cieľom nasadiť do systému HermeticWiper. Rovnaký proces prebieha aj v prípade protokolu SMB [33].

### 3.3 Dopad na našu infraštruktúru

Stále vyššiu popularitu tohto malvéru si ukážeme aj na nasledujúcej štatistike, z ktorej dostávame výstup zobrazujúci celkové škody spôsobené týmto malvérom za rok 2021. Zároveň sa budeme snažiť poukázať na možné škody, ktoré by mohli vzniknúť aj v nami zabezpečovanej infraštruktúre.

Za minulý rok 2021 bolo zaznamenaných viac než 304 tisíc útokov malvérom ransomware po celom svete. Zároveň sa ukázalo, že každá novo-vzniknutá organizácia je napadnutá každých 11-14 sekúnd. Z toho až 73% útokov dosiahlo úspech zašifrovaním dát. Zároveň sa ukázalo, že až 97% útokov za úspešne infiltrovalo do systému za menej ako 4 hodiny. Tie najrýchlejšie to dokonca stihli aj za menej ako 45 minút.

V dôsledku úspešných útokov za posledný rok pozastavenie biznisu cielených spoločností vzrástlo až o 200% a náklady, ktoré boli potrebné na toto pozastavenie, sú o neuveriteľných 2300% vyššie ako je priemerná hodnota sumy v žiadosti o výkupné.

Celkové globálne náklady spojené s obnovou po útoku malvérom ransomware presiahla v roku 2021 hodnotu 20 miliárd amerických dolárov [34].

Z uvedených faktov je jasné, že úspešný útok by mal obrovský dopad aj na našu infraštruktúru a škody by boli rovnako enormné a vysoké, čo nám zobrazuje štatistika vyššie.

Z pohľadu nami zabezpečovanej infraštruktúry spoločnosti by bola ovplyvnená najmä nedostupnosť digitálnych komplexných projektov v spolupráci s externými spoločnosťami, problém vo vývoji webových či mobilných aplikácií, problém pri riadení projektov či poskytovaní podpory prostredníctvom zákazníckeho call centra a helpdesku. Nebolo by možné ani

pokračovať v monitoringu sociálnych médií, vytváraní grafického UI a UX dizajnu alebo optimalizácia firemných procesov ďalším firmám. Ďalej by to mohla byť nedostupnosť programov na administratívu miezd a ďalšie dáta s tým spojené vrátane osobných údajov a zmlúv zamestnancov. Taktiež by bola vo veľkej miere obmedzená aj práca samotných zamestnancov. V neposlednom rade by bola nedostupná aj SMS brána, profesionálny nástroj na online správu spotrebiteľských súťaží, ďalej nástroj na centrálné riadenie pobočiek, ich zamestnancov a marketingových kampaní. Taktiež by nebolo možné využívať online bezpečnostné prvky a mnohé ďalšie produkty a služby, ktoré spoločnosť poskytuje.

Preto bude potrebné sa dôkladne zamerať na detailný prevádzkový monitoring siete hlavne aktívnych a pasívnych prvkov v spolupráci s hľadaním anomálii. Dôležitou úlohou bude zabezpečiť infraštruktúru aj na všetkých koncových zariadeniach a zabezpečiť ich aktuálnosť hardvéru a aktualizácie OS a ďalšieho softvéru vrátane antivírusových riešení, na ktoré sme upozornili a zabezpečenie týchto prostriedkov bude mať na zodpovednosť administrátor spoločnosti.



## 4. DETEKCIA ZRANITEĽNOSTÍ

V tejto kapitole venujeme pozornosť potenciálne vhodným kandidátom na detekciu zraniteľností v sieti. Ako vhodných kandidátov sme vybrali nástroj AlienVault OSSIM, Greenbone či Nessus. Na každý nástroj sa pozrieme detailnejšie v ďalších podkapitolách a rozoberieme si ich možnosti, ktoré poskytujú. Dôležitou časťou bude aj schopnosť objavovania zraniteľností či detekcia anomálií v sieti. S každým jedným nástrojom sa v krátkosti zoznámime vo vlastnej testovacej infraštruktúre. Nástroje budeme inštalovať vo virtuálnom prostredí pomocou *Vmware Workstation Pro*. V závere tejto kapitoly zhrnieme dôležité vlastnosti nástrojov, spravíme ich krátke porovnanie. Následne vyberieme najvhodnejší nástroj, ktorý použijeme v riešení tejto práce.

### 4.1 AlienVault OSSIM

#### 4.1.1 Základný popis

AlienVault OSSIM je bezpečnostný, celosvetovo uznávaný open-source nástroj označovaný ako SIEM, ktorý poskytuje množstvo funkcií doplnených zberom udalostí, normalizáciou a koreláciou dát. Tvorcovia tohto nástroja priniesli tento nástroj kvôli nedostatku produktov s otvoreným zdrojovým kódom. Jeho prínosom malo byť hlavne zlepšenie kvality v oblasti bezpečnosti, pretože v tejto oblasti sa stretávame najmä s komerčným vývojom nástrojov.

Tento nástroj dopĺňa prázdne miesta medzi open-source nástrojmi tým, že poskytuje jednotnú platformu s mnohými základnými bezpečnostnými funkciami, akými sú:

- Objavovanie aktív v sieti, tzv. *asset discovery*
- Vyhľadávanie a ohodnotenie zraniteľností
- Detekcia neúspešných prihlásení
- Monitoring celkového sieťového správania sa
- Monitoring služieb na zariadeniach
- Normalizácia a korelácia SIEM udalostí
- Jednoduchá podpora cez produktové fórum
- Manažment alarmov
- Analýza rizika
- Notifikácie v reálnom čase
- Grafické užívateľsky prívetivé rozhranie

- Štatistika prevádzky vykreslená v rôznych grafoch
- Detailná dokumentácia v online či off-line režime

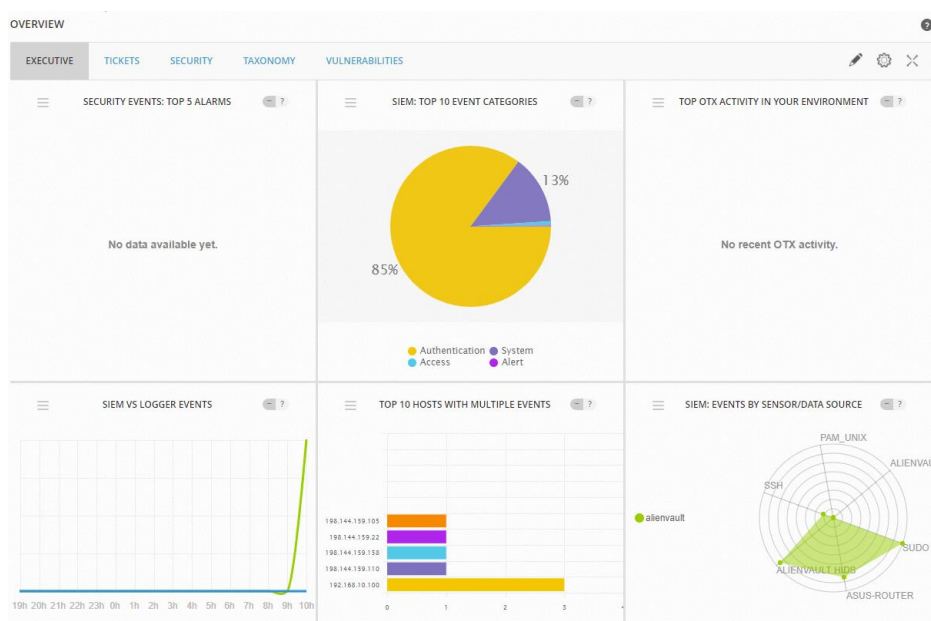
Tento nástroj naberá na sile tým, že ponúka využívať komunitu OTX, čo umožňuje používateľov pridávať, ale aj prijímať informácie o škodlivých hostiteľoch a udalostiach v reálnom čase. Dôležitým faktom je neustály vývoj nástroja proti stále novším, a sofistikovanejším hackerským aktivitám. Autori sa snažia stále inovovať bezpečnostné technológie na zlepšenie bezpečnosti všetkých. Ďalšou snahou tohto nástroja je presvedčiť spoločnosti, ktoré berú bezpečnosť na ľahkú váhu, že táto oblasť pre biznis skutočne veľmi dôležitá. AlienVault OSSIM ponúka šancu zvýšiť viditeľnosť, prehľadnosť a kontrolu bezpečia v sieťovej infraštruktúre. Možnosti tohto nástroja však nekončia a je možné ich rozšíriť komerčnou licenciou o mnohé ďalšie funkcionality [35].

#### 4.1.2 Možnosti nástroja

Nástroj bolo potrebné najskôr nainštalovať. Inšalačný súbor sme stiahli z oficiálnej stránky [cybersecurity.att.com](http://cybersecurity.att.com) vo formáte .iso s verziou 8.5.8.

Inštalácia pozostávala z niekoľkých jednoduchých krokov ako je sieťová konfigurácia, voľba jazyka, rozloženie klávesnice a podobne. Inštaláciu sme dokončili konfiguráciou vyplnením údajov prostredníctvom webového rozhrania.

Po prihlásení sa nám zobrazila úvodná stránka, kde sa nachádza prehľad o sieťovej prevádzke a zachytených aktivitách.



Obrázok 4.1 Úvodná stránka v nástroji AlienVault OSSIM, zdroj vlastný

Pri tomto prehľade sa nachádza aj niekoľko ďalších prehľadných údajov, napríklad o bezpečnostných tiketoch, bezpečnosti, klasifikácií údajov alebo o objavených zraniteľnostiach.

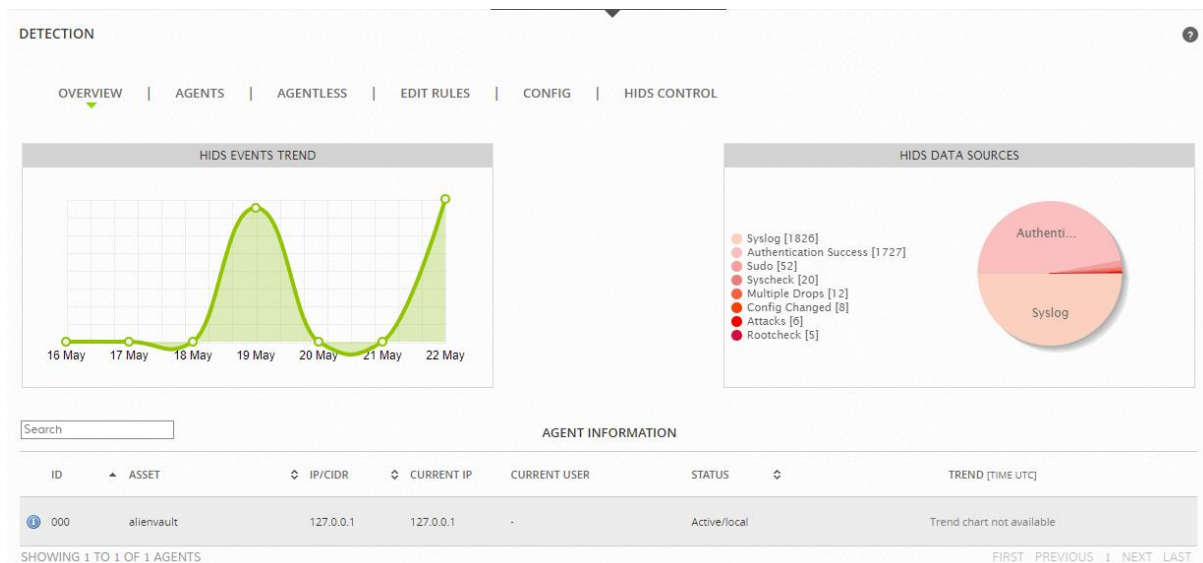
Ďalej tento softvér ponúka možnosti na analýzu dát v záložke *ANALYSIS*, kde máme možnosť si zobrazit' údaje o aktuálnych alarmoch, tzv. surových dátach, tiketoch či SIEM.

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS. 10,694 TOTAL EVENTS IN DATABASE.

<input type="checkbox"/> EVENT NAME	▼ DATE GMT+2:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
Asus-router: Generic event	2022-05-22 11:57:43	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
Asus-router: Generic event	2022-05-22 11:57:32	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
Asus-router: Generic event	2022-05-22 11:57:26	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
Asus-router: Generic event	2022-05-22 11:57:12	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session closed.	2022-05-22 11:57:02	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2022-05-22 11:57:02	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
SSHD: Session disconnected	2022-05-22 11:57:02	alienvault	N/A	alienvault:50330	alienvault:22	2->2	LOW (0)
sudo: Session opened	2022-05-22 11:57:00	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
SSHD: Session disconnected	2022-05-22 11:57:00	alienvault	N/A	alienvault:50328	alienvault:22	2->2	LOW (0)
SSHD: Session disconnected	2022-05-22 11:57:00	alienvault	N/A	alienvault:50326	alienvault:22	2->2	LOW (0)

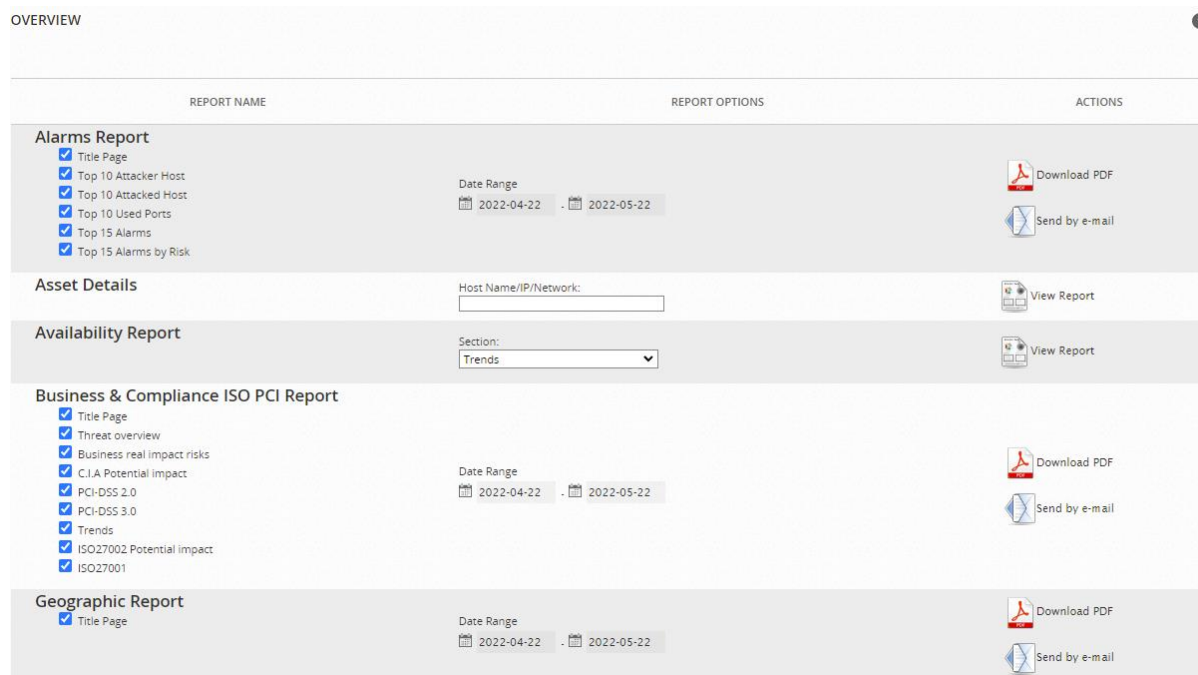
Obrázok 4.2 Dáta zachytené prostredníctvom SIEM v nástroji AlienVault OSSIM, zdroj vlastný

Hlavné menu nám ponúka ďalšiu kategóriu, ktorou je záložka *ENVIRONMENT*, v ktorej máme možnosti konfigurovať a pridávať zariadenia, skupiny, netflow, dostupnosť zariadení alebo služieb či detekciu zraniteľností. V časti detekcia máme možnosť nasadiť monitorovací nástroj priamo na koncové stanice cez tzv. *HIDS* agentov alebo *agentless* cez protokol *ssh*.



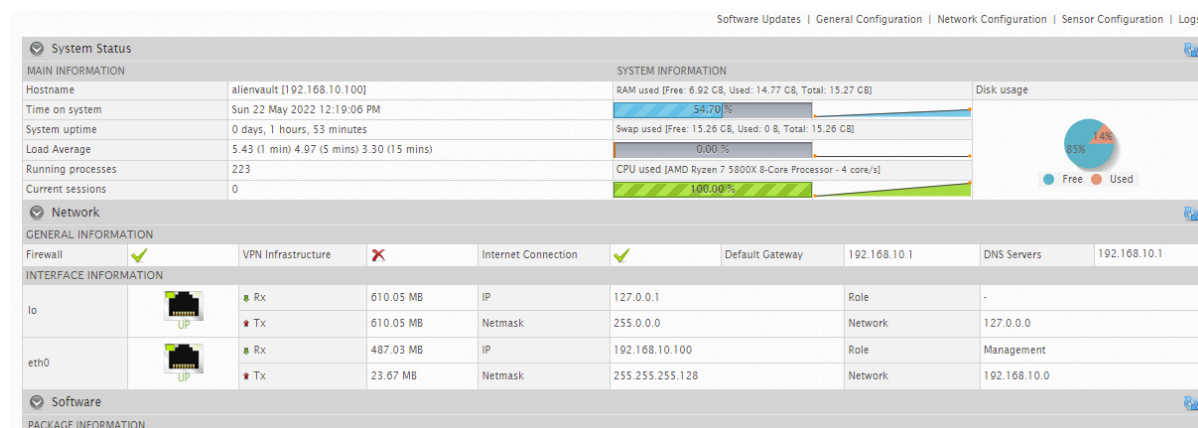
Obrázok 4.3 Správa a aplikácia agentov na koncové zariadenia v nástroji AlienVault OSSIM, zdroj vlastný

Nástroj ponúka aj generovať a stiahnuť report podľa vlastných kritérií. Táto možnosť je dostupná v časti z hlavného menu *REPORTS*. Reporty máme možnosť si nechať poslať emailom, zobrazit' vo formáte *HTML* alebo si ich priamo stiahnuť cez prehliadač v *.pdf* súbore.



Obrázok 4.4 Možnosti reportov v nástroji AlienVault OSSIM, zdroj vlastný

V poslednej časti sa nachádzajú možnosti konfigurácie celého nástroja, ktorá zahŕňa administratívu, konfiguráciu senzorov, možnosti na aktualizáciu či zmenu sieťových alebo všeobecných nastavení. Taktiež sa tam nachádza aj konfigurácia direktív, ktorý je možné zabezpečiť zachytávaním incidentov, z ktorých môže vzniknúť vytvorenie alarmov.



Obrázok 4.5 Všeobecné konfiguračné možnosti v nástroji AlienVault OSSIM, zdroj vlastný

#### 4.1.3 Test skenera hľadáním zraniteľností

V tejto časti otestujeme skener hľadáním zraniteľností na sieťovom prvku router od spoločnosti, ktorý sa nachádza v našej testovacej infraštruktúre. Testovanie sa konfiguruje v časti

*ENVIRONMENT / VULNERABILITIES* v záložce *SCAN JOBS*. Tlačítkem *NEW SCAN JOB* vytvoříme nové skenovanie, kde spomedzi zariadení vyberieme náš router a názov skenovanie zvolíme pre prehľadnosť *scan router*.



NEW SCAN JOB

IMPORT ALIENVAULT SCAN

PROFILES

SETTINGS

1 RUNNING SCAN

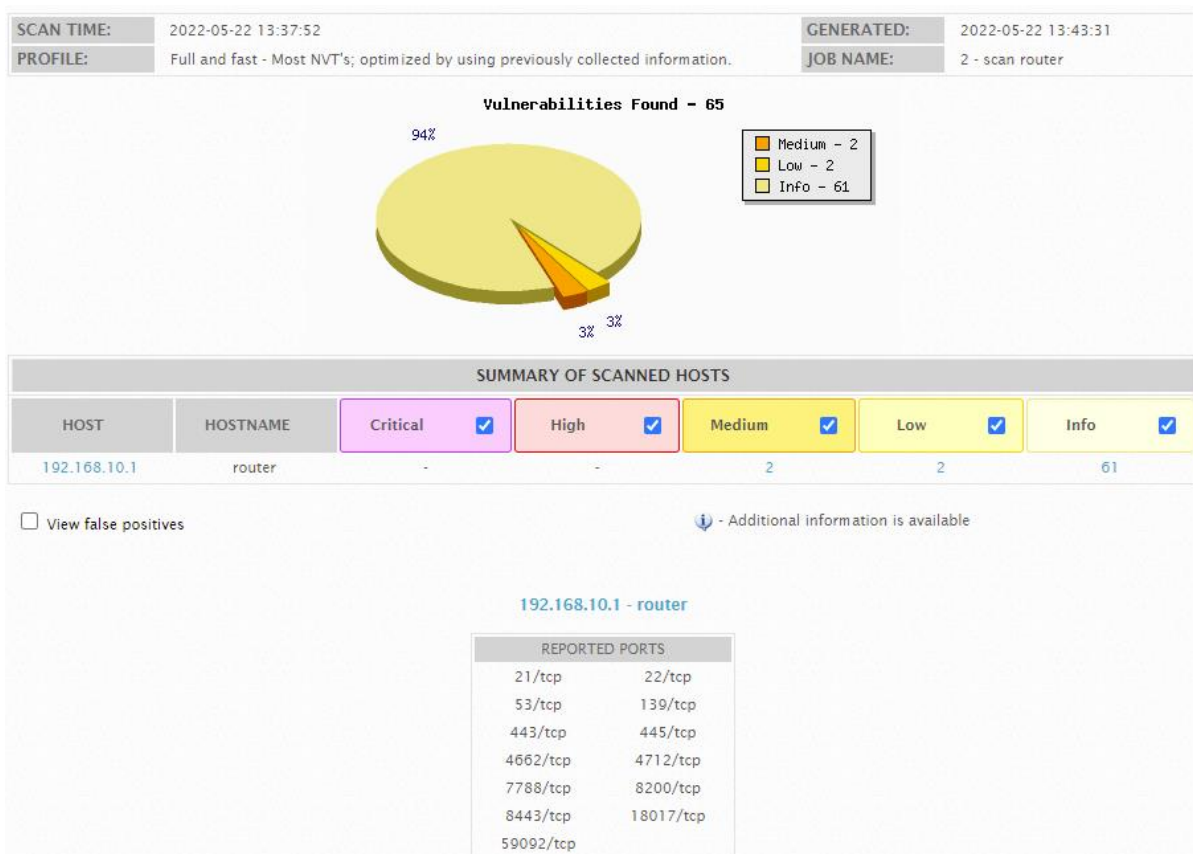
JOB NAME	OWNER	SCAN TIME	PROGRESS	ACTION
 scan router	admin	RUN >16 mins	<div>96%</div>	

SCHEDULED JOBS

No Scheduled Jobs

Obrázok 4.6 Progres skúšobného skenovania v nástroji AlienVault OSSIM, zdroj vlastný

Profil skenovania sme zvolili úplný a rýchly, ktorý hľadal zraniteľnosti približne 30 minút. Objavené zraniteľnosti sa nám zobrazili prehľadne v grafoch a tabuľkách s dostatočným množstvom detailov.



Obrázok 4.7 Výsledok skúšobného testu zraniteľností v nástroji AlienVault OSSIM, zdroj vlastný

## 4.2 Greenbone

#### 4.2.1 Základný popis

Nástroj Greenbone, ktorý využíva kvalitný a plnohodnotný OpenVAS skener zraniteľností. Jeho schopnosti zahŕňajú overené, ale aj neoverené testovanie, rôzne vysoko-úrovňové a nízko-úrovňové internetové a priemyselné protokoly, ladenie výkonu pre rozsiahle skenovanie a výkonný interný programovací jazyk na implementáciu akéhokoľvek typu testu zraniteľností. Skener je napojený na informačný kanál s bohatou históriou, prostredníctvom ktorého získava testy na detekciu zraniteľností a takmer denné aktualizácie.

OpenVAS skener bol vyvinutý spoločnosťou Greenbone v roku 2006 a jeho podporu zaručuje až doteraz. Tento skener bol najskôr uvedený do komerčnej rodiny produktov na detekciu a právu zraniteľností, no časom sa začal skener spájať aj s open-source modulmi.

Tento nástroj ponúka niekoľko dostupných riešení a vymožeností:

- Mnohé bezpečnostné riešenia v hardvérovej alebo virtuálnej forme
- Možnosť vyskúšať si softvér bez potrebného „know-how“
- Produktovú online dokumentáciu na rôzne verzie vrátane API
- Viac-úrovňový proces zabezpečenia kvality
- Globálne prepojený vývojový tím
- Zdrojové kódy v podobe open-source
- Šifrovaný prenos
- Plánovanie skenovaní na cielených zariadeniach s digitálnym podpisom
- Skenovanie aplikácií a OS systémov zariadení aj pomocou vzdialeného prístupu
- Komunitné fórum [36]

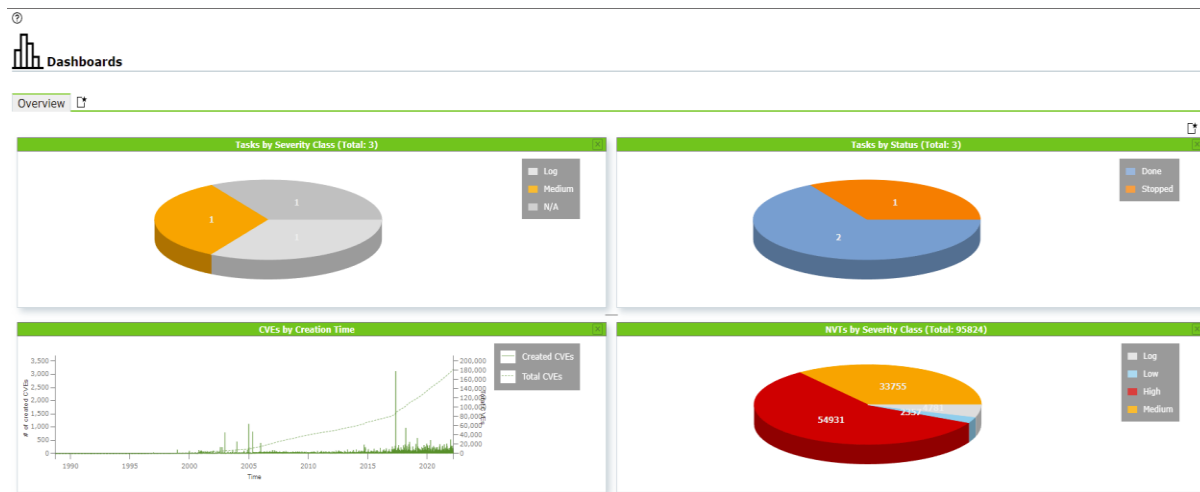
Nástroj Greenbone spravuje a riadi proces detekcie, odstraňovania a kontroly rizika zraniteľností počas celého životného cyklu OS alebo aplikácii. Automaticky testuje IT sieť a všetky zariadenia k nej pripojené na viac ako 76 000 zraniteľností s pravidelnými dennými aktualizáciami. Objavené zraniteľnosti sú ohodnotené prioritou podľa závažnosti, ktoré signalizujú naliehavosť úpravy konfigurácie alebo opravy v softvéri. Tento nástroj je dostupný vo voľne dostupnej verzii, ktorú budeme testovať, avšak rovnako ako nástroj AlienVault OSSIM ponúka aj pokročilé možnosti s potrebnou licenciou [37].

#### 4.2.2 Možnosti nástroja

Nástroj Greenbone bolo potrebné najskôr nainštalovať vo virtuálnom prostredí od spoločnosti *Vmware* vo verzií *21.04.14*. Inštalácia je pomerne jednoduchá, keďže sme si mohli stiahnuť hotový, predinštalovaný súbor vo formáte *.ova*, ktorý obsahoval pripravené všetky

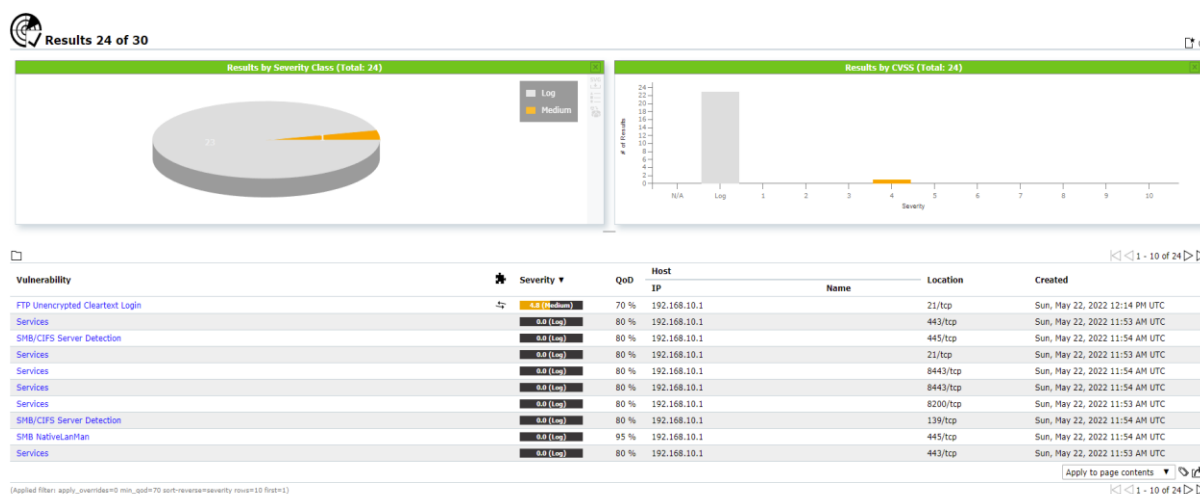
potrebné inštačné kroky. Tento súbor sme jednoducho importovali do virtuálneho prostredia, upravili sieťovú konfiguráciu a vytvorili administrátorské heslo.

Následne sme sa prihlásili prostredníctvom webového prehliadača do nástroja pomocou prihlasovacieho mena *admin* a vytvoreného administrátorského hesla. Na úvodnej stránke v časti *Dashboard* sa nám zobrazili rôzne dáta v koláčových grafoch.



Obrázok 4.8 Dashboard po spustení nástroja Greenbone, zdroj vlastný

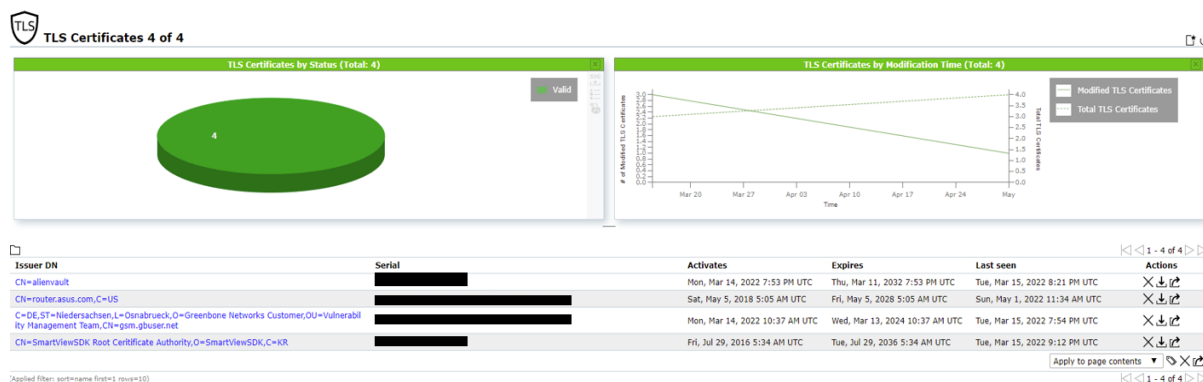
V nástroji okrem záložky *Dashboard* z hlavnej ponuky máme dostupné aj ďalšie možnosti. Patrí tam aj kategória *Scans*, v ktorej sa nachádzajú možnosti konfigurácie, plánovania a reportovania zraniteľností.



Obrázok 4.9 Prehľad výsledkov zraniteľností v nástroji Greenbone, zdroj vlastný

V ďalšej položke z hlavného menu sa nachádza možnosť *Assets*, v ktorej je možné pridávať zariadenia v sieti, pridávať informácie o ich OS s možnosťou exportu či nahrávaním a spravovaním TLS certifikátov.

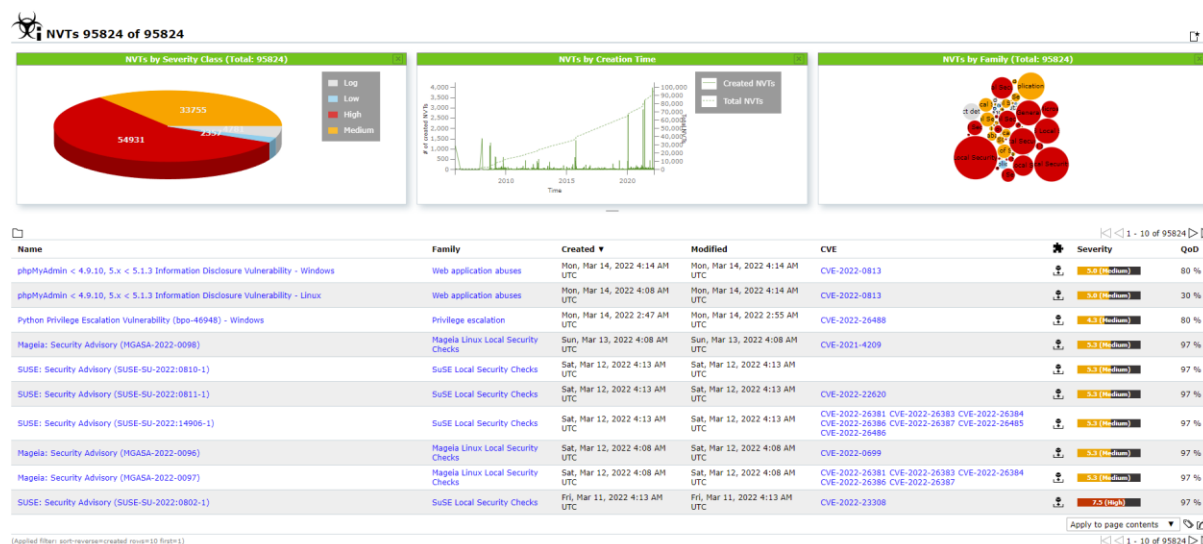




Obrázok 4.10 Možnosti správy certifikátov v nástroji Greenbone, zdroj vlastný

V nasledujúcej možnosti v poradí je kategória *Resilience*, v ktorej je možnosť si nastaviť dodržiavanie zásadných pravidiel a ich následný audit. V tejto kategórii nám nástroj ponúka možnosť vytvoriť si vlastnú mapu obchodných procesov.

Aktuálnosť zraniteľností, ich popis, prioritu a ďalšie informácie môžeme objavovať prostredníctvom kategórie *SecInfo*. Táto kategória obsahuje obrovské množstvo zraniteľností vrátane *NVT*, *CVE*, *CPE*, *Oval definitions*, *CERT-bound Advisories* a *DFN-CERT advisories*. Každá z týchto kategórií obsahuje veľmi množstvo informácií, a zároveň sú dáta podané prehľadnou štatistikou pomocou grafov a tabuliek.



Obrázok 4.11 Detaily zraniteľností NVTs dostupné v nástroji Greenbone, zdroj vlastný

V posledných možnostiach *Configuration*, *Administration* a *Help* sa nachádzajú konfiguračné možnosti cieľov skenovania, zoznamu portov, prihlasovacích údajov, úpravu skenovacích plánov a profilov, zmenu vo formáte reportov či nastavení skenera. Dostupné sú v nich aj možnosti používateľov, skupín, rolí, výkonnosti či aktualizácia databázy zraniteľností.

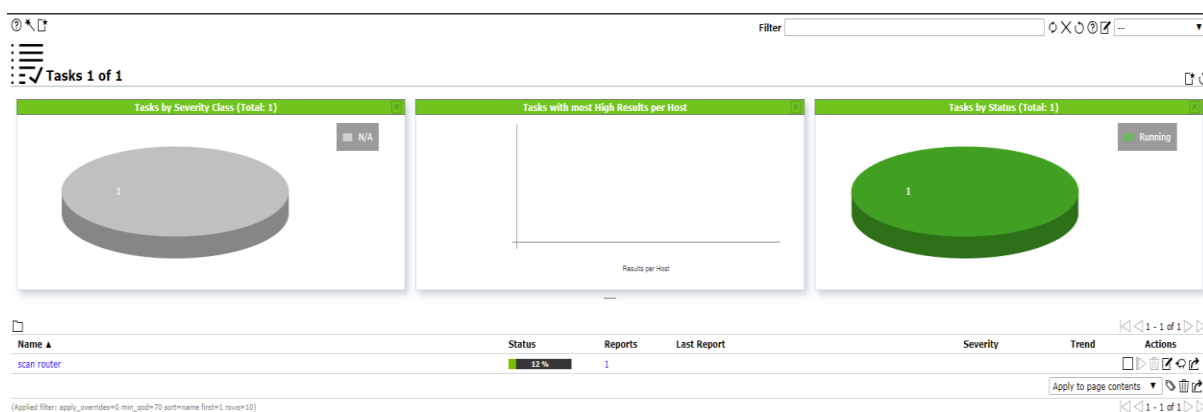


V časti *Help* sa nachádza odkaz na oficiálnu dokumentáciu, kalkulačka CVSS či popis aktuálnej verzie nástroja.

### 4.2.3 Test skenera hľadáním zraniteľností

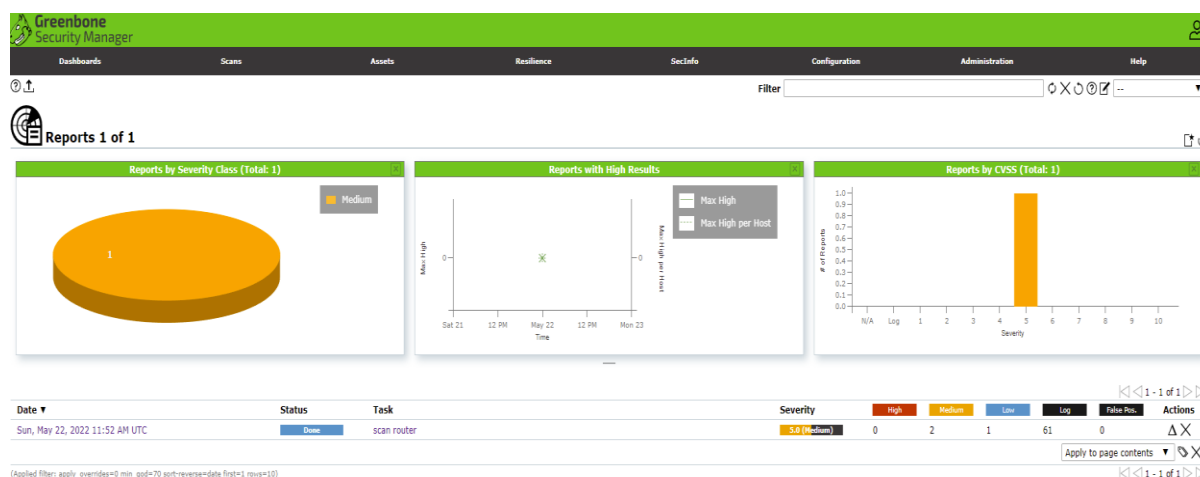
V tejto časti sa zameriame na test skenera pre hľadanie zraniteľností rovnako, ako sme to spravili aj v prípade predchádzajúceho nástroja.

Skenovanie sme vytvorili cez hlavné menu *Scans / Tasks* a pomocou tlačidla (papier s hviezdíčkom) *New task* sme pridali skenovanie. Názov sme zvolili rovnaký ako pri predchádzajúcom nástroji AlienVault OSSIM, takže *scan router*. Ako cieľ sme pridali náš sieťový router a konfiguráciu sme zvolili taktiež ako pri predchádzajúcom nástroji úplnú a rýchlu. Po pridaní úlohy sme skenovanie spustili tlačidlom *start* pri vytvorenej úlohe.



Obrázok 4.12 Progres skúšobného skenovania zraniteľností v nástroji Greenbone, zdroj vlastný

Skenovanie zraniteľností na sieťovom prvku router trvalo približne 5 hodín, čo bolo omnoho viac, ako sme očakávali. Vzhľadom na časové zaťaženie sme očakávali, že výsledok by mal obsahovať najviac objavených zraniteľností a udalostí. Po porovnaní výsledkov s nástrojom AlienVault OSSIM môžeme prehlásiť, že skener v nástroji AlienVault OSSIM objavil rovnaké zraniteľnosti s rovnakou prioritou, ale v značne kratšom čase.



Obrázok 4.13 Výsledok skúšobného skenovania zraniteľnosti v nástroji Greenbone, zdroj vlastný

## 4.3 Nessus

### 4.3.1 Základný popis

Nessus je proprietárny skener zraniteľností vyvinutý spoločnosťou *Tenable, Inc.* Tento skener sa radí do rodiny open-source nástrojov na skenovanie zraniteľností, ktorý využíva architektúru *Common Vulnerabilities and Exposures* na jednoduché prepojenie medzi ďalšími bezpečnostnými skenermi.

Nástroj Nessus funguje tak, že sa snaží otestovať každý port na cieľovom zariadení, čím zistí, aká služba je spustená. Po objavení spustenej služby v nej začne hľadať slabé a zraniteľné miesta, ktoré by mohol útočník neskôr zneužiť na spúšťanie škodlivého kódu.

Počas skenovania sa snaží skenovať tieto zraniteľnosti a expozície:

- Zraniteľnosť, ktorá by mohla zneužiť neoprávnenú kontrolu alebo prístup k citlivým dátam v systéme
- Nedostatočná konfigurácia zariadenia alebo služby
- Odolnosť voči DoS útokom
- Predvolené prihlasovacie údaje
- Chýbajúce softvérové záplaty, hľadanie malvérov a chýb v operačnom systéme

Medzi hlavné prednosti tohto nástroja patria:

- Plánovanie bezpečnostných auditov
- Detekcia bezpečnostných dier v lokálnych alebo vzdialených hostiteľoch
- Vyhľadávanie aktív v sieti (asset discovery)

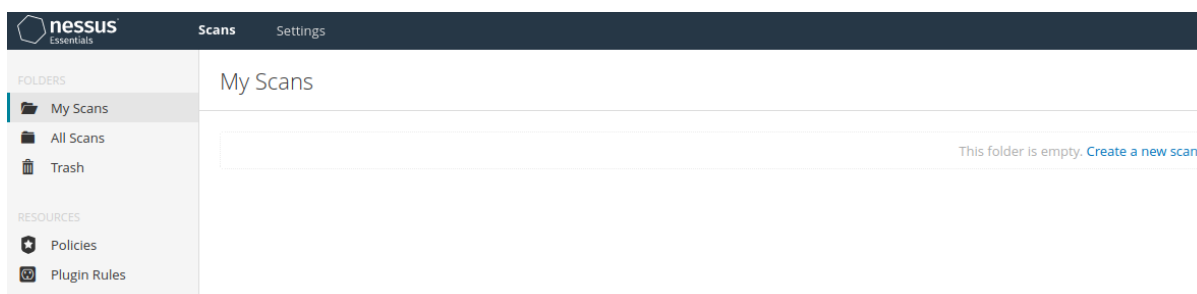
- Pridelovanie priority problémom
- Skenovanie webu
- Manažment pravidiel
- Simulované útoky
- Skenovanie vnútornej siete podľa požiadaviek definovaných v PCI DSS
- Možnosť inštalácie Nessus agentov na koncové zariadenia
- Možnosť exportu reportov v rôznych formátoch (text, XML, HTML, PDF)

Vyššie spomínané inštalovanie Nessus agentov je možné previezť na rôznych OS ako sú Windows Server, Windows, Amazon Linux, CentOS, Debian, OS X a Linuxové distribúcie Red Hat Enterprise a Ubuntu [38].

#### 4.3.2 Možnosti nástroja

Inštalácia tohto nástroja je dostupná na rôzne operačné systémy. My sme použili zariadenie, na ktorom bol nainštalovaný OS Kali Linux. Následne sme z oficiálnej stránky spoločnosti *Tenable* stiahli inštalačný súbor a začali inštaláciu. Tá pozostávala z rozbalenia potrebných balíčkov, a následnou úvodnou konfiguráciou cez webové rozhranie, kde sme vybrali verziu *Essentials*, vytvorili sme administrátorský účet a zadali aktivačný kód, ktorý sme získali po registrácii.

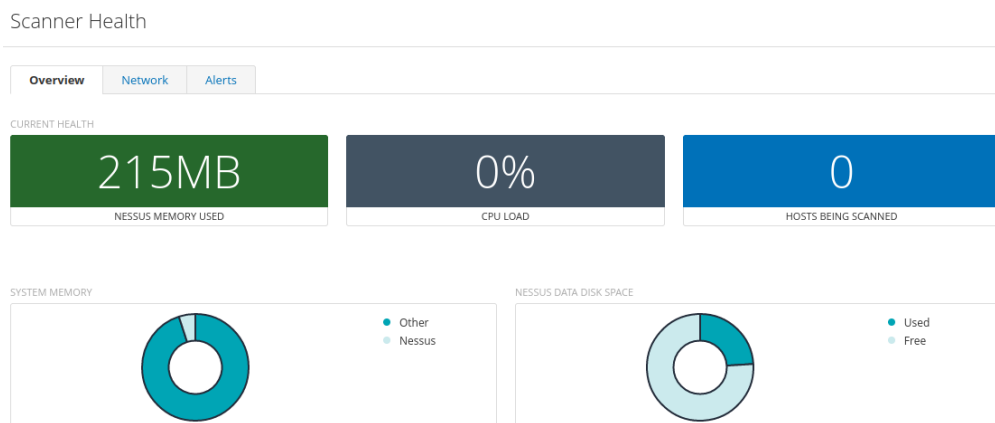
Po dokončení inštalácie, konfigurácie a úvodnej inicializácie nástroja sme sa dostali na úvodnú stránku, ktorá ponúkala skenovanie.



Obrázok 4.14 Úvodná stránka nástroja Nessus, zdroj vlastný

Tento nástroj v porovnaní s ostatnými v bezplatnej verzii má výrazne obmedzenú ponuku svojich možností. V navigačnom menu môžeme vidieť dve záložky. V prvej sa nachádza správa pravidiel, pluginov a skenovaní zraniteľností. V tej druhej sa nachádzajú možnosti konfigurácie nástroja vrátane jeho aktualizácie, konfigurácie SMTP servera, sledovania stavu

skenera či zoznam upozornení. Rovnako sa tam nachádzajú aj možnosti komplexnosti hesla, správa certifikátov či úprava používateľských účtov.

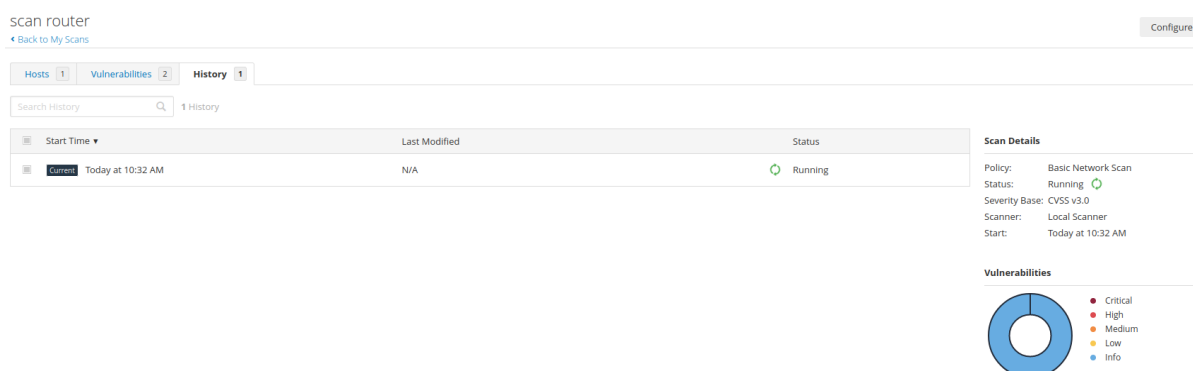


Obrázok 4.15 Možnosti sledovania stavu skenera v nástroji Nessus, zdroj vlastný

### 4.3.3 Test skenera hľadaním zraniteľností

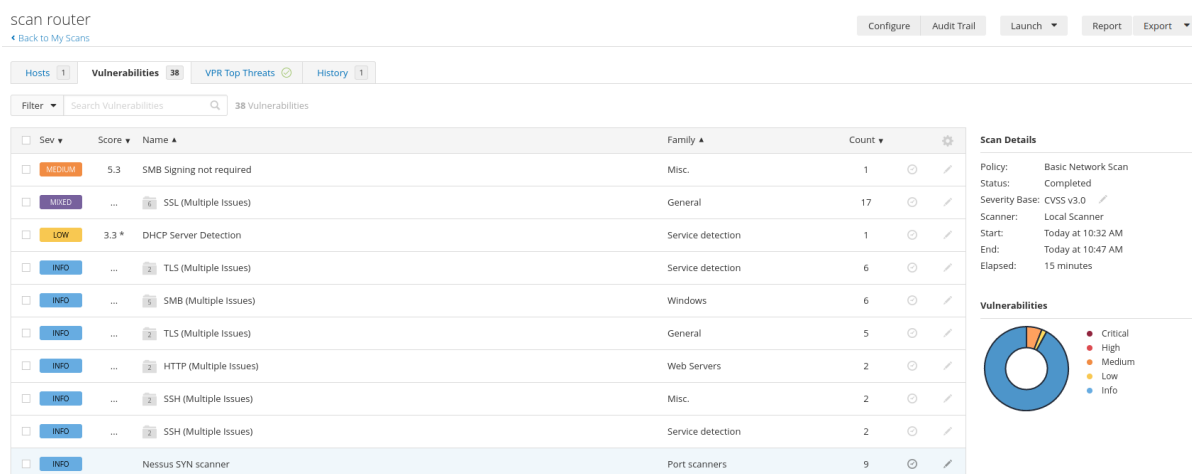
Vytvorenie skenovania siete alebo zariadenia je veľmi jednoduché, v záložke *Scans* tlačidlom *New Scan* prejdeme do konfigurácie skenovania. Tam máme možnosť si zvoliť jednu z predpripravených šablón zameraných na bežné skenovanie zariadenia či siete. Zároveň sa môžeme zamerať aj na prehľadávanie konkrétnej zraniteľnosti v zariadení, napríklad vyhľadávanie aktivity malvéru *WannaCry* alebo *Log4Shell*.

My zvolíme šablónu *Basic Network Scan*, kde zadáme rovnaký názov ako v prípade dvoch predchádzajúcich nástrojov *scan router*. Ako cieľové zariadenie zadáme IP adresu routera, ktorý je dostupný na adrese *192.168.10.1* a skenovanie uložíme tlačidlom *Save*. V záložke *My Scans* sa objavilo naše vytvorené skenovanie zariadenia, ktoré jednoducho označíme a tlačidlom na konci riadku štart ho spustíme.



Obrázok 4.16 Progres skúšobného skenovania zraniteľností v nástroji Nessus, zdroj vlastný

Skenovanie týmto nástrojom trvalo približne 15 minút a objavené bolo v porovnaní s predchádzajúcimi nástrojmi o niečo menej incidentov, ako to bolo v prípade 2 predchádzajúcich nástrojov.



Obrázok 4.17 Výsledok skúšobného skenovania zraniteľností v nástroji Nessus, zdroj vlastný

## 4.4 Výber nástroja na ďalšie použitie

V tejto kapitole sme sa zoznámili s možnosťami vybraných nástrojov na detekciu zraniteľností. V každom nástroji sme si prešli jeho konfiguračné možnosti, a zároveň sme pomocou každého nástroju otestovali skener hľadáním zraniteľností na tom istom sieťovom zariadení.

Nástroj AlienVault OSSIM má skutočne rozsiahle možnosti konfigurácie vrátane vyhľadávania aktív v sieti, pokročilé detekčné možnosti, normalizáciu a koreláciu udalostí SIEM v reálnom čase a mnohé ďalšie. Taktiež má bohaté možnosti konfigurácie pravidiel na vytvorenie alarmov, rôzne možnosti notifikácie, prehľadné grafy, podľa vlastnej vôle upraviteľné *dashboards*. Nechýba ani možnosť zbierať sieťovú prevádzku zo zariadení prostredníctvom netflow, prijímať logy z iných zariadení a podobne.

Nástroj Greenbone má tiež veľmi použiteľné možnosti hľadania zraniteľností v sieti, ktorý ponúka rovnako ako nástroj AlienVault rozsiahle možnosti konfigurácie sieťových aktív, hľadanie zraniteľností a podobne. Rovnako má dostupné prehľadné grafy a podobne. Ako nedostatok sme objavili nemožnosť zachytiť a normalizovať dáta v reálnom čase, chýbajúce možnosti notifikácie či absencia možnosti zbierania logov prostredníctvom netflow.

Posledný nástroj Nessus má dostatočne výkonný skener na prehľadávanie zraniteľností a prehľadné grafické rozhranie. Avšak tento nástroj v porovnaní s dvomi predchádzajúcimi

značne zaostáva v konfiguračných možnostiach, a preto tento nástroj nie je vhodný na riešenie stanovených problémov v tejto práci.

Zo vzájomného porovnania vyššie zmienených nástrojov môžeme konštatovať, že na ďalšie použitie a našu infraštruktúru, ktorú budeme zabezpečovať, sa nám najviac hodí nástroj AlienVault OSSIM, ktorý obsahuje obrovské možnosti konfigurácie vrátane detekcie zraniteľností a hľadanie anomálií v reálnom čase. Zároveň tento nástroj ponúka hlbokú flexibilitu v spôsobe zbierania a analýzy logov zo zariadení prostredníctvom nasadenia HIDS agentov na koncových zariadenia alebo odosielaním logov na vzdialený server.

## 5. PREVÁDZKOVÝ MONITORING

V tejto kapitole sa venujeme dvom potencionalne vhodným nástrojom na prevádzkové monitorovanie zariadení v sieti. Cieľom je sledovať vyťaženosť pamäte, procesora, stav disku na sieťových prvkoch a serveroch v sieti.

Ako najvhodnejších kandidátov na riešenie tohto problému sme našli nástroje zabbix a Nagios. Každý nástroj si nainštalujeme v našej testovacej infraštruktúre, kde sa zoznámime s možnosťami konfigurácie. Nástroje budeme inštalovať rovnako vo virtuálnom prostredí pomocou *Vmware Workstation Pro*, ako tomu bolo aj pri nástrojoch na detekciu zraniteľností. V závere kapitoly zhrnieme dôležité vlastnosti nástrojov, spravíme ich krátke porovnanie a lepší z nich použijeme na riešenie stanovených problémov v našej práci.

### 5.1 Nagios

#### 5.1.1 Základný popis

Nástroj nagios je open-source softvér, ktorý poskytuje nepretržité monitorovanie systémov a sietí. Je založený na pluginoch uložených na serveri, ktoré sú prepojené a aplikované priamo na sieťové prvky, servery a koncové zariadenia. V prípade výskytu nejakého problému, nagios upozorní o probléme technický tím, ktorý môže okamžite začať s jeho odstraňovaním [40].

Nástroj nagios bol prvýkrát nasadený do produkcie už v roku 1999, a do dnešných čias sa tento nástroj rozrástol o tisíce projektov, na ktorom sa podieľa celosvetovo komunita Nagios. Tento nástroj je oficiálne sponzorovaný spoločnosťou Nagios Enterprises, ktorá podporuje komunitu rôznymi spôsobmi, napríklad prostredníctvom predaja svojich komerčných produktov a služieb.

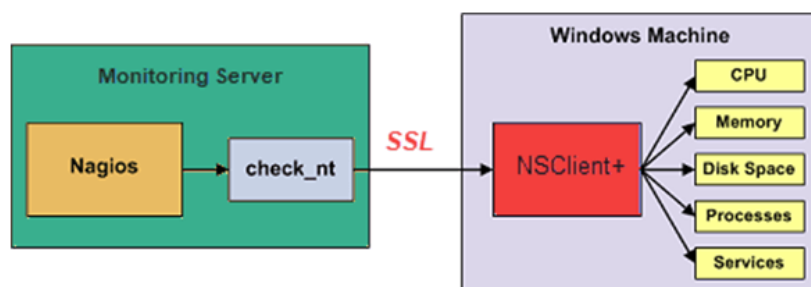
Tento nástroj poskytuje monitoring celej infraštruktúry vrátane stavu systémov, aplikácií, služieb a obchodných procesov. V prípade zlyhania niektorého z nich nagios môže upozorniť technický personál alebo administrátora siete na problém, čo umožní riešiť vzniknutý problém ešte predtým, ako výpadky zariadení alebo služieb ovplyvnia obchodné procesy koncových zákazníkov alebo používateľov [39].

Ponuka možností tohto nástroja je nasledovná:

- Detekcia všetkých typov problému so sieťou alebo sieťovým prvkom
- Analýza príčiny vzniku problému

- Aktívny monitoring celej infraštruktúry
- Monitoring vyťaženia a výkonu zariadenia
- Upozorní na potrebné aktualizácie zariadení v infraštruktúre
- Zvýšenie bezpečnosti a dostupnosti služieb
- Možnosť automaticky spustiť protiopatrenie na vzniknutú situáciu
- Dobré škálovateľné a spravovateľné prostredie
- Atraktívne webové rozhranie
- Podpora pre implementáciu redundantných hostiteľov

Plugins tohto nástroja poskytujú informácie na nízkej úrovni o tom, ako možno nakonfigurovať monitoring čohokoľvek pomocou jadra nagios. V princípe fungujú ako samostatná aplikácia, ktoré sú navrhnuté tak, aby boli spúšťané jadrom nagios core. Jadro sa následne pripojí k službe *Apache*, ktorý zabezpečí zobrazenie výsledku. Tieto údaje sa zároveň prenášajú aj do databázy v podobe logov [40].



Obrázok 5.1 Graf zobrazujúci princíp, ktorým pracujú pluginy v nástroji Nagios, zdroj [40]

### 5.1.2 Možnosti nástroja

Nástroj sme inštalovali vo verzii 4.4.6 na zariadení s OS Linux Ubuntu pomocou príkazového riadku a oficiálnej dokumentácie pre nástroj nagios. Po stiahnutí potrebných balíčkov a inicializácii repozitáru sme si stiahli inštalačný súbor do zariadenia, ktorý sme následne spustili, a úvod inštalácie dokončili.

Pokračovali si prípravou databázy, vytváraním potrebných pravidiel na firewall zariadenia, a všetko sme zavřili vytvorením administrátorského účtu a reštartovaním potrebných služieb. Následne sme mali možnosť sa prostredníctvom webového prehliadača prihlásiť do nástroja zadáním administrátorských prihlasovacích údajov. Po prihlásení sa nám zobrazila úvodná stránka nástroja.



**Nagios®**

General  
Home  
Documentation

**Current Status**  
Tactical Overview  
Map (Legacy)  
Hosts  
Services  
Host Groups  
Summary  
Grid  
Service Groups  
Summary  
Grid  
**Problems**  
Services (Unhandled)  
Hosts (Unhandled)  
Network Outages  
Quick Search:

**Reports**  
Availability  
Trends (Legacy)  
Alerts  
History  
Summary  
Histogram (Legacy)  
Notifications  
Event Log

**System**  
Comments  
Downtime  
Process Info  
Performance Info  
Scheduling Queue  
Configuration

**Nagios® Core™**  
✓ Daemon running with PID 20920

**Nagios® Core™**  
Version 4.4.6  
April 28, 2020  
[Check for updates](#)

A new version of Nagios Core is available!  
Visit [nagios.org](https://nagios.org) to download Nagios 4.4.7.

**Nagios XI**  
Easy Configuration  
Advanced Reporting  
[Download](#)

**Nagios Log Server**  
Monitor and analyze  
logs from anywhere  
[Download](#)

**Nagios Network Analyzer**  
Real-time netflow and  
bandwidth analysis  
[Download](#)

**Get Started**  
• Start monitoring your infrastructure  
• Change the look and feel of Nagios  
• Extend Nagios with hundreds of  
addons  
• Get support  
• Get training  
• Get certified

**Quick Links**  
• Nagios Library (tutorials and docs)  
• Nagios Labs (development blog)  
• Nagios Exchange (plugins and  
addons)  
• Nagios Support (tech support)  
• Nagios.com (company)  
• Nagios.org (project)

**Latest News**  
• Nagios Update: XI 5.6.6  
• Nagios Update: XI 5.6.5  
• Nagios Update: XI 5.6.4  
• More news...

**Don't Miss...**  
• **Monitoring Log Data with Nagios** - Nagios Log Server can handle all log data  
in one central location.  
• **Can Nagios monitor netflow?** - Yes! Nagios Network Analyzer can take in a  
variety of flow data. [Learn More](#)  
• **Nagios XI 5 Available Now!** - Easier configuration, Advanced Reporting.  
[Download Today!](#)

Copyright © 2010-2020 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors.

Nagios Core is licensed under the GNU General Public License and is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Nagios, Nagios Core and the Nagios logo are trademarks, servicemarks, registered trademarks or registered servicemarks owned by Nagios Enterprises, LLC. Use of the Nagios marks is governed by the trademark use restrictions.

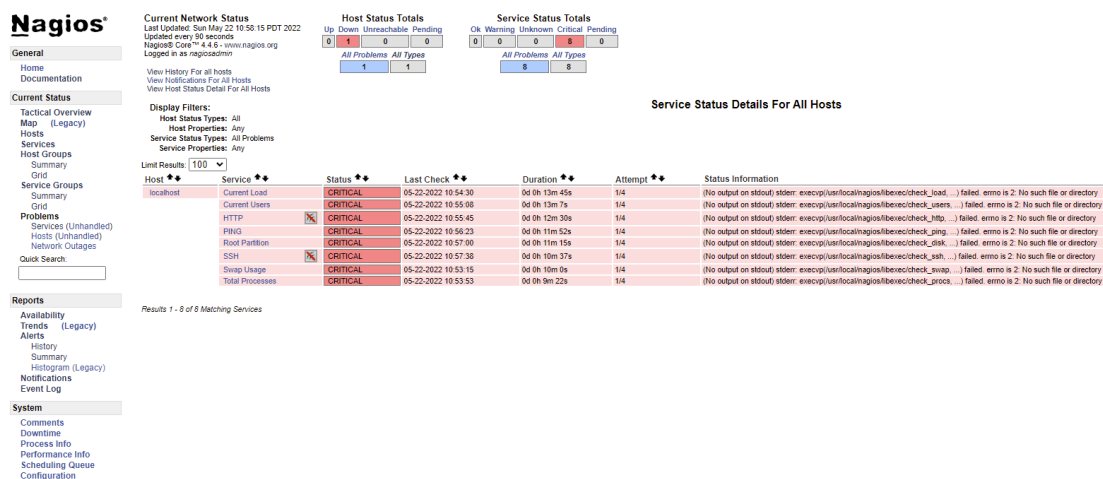
**Nagios**  
NAGIOS CORE  
NAGIOS XI

SOURCEFORGE.NET

Obrázok 5.2 Úvodná obrazovka nástroja Nagios, zdroj vlastný

V navigačnej časti sa nachádza niekoľko kategórií, ktoré sú od seba logicky odčlenené. Vo všeobecnej časti *General* sa nachádzajú odkazy na domovskú obrazovku a online technickú dokumentáciu.

Nasledujúca kategória je zameraná na manažment zariadení a služieb, ktoré môžu byť do nástroju priradené. Ďalej sa tam nachádzajú možnosti vytvárania rôznych skupín zariadení a služieb, z ktorých si môžeme následne vytvárať reporty na základne rôznych parametrov pomocou filtru. Taktiež sa tam nachádza aj podkategória s názvom *Problems*, v ktorej je možnosť sledovať oznámenia o problémoch v sieti, na zariadeniach alebo v službách.



Obrázok 5.3 Kategória v nástroji Nagios, ktorá zobrazuje objavené problémy v službách, zdroj vlastný

Ďalšou kategóriou je časť *Report*, v ktorej máme možnosť si vytvoriť reporty na základe dostupnosti zariadení, služieb, alarmov, notifikácií alebo logov udalostí.



Obrázok 5.4 Report vytvorený na základe histórie alarmov v nástroji Nagios, zdroj vlastný

V ďalšej časti tento nástroj poskytuje systémové možnosti zamerané na komentáre, konfiguráciu výkonu a procesov a zopár ďalších, nie veľmi dôležitých možností. Dôležitou časťou je však aplikácia pluginov na zariadenie alebo službu, ktoré chceli určitým spôsobom monitorovať. Nástroj Nagios túto možnosť poskytuje nie veľmi prehľadným, a užívateľsky prívetivým spôsobom. Nadanie pluginov na zariadenie je potrebné vykonať prostredníctvom príkazového riadku, čo je z nášho pohľadu menšia komplikácia a nepohodlie pri konfigurácii.

## 5.2 Zabbix

### 5.2.1 Základný popis

Zabbix je definovaný ako open-source monitorovací nástroj používaných na sledovanie serverov, siete, IT komponentov, cloudových služieb a virtuálnych nástrojov. Taktiež sa využíva monitoring pomocou tohto nástroja na poskytovanie monitorovacích metrík a sledovanie vyťaženie siete, spotreby miesta na disku a vyťaženie procesora. Nástroj podporuje rôzne operačné systémy ako sú Mac OS, Solaris, Linux a mnoho ďalších. Nástroj je naprogramovaný tak, aby používal inú databázu na ukladanie údajov, a inú na monitorovanie služieb a aplikácii. Monitorovací nástroj zabbix je vyvinutý v programovacom jazyku *C* a pre webové rozhranie sa používa jazyk *PHP* [41].

Nástroj zabbix je často definovaný aj ako špičkový softvér na podnikovej úrovni určený na monitorovanie miliónov metrík zhromaždených z desiatok tisíc serverov, virtuálnych strojov a sieťových zariadení v reálnom čase. Tento nástroj je na trhu už viac ako 19 rokov a svoje miesto si už našiel na viac ako 300 tisíc inštalácií po celom svete.

Možnosti monitoringu týmto nástrojom vo všeobecnosti sú nasledovné:

- Sieťové monitorovanie
- Monitorovanie serverov
- Cloud monitoring
- Monitorovanie služieb
- Monitorovanie KPI/SLA

Zbieranie dát zo zariadení, systémov a aplikácii je možné pomocou nasledovných možností:

- Multi platformný agent Zabbix
- Agenti protokolmi SNMP a IPMI
- Monitorovanie používateľských služieb bez agentov
- Vlastné metódy
- Výpočet a integrácia
- Monitorovanie webu u koncového používateľa

Detekciu problémov definujú inteligentné prahové hodnoty, ktoré oddeľujú bežné hodnoty od kritických. Pomocou týchto hodnôt je nástroj schopný zistiť problémový stav v rámci prichádzajúceho metrického toku dát.

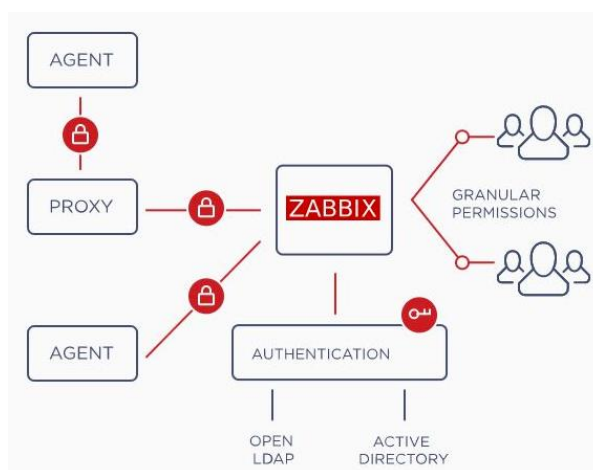
V tejto oblasti detekcie problému nástroj zabbix ponúka vysoko flexibilné možnosti ich definície, oddelenie problémových stavov a podmienok riešenia, rôzne stupne závažnosti, analýzu príčiny, detekciu anomálií alebo predikciu trendu.

Vizualizáciu dát nástroj poskytuje viacero spôsobov prezentácie vizuálneho prehľadu IT prostredia. Ponúka rôzne panely založené na miniaplikáciách, grafy, sieťové mapy či rozbalovací prehľad.

Možnosti oznámení v nástroji zabbix tiež zohrávajú dôležitú úlohu v prípade, že sa v sieti alebo na zariadení objaví akýkoľvek problém. Informovať zodpovedné osoby o vzniknutých udalostiach pomocou rôznych kanálov s rôznym typom média alebo neinformovať, ale priamo sa pokúsiť objavený problém napraviť.

Bezpečnosť a autentifikácia tiež nie sú tomuto nástroju cudzie. Zameraný je na množstvo nasledujúcich spôsobov:

- Silné šifrovanie medzi všetkými komponentami zabbix-u
- Viacero autentifikačných metód – LDAP alebo Active Directory
- Flexibilná schéma povolení pre používateľa
- Kód zabbix-u je otvorený aj pre bezpečnostný audit



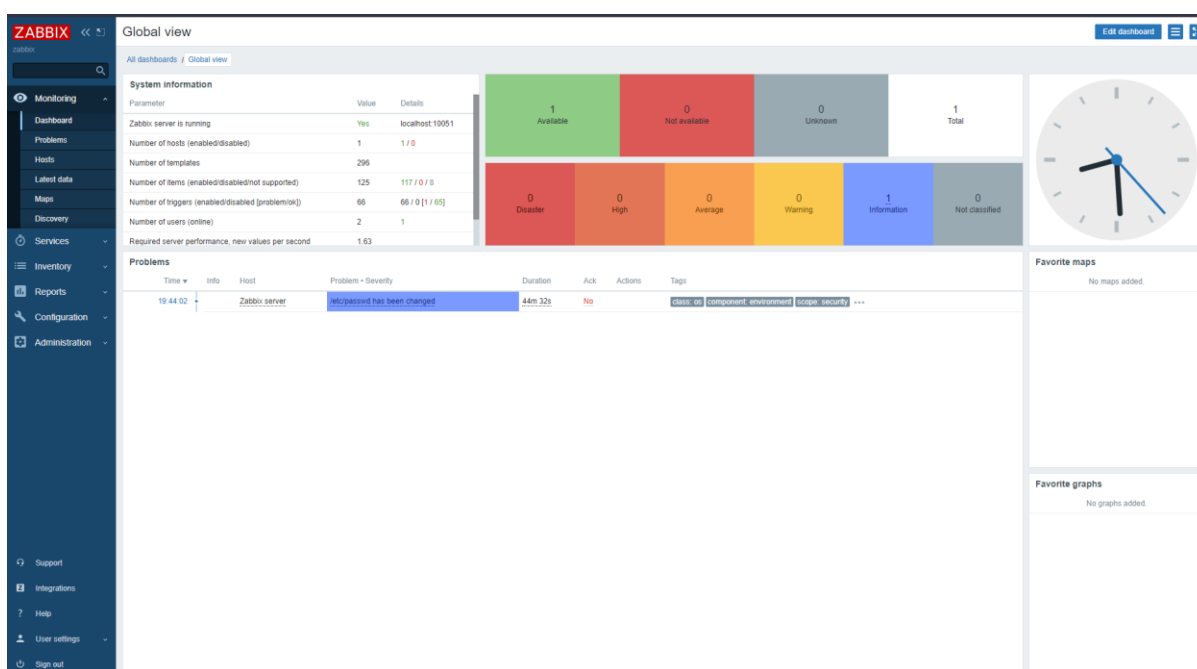
Obrázok 5.5 Bezpečnosť a autentifikácia medzi komponentami zabbix-u, zdroj [42]

Nástroj zabbix obsahuje ešte aj mnohé ďalšie prístupy či možnosti integrácie do prevádzkového monitoringu. Vzhľadom na dostupné možnosti nástroja a jeho open-source dostupnosť je tento nástroj skvelým kandidátom pre každého administrátora, ktorý chce zlepšiť prehľadnosť vo vlastnej infraštruktúre [42].

### 5.2.2 Možnosti nástroja

Nástroj zabbix a jeho inštalácia sú veľmi podobné nástroju nagios. Rovnako sme na tento nástroj využili zariadenie s prostredím OS Linux Ubuntu. Inštaláciu nástroja sme vykonali tiež pomocou príkazového riadku a postupu z oficiálnej dokumentácie podľa zvolených parametrov.

Po dokončení inštalácie v príkazovom riadku sme sa presunuli na webové rozhranie, kde sme inštaláciu dokončili konfiguráciou prihlasovacích údajov na databázu, a kontrolou potrebných parametrov na správne fungovanie nástroja. Po dokončení posledných krokov sme sa dostali na úvodnú obrazovku nástroja zabbix.



Obrázok 5.6 Dashboard ako úvodná obrazovka nástroja zabbix, zdroj vlastný

V tomto nástroji sa nachádza niekoľko dobre predpripravených, a hlavne graficky dobre spracovaných kategórií. Prvou z nich je časť *Monitoring*, v ktorej sa nachádza niekoľko podkategórií. Tie sú zamerané na zobrazenie a filtráciu problémov, pridávanie zariadení, zobrazenie posledných monitorovaných dát, možnosť vytvorenia mapy siete sledovanie dostupnosti zariadení alebo služieb. Problémy sa zároveň objavujú aj hlavnej časti, ktorou je *dashboard*.

Subfilter affects only filtered data

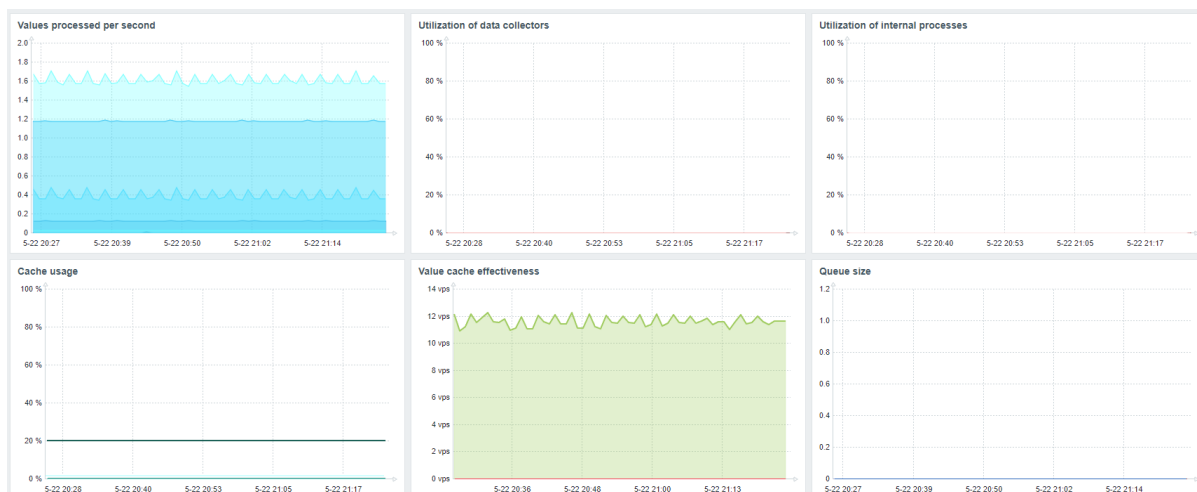
TAGS  
component 125 disk 6 filesystem 4 interface 9 node-id 4 node-name 4

TAG VALUES  
component: application 1 cluster 4 cpu 17 data-collector 13 environment 2 internal-process 20 memory 7 network 9 os 3 raw 2 storage 15 system 35  
disk: sda 0  
filesystem: / 4  
interface: ens33 9  
node-id: c3eb8dux0001o1jxa5hv0v9h 4  
node-name: None 4

<input type="checkbox"/>	Host	Name ▲	Last check	Last value	Change	Tags	
<input type="checkbox"/>	Zabbix server	/ Free nodes in %	38s	88.3622 %		component: storage filesystem: /	Graph
<input type="checkbox"/>	Zabbix server	/ Space utilization	37s	34.8028 %	+0.000202 %	component: storage filesystem: /	Graph
<input type="checkbox"/>	Zabbix server	/ Total space	38s	23.99 GB		component: storage filesystem: /	Graph
<input type="checkbox"/>	Zabbix server	/ Used space	35s	7.92 GB	+48 KB	component: storage filesystem: /	Graph
<input type="checkbox"/>	Zabbix server	Available memory	29s	5.95 GB	-6.31 MB	component: memory	Graph
<input type="checkbox"/>	Zabbix server	Available memory in %	28s	77.0024 %	-0.07975 %	component: memory	Graph
<input type="checkbox"/>	Zabbix server	Checksum of /etc/passwd	53m 30s	e90d8a37375d92e0980a...		component: environment	History
<input type="checkbox"/>	Zabbix server	Cluster node [i] Address	10h 11m 7s	localhost:10051		component: cluster node-id: c3eb8dux00... node-name	History
<input type="checkbox"/>	Zabbix server	Cluster node [i] Last access age	7s	00:00:05		component: cluster node-id: c3eb8dux00... node-name	Graph
<input type="checkbox"/>	Zabbix server	Cluster node [i] Last access time	7s	2022-05-22 20:37:20	+00:01:00	component: cluster node-id: c3eb8dux00... node-name	Graph
<input type="checkbox"/>	Zabbix server	Cluster node [i] Status	10h 11m 7s	Active (3)		component: cluster node-id: c3eb8dux00... node-name	Graph
<input type="checkbox"/>	Zabbix server	Context switches per second	11s	941.593	+115.1303	component: cpu	Graph
<input type="checkbox"/>	Zabbix server	CPU guest nice time	9s	0 %		component: cpu	Graph
<input type="checkbox"/>	Zabbix server	CPU guest time	10s	0 %		component: cpu	Graph
<input type="checkbox"/>	Zabbix server	CPU idle time	8s	99.5624 %	-0.2042 %	component: cpu	Graph
<input type="checkbox"/>	Zabbix server	CPU interrupt time	7s	0 %		component: cpu	Graph

Obrázok 5.7 Zachytenie posledných monitorovaných dát nástrojom zabbix, zdroj vlastný

Nasledujúca kategória *Services* je zameraná na pridávanie služieb, u ktorých máme záujem o ich monitoring. Rovnako sa tam nachádza aj možnosť definovať proti akciu, ktorá by bola vykonaná v prípade, že by naša monitorovaná služba nebola dostupná alebo by sa nachádzala v nami neželanom stave. V tejto časti sa nachádzajú aj konfigurácie SLA a aj možnosť ich reportov.



Obrázok 5.8 Prehľad využívania hardvérových prostriedkov v nástroji zabbix, zdroj vlastný

Ďalšími časťami hlavného menu sú časť *Inventory* a *Reports*, v ktorých môžeme využiť nespočetné množstvo funkcií, akými je napríklad vytváranie *alias* názvov zariadeniam a podobne. V časti *Reports* máme širokú možnosť vytvorenia rôznych, či už systémových, alebo obrovské množstvo iných typov reportov založených napríklad na dostupnosti zariadení alebo služieb. Rovnako máme možnosť si tieto reporty aj plánovať v časových intervaloch alebo

dokonce vykonať audit posledných vykonaných udalostí. Zároveň z množstva týchto dát máme možnosť vytvoriť aj grafickú reprezentáciu dát v podobe grafov.

Host	Name	Problems	Ok	Graph
Zabbix server	/: Disk space is critically low		100.0000%	<a href="#">Show</a>
Zabbix server	/: Disk space is low		100.0000%	<a href="#">Show</a>
Zabbix server	/: Running out of free inodes		100.0000%	<a href="#">Show</a>
Zabbix server	/: Running out of free inodes		100.0000%	<a href="#">Show</a>
Zabbix server	/etc/passwd has been changed	92.6111%	7.3889%	<a href="#">Show</a>
Zabbix server	Cluster node [1]: Status changed		100.0000%	<a href="#">Show</a>
Zabbix server	Configured max number of open file descriptors is too low		100.0000%	<a href="#">Show</a>
Zabbix server	Configured max number of processes is too low		100.0000%	<a href="#">Show</a>
Zabbix server	Getting closer to process limit		100.0000%	<a href="#">Show</a>
Zabbix server	has been restarted		100.0000%	<a href="#">Show</a>
Zabbix server	High CPU utilization		100.0000%	<a href="#">Show</a>
Zabbix server	High memory utilization		100.0000%	<a href="#">Show</a>
Zabbix server	High swap space usage		100.0000%	<a href="#">Show</a>
Zabbix server	Interface ens33: Ethernet has changed to lower speed than it was before		100.0000%	<a href="#">Show</a>
Zabbix server	Interface ens33: High bandwidth usage		100.0000%	<a href="#">Show</a>
Zabbix server	Interface ens33: High error rate		100.0000%	<a href="#">Show</a>
Zabbix server	Interface ens33: Link down		100.0000%	<a href="#">Show</a>
Zabbix server	Lack of available memory		100.0000%	<a href="#">Show</a>
Zabbix server	Load average is too high		100.0000%	<a href="#">Show</a>
Zabbix server	Operating system description has changed		100.0000%	<a href="#">Show</a>

Obrázok 5.9 Report z monitoringu dostupnosti zariadenia zabbix server, zdroj vlastný

V ďalšej kapitole *Configuration* sa nachádzajú možnosti konfigurácie skupín zariadení, úprava alebo pridávanie šablón, ku ktorým sa ešte v tejto kapitole dostaneme. Ďalej je tam možnosť plánovať údržbu, pridávať rozsahy sietí, pridávať koreláciu udalostí či pripravovať proti akcie, ktoré sa vykonajú v prípade aktivity inej udalosti. Rovnako je tu dostupná konfigurácia makier a množstvo ďalších.

V administratívnej časti sa nachádza taktiež nespočetné množstvo možností konfigurácie vrátane definície autentifikačných pravidiel, proxy, administratívu používateľských skupín a rolí, používateľov, médií skriptov a ďalšie.

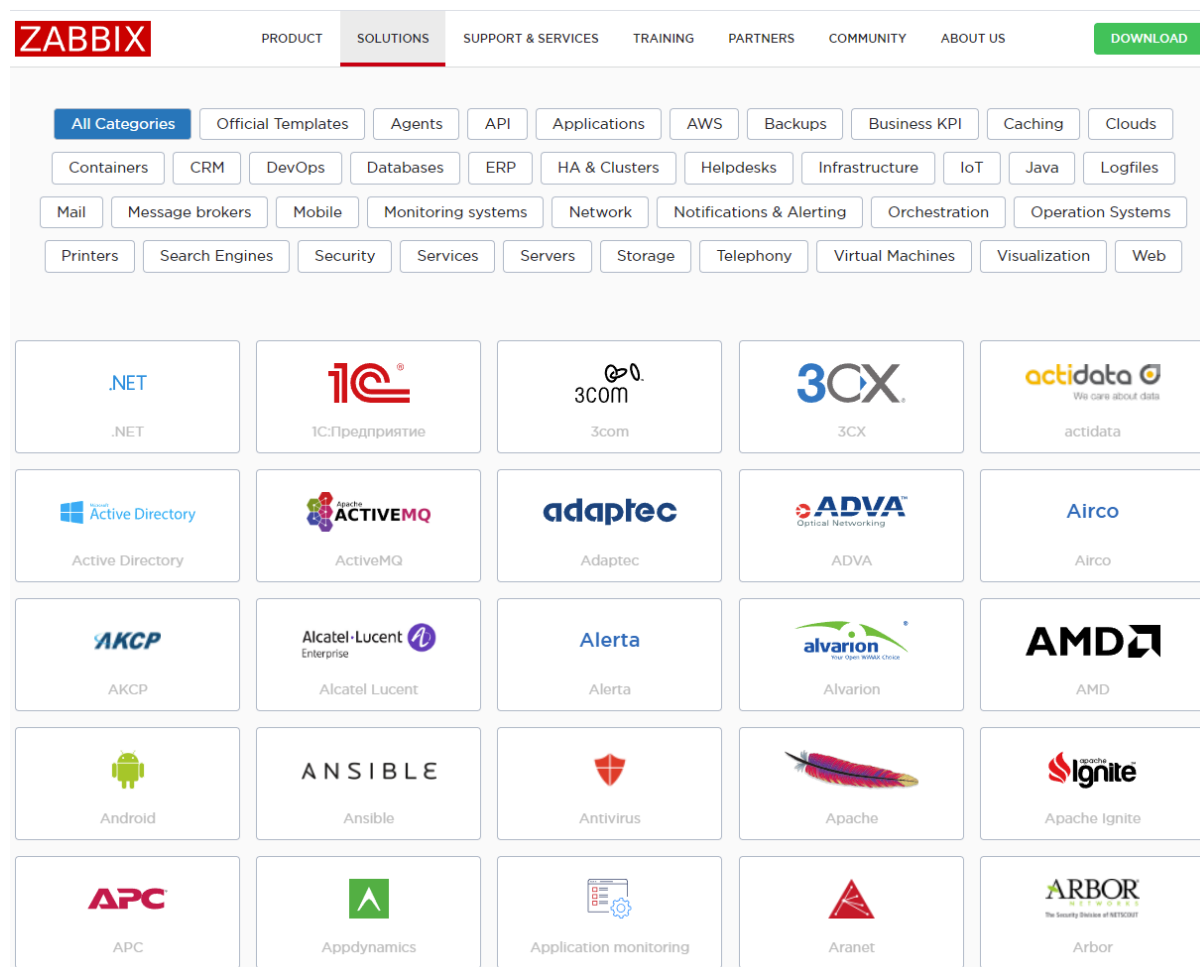
The screenshot shows the Zabbix web interface for configuring media types. The left sidebar is on the 'Administration' section, with 'Media types' selected. The main content area is titled 'Media types' and contains a table of configured media types. At the top of the table, there are filters for 'Name' and 'Status' (Any, Enabled, Disabled), along with 'Apply' and 'Reset' buttons. The table has columns for Name, Type, Status, Used in actions, and Details. All listed media types are currently 'Enabled'.

Name	Type	Status	Used in actions	Details
Brevis.one	Webhook	Enabled		
Discord	Webhook	Enabled		
Email	Email	Enabled		SMTP server: "mail.example.com"; SMTP helo: "example.com"; SMTP email: "zabbix@example.com"
Email (HTML)	Email	Enabled		SMTP server: "mail.example.com"; SMTP helo: "example.com"; SMTP email: "zabbix@example.com"
Express.ms	Webhook	Enabled		
Github	Webhook	Enabled		
GLPI	Webhook	Enabled		
ilert	Webhook	Enabled		
ITop	Webhook	Enabled		
Jira	Webhook	Enabled		
Jira ServiceDesk	Webhook	Enabled		
Jira with CustomFields	Webhook	Enabled		
ManageEngine ServiceDesk	Webhook	Enabled		
Mattermost	Webhook	Enabled		
MS Teams	Webhook	Enabled		
Opsgenie	Webhook	Enabled		
OTRS	Webhook	Enabled		
PagerDuty	Webhook	Enabled		
Pushover	Webhook	Enabled		
Redmine	Webhook	Enabled		
Rocket Chat	Webhook	Enabled		
ServiceNow	Webhook	Enabled		
SIGNAL4	Webhook	Enabled		
Slack	Webhook	Enabled		
SMS	SMS	Enabled		GSM modem: "/dev/ttyS0"
SolarWinds Service Desk	Webhook	Enabled		
SysAid	Webhook	Enabled		

Obrázok 5.10 Ponuka konfigurácie rôznych sociálnych médií v nástroji zabbix, zdroj vlastný

Nie poslednou, ale tiež veľmi dôležitou časťou je dostupnosť a možnosť monitoringu zariadení a služieb, na ktoré je potrebné získať, a následne nasadiť určité šablóny, pomocou ktorých sme schopný zo zariadení prijímať klasifikované dáta.





Obrázok 5.11 Voľne dostupné šablóny na rôzne zariadenia a služby v nástroji zabbix, zdroj vlastný

Samotná inštalácia nástroja obsahuje približne 300 predvolených šablón, ktoré je možné rozšíriť práve prostredníctvom integrácii dostupných z oficiálnych stránok nástroja. Importovanie týchto šablón je veľmi jednoduché, stačí si šablónu jednoducho do zariadenia z githubu stiahnuť, a následne ju importovať pomocou tlačidla *Import template* do nástroja.

Nesmieme zabudnúť spomenúť ani odkaz na dokumentáciu alebo plne hodnotnú komunitu, na ktorú je možné sa dostať tlačidlom *Help*. Dôležitou informáciou je tiež fakt, ktorý nám umožňuje maximálnu flexibilitu v nástroji aj práve jednoduchou úpravou tabuliek, grafov, šablón a podobne. To znamená, že celý nástroj je univerzálne vložený do rúk administrátora.

### 5.3 Výber nástroja na ďalšie použitie

V tejto kapitole sme venovali dostatočnú pozornosť obom nástrojom, ktoré sú určené na prevádzkový monitoring zariadení a služieb v sieti. Po zoznámení sa s nástrojmi a ich možnosťami, ktoré sme si vo vlastnej testovacej infraštruktúre vyskúšali môžeme prehlásiť, že na

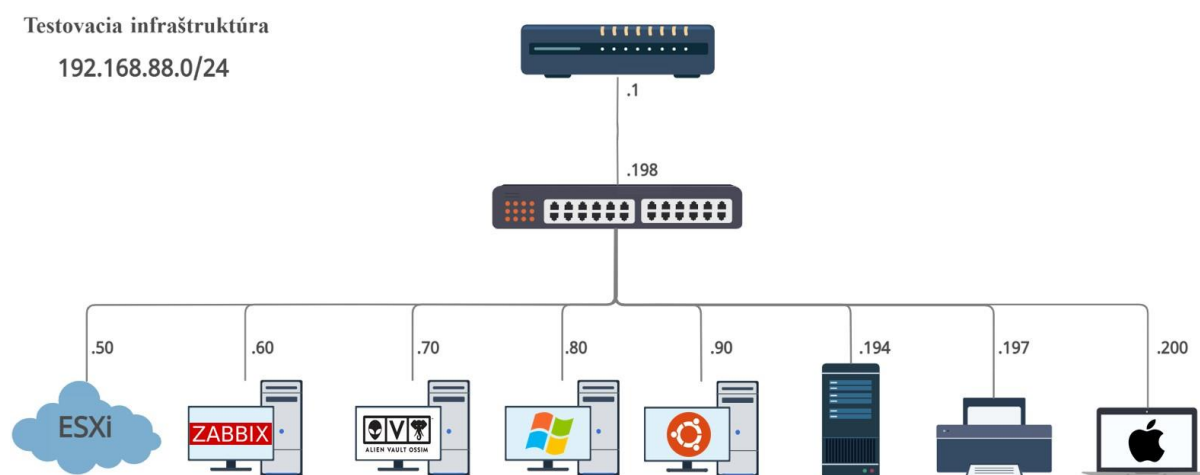
stanovené požiadavky práce sa nám viac hodí nástroj Zabbix. Dôvodom je omnoho jednoduchšia správa nástroja s lepšie graficky dostupným rozhraním. Zároveň má nástroj zabbix širšie spektrum funkcií a možností, ktoré v riešení našej práce hravo využijeme. Hlavnou výhodou tohto nástroju je aj obrovská flexibilita, prehľadný prevádzkový monitoring v podobe grafov, obrovské množstvo voľne dostupných šablón na zariadenia a služby. Rovnako musíme oceniť aj veľmi prehľadnú, a dobre spracovanú dokumentáciu v online forme.

## **II. PRAKTICKÁ ČASŤ**

## 6. TESTOVACIA INFRAŠTRUKTÚRA

Navrhnuté riešenie s potrebnými nástrojmi bolo potrebné najskôr niekde pripraviť, nasadiť, implementovať a na záver celú funkčnosť otestovať. Avšak po konzultácií s externou spoločnosťou nám nebolo umožnené implementovať riešenie v živej prevádzke organizácie.

Po vzájomnej dohode sme dospeli k záveru, aby sme spoločnými silami vytvorili testovaciu infraštruktúru v oddelenej sieti spoločnosti tak, aby sa tam nachádzali kópie reálnych zariadení z prevádzky, a zároveň nebola reálna prevádzka ohrozená. Testovacia infraštruktúra bola vytvorená len na to, aby sa mohlo navrhnuté riešenie najskôr v bezpečí implementovať, otestovať a na záver toto riešenie nasadiť aj do reálnej prevádzky spoločnosti. Spoločnosť si nasadenie nástrojov a ich konfiguráciu viedla vo vlastnej réžii.



Obrázok 6.1 Testovacia infrastruktúra v externej spoločnosti, zdroj vlastný

Testovacia infraštruktúra dostala adresný rozsah 192.168.88.0/24, do ktorého boli priradené všetky potrebné zariadenia a nástroje vyplývajúce z požiadaviek spoločnosti. Zloženie zariadení a priradené IP adresy sú zobrazené na obrázku vyššie.

V oddelenej sieti sa nachádzal centrálny router, switch a zariadenia, akým sú Vmware ESXi, ktorý mal priradenú IP adresu 192.168.88.50. Na tomto virtualizačnom serveri boli vytvorené 2 zariadenia, a tým bol Zabbix (192.168.88.60) a AlienVault (192.168.88.70). počítače s OS Windows (192.168.88.80), Linux Ubuntu (192.168.88.90) a macbook (192.168.88.200) boli pripravené a nasadené administrátorom spoločnosti. V sieti sa nachádzal aj Synology NAS server (192.168.88.194) a tlačiareň Xerox Workcenter 3220 (192.168.88.197).

Inštalácia a príprava nástrojov AlienVault a Zabbix boli zabezpečené v našej vlastnej testovacej infraštruktúre mimo spoločnosti, ktoré sú popísané v nasledujúcej kapitole.

IP adresa, ktorá bola priradená nášmu zariadeniu, z ktorého sme sa do testovacej infraštruktúry pripájali bola *192.168.89.202*, čo znamená, že táto IP adresa pochádzala z inej siete, ako sme mali testovaciu infraštruktúru. Táto druhá sieť *192.168.89.0/24* bola vytvorená tiež na testovacie účely, ale použila sa na logické oddelenie zariadení z testovacej infraštruktúry od tých, ktorými sme testovali implementáciu alebo z ktorých sme konfigurovali zariadenia a nástroje.

## 7. PRÍPRAVA NÁSTROJOV

Nástroje, ktoré boli vybraté, a následne budú nasadené a implementované v tejto práci, boli inštalované v našej testovacej infraštruktúre v aplikácii VMware Workstation Pro. V tejto kapitole sme sa zamerali na inštaláciu nástrojov a ich prípravu na export do testovacej infraštruktúry spoločnosti, kde bude aplikované riešenie tejto práce.

Pred nasadením nástrojov do infraštruktúry spoločnosti, nástroje budú nasadené a overené vedúcim práce na zariadeniach fakulty, aby sme predišli zbytočným komplikáciám počas nasadzovania nástrojov do infraštruktúry spoločnosti.

Zvolený nástroj na detekciu zraniteľností AlienVault OSSIM a nástroj na prevádzkové monitorovanie siete Zabbix a ich inštalácia či príprava na export, sú popísané v nasledujúcej podkapitole. Oba tieto nástroje boli inštalované v hardvérovej kompatibilite ESXi 7.0.

Zvolený adresný rozsah našej vlastnej testovacej infraštruktúry je *192.168.10.0/25*, kde nástroju AlienVault sme priradili IP adresu *192.168.10.50* a nástroju Zabbix sme priradili IP adresu *192.168.10.51*. Ako predvolenú bránu sme použili IP adresu *192.168.10.1* s maskou *255.255.255.128*. Všetky tieto sieťové nastavenia boli použité iba v našej testovacej infraštruktúre, po nasadení nástrojov do infraštruktúry spoločnosti boli tieto nastavenia upravené do zvoleného sieťového rozsahu spoločnosti, ktoré sú popísané v ďalších podkapitolách.

### 7.1 Inštalácia nástroja AlienVault OSSIM

V tejto kapitole sme popísali inštaláciu a prípravu nástroja AlienVault vo verzií 8.5.8 vo vlastnej testovacej infraštruktúre. Po inštalácii sme zmenili predvolené mená a heslá administrátorských účtov a pripravili nástroj na export. Všetky kroky sú popísané v nasledujúcich podkapitolách.

#### 7.1.1 Systémové prostriedky

Na inštaláciu tohto nástroja sú stanovené nasledovné minimálne systémové prostriedky:

- 2 jadrá CPU
- 4-8 GB RAM
- 50 GB HDD
- 1 Gbps sieťovú kartu

Pre plynulý chod nástroja sme zvolili nasledovné hardvérové prostriedky:

- 4 jadrá CPU
- 12 GB RAM
- 80 GB HDD
- 2.5 Gbps sieťovú kartu

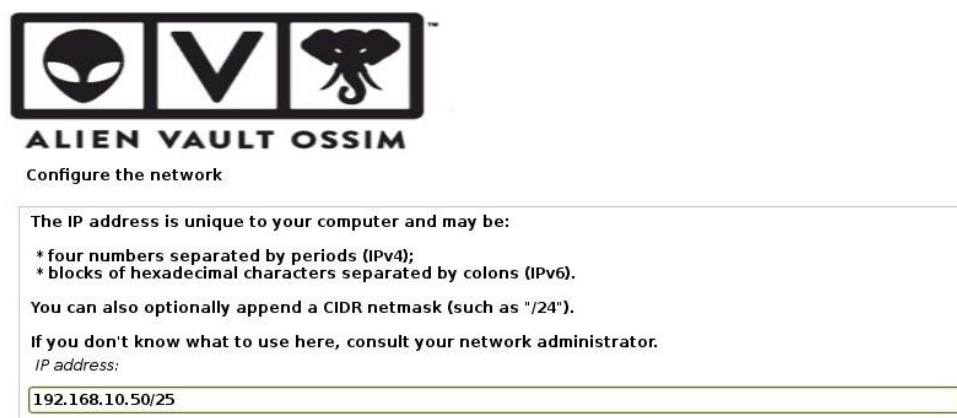
### 7.1.2 Inštalácia

Po nastavení systémových prostriedkov sme priradili na virtuálne zariadenie inštaláčny súbor vo formáte .iso, zariadenie sme spustili a začali inštaláciu:



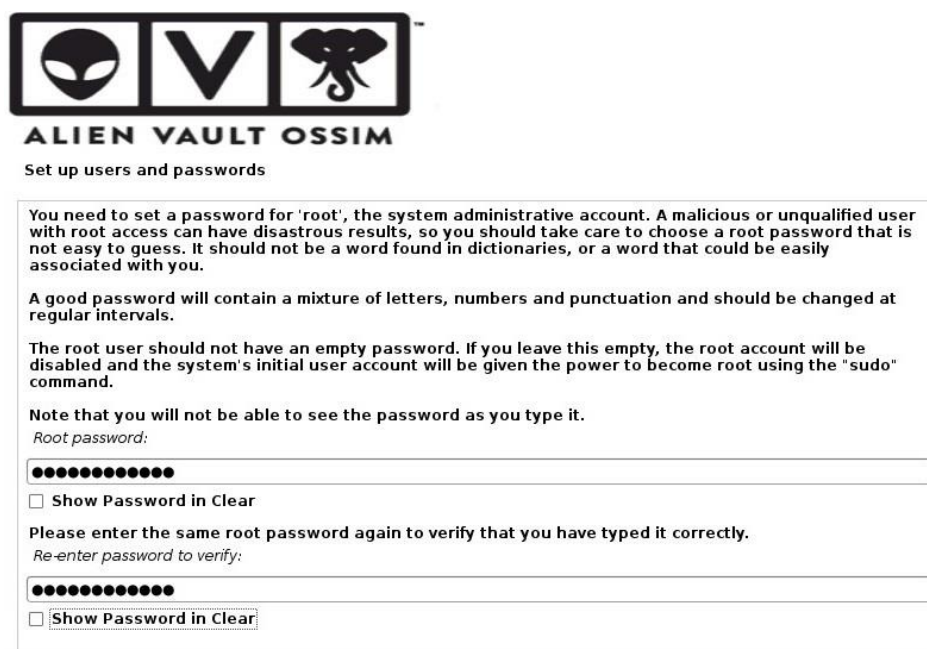
Obrázok 7.1 Úvodná obrazovka inštalácie AlienVault, zdroj vlastný

Inštalácia sa skladá z niekoľkých krokov, kde je možnosť výberu jazyka, regiónu či rozloženia klávesnice. Ďalej je potrebné nakonfigurovať sieťové rozhranie, kde sme zadali IP adresu *192.168.10.50/25*, čo je sieťový rozsah našej vlastnej testovacej infraštruktúry. Táto adresa bude zároveň použitá aj vo webovom rozhraní po dokončení inštalácie. V nasledujúcom kroku sme zadali predvolenú bránu (gateway) prvú z rozsahu, teda *192.168.10.1*.



Obrázok 7.2 Sieťová konfigurácia v vo vlastnej infraštruktúre AlienVault, zdroj vlastný

Poslednými krokmi inštalácie boli vytvoriť heslo pre používateľa *root* a zadať časovú zónu. Heslo, ktoré sme zadali budeme neskôr používať na prihlásenie sa do systémovej konzoly.



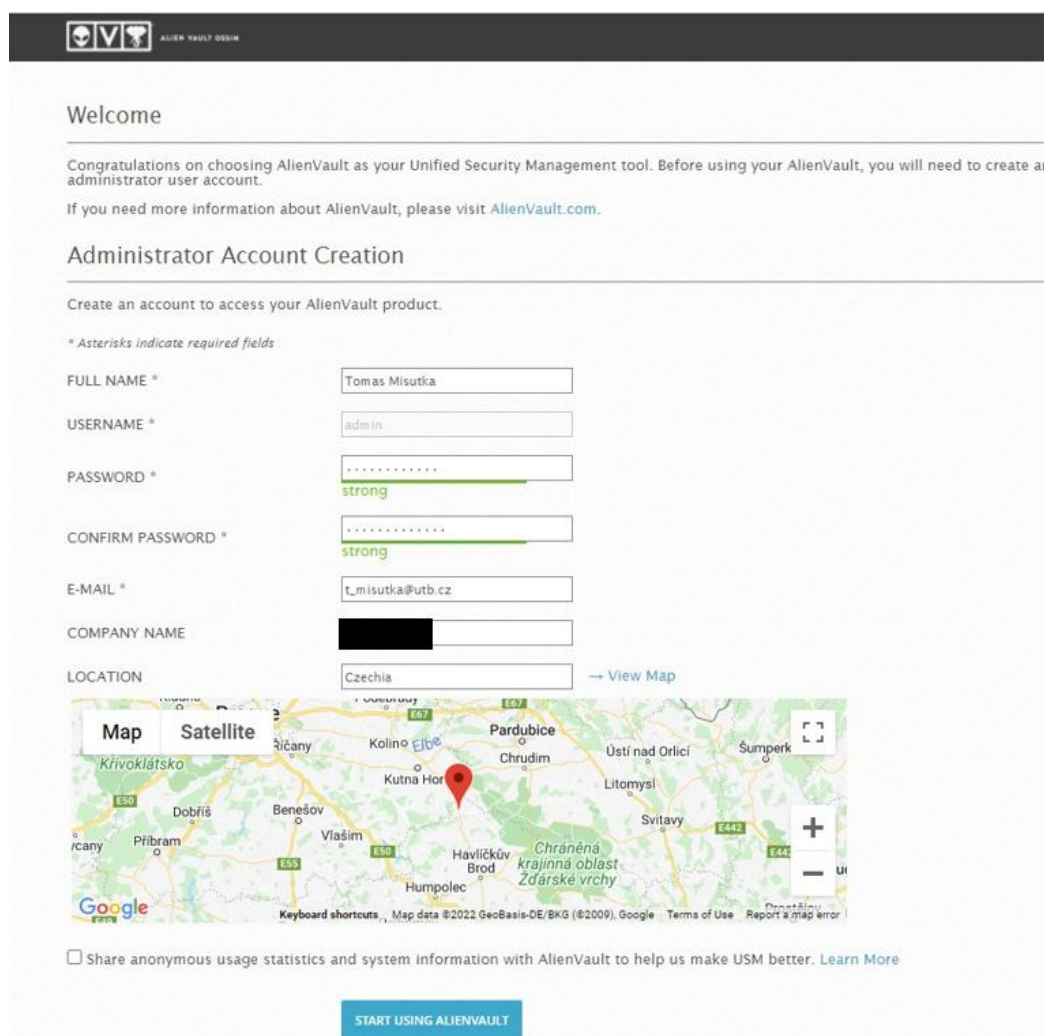
The screenshot shows the 'Set up users and passwords' screen of the AlienVault OSSIM installer. At the top is the AlienVault logo (three squares: an alien head, a 'V', and an elephant) and the text 'ALIEN VAULT OSSIM'. Below the logo is the title 'Set up users and passwords'. The main content area contains several paragraphs of instructions: 'You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.', 'A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.', 'The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.', and 'Note that you will not be able to see the password as you type it.' Below these instructions is a section for 'Root password:' with a password input field (masked with dots), a checkbox for 'Show Password in Clear', and a 'Please enter the same root password again to verify that you have typed it correctly.' prompt. This is followed by a 'Re-enter password to verify:' section with another masked password input field and a 'Show Password in Clear' checkbox.

Obrázok 7.3 Vytvorenie hesla pre používateľa *root* – AlienVault, zdroj vlastný

### 7.1.3 Dokončenie inštalácie grafickým zohraním

Po dokončení inštalácie sa zariadenie reštartuje a po úvodnej inicializácii sa systém načíta v režime konzoly. Presunuli sme sa pomocou prehliadača na grafické rozhranie a zadaním URL adresy *https://192.168.10.50/* sme nastavili administrátorský účet vyplnením mena, administrátorského hesla, emailu a lokácie.





AlienVault OSSIM

## Welcome

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.

If you need more information about AlienVault, please visit [AlienVault.com](https://www.alienvault.com).

### Administrator Account Creation

Create an account to access your AlienVault product.

\* Asterisks indicate required fields:

FULL NAME \*

USERNAME \*

PASSWORD \*   
strong

CONFIRM PASSWORD \*   
strong

E-MAIL \*

COMPANY NAME

LOCATION  [View Map](#)

☐ Share anonymous usage statistics and system information with AlienVault to help us make USM better. [Learn More](#)

[START USING ALIENVAULT](#)

Obrázok 7.4 AlienVault - vytvorenie účtu admin pomocou grafického rozhrania, zdroj vlastný

Pokračovali sme kontrolou IP adries pre management, úvodným skenovaním siete a zariadení pripojených do nej, nastavením log managementu a nepovinnou, ale odporúčanou registráciou do projektu OTX.

### 7.1.4 Úprava sieťovej konfigurácie v spoločnosti

Po nasadení nástroja AlienVault OSSIM v testovacej infraštruktúre spoločnosti bolo nutné upraviť sieťovú konfiguráciu nástroja do siete spoločnosti, pre ktorý bola vyhradená IP adresa 192.168.88.70, maska siete 255.255.255.0 a default gateway 192.168.88.1. DNS sme museli zvoliť z externej siete, a to 8.8.8.8, aby bol tento nástroj prístup na internet.

Po základnej kontrole nástroja bolo zistené, že z neznámych príčin nie je dostupný skener na zisťovanie zraniteľností. Problém sa nám nepodarilo odstrániť ani prostredníctvom logov či reštartom skenera. Po vzájomnej dohode bolo nutné spraviť inštaláciu nástroja znovu priamo

v testovacej infraštruktúre spoločnosti. Konfigurácia nástroja pri inštalácii bola zachovaná a použila sa rovnaká ako v príprave nástroja v našej vlastnej sieti.

## 7.2 Inštalácia nástroja Zabbix

Na inštaláciu nástroja Zabbix sme najskôr potrebovali stiahnuť OS s distribúciou Linux, my sme zvolili Linux Ubuntu vo verzií 20.04.4 LTS, ktorý zaručuje podporu až do roku 2025.

### 7.2.1 Systémové prostriedky

Na plynulý chod systému sme zvolili nasledovnú konfiguráciu:

- 4 jadrá CPU
- 8 GB RAM
- 40 GB HDD
- 2.5 Gbps sieťovú kartu

Inštalácia OS Linux Ubuntu 20.04.4 nie je súčasťou tejto práce, nakoľko bol použitý štandardný postup inštalácie. Po inštalácii sme pomocou konzoly aktualizovali všetky balíčky a zmenili IP adresu na statickú pomocou textového editora *nano* v systémovom súbore */etc/netplan/01-network-manager-all.yaml* a príkazom *sudo netplan apply* potvrdili sieťové nastavenia.



```
:-$ sudo cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  ethernets:
    ens33:
      addresses: [192.168.10.51/25]
      gateway4: 192.168.10.1
      nameservers:
        addresses: [192.168.10.1, 8.8.8.8, 4.2.2.2]
  version: 2
  renderer: NetworkManager
```

Obrázok 7.5 Ubuntu sieťové nastavenia vo vlastnej infraštruktúre, zdroj vlastný

V tomto stave bol systém s OS Linux pripravený na inštaláciu nástroja Zabbix.

### 7.2.2 Inštalácia

Na úvod pod používateľom *root* bolo nutné inicializovať repozitár Zabbix, kde sme postupovali odporúčenou inicializáciou verzie Zabbixu 6.0 LTS, distribúciou Linux Ubuntu vo verzií 20.04.

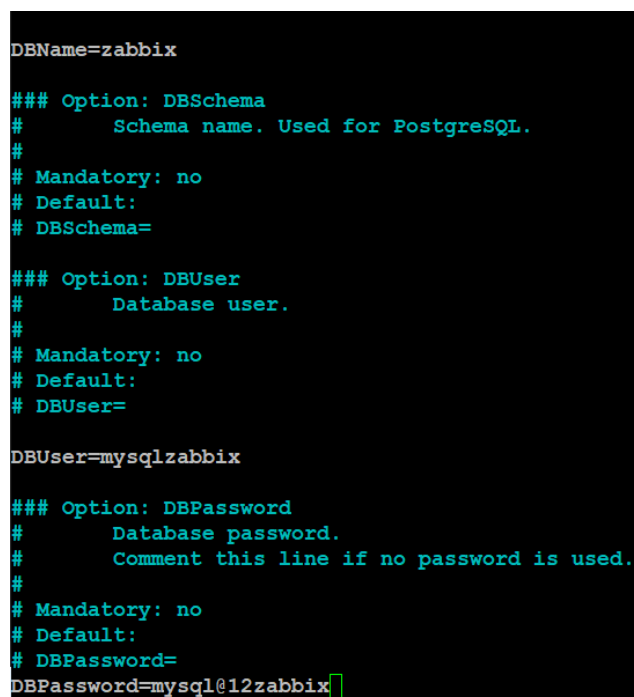
```
# wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
```

Po úvodnej inicializácii sme nainštalovali všetky potrebné balíčky k inštalácii nástroja Zabbix nasledujúcim príkazom:

```
# sudo apt install zabbix-server-mysql mysql-server zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

Ďalej sme pokračovali konfiguráciou databázy, kde sme vytvorili databázu *zabbix*, nového používateľa *mysqlzabbix* a priradili mu všetky potrebné privilégia.

V konfiguračnom súbore */etc/zabbix/zabbix\_server.conf*, sme nastavili názov databázy, používateľa databázy a jeho heslo.



```
DBName=zabbix

### Option: DBSchema
#   Schema name. Used for PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=

### Option: DBUser
#   Database user.
#
# Mandatory: no
# Default:
# DBUser=

DBUser=mysqlzabbix

### Option: DBPassword
#   Database password.
#   Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=

DBPassword=mysql@12zabbix
```

Obrázok 7.6 Konfigurácia databázy serverovej časti zabbix, zdroj vlastný

Súbor sme uložili a následne reštartovali služby *zabbix-server* *zabbix-agent* a *apache2*, aby sa aplikovali všetky vykonané zmeny, a tým by bola úvodná inštalácia hotová.

Následne sme sa presunuli do grafickej časti nástroja zadaním URL adresy *https://192.168.10.51/zabbix/* do prehliadača. Na úvodnej stránke sme skontrolovali potrebné balíčky, verzie a ich hodnoty, či sú v požadovanom stave a doplnili sme konfiguráciu databázy. Ostatné hodnoty parametrov sme nechali na predvolených hodnotách.

**ZABBIX**

Welcome  
Check of pre-requisites  
Configure DB connection  
Settings  
Pre-installation summary  
Install

### Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database.  
Press "Next step" button when done.

Database type:

Database host:

Database port:  0 - use default port

Database name:

Store credentials in: ☒ Plain text ☐ HashiCorp Vault

User:

Password:

Database TLS encryption: Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

Obrázok 7.7 Konfigurácia databázy cez management zabbix-u, zdroj vlastný

Nasledovalo už len nastavenie doménového mena, časovú zónu a výber farebnej témy, ktorú chceli zvoliť ako predvolenú v zobrazení. Po dokončení úvodnej konfigurácie sme sa prihlásili na management nástroja zabbix pomocou predvoleného prihlasovacieho mena *Admin* a hesla *zabbix*.

### 7.2.3 Zmena predvolených prihlasovacích údajov

V navigačnej časti sme prešli do sekcie *Administration* a tam sme zvolili podkategóriu *Users* a v dostupnej tabuľke sme klikli na používateľa s menom *Admin*. Následne sme upravili predvolené prihlasovacie heslo administrátorského účtu. Zmeny sme potvrdili tlačidlom *update*.

The screenshot shows the Zabbix web interface for editing a user. The left sidebar is dark blue with the Zabbix logo and a search bar. The 'Administration' section is expanded, showing options like General, Proxies, Authentication, User groups, User roles, Users, Media types, Scripts, and Queue. The 'Users' page has tabs for 'User', 'Media', and 'Permissions'. The 'User' tab is active, showing a form for the 'Admin' user. The form includes fields for Username, Name, Last name, Groups, Password, Password (once again), Language, Time zone, Theme, Auto-login, Auto-logout, Refresh, Rows per page, and URL (after login). The 'Update' button is highlighted in blue.

Obrázok 7.8 Zabbix - zmena predvolených administrátorských údajov, zdroj vlastný

## 7.2.4 Úprava sieťovej konfigurácie v spoločnosti

Nástroj Zabbix, ktorý bol nainštalovaný na OS Linux Ubuntu a nasadený do testovacej infraštruktúry v spoločnosti mal nesprávne sieťové nastavenia. Tieto nastavenia sme museli upraviť na IP adresu *192.168.88.60/24* a default gateway bol *192.168.88.1*. Následne sme ich upravili pomocou príkazového riadku a rovnakých balíčkov, ktoré boli použité počas inštalácie. V konfigurácii DNS serverov sme okrem IP adresy routera museli pridať aj externú IP adresu, a to *8.8.8.8*, čím sme zabezpečili, že malo zariadenie prístup na internet.

## 7.3 Export, overenie inštalácie a nasadenie nástrojov v spoločnosti

Pred samotným exportom nástrojov bolo nutné odpojiť ich od inštaláčného média, aby sme sa po nasadení nástrojov vyhli zbytočným upozorneniam počas štartu nástrojov v ESXi. Export nástrojov sme vykonali do súboru s príponou *.ova* pomocou aplikácie vmware Workstation PRO, kde boli nástroje inštalované a konfigurované.

### 7.3.1 Overenie inštalácie

Pred nasadením nástrojov v spoločnosti sme overili funkčnosť inštalácie v spolupráci s vedúcim práce na fyzických zariadeniach fakulty, ktoré boli nasadené, overené a povolené na ďalšie použitie.

### 7.3.2 Nasadenie nástrojov v testovacej infraštruktúre

Nasadenie nástrojov v spoločnosti bolo aplikované administrátorom zo strany spoločnosti v spolupráci s vedúcim práce. Nástroje boli nasadené do testovacej infraštruktúry, v ktorej sme implementovali a testovali navrhnuté riešenie vo virtualizačnom prostredí *vmware esxi*.

## 8. IMPLEMENTÁCIA RIEŠENIA

V tejto kapitole sme vypracovali implementáciu navrhnutého riešenia v testovacej infraštruktúre spoločnosti. Zariadenia, popis siete a IP rozsahy sú popísané v predchádzajúcich kapitolách. Cieľom bolo implementovať riešenie na detekciu zraniteľností v sieti s hľadaním anomálií pomocou nástroja AlienVault OSSIM. Na sieťový monitoring testovacej prevádzky bol zvolený nástroj Zabbix. Testovanie implementácie a dosiahnuté výsledky sme popisovali v nasledujúcej kapitole.

V konfigurácii nástroja AlienVault bolo potrebné v úvode pridať testovaciu infraštruktúru na monitoring, rozsah *192.168.88.0/24* a následne všetky zariadenia do nej manuálne pridať. Hneď za tým sme vykonali konfiguráciu skupín, kde sme si jednotlivé zariadenia roztriedili podľa dôležitosti a využitia. Následne sme nainštalovali HIDS agentov na všetky zariadenia, kde bola inštalácia možná. Na zariadeniach, kde nebola možnosť zbierania logov pomocou HIDS agentov, bolo potrebné konfigurovať odosielanie logov na vzdialený server. Nesmela chýbať ani aplikácia pluginov na zariadenia, monitoring dostupnosti zariadení a služieb. Tak tiež sme konfigurovali odosielanie emailov z nástroja pri výskyte alarmu, plánovali sme hľadanie zraniteľností v sieti a konfiguráciu sme zavŕšili zbieraním sieťovej prevádzky protokolom netflow zo zariadenia router a konfiguráciou direktívy na vytvorenie alarmu pri zachytení útoku skenovaním portov.

V konfigurácii nástroja Zabbix sme v úvode spravili analýzu aktuálne dostupných šablón, ktoré by sme mohli na zariadeniach použiť. Zvolené šablóny sme následne do nástroja importovali a neskôr ich na zariadenia nasadili. Následne sme konfigurovali monitorovanie zariadení protokolom SNMP prevažne verzie 3, kde museli byť konfigurované obe strany komunikácie s rovnakými hodnotami parametrov. Ďalej sme nakonfigurovali odoslanie notifikácií prostredníctvom emailu v prípade, že by sa objavili nové problémy v niektorom zo zariadení. V závere sme implementovali vlastné položky do šablóny určenej na tlačiareň, pretože šablónu, ktorú sme používali neumožnila monitorovať všetky hodnoty, ktoré boli v požiadavkách. Následne sme na jeden z dvoch vytvorených položiek pripravili trigger, ktorým sme zabezpečili, že ak sa aktuálny počet papiera dostane pod hodnotu 5, systém vyhlási problém a odošle email o potrebnom doplnení papiera.

### 8.1 AlienVault OSSIM

Najskôr bolo potrebné sa prihlásiť prostredníctvom webového rozhrania pod administrátorským účtom, ktorý bol dostupný na IP adrese *192.168.88.70*. Do webového rozhrania sme sa prihlásili pomocou URL adresy *https://192.168.88.70* a následne sme zadali prihlasovacie údaje administrátora.

V tejto kapitole sme sa zamerali na konfiguráciu testovacej infraštruktúry a pridávanie zariadení do nej. Pokračovali sme vytvorením skupín, aplikáciou HIDS agentov, konfiguráciou vzdialených logov, aplikáciou pluginov na zariadenia, konfiguráciu sledovania dostupnosti zariadení a služieb, ďalej sme definovali podmienky na odoslanie emailu a konfiguráciu sme zavýšili prehľadávaním siete a hľadaním zraniteľností, konfiguráciou netflow a prípravou direktívy na vytvorenie alarmu pri útoku skenovaním portov.

### 8.1.1 Konfigurácia siete

Testovaciu sieť, v ktorej sme hľadali zraniteľnosti a anomálie sme museli najskôr manuálne pridať do nástroja. Bola tam aj možnosť pridať sieť prostredníctvom skenovania, my sme zvolili cestu manuálneho pridávania, keďže sme poznali presný rozsah siete.

Prešli sme do časti *Environment/Asset & Groups*, zvolili sme záložku *Networks* a sieť sme pridali tlačidlom *ADD NETWORK*.

Vyplnili sme názov siete *testing\_infrastructure*, CIDR *192.168.88.0/24*, dôležitosť siete sme nastavili na hodnotu *3*.



Obrázok 8.1 Pridanie testovacej siete v nástroji ALIENVAULT, zdroj vlastný

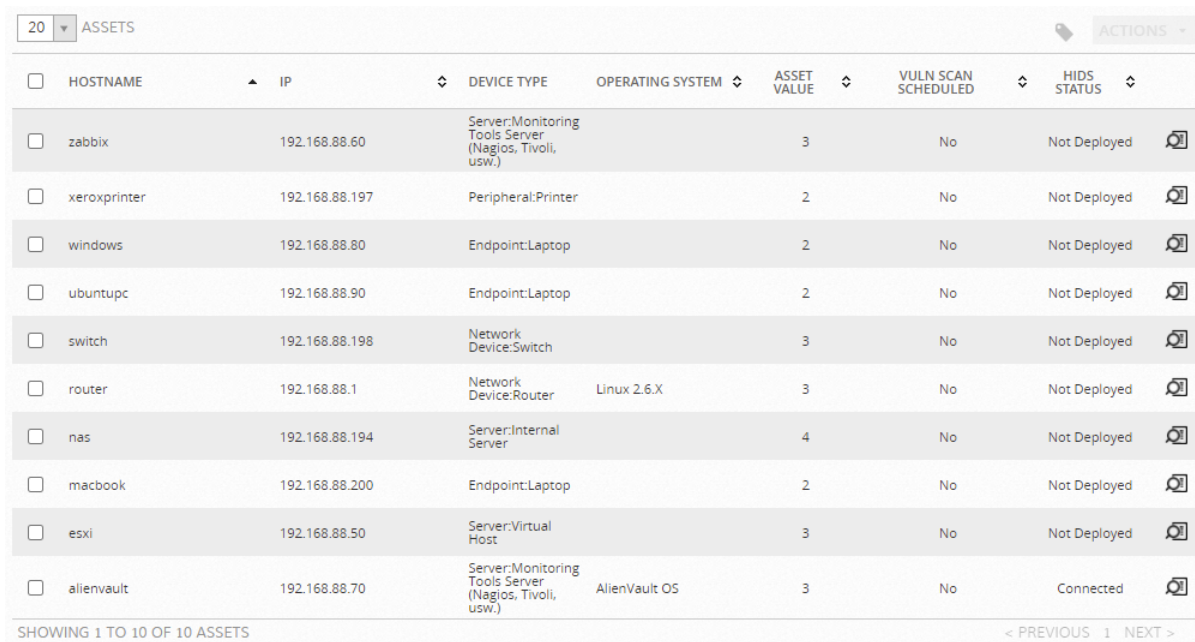
### 8.1.2 Assety a grupy

#### Assety

V časti *Environment/ Asset & Groups* sme zvolili záložku *ASSETS*, kde sme manuálne pridali jednotlivé zariadenia z testovacej infraštruktúry. Pri každom zariadení sme vyplnili jeho názov, IP adresu podľa návrhu testovacej infraštruktúry, FQDN, typ zariadenia. OS a model



sme nevyplnili, pretože možnosti, ktoré sú dostupné, nie sú úplne aktuálne, a boli nám ponúknuté iba staré verzie OS. Na zariadeniach, pri ktorých nemôže nastať pripojenie z externej siete prostredníctvom VPN, ako sú napríklad servery alebo aktívne sieťové prvky, ponecháme možnosť *internal asset*, a ostatné zariadenia nastavíme ako *external*. Takto sme postupovali pri každom zariadení z testovacej infraštruktúry. Aktívnym prvkom a serverom sme zadali dôlezitosť na hodnotu 3, NAS serveru sme priradili hodnotu 4 a ostatné sme nechali na predvolenej hodnote 2. Zariadenie sme pridali tlačidlom *SAVE*.



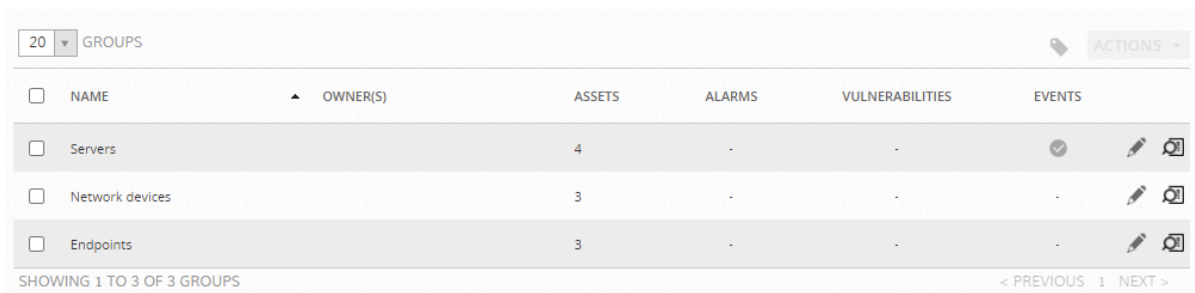
<input type="checkbox"/>	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS	
<input type="checkbox"/>	zabbix	192.168.88.60	Server:Monitoring Tools Server (Nagios, Tivoli, usw.)		3	No	Not Deployed	
<input type="checkbox"/>	xeroxprinter	192.168.88.197	Peripheral:Printer		2	No	Not Deployed	
<input type="checkbox"/>	windows	192.168.88.80	Endpoint:Laptop		2	No	Not Deployed	
<input type="checkbox"/>	ubuntupc	192.168.88.90	Endpoint:Laptop		2	No	Not Deployed	
<input type="checkbox"/>	switch	192.168.88.198	Network Device:Switch		3	No	Not Deployed	
<input type="checkbox"/>	router	192.168.88.1	Network Device:Router	Linux 2.6.X	3	No	Not Deployed	
<input type="checkbox"/>	nas	192.168.88.194	Server:Internal Server		4	No	Not Deployed	
<input type="checkbox"/>	macbook	192.168.88.200	Endpoint:Laptop		2	No	Not Deployed	
<input type="checkbox"/>	esxi	192.168.88.50	Server:Virtual Host		3	No	Not Deployed	
<input type="checkbox"/>	alienvault	192.168.88.70	Server:Monitoring Tools Server (Nagios, Tivoli, usw.)	AlienVault OS	3	No	Connected	

SHOWING 1 TO 10 OF 10 ASSETS

Obrázok 8.2 Pridanie zariadení do nástroja AlienVault, zdroj vlastný

## Grupy

V tej istej sekcii *ASSETS & GROUPS* sme prešli do záložky *ASSET GROUPS*, kde sme vytvorili skupiny s názvom *Servers*, *Network devices* a *Endpoints*. Do skupiny *Servers* sme pridali zariadenia NAS, ESXi, Zabbix a AlienVault, do skupiny *Network\_devices* sme zaradili tlačiareň, router, switch a do poslednej skupiny *Endpoints* sme zaradili zariadenia s OS Windows, Linux Ubuntu a Mac OS. Spolu sme do skupín priradili všetkých 10 zariadení z testovacej infraštruktúry.



<input type="checkbox"/>	NAME	OWNER(S)	ASSETS	ALARMS	VULNERABILITIES	EVENTS
<input type="checkbox"/>	Servers		4	-	-	
<input type="checkbox"/>	Network devices		3	-	-	
<input type="checkbox"/>	Endpoints		3	-	-	

SHOWING 1 TO 3 OF 3 GROUPS

Obrázok 8.3 Pridanie zariadení do skupín, zdroj vlastný

### 8.1.3 HIDS agenti

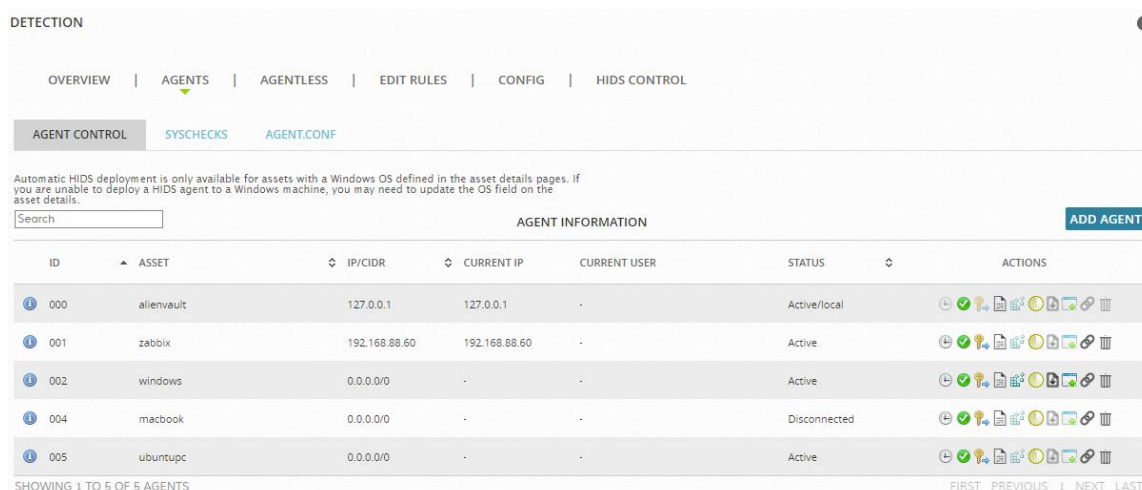
Konfigurácia HIDS agentov bola dôležitá, pretože umožňuje monitoring a aktuálny stav daných PC systémov. Zároveň umožňuje vzdialené posielanie logov do nástroja vrátane *file integrity monitoring*, *rootkit detection* a *event log collection*. Agentov sme chceli nasadiť na zariadenia *windows*, *zabbix*, *ubuntupc* a *macbook*.

Konfigurácia agentov v nástroji AlienVault sa nachádzala pod kategóriou *ENVIRONMENT / DETECTION* v podkategórii *AGENTS*. V tejto časti sa nám zobrazila aktuálne konfigurácia agentov, kde sa nachádzalo iba 1 zariadenie AlienVault, čo je v predvolenej konfigurácii automaticky zapnuté.

Pridanie agentov sme vykonali v časti *AGENT CONTROL* tlačidlom *ADD AGENT*, kde sme vyhľadali každé, už existujúce zariadenie v kategórii *Assets*. Automaticky bolo doplnené meno agenta podľa FQDN, ktoré bolo možno upraviť podľa vlastnej potreby.

Pri zariadeniach, ktoré môžu byť pripojené prostredníctvom VPN, ako je laptop s OS Windows, Ubuntu alebo Mac OS sme zaškrtnuli možnosť dynamickej IP adresy a pridávanie sme ukončili tlačidlom *SAVE*.

Nasadenie agentov bolo pre jednotlivé OS odlišné, preto sme popísali možnosti a proces nasadenia pre každý OS zvlášť.



ID	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault	127.0.0.1	127.0.0.1	-	Active/local	[Icons]
001	zabbix	192.168.88.60	192.168.88.60	-	Active	[Icons]
002	windows	0.0.0.0/0	-	-	Active	[Icons]
004	macbook	0.0.0.0/0	-	-	Disconnected	[Icons]
005	ubuntupc	0.0.0.0/0	-	-	Active	[Icons]

SHOWING 1 TO 5 OF 5 AGENTS

Obrázok 8.4 Konfigurácia HIDS agentov v nástroji AlienVault, zdroj vlastný

## Windows

Na zariadeniach s OS Windows máme 2 možnosti, ako sme mohli nasadiť agenta na zariadenie. Prvou možnosťou bolo automatická inštalácia priamo z prostredia AlienVault, ktorá však vyžadovala doplňujúcu konfiguráciu systému zdieľania súborov a systémových politík Windows, čo nebola najvhodnejšia alternatíva.

Druhou možnosťou bolo stiahnutie binárneho inštalačného súboru, ktorý bol vygenerovaný v nástroji AlienVault s predpripravenou serverovou konfiguráciou spolu s autentifikačným kľúčom, ktorý je potrebné nainštalovať s administrátorskými právami. Toto druhé riešenie bolo pre nás oveľa výhodnejšie, preto sme využili túto alternatívu.

Vygenerovanie binárneho inštalačného súboru sme spravili prostredníctvom označeného tlačidla, ktoré je zobrazené na obrázku nižšie.

Automatic HIDS deployment is only available for assets with a Windows OS defined in the asset details pages. If you are unable to deploy a HIDS agent to a Windows machine, you may need to update the OS field on the asset details.

ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/local	
001	windows	windows	192.168.88.80	-	-	Disconnected	
2	zabbix	zabbix	192.168.88.60	-	-	Disconnected	

Obrázok 8.5 Generovanie binárneho súboru pre inštaláciu HIDS agenta s OS Windows, zdroj vlastný

Tento vygenerovaný binárny súbor sme prekopírovali prostredníctvom protokolu RDP na zariadenie a spustili inštaláciu s administrátorskými právami. Po dokončení bolo nasadenie HIDS agenta na zariadení s OS Windows hotové.

## Linux

Postup na inštaláciu HIDS agenta pre OS Linux bol aplikovaný na zariadenia *zabbix* a *ubuntupc*. Do systémov sme sa prihlasovali pomocou protokolu *ssh* s administrátorskými právami *sudo*.

Na úvod bolo potrebné aktualizovať všetky balíčky a nainštalovali ďalšie potrebné, ktoré sme potrebovali na inštaláciu HIDS agenta.

```
# sudo apt update

# sudo apt upgrade

# sudo apt -y install wget git vim unzip make gcc build-essential php php-cli
php-common libapache2-mod-php apache2-utils inotify-tools libpcre2-dev zlib1g-dev
libz-dev libssl-dev libevent-dev build-essential libsystemd-dev
```

Následne sme si pripravili premennú s názvom *VER*, ktorej sme prideliť najnovšiu dostupnú verziu agenta 3.7.0. Túto premennú sme používali v nasledujúcich krokoch inštalácie.

```
# export VER="3.7.0"
```

Ďalej sme si stiahli inštalačný súbor v archívnom formáte *.tar* vo verzií podľa premennej *VER* z oficiálneho repozitáru ossec a rovno tento archív rozbalili. Následne sme sa presunuli do adresáru, ktorý bol po rozbalení vytvorený.

```
# wget https://github.com/ossec/ossec-hids/archive/${VER}.tar.gz
# tar -xvzf ${VER}.tar.gz
# cd ossec-hids-${VER}
```

Spustili sme inštaláciu, kde sme zvolili jazyk *en*, pokračovali v inštalácii tlačení klávesy *ENTER* a počkali na dokončenie inštalácie. Ako typ inštalácie sme zadali *agent*, následne sme zadali IP adresu HIDS servera *192.168.88.70* a povolíme všetky nasledujúce možnosti monitoringu.

```
# sudo sh install.sh
```

Po dokončení inštalácie sme v súbore *ossec.conf*, ktorý bol umiestnený v */var/ossec/etc/* upravili IP adresu HIDS serveru v prípade, že by nebola správne vyplnená inštaláciou. V našom prípade tam bola IP adresa *192.168.88.70*.

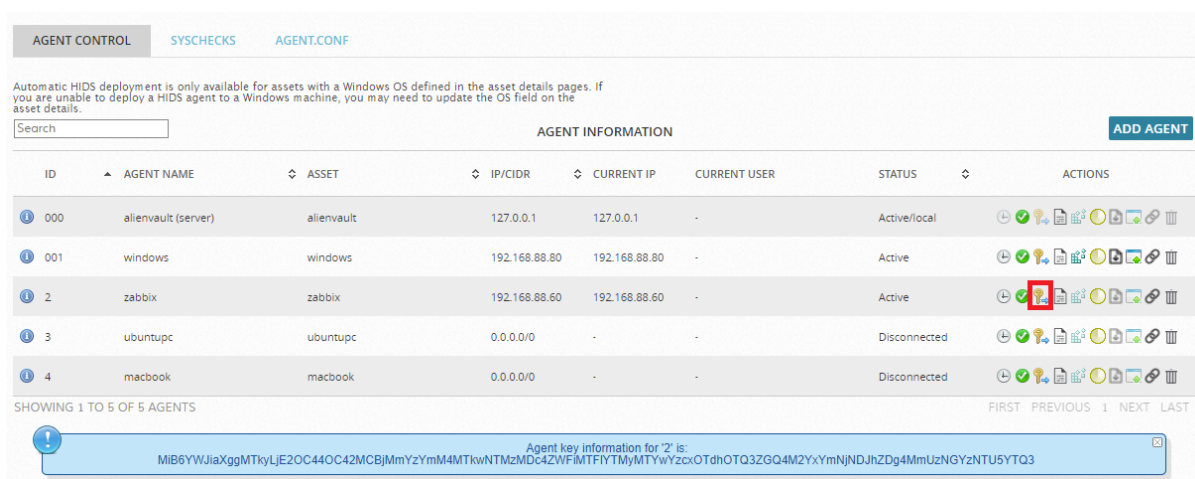


```
GNU nano 4.8
<!-- OSSEC example config -->

<ossec_config>
  <client>
    <server-ip>192.168.88.70</server-ip>
  </client>
```

Obrázok 8.6 Konfigurácia IP adresy HIDS servera na zariadeniach s OS Linux, zdroj vlastný

V ďalšom kroku bolo potrebné priradiť zariadeniu HIDS agent kľúč, ktorý bol vygenerovaný a skopírovaný v nástroji AlienVault.



ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/local	
001	windows	windows	192.168.88.80	192.168.88.80	-	Active	
2	zabbix	zabbix	192.168.88.60	192.168.88.60	-	Active	
3	ubuntupc	ubuntupc	0.0.0.0/0	-	-	Disconnected	
4	macbook	macbook	0.0.0.0/0	-	-	Disconnected	

Agent key information for "2" is:  
MIB6YWJiaXggMTkyLjE2OC44OC42MCBjMmYzYmM4MTkwNTMzMdC4ZWFiMTFhYmYyYzcxOTdhOTQ3ZGQ4M2YxYmNjNDJhZDg4MmUzNGYzNTU5YTQ3

Obrázok 8.7 Zobrazenie unikátneho kľúču HIDS agenta pre zariadenie zabbix, zdroj vlastný

Tento unikátny kľúč bol vložený pomocou aplikácie *manage\_agents* umiestnený v */var/ossec/bin/*, ktorá bola spustená pod administrátorskými právami *sudo*. Po spustení

aplikácie sme zvolili možnosť *I*, pomocou ktorej sme dostali možnosť zadať kľúč HIDS agenta. Nakoniec sme konfiguráciu potvrdili.

```
# sudo su -

# cd /var/ossec/bin

# ./manage_agents

*****
* OSSEC HIDS v3.7.0 Agent manager.      *
* The following options are available: *
*****
(I) Import key from the server (I).
(Q) Quit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MiB6YwJiaXggMTkyLjE2OC44OC42MCEjMmYzYmM4MTkwNTMzMDC4ZWF1MTFlYTM5MTYwYzcxOTdhOTQ3ZGQ4M2YxYmNjNDJhZDg4MmUzNGYzNTU5YTQ3

Agent information:
  ID:2
  Name:zabbix
  IP Address:192.168.88.60

Confirm adding it?(y/n): y
2022/05/07 11:48:21 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory
Added.
** Press ENTER to return to the main menu.
```

Obrázok 8.8 Priradenie unikátneho kľúču HIDS agenta do zariadenia, zdroj vlastný

Dokončenie inštalácie sme previedli príkazmi, ktorými sme povolili štart HIDS agenta po načítaní OS, a zároveň sme tento proces spustili.

```
# sudo /var/ossec/bin/ossec-control start

# sudo systemctl enable ossec

# sudo systemctl start ossec
```

## Mac OS

Inštalácia HIDS agenta na zariadenie Mac mala byť veľmi podobná ako na zariadeniach s OS Linux. Avšak počas inštalácie agenta sa vyskytli problémy s určitými knižnicami, ktoré sú na Mac OS rozdielne. Pri niektorých z nich sa objavili problémy, ktoré nám nedovolili inštaláciu dokončiť. Následne sme prešli do oficiálnej dokumentácie, v ktorej sme zistili, že zariadenia s Mac OS mali poslednú podporu pred niekoľkými rokmi. Po zistení tejto skutočnosti sme sa rozhodli inštaláciu HIDS agenta na tomto zariadení a aj z celého riešenia vynechať.

## Nedostatky HIDS agentov

Obmedzenie, ktoré sme objavili počas implementácie a overovaní riešenia bolo, že sme neboli schopní odhaliť pomocou týchto agentov útok skenovaním portov pomocou programu *NMAP*, ktorý bol vedený L2 vrstvou OSI modelu. Túto skutočnosť sme museli akceptovať

a hľadať iné riešenie, ktoré by nám túto funkcionálnosť umožnilo. Detekciu útoku takéhoto typu museli implementovať na úrovni *netflow*. Konfigurácia *netflow* bola popísaná v nasledujúcich kapitolách práce.

#### 8.1.4 Aplikácia pluginov

Pluginy, ktoré sme aplikovali na zariadenia boli z hľadiska logov veľmi dôležité. Dôvodom bolo zbieranie logov zo zariadení iným spôsobom ako použiť HIDS agentov. Preto bolo nutné použiť podľa typu zariadenia aj k tomu prislúchajúci plugin, ktorým sme zabezpečili rozdelenie a normalizáciu logov, ktoré prichádzali zo zariadení. Dôležité bolo poznamenať, že na každé zariadenie mohlo byť aplikovaných maximálne 10 pluginov a na celom senzore mohlo byť maximálne spolu 100 pluginov. Tieto údaje boli vyčítané z dokumentácie.

Pluginy, ktoré sme použili na jednotlivé zariadenia boli zaznamenané v nasledujúcej tabuľke. Na zariadeniach, na ktorých neboli aplikované žiadne pluginy, posielali logy prostredníctvom HIDS agentov. Výnimkou tu bola tlačiareň, z ktorej nebolo možné posielat' logy žiadnym spôsobom a monitorovanie tohto zariadenia sme riešili pomocou nástroja *zabbix*.

Plugin / Zariadenie	router	esxi	zabbix	windows	ubuntupc	nas	xeroxprinter	switch	macbook
Mikrotik router	x	-	-	-	-	-	-	x	-
Vmware ESXi	-	x	-	-	-	-	-	-	-
Syslog	-	x	-	-	-	x	-	-	-
OpenBSD OpenSSH	-	x	-	-	-	x	-	-	-
Synology DiskStation	-	-	-	-	-	x	-	-	-

Tabuľka 1 Zoznam pluginov, ktoré sa aplikovali na jednotlivé zariadenia, zdroj vlastný

#### 8.1.5 Vzdialené logy

Tento spôsob zbierania logov sme použili na zariadeniach, na ktorých nebolo možné nainštalovať HIDS agenta. Jednalo sa o zariadenia *router*, *esxi*, a *nas*.

V zariadení *mikrotik switch* bol nahratý OS *Mikrotik SwOS*, v ktorom chýbala funkcionálnosť na posielanie logov na vzdialený server, v našom prípade *AlienVault*. Rovnako nebolo možné na tento switch konfigurovať monitoring na úrovni *netflow*, preto toto zariadenie bolo možné monitorovať len pomocou nástroja *zabbix*, čomu sme sa venovali v ďalších kapitolách.

#### Router

Do zariadenia sme sa prihlásili cez prehliadač na URL adresa *http://192.168.88.1* s administrátorskými právami a zvolili sme režim *WebFig*, pomocou ktorého sme mohli konfigurovať zariadenie v interaktívnom režime.

V ľavom navigačnom paneli sme zvolili možnosť *System* a podkategóriu *Logging*, kde sa nachádzajú záložky *Rules* a *Actions*. Na úvod sme prešli do záložky *Actions* a klikli sme na záznam s názvom a typom *remote*, kde bolo potrebné nakonfigurovať posielanie logov do nástroja AlienVault.

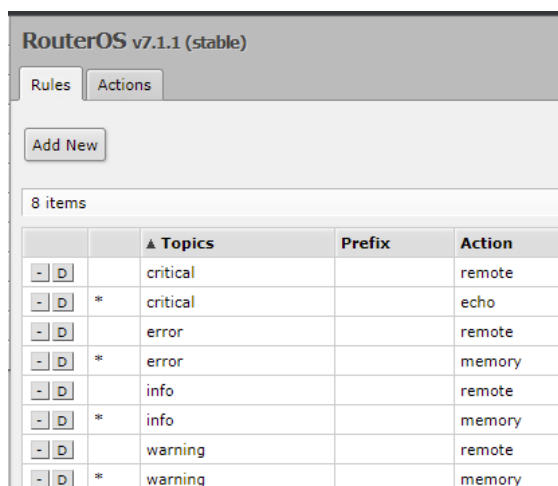
Ako vzdialenú IP adresu sme nastavili adresu nástroja AlienVault *192.168.88.70*, port sme zvolili *514*, zdrojovú IP adresu sme vyplnili podľa IP adresy routra *192.168.88.1*, zaškrtnuli sme možnosť *BSD Syslog*. V časti *Syslog Facility* sme zvolili možnosť *syslog*. Následne sme konfiguráciu uložili tlačidlom *Apply*.

default	
Name	remote
Type	remote ▼
Remote Address	192.168.88.70
Remote Port	514
Src. Address ▲	192.168.88.1
BSD Syslog	<input checked="" type="checkbox"/>
Syslog Facility	5 (syslog) ▼
Syslog Severity ▲	3 (error) ▼

Obrázok 8.9 Konfigurácia posielania logov na vzdialený server zo zariadenia router, zdroj vlastný

V časti *Rules* sme k 4 existujúcim záznamom vytvorili ďalšie 4 pravidlá pomocou tlačidla *Add New*, a to nasledovne. Ku každému existujúcemu záznamu s určitou témou a akciou sme vytvorili nový záznam, ktorý obsahoval rovnakú tému, ale akciu sme zvolili *remote*, čím sme umožnili posielanie logov na vzdialený server. Všetky zmeny sme uložili.





	▲ Topics	Prefix	Action
- D	critical		remote
- D *	critical		echo
- D	error		remote
- D *	error		memory
- D	info		remote
- D *	info		memory
- D	warning		remote
- D *	warning		memory

Obrázok 8.10 Pravidlá na posielanie logov na vzdialený server na zariadení router, zdroj vlastný

## Esxi

Ešte predtým, ako sme sa pustili do samotnej konfigurácie bolo potrebné zmeniť názov klienta, ktorý bol nastavený na *localhost.localdomain*, čo by nám spôsobovalo problémy. Nový názov zariadeniu *ESXi* sme zvolili *ESXiServer*.

Ihneď potom sme sa prihlásili na zariadenie prostredníctvom *ssh* protokolu, kde sme zadali administrátorské prihlasovacie údaje. Ďalej sme pokračovali príkazmi, ktorými sme nastavili odosielanie logov na vzdialený server, v našom prípade na nástroj AlienVault, kde sme použili protokol *udp* a číslo portu *514*. Rovnako bolo nevyhnutné na tomto zariadení povoliť *syslog* na firewallle.

```
# esxcli system syslog config set --loghost=udp://192.168.88.70:514
# esxcli network firewall ruleset set ruleset set --ruleset-id=syslog --enabled=true
# esxcli network firewall refresh
# esxcli system syslog reload
```

Konfiguráciu sme si overili výpisom, a následne aj testovacou správou, ktoré sme odoslali do nástroja AlienVault. Na testovaciu správu sme dostali odpoveď s výsledkom *success!*.

```
# esxcli system syslog config get
# nc -z 192.168.88.70 514
Connection to 192.168.88.70 514 port [tcp/shell] succeeded!
```

## Sylogogy NAS

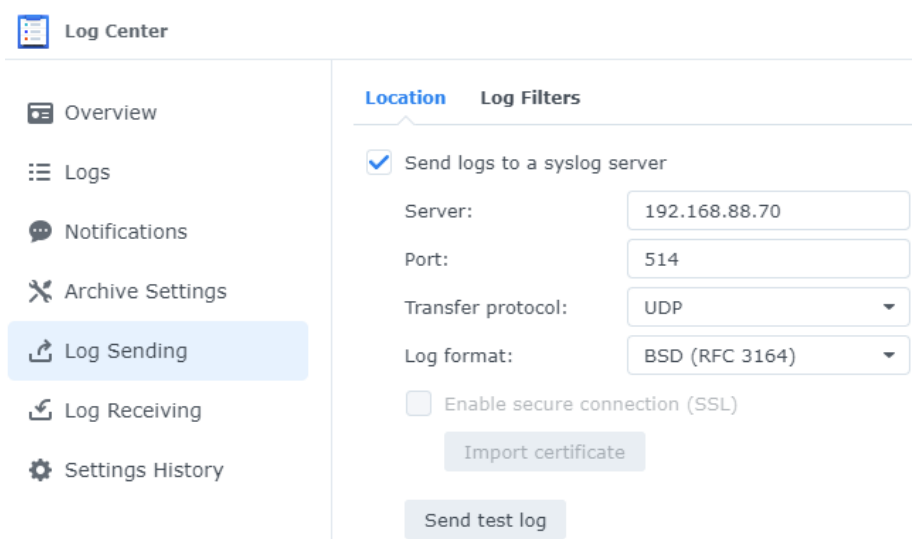


Na konfiguráciu bolo potrebné si nainštalovať prostredníctvom *Package Centra* aplikáciu *Log Center*. Túto aplikáciu sme následne použili na konfiguráciu posielanie logov na vzdialený server, čo bol v našom prípade AlienVault.

V aplikácii *Log Center* sme v navigačnom paneli na ľavej strane zvolili možnosť *Log Sending*, kde sme parametrom priradili nasledovné hodnoty:

- ✓ Povolili sme možnosť *Send logs to a syslog server*
- ✓ Server = *192.168.88.70*
- ✓ Port = *514*
- ✓ Transfer protocol = *UDP*
- ✓ Log format = *BSD (RFC 3164)*

Testovacie odoslanie logov sme vykonali tlačidlom *Send test log* a konfiguráciu sme uložili tlačidlom *Apply* v pravom dolnom rohu obrazovky.



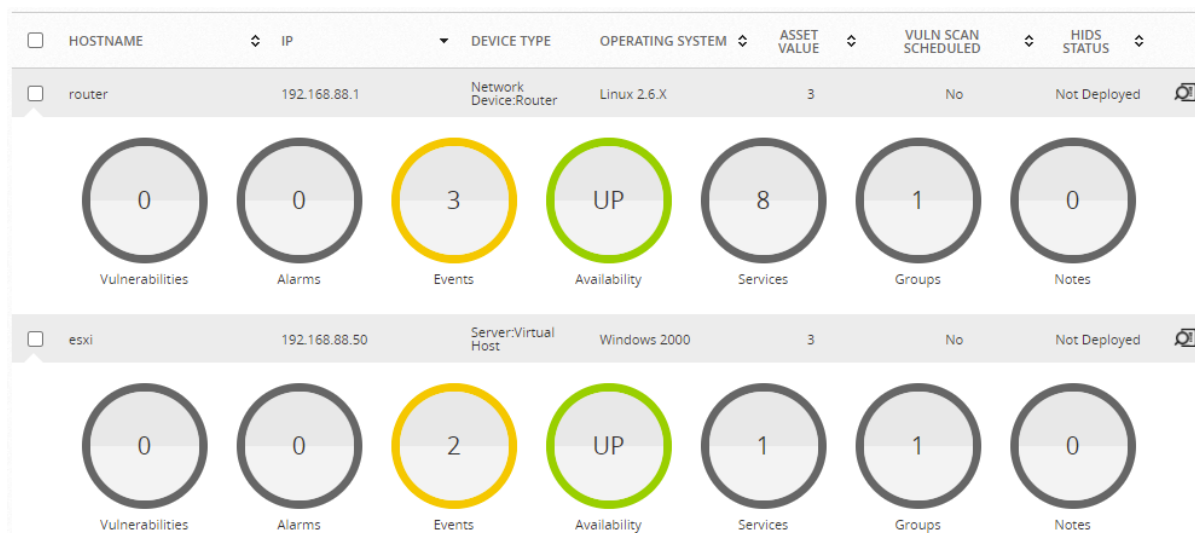
Obrázok 8.11 Konfigurácia posielania vzdialených logov na zariadení Synology NAS, zdroj vlastný

### 8.1.6 Dostupnosť zariadení a služieb

Pri zisťovaní dostupnosti zariadenia sme monitorovali, či bolo zariadenie dostupné v sieti alebo nie. Rovnakým spôsobom sme mali možnosť monitorovať aj dostupnosť jednotlivých portov, čím sme nakonfigurovali monitoring dostupnosti služieb. Druhý menovaný spôsob monitoringu dostupnosti sme využili práve pri zariadení *nas*. Dostupnosť zariadení sme spustili na každom zariadení z testovacej infraštruktúry.

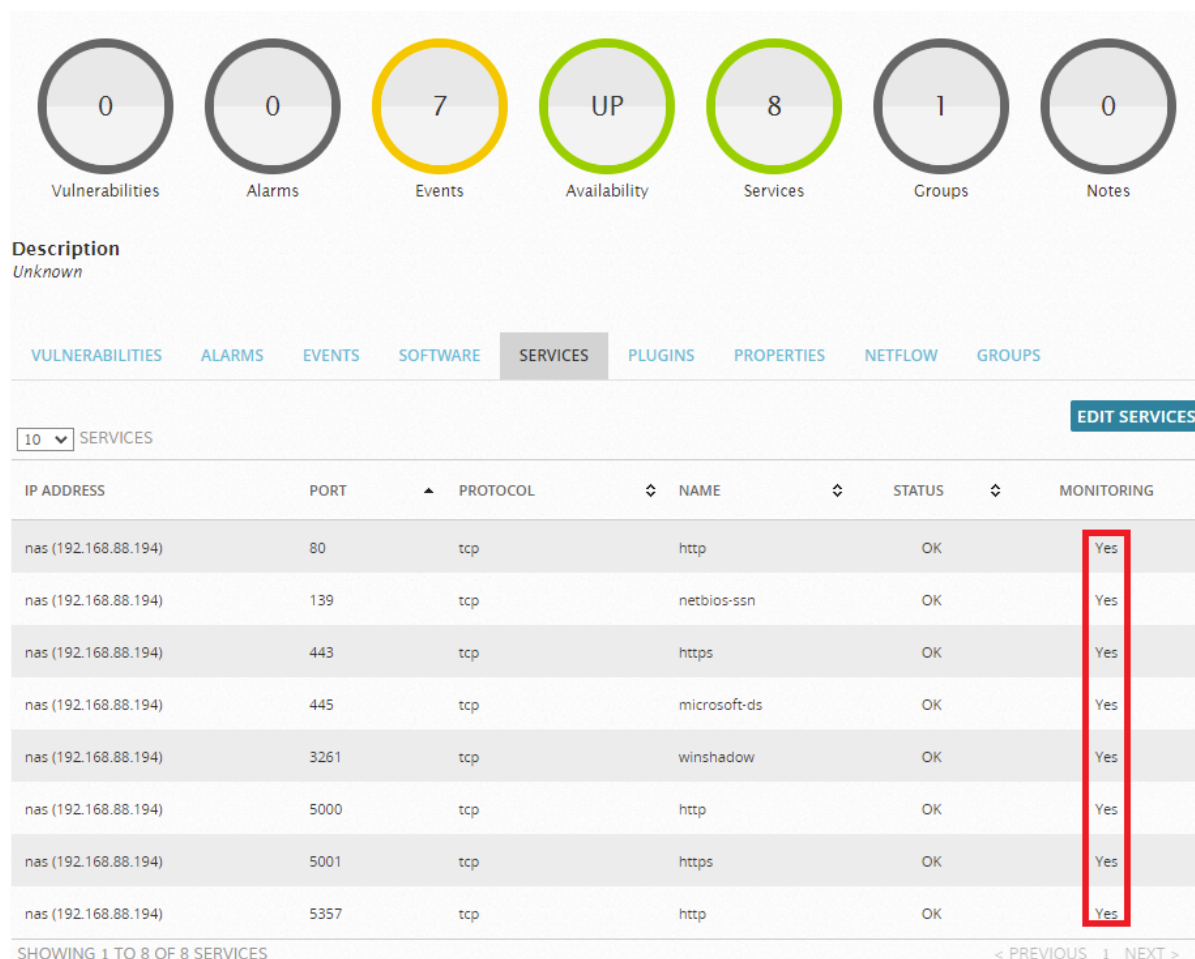
Dostupnosť zariadení sme konfigurovali cez *ENVIRONMENT / ASSET & GROUPS / ASSETS*. Zvolili sme všetky dostupné zariadenia, a tlačidlom *ACTION* a možnosťou *Enable*

*Availability Monitoring* sme spustili monitorovanie dostupnosti zariadení. Dostupné zariadenie boli v stave *UP* a v zelenom krúžku, čo môžeme vidieť aj na obrázku nižšie.



Obrázok 8.12 Monitoring dostupnosti zariadení je v stave *UP*, zdroj vlastný

Dostupnosť služieb zariadenia *nas* sme konfigurovali priamo v detaile zariadenia, v záložke *SERVICES*. Tlačidlom *EDIT SERVICES* sme prešli na konfiguráciu monitoringu služieb. Monitoring služieb sme spustili jednoduchým kliknutím na prepínač pod kategóriou *MONITORING*. Aktuálne monitorované porty boli zobrazené v tabuľke.



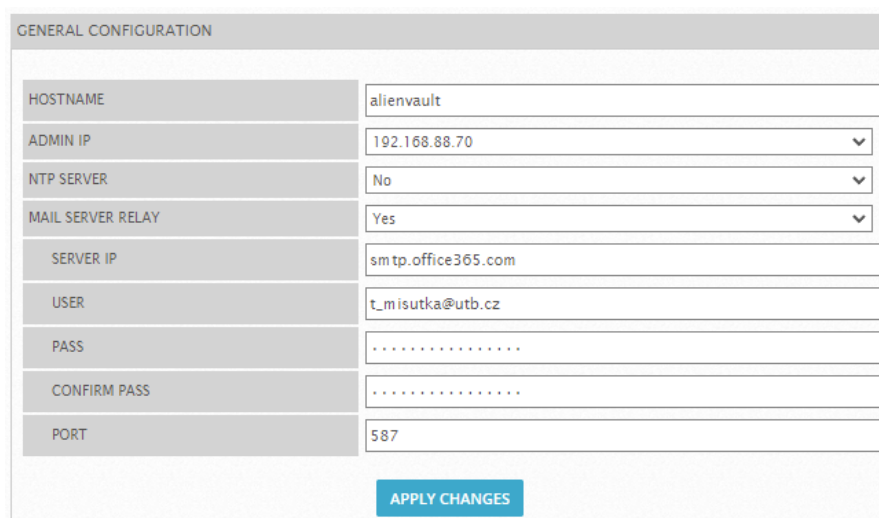
Obrázok 8.13 Monitoring dostupnosti portov na zariadení nas, zdroj vlastný

### 8.1.7 Email Relay

V tejto časti sme nakonfigurovali spôsob, ktorým bolo možné dostávať upozornenia prostredníctvom emailov, ak by sa v sieti objavila neželaná činnosť a vznikol alarm. Ešte predtým, ako sme definovali podmienky, v ktorých sme definovali prípady, kedy sa emaily budú posieľať, bolo nutné nakonfigurovať *Email Relay*.

V hlavnom menu sme zvolili *CONFIGURATION / DEPLOYMENT* a klikli sme na možnosť pre zobrazenie detailov o systéme. V nasledujúcom kroku sme klikli na možnosť *GENERAL CONFIGURATION* a možnosť *MAIL SERVER RELAY* sme zmenili na *Yes*.

Do časti *SERVER IP* sme zadali *smtp.office365.com*, do časti *USER* sme zadali našu emailovú adresu *t\_misutka@utb.cz* a na záver sme zadali 2-krát heslo a port sme zvolili 587. Konfiguráciu sme uložili tlačidlom *APPLY CHANGES*.



The screenshot shows the 'GENERAL CONFIGURATION' section of the AlienVault interface. It contains a table of configuration fields:

GENERAL CONFIGURATION	
HOSTNAME	alienvault
ADMIN IP	192.168.88.70
NTP SERVER	No
MAIL SERVER RELAY	Yes
SERVER IP	smtp.office365.com
USER	t_misutka@utb.cz
PASS	.....
CONFIRM PASS	.....
PORT	587

At the bottom right of the configuration area is a blue button labeled 'APPLY CHANGES'.

Obrázok 8.14 Konfigurácia Email Relay, zdroj vlastný

### Zmena emailu odosielateľa

Pre prehľadnosť sme zmenili aj emailovú adresu odosielateľa, aby v prípade prijatia emailu z nástroja AlienVault bolo okamžite jasné a zrozumiteľné, odkiaľ a prečo tento email prišiel.

Prešli sme v časti *CONFIGURATION / ADMINISTRATION* do kategórie *MAIN* a tam sme vybrali podkategóriu *OSSIM FRAMEWORK*.

Tam sme upravili parameter *Sender's Email Address for notifications* na hodnotu *t\_misutka@utb.cz*. Konfiguráciu sme uložili tlačidlom *UPDATE CONFIGURATION*.

### Príprava akcie

Potrebné bolo nakonfigurovať aj reakciu na udalosti, pri ktorých bol vygenerovaný alarm a chceli sme prostredníctvom emailu byť o tom informovaní.

Túto akciu sme definovali v nástroji pod položkou *CONFIGURATION / THREAT INTELLIGENCE*, kde sme vybrali záložku *ACTIONS*. Pridali sme novú akciu, ktorej sme definovali názov *Notify\_via\_email*, typ akcie *Send an email message*. Ďalej zdrojovú, cieľovú emailovú adresu a obsah emailu, v ktorom sme definovali nevyhnutné informácie o vzniknutej udalosti, čo s prehľadnosťou popis problému pre administrátora. Dôležité bolo použitie rovnakej zdrojovej emailovej adresy, ako bola konfigurovaná v časti *Email Relay*. Obsah správy môže byť upravený podľa vôle administrátora. Konfiguráciu sme uložili tlačidlom *SAVE*.

You can use the following keywords within the fields (Description) which will be substituted by its matching value upon action execution:

- DATE
- PLUGIN\_ID
- PLUGIN\_SID
- RISK
- PRIORITY
- RELIABILITY
- SRC\_IP\_HOSTNAME
- DST\_IP\_HOSTNAME
- SRC\_IP
- DST\_IP
- SRC\_PORT
- DST\_PORT
- PROTOCOL
- SENSOR
- BACKLOG\_ID
- EVENT\_ID
- PLUGIN\_NAME
- SID\_NAME
- USERNAME
- PASSWORD
- FILENAME
- USERDATA1
- USERDATA2
- USERDATA3
- USERDATA4
- USERDATA5
- USERDATA6
- USERDATA7
- USERDATA8
- USERDATA9

NAME *	Notify_via_email
DESCRIPTION *	Action to notify administrator via email
TYPE *	Send an email message
CONDITION	<input type="radio"/> Any <input checked="" type="radio"/> Only if it is an alarm <input type="radio"/> Define logical condition
FROM: *	t_misutka@utb.cz
TO: *	tomasmisutka@gmail.com
SUBJECT: *	Event appears
MESSAGE: *	High priority event appears to monitoring asset Date: DATE, priority: PRIORITY, Risk: RISK Source IP: SRC_IP : SRC_PORT Destin: IP: DST_IP : DST_PORT Reliability: RELIABILITY
APPEND EMAIL WITH ALL EVENT FIELDS:	<input type="checkbox"/>

SAVE

Obrázok 8.15 Konfigurácia akcie, ktorá vyvolá odoslanie emailu, zdroj vlastný

### Posielanie emailov pri výskyte alarmu

Touto konfiguráciou sme zabezpečili, aby sa pri výskyte alarmu vytvoril tiket a odoslala notifikácia emailom. Pripomienku alarmu vzniku alarmu v prípade jeho nevyriešenia sme zvolili v časovom rozmedzí 7 dní. V hlavnej navigácii sme zvolili kategóriu *CONFIGURAITON / ADMINISTRATION* a v nej záložku *MAIN*.

Vybrali sme možnosť *TICKETS* a parametre sme vyplnili nasledovne:

- ✓ Open Tickets for new alarms automatically = *Yes*
- ✓ Automatic ticket generation default in=charge user/entity = *Admin*
- ✓ Send email notification = *Yes*
- ✓ Open tickets reminder = *7*

Konfiguráciu sme uložili tlačidlom *UPDATE CONFIGURATION*.

### Podmienky na odoslanie emailu

Podozrivé udalosti týkajúce sa len určitých, prípadne aj všetkých zariadení, ktoré by mohli vygenerovať alarm a chceli sme byť o ňom informovaní emailom, bolo nutné definovať podmienky v časti *CONFIGURATION / THREAT INTELLIGENCE* záložka *POLICY*. Nový

záznam sme pridali do časti *Default policy group*, kde pomocou tlačidla *New* sme pridali zaznamenávanie politiky a udalostí nášho najkritickejšieho zariadenia *nas*.

V *POLICY CONDITIONS* sme ako zdrojovú adresu vybrali *ANY*, čím sme definovali akúkoľvek zdrojovú IP adresu. Ako cieľovú sme zvolili náš, už definovaný asset s názvom *nas*. V časti *REPUTATION* sme vybrali aktivitu *Malicious host* s prioritou  $> 4$  a spoľahlivosť  $> 7$  v smere *Destination*. Tieto parametre sme pridali pomocou tlačidla *ADD NEW*.

V časti *POLICY CONSEQUENCES* sme z dostupných akcií presunuli našu akciu s názvom *Notify\_via\_email* medzi aktívne časti. Názov politiky sme zvolili *nas\_policy* a záznam sme pridali tlačidlom *UPDATE POLICY*.

Obrázok 8.16 Konfigurácia politiky pre kritické zariadenie Synology NAS, zdroj vlastný

Ďalší záznam sme pridali v časti s názvom *Policies for events generated in server* rovnako pomocou tlačidla *New*.

V časti *POLICY CONDITION* sme zaškrtnuli možnosť *Directive events*, čím sme povolili sledovanie politiky každého typu udalosti. Potom sme klikli v tabuľke *CONSEQUENCES* na záznam pod stĺpcom *ACTION*, kde sme presunuli záznam z dostupných akcií do aktívnych. Akcia mala názov *Notify\_via\_email*. Názov politiky sme zvolili *default\_server\_policy* a politiku sme pridali tlačidlom *UPDATE POLICY*.

Na záver bolo nutné zmeny aplikovať kliknutím na jedno z dvoch červených tlačidiel s názvom *Reload Policies*, čím sa aktualizovali vytvorené politiky.

Policy Rule Name: \* default\_server\_policy ✓ Enable: \* ☒ Yes ☐ No Policy Group: \* Policies generated in: alienvault ▼

**CONDITIONS**

EVENT TYPES ✓  
DS Groups  
Directive events

**ACTIONS** ✓  
Notify\_via\_email

**CONSEQUENCES**

SIEM ✓  
SIEM (Yes)  
Set Event Priority: Do not change  
Risk Assessment: Yes  
Logical Correlation: Yes  
Cross-correlation: Yes  
SQL Storage: Yes

**FORWARDING** ✓  
Forward Events (No)

► POLICY CONDITIONS  
► POLICY CONSEQUENCES

ADD MORE CONDITIONS

**ACTIONS** INSERT NEW ACTION?

ACTIVE ACTIONS	AVAILABLE ACTIONS
1 items selected Remove all	Add all
Notify_via_email	

UPDATE POLICY

Obrázok 8.17 Konfigurácia politiky na serveri, ktorá zabezpečí odoslanie emailu, zdroj vlastný

### 8.1.8 Pravidelné prehľadávanie siete

Touto konfiguráciou sme zabezpečili pravidelné skenovanie nových zariadení, ich OS a služieb zo zariadení. Tento proces je známy aj z anglického spojenia „*asset discovery scan*“. Tento krok umožňuje identifikáciu nových vírusov a zraniteľností.

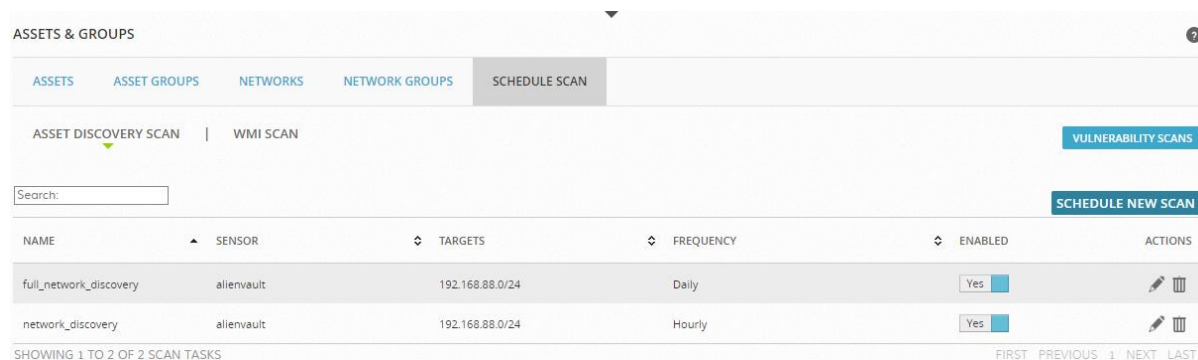
Do konfigurácie sme sa dostali prostredníctvom hlavného panelu, záložka *ENVIRONMENT* a vybrali sme podkategóriu *ASSETS AND GROUPS*, záložku *SCHEDULE SCAN*. V časti *ASSET DISCOVERY SCAN* sme zvolili možnosť *SCHEDULE SCAN* a pomocou tlačidla *SCHEDULE NEW SCAN* sme pripravili pravidelné vyhľadávacie skenovanie zariadení. Pripravili sme 2 typy skenovania.

Prvým bolo skenovanie na hodinovej báze, a to zisťovaním nových zariadení a základných služieb v celej testovacej infraštruktúre prostredníctvom rýchleho skenovania. Tomuto vyhľadávaniu sme prideliť názov *network\_discovery*, kde sme ako cieľ pridali našu celú testovaciu infraštruktúru *192.168.88.0/24*.

Druhým skenovaním bolo kompletne prehľadávanie siete našej testovacej infraštruktúry. Pravidelnosť sme nastavili na 1 deň a typ skenovania sme zvolili *Full Scan*, čo je hlboké skenovanie zariadení. Názov skenovanie sme zvolili *full\_network\_discovery*, kde sme ako cieľ



tiež pridali rozsah našej testovacej infraštruktúry *192.168.88.0/24*, ako to bolo aj v prípade konfigurácie prvého skenovania.



Obrázok 8.18 Konfigurácia pravidelného prehľadávania testovacej infraštruktúry, zdroj vlastný

### 8.1.9 Hľadanie zraniteľností v sieti

Skenovanie celej siete alebo určitých zariadení či skupín nám umožňuje hľadať ich aktuálne zraniteľnosti. Vďaka eliminácii týchto nedostatkov ich nebude môcť hacker v našej sieti využiť, čo mu značne skomplikuje ceste k úspechu. Typ a dĺžka skenovania by mala byť dobre zvážená a vhodne nakonfigurovaná, aby sme predišli problémom s nedostupnosťou zariadení a služieb spôsobené skenovaním počas pracovných hodín. Typickým príkladom je, že nie je vhodné spustiť úplné hlboké skenovanie zraniteľností v sieti počas noci na zariadeniach, ktoré pripadajú zamestnancom a hrozí riziko ich nedostupnosti. Naopak by mohol nastať prípad, že by mohli byť potrebné služby nedostupné, v prípade použitia deštruktívneho skenovania počas pracovných hodín dňa.

Po dôkladnom zvážení týchto skutočností sme odporučili vykonávať skenovanie sieťových zariadení alebo serverov v nočných hodinách s úplným hlbokým a deštruktívnym prehľadávaním, ktoré je časovo dosť náročné. Dĺžka skenovania závisí od počtu zariadení v sieti a rovnako aj od typu skenovania. Frekvenciu skenovania sme však ponechali na zodpovednosť administrátorovi externej spoločnosti. Deštruktívne skenovanie sme odporučili vykonávať iba v čase a sieti, ktorú dobre poznáme a eliminujeme riziko nedostupnosti služieb.

V našej testovacej infraštruktúre sme spustili dva typy skenovania. 1. bolo úplné hlboké skenovanie počas dňa a 2. deštruktívne ultimate hlboké skenovanie všetkých zariadení z testovacej infraštruktúry počas noci, tak ako to bolo aj nami odporúčanom skenovaním.

Skenovanie bolo možné naplánovať v pravidelných intervaloch na dennej, týždennej či mesačnej báze, okamžite alebo 1-krát v konkrétnom čase a dni. To dáva administrátorovi úplnú flexibilitu pri plánovaní skenovania.



### Full and very deep

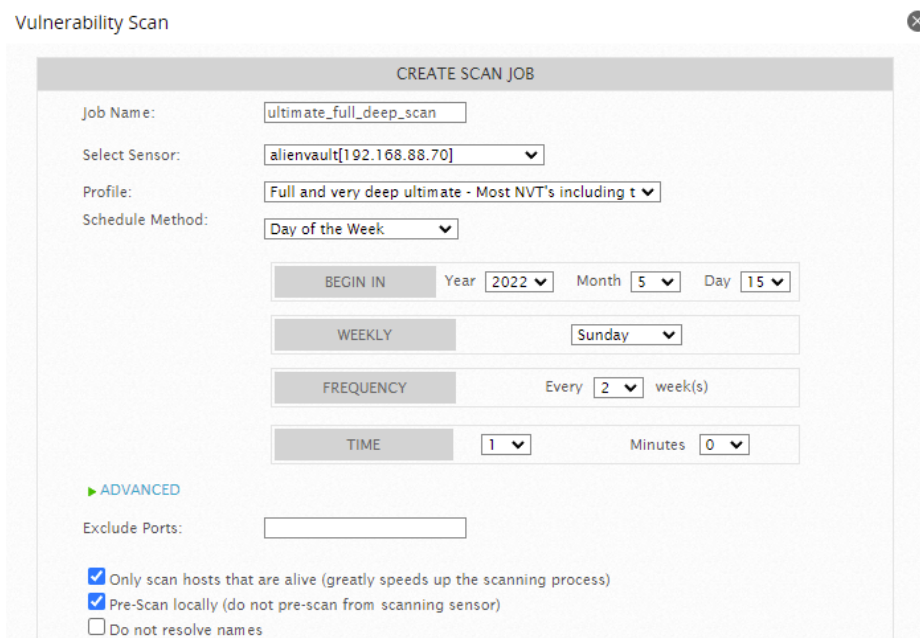
Do konfigurácie sme prešli cez hlavné menu *ENVIRONMENT / VULNERABILITIES*, kde sme zvolili podkategóriu *SCAN JOB* a tam sme pomocou tlačidla *NEW SCAN JOB* mohli pridať skenovanie zraniteľností v sieti.

Názov 1. skenovania sme zvolili *full\_very\_deep\_scan* a profil *Full and very deep*, ktorý obsahoval väčšinu NVT testov. Čas skenovania sme nechali spustiť ihneď po dokončení konfigurácie a za cieľ sme zvolili rozsah našej testovacej infraštruktúry *192.168.88.0/24*. Dôležité bolo tiež spomenúť, že tento typ skenovania je vhodný aj do nočných, aj do pracovných hodín.

### Full and very deep ultimate

Druhým bolo úplne a veľmi hlboké ultimátne skenovanie serverov, sieťových a kritických zariadení našej testovacej infraštruktúry.

Vzhľadom na to, že toto skenovanie bolo vyhradené len pre niektoré zariadenia, konfiguráciu sme spravili iným spôsobom ako tú predchádzajúcu. Prešli sme do časti *ENVIRONMENT / ASSETS & GROUPS* a vybrali sme záložku *ASSET GROUPS*. Tam sme pomocou checkbox-u vybrali skupinu *Servers* a *Network devices*. Následne sme tlačidlom *ACTIONS / Run vulnerability scan* mohli nakonfigurovať a naplánovať 2. skenovanie. Toto skenovanie sme pomenovali *ultimate\_very\_deep\_scan* s profilom *Full and very deep ultimate*, čo predstavovalo úplné, hlboké, kompletné a deštruktívne skenovanie sieťových a kritických zariadení. Počas tohto skenovania mohli byť niektoré služby nedostupné, preto sme zvolili skenovanie počas nočných hodín. Skenovanie sme nastavili v pravidelných intervaloch raz za 2 týždne vždy v nedeľu od 01:00 ráno. Konfiguráciu skenovania sme uložili tlačidlom *SAVE*.



Vulnerability Scan

CREATE SCAN JOB

Job Name:

Select Sensor:

Profile:

Schedule Method:

BEGIN IN Year  Month  Day

WEEKLY

FREQUENCY Every  week(s)

TIME  Minutes

▶ ADVANCED

Exclude Ports:

☒ Only scan hosts that are alive (greatly speeds up the scanning process)

☒ Pre-Scan locally (do not pre-scan from scanning sensor)

☐ Do not resolve names

Obrázok 8.19 Konfigurácia pravidelného skenovania kritických zariadení, zdroj vlastný

### 8.1.10 NetFlow

*NetFlow* je protokol, ktorý bol vytvorený spoločnosťou *CISCO*, a ten nám umožňuje aktívne monitorovať sieťovú prevádzku smerom dnu a von zo zariadenia. Táto prevádzka môže byť ďalej použitá pri analýze sieťovej prevádzky s hľadaním anomálií.

Toto riešenie sme implementovali iba na zariadení mikrotik *router*, pretože switch, ktorý sa nachádzal v našej testovacej infraštruktúre neobsahoval konfigurovať túto možnosť. Z praktického hľadiska to pre nás znamenalo, že sme neboli schopní ďalej zaznamenať v lokálnej sieti útok prostredníctvom skenovania portov v sieti, práve kvôli nedostatočnému výkonu switchu v našej sieti.

Implementácia pozostáva zo zachytenej prevádzky na zariadení *router* a posielaní tejto prevádzky do nástroja *AlienVault*. Zároveň v tomto nástroji bolo potrebné pripraviť nový senzor, na ktorom bude túto prevádzku z routra prijímať.

### UPOZORNENIE

V nástroji *AlienVault*, ktorý sme doteraz používali vo verzií 8.5.8 bola počas implementácie tejto funkcionality objavená chyba v softvéri, ktorý nám neumožňoval dokončiť konfiguráciu senzoru. Konkrétne nám chýbala možnosť nastaviť port, na ktorom by sa prevádzka z routra mohla prijímať.

Preto sme sa pokúsili o aktualizáciu z nástroja z verzie 8.5.8 na verziu 8.5.11, čo však neprebehlo úspešne a spôsobilo to zničenie celého nástroja. Preto sme vykonali novú čistú inštaláciu nástroja vo verzií 8.5.11, ktorá prebehla úplne v poriadku a možnosť konfigurovať NetFlow bola opäť dostupná. Celú doterajšiu konfiguráciu sme však museli zopakovať, čo nás mierne spomalilo počas implementácie riešenia.

## Router

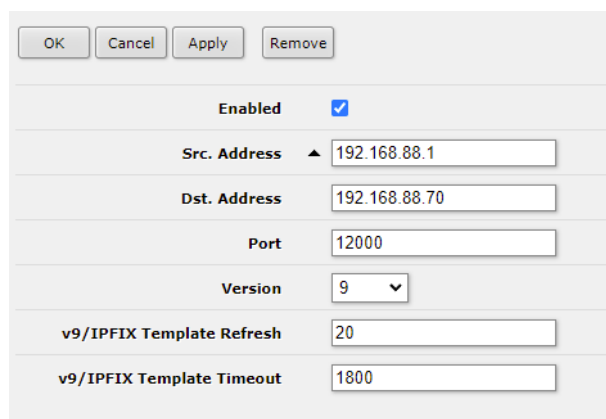
Do zariadenia sme sa prihlásili administrátorskými právami cez prehliadač a prepli sme si interaktívne zobrazenie *WebFig*. Ďalej sme v navigačnom paneli zvolili kategóriu IP a vybrali sme možnosť *Traffic Flow*.

Tu bolo potrebné povoliť zaznamenávanie sieťovej prevádzky povolením *checkboxu*, kde sme vybrali zaznamenávanie na všetkých rozhraniach, cache sme vybrali na 256k a zvyšnú konfiguráciu sme nechali v predvolenom stave. Tá obsahovala zbierať netflow celej prevádzky. Konfiguráciu sme uložili tlačidlom v hornej časti *Apply*.

Enabled	<input checked="" type="checkbox"/>
Interfaces	<div>▼ all ▼ ▲</div>
Cache Entries	<div>256k ▼</div>
Active Flow Timeout	<div>00:30:00</div>
Inactive Flow Timeout	<div>00:00:15</div>
Packet Sampling	<input type="checkbox"/>

Obrázok 8.20 Povolenie netflow na zariadení mikrotik router, zdroj vlastný

V ďalšom kroku sme v možnosti konfigurácie prešli tlačidlom *Targets* na konfiguráciu, kam sa má zachytená sieťová prevádzka zaslať. Tam sa zatiaľ nenachádzal žiadny záznam, nový sme pridali tlačidlom *Add New*. Nutnosťou bolo túto možnosť povoliť, vyplniť zdrojovú IP adresu 192.168.88.1 a cieľovú IP adresu 192.168.88.70. Port sme použili podľa odporúčaní z dokumentácie 12000, verziu sme zvolili 9 a zvyšné hodnoty sme nechali v predvolenom stave. Konfiguráciu sme potvrdili a uložili tlačidlom *Apply*.



OK Cancel Apply Remove	
Enabled	<input checked="" type="checkbox"/>
Src. Address	192.168.88.1
Dst. Address	192.168.88.70
Port	12000
Version	9
v9/IPFIX Template Refresh	20
v9/IPFIX Template Timeout	1800

Obrázok 8.21 Konfigurácia odoslania netflow zachytený na routri, zdroj vlastný

## AlienVault

V nástroji sme prešli do konfigurácie skenovacích senzorov cez hlavné menu *CONFIGURATION / DEPLOYMENT*, kde sme prešli na záložku *SENSORS*. Tam sa nachádzal iba jeden záznam a to bol aktuálne používaný senzor nástroja na IP adrese *192.168.88.70*.

V možnostiach sme pridali pomocou tlačidla *NEW* nový senzor, ktorý sme nazvali *routerSenzor*, ktorému sme nechali predvolenú prioritu a časovú zónu, a pridali sme IP adresu routera *192.168.88.1*. Senzor sme pridali a uložili tlačidlom *SAVE*.

Po pridaní senzoru sa nám zobrazil v tabuľke nový záznam, čo bol náš novovytvorený senzor, ktorý sme označili a stlačili tlačidlo *MODIFY*. Tam sa nám zobrazila možnosť konfigurácie *FLOWS*, ktorá vo verzií 8.5.8 nebola dostupná.


Port sme zvolili na *12000*, typ sme zvolili na netflow, farbu zelenú a konfiguráciu senzoru sme dokončili tlačidlom *RUN AND CONFIGURE*.

Values marked with (\*) are mandatory

NAME *	routerSenzor
IP *	192.168.88.1
PRIORITY	5
TIMEZONE	UTC
DESCRIPTION	mikrotik router senzor to collect netflow data

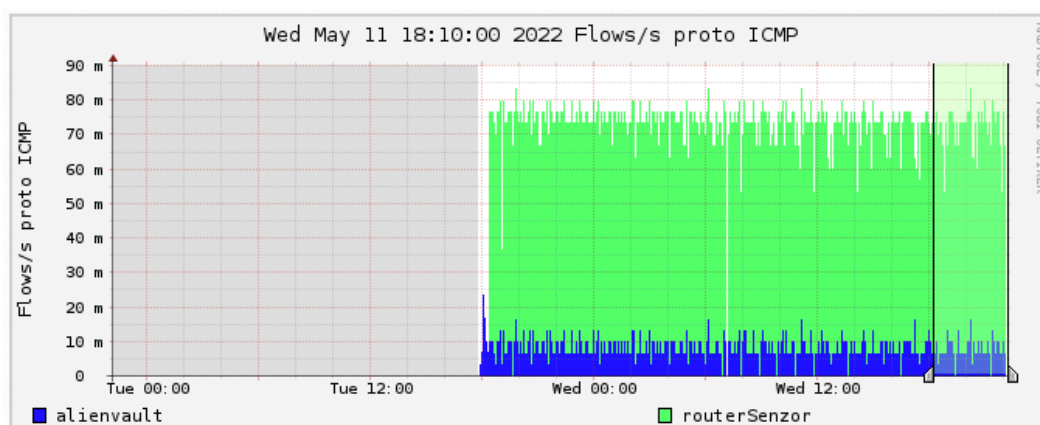
SAVE

FLows

NETFLOW COLLECTION CONFIGURATION		ACTION
Port:	12000	Color: 
Type:	netflow	Status: <b>is running</b>
		<a href="#">STOP AND REMOVE</a>
		<a href="#">Configuration help ?</a>

Obrázok 8.22 Konfigurácia senzoru na prijímanie netflow z routra, zdroj vlastný

Po uložení konfigurácie sme prešli do sekcie *ENVIRONMENT / NETFLOW*, kde sa nám začali pomaly začala objavovať sieťová prevádzka, ktorú sme obdržali z routra, viditeľná bola zelenou farbou. Na ďalšom obrázku sme zobrazili TOP 10 zdrojových zariadení, ktoré boli zachytené prostredníctvom *netflow*.



Obrázok 8.23 Prijímanie sieťovej prevádzky z routra cez netflow, zdroj vlastný

FLOWS INFO									
DATE FLOW SEEN GMT+2:00	DURATION	PROTO	IP ADDR	FLOWS(%)	PACKETS(%)	BYTES(%)	PPS	BPS	BPP
2022-05-21 16:10:48.569	7694.328	any	esxi	761(2.5)	212634(36.1)	48.5M(37.5)	27	50408	228
2022-05-21 16:10:48.569	7712.301	any	alienvault	10214(33.2)	243705(41.3)	31.4M(24.3)	31	32564	128
2022-05-21 16:14:22.800	7519.720	any	[REDACTED]	8539(27.7)	37882(6.4)	27.4M(21.2)	5	29131	722
2022-05-21 16:13:34.041	7535.899	any	Host-192-168-89-202	2928(9.5)	30019(5.1)	6.5M(5.0)	3	6914	216
2022-05-21 16:15:16.090	7433.850	any	[REDACTED]	100(0.3)	21709(3.7)	5.9M(4.6)	2	6346	271
2022-05-21 15:58:12.900	8489.610	any	router	2150(7.0)	12636(2.1)	4.3M(3.4)	1	4089	343
2022-05-21 15:47:32.200	9030.310	any	127.0.0.1	48(0.2)	11112(1.9)	2.1M(1.6)	1	1870	190
2022-05-21 16:13:03.060	7553.490	any	ubuntupc	381(1.2)	4051(0.7)	691630(0.5)	0	732	170
2022-05-21 16:14:07.825	7527.135	any	zabbix	1999(6.5)	4000(0.7)	598950(0.5)	0	636	149
2022-05-21 16:13:12.914	7587.596	any	windows	887(2.9)	4588(0.8)	448057(0.3)	0	472	97
SUMMARY total flows: 30789 TOTAL BYTES 129160789 TOTAL PACKETS 589784 AVG BPS 113170 AVG PPS 64 AVG BPP 218									
TIME WINDOW 2022-05-21 15:47:32 - 2022-05-21 18:19:42									
TOTAL FLOWS PROCESSED 30789 BLOCKS SKIPPED 0 BYTES READ 1893584									
SYS 0.007s flows/second: 4297738.7 WALL 0.005s flows/second: 5962238.6									

Obrázok 8.24 Top 10 zdrojových zariadení zachytených prostredníctvom netflow, zdroj vlastný

### 8.1.11 Konfigurácia direktívy proti útoku skenovaním portov

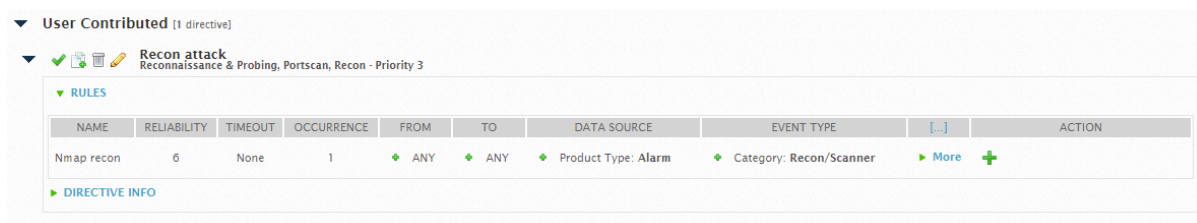
V jednej z požiadaviek bol stanovený záujem dostať notifikáciu o útoku skenovaní portov v sieti. Na túto funkcionality sme konfigurovali tzv. direktívu, v ktorej sme definovali pravidlá s prioritou a spoľahlivosťou, ktoré zabezpečia pri zachytení takéhoto útoku vytvorenie alarmu.

Do konfigurácie sme prešli z hlavného menu *CONFIGURATION / THREAT INTELLIGENCE* a tam sme vybrali záložku *DIRECTIVES* a tlačidlom *New Directive* sme začali pridávanie.

Názov sme zvolili *Recon attack* s predvolenou prioritou 3. V časti *TAXONOMY* sme vyplnili nasledovné hodnoty:

- ✓ Intent = *Reconnaissance & Probing*
- ✓ Strategy = *Portscan*
- ✓ Method = *Recon*

Tlačidlom *NEXT* sme prešli na ďalšiu stránku konfigurácie, kde sme zvolili názov pravidla *Nmap recon* a pokračovali sme tlačidlom *NEXT*. Pri výbere typu udalosti sme vybrali *Taxonomy* a vyznačili sme si typ produktu *Alarm*. Na ďalšej stránke sme vyplnili kategóriu *Recon* a podkategóriu *Scanner* a pokračovali tlačidlom *NEXT*. V sieťovej časti sme nepridávali žiadny záznam, pretože sme chceli zachytiť útok skenovaním portov z každého zdroju na každý cieľ bez výnimky, čiže konfiguráciu tejto časti sme vynechali, čo nastavilo predvolené *ANY ANY* ako zdrojovú a cieľovú adresu. V poslednej časti sme vybrali hodnotu 6 vyjadrujúcu spoľahlivosť a konfiguráciu sme dokončili tlačidlom *FINISH*. V poslednom zostávajúcom kroku bolo ešte potrebné načítať direktívy, to sme spravili tlačidlom *Reload Directives*.



Obrázok 8.25 Konfigurácia direktívy na vytvorenie alarmu pri útoku skenovaním portov, zdroj vlastný

## 8.2 Zabbix

Zabbix je nástroj, pomocou ktorého sme monitorovali dostupnosť a vytáženosť zariadení a služieb z testovacej infraštruktúry. Pri konfigurácii monitoringu zariadení sme využili protokol *SNMP*, prevažne verzie 3. Niektoré zariadenia z testovacej infraštruktúry boli na bežnej používateľskej úrovni bez možnosti pokročilej konfigurácie, kde verzia protokolu *SNMPv3* nebola dostupná. To viedlo ku konfigurácii pomocou nižšej, ale nie odporúčanej verzie 2.

Nastaviť protokol *SNMP* bolo potrebné vždy na oboch stranách, to znamená konfigurácia na strane nástroja Zabbix, aj na strane zariadenia z testovacej infraštruktúry s rovnakými autentifikačnými parametrami a komunitou.

V úvode bolo potrebné pripraviť všetky šablóny, ktoré nie sú vstavané v nástroji zabbix a boli použité pri monitoringu zariadení. Následne bolo nutné na zariadeniach konfigurovať protokol *SNMP* a pred koncom konfigurácie sme nastavili informovanie administrátora prostredníctvom emailov o nedostupnosti zariadenia *Synology NAS*. V samotnom závere sme museli analyzovať *SNMP* OID na tlačiarňu na to, aby sme mohli vytvoriť 2 nové položky, ktoré sme chceli monitorovať. Následne na 1 z položiek sme vytvorili trigger, ktorý sledoval aktuálny stav papiera v tlačiarňu a v prípade jeho nedostatku bol zhlásený problém.

### 8.2.1 Import šablón

V tejto časti sme popísali spôsob, akým bolo potrebné importovať šablóny do nástroja zabbix, ktoré neboli dostupné po inštalácii a zároveň boli potrebné na monitorovanie zariadení v našej testovacej infraštruktúre. Importovali sme spolu 3 šablóny, ktoré boli určené na zariadenia *Synology NAS*, *Wmware ESXi* a tlačiareň *Xerox*. Tieto šablóny sme stiahli na lokálny disk vlastného počítača, odkiaľ sme ich následne importovali do nástroja.

V hlavnom navigačnom paneli sme zvolili možnosť *Configuration / Templates* a v pravom hornom hornu sme klikli na tlačidlo *Import*. V časti *Import file* sme vybrali šablónu a tlačidlom *Import* sme ju nahrali do nástroja.

### 8.2.2 MIKROTIK router

Na monitoring tohto zariadenie bolo možné použiť *SNMPv1*, *SNMPv2* aj *SNMPv3*. Vzhľadom na skutočnosť, že prvé 2 verzie nie sú úplne bezpečné, monitoring sme zabezpečili pomocou *SNMPv3*, ktorá umožňuje monitoring spojený s autentifikáciou.

#### Router

Do routra sme sa prihlásili administrátorskými právami cez webový prehliadač a prepli sa do interaktívneho rozhrania *WebFig*. Tam prešli do kategórie *IP / SNMP*. Najskôr bolo potrebné upraviť konfiguráciu komunity. Kliknutím na existujúci záznam *public* sme upravili konfiguráciu. Údaje o komunite sme upravili nasledovne:

- ✓ Povolili sme *Enabled*
- ✓ Name = *router-snmp*
- ✓ Address = *192.168.88.60/32*
- ✓ Security = *private*
- ✓ Authentication, Encryption Protocol = *SHA1, AES*
- ✓ Authentication, Encryption Password = *RouterSnmp., routerSnmp@AES1234*

Údaje sme uložili tlačidlom *Apply* a zmeny potvrdili tlačidlom *OK*, a vrátili sme sa do konfigurácie *SNMP*. Implementáciou sme pokračovali nasledujúcimi údajmi:

- ✓ Povolili sme možnosť *Enabled*
- ✓ Contact Info = *t\_misutka@utb.cz*
- ✓ Location = *testing infrastructure*
- ✓ Trap Target = *192.168.88.60*
- ✓ Trap Community = *router-snmp*
- ✓ Trap version = *3*
- ✓ Trap Generators = *interfaces, start-trap, temp-exception*
- ✓ Trap Interfaces = *all*
- ✓ Src. Address = *192.168.88.1*



Obrázok 8.26 Konfigurácia SNMP na zariadení mikrotik router, zdroj vlastný

Konfiguráciu sme uložili kliknutím na tlačidlo *Apply*.

## Zabbix

V nástroji Zabbix sme prešli v menu do časti *Monitoring / Hosts, Create host*. Údaje o zariadení router sme vyplnili nasledovne:

- ✓ Host name = *Mikrotik router*
- ✓ Templates = *Mikrotik SNMP*
- ✓ Groups = *Network devices*
- ✓ SNMP IP address = *192.168.88.1*
- ✓ SNMP version = *SNMPv3*
- ✓ Security level = *authPriv*
- ✓ Security name = *{ \$SECURITY\_NAME }*
- ✓ Authentication protokol = *SHA1*
- ✓ Authentication passphrase = *{ \$AUTH\_PASS }*
- ✓ Privacy protocol = *AES128*
- ✓ Privacy passphrase = *{ \$PRIVACY\_PASS }*

V záložke *Macros* sme ku každému makru zo záložky *Host* priradili hodnoty nasledovne:

- ✓ *{ \$AUTH\_PASS }* = *RouterSnmp*.
- ✓ *{ \$PRIVACY\_PASS }* = *routerSnmp@AES1234*

- ✓  $\{\$SECURITY\_NAME\} = router-snmp$
- ✓  $\{\$SNMP\_COMMUNITY\} = router-snmp$

Zariadenie mikrotik router sme pridali tlačidlom *Add*. To sa nám pridalo do tabuľky, a po krátkej chvíli sa objavila aj dostupnosť zariadenia prostredníctvom protokolu *SNMP* pomocou zeleného indikátora *SNMP*.

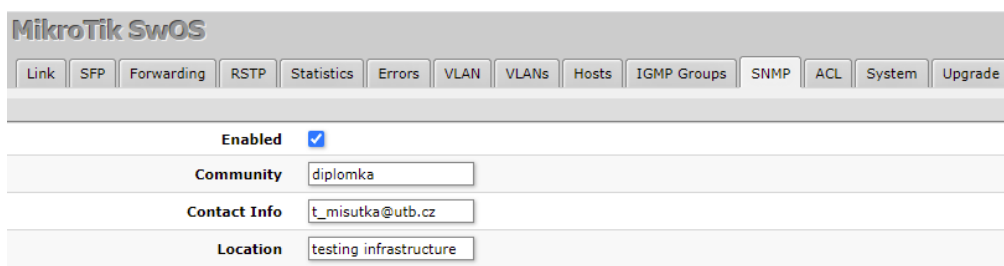
### 8.2.3 MIKROTIK switch

Výkon a možnosti tohto zariadenia neboli na pokročilej úrovni, čo sa prejavilo aj na protokole *SNMP*. Verzia 3 totiž nebola dostupná, a preto sme boli nútení použiť tento protokol s nižšou, ale menej bezpečnou verziou.

#### Switch

Do switchu sme sa prihlásili administrátorskými právami a v hlavnom menu sme zvolili záložku *SNMP*. Na tomto zariadení sme vyplnili nasledujúce parametre:

- ✓ Povolili sme možnosť *Enabled*
- ✓ Community = *diplomka*
- ✓ Contact Info = *t\_misutka@utb.cz*
- ✓ Location = *testing infrastructure*



Obrázok 8.27 Konfigurácia *SNMP* na zariadení mikrotik switch, zdroj vlastný

#### Zabbix

V nástroji Zabbix sme prešli v menu do časti *Monitoring / Hosts, Create host*. O tomto zariadení sme vyplnili nasledovné údaje:

- ✓ Host name = *mikrotik switch*
- ✓ Templates = *Mikrotik SNMP*
- ✓ Groups = *Network devices, SNMP devices*
- ✓ SNMP IP address = *192.168.88.198*
- ✓ SNMP version = *SNMPv2*
- ✓ SNMP community =  $\{\$SNMP\_COMMUNITY\}$

V záložce *Macros* sme makru priradili hodnotu nasledovne:

✓ {*\$SNMP\_COMMUNITY*} = *diplomka*

Zariadenie sme pridali tlačidlom *Add*, ktoré sa po krátkej chvíli stalo dostupným prostredníctvom protokolu *SNMP*.

#### 8.2.4 Synology NAS

Toto zariadenie podporovalo monitorovanie prostredníctvom protokolov *SNMPv1*, *SNMPv2* aj verzie *SNMPv3*. Preferovali sme možnosť verzie 3.

##### NAS

Konfigurácia *SNMP* je dostupná aj prostredníctvom príkazového riadku, ale v tomto prípade bolo pre nás jednoduchšie využiť grafické rozhranie. Do Synology NAS sme sa prihlásili s administrátorskými právami a v aplikácii *Control Panel* sme prešli do kategórie *Terminal & SNMP*, záložka *SNMP*. Parametre sme vyplnili nasledovne:

✓ Povolili sme *Enable SNMP service*

✓ Povolili sme *SNMPv3 service*

✓ Username:Protocol:Password = *nas-snmp:SHA: NasSnmp123*.

✓ Povolili sme *SNMP privacy*

✓ Protocol:Password = *AES: nasSnmp@AES1234*

Ďalej sme doplnili nepovinné údaje, ako je názov zariadenia, lokalizácia či kontakt. Konfiguráciu sme uložili tlačidlom *Apply*.

Terminal **SNMP**

Enable SNMP to monitor the server with network management software.

☒ Enable SNMP service

☐ SNMPv1, SNMPv2c service [i](#)

Community:

☒ SNMPv3 service

Username:

Protocol:

Password:

☒ Enable SNMP privacy

Protocol:

Password:

SNMP Device Information

Device Name:

Device Location:

Contact:

Visit [Synology's website](#) to download the Synology MIB files.

Obrázok 8.28 Konfigurácia SNMPv3 na zariadení Synology NAS, zdroj vlastný

## Zabbix

V nástroji Zabbix sme prešli v menu do časti *Monitoring / Hosts, Create host*. Vyplnili sme nasledovné údaje:

- ✓ Host name = *Synology NAS*
- ✓ Templates = *Linux memory, CPU, filesystems SNMP, SNMP QNAP*
- ✓ Groups = *Servers, SNMP devices*
- ✓ SNMP IP address = *192.168.88.194*
- ✓ SNMP version = *SNMPv3*
- ✓ Security level = *authPriv*
- ✓ Security name = *{ \$SECURITY\_NAME }*
- ✓ Authentication protokol = *SHA1*
- ✓ Authentication passphrase = *{ \$AUTH\_PASS }*
- ✓ Privacy protocol = *AES128*
- ✓ Privacy passphrase = *{ \$PRIVACY\_PASS }*

V záložke *Macros* sme ku každému makru priradili hodnotu nasledovne:

- ✓ *{ \$AUTH\_PASS }* = *NasSnmp123*.
- ✓ *{ \$PRIVACY\_PASS }* = *nasSnmp@AES1234*

✓  $\{\$SECURITY\_NAME\} = nas-snmpp$

Pridávanie zariadenia sme ukončili tlačidlom *Add*. To sa nám pridalo do tabuľky, a po krátkej chvíli sa objavila aj dostupnosť zariadenia prostredníctvom protokolu *SNMP* v zelenom pozadí.

### 8.2.5 Tlačiareň Xerox

Táto tlačiareň obsahovala možnosť konfigurovať všetky verzie protokolu *SNMP*, konfigurovali sme verziu 3.

#### Xerox

Do konfigurácie tlačiarne sme sa dostali zadaním IP adresy *192.168.88.197* do URL prehliadača. Implementáciu sme začali v možnosti *Properties / Protocol / SNMPv3*. Použili sme nasledujúce údaje:

- ✓ Povolili sme možnosť *Enable*
- ✓ Context name = *xerox-snmpp*
- ✓ Authentication Password = *Xerox@123*
- ✓ Algorithm = *SHA*
- ✓ Privacy Password = *DESxeroX.123*.

Obrázok 8.29 Konfigurácia SNMP na tlačiarňi Xerox, zdroj vlastný

Konfigurácie sme uložili tlačidlom *Save Changes*, kde sme následne zadali administrátorské prihlasovacie údaje, čím sme konfiguráciu potvrdili.

#### Zabbix

Tlačiareň bolo tiež potrebné pridať aj v nástroji Zabbix. Prešli sme v menu do časti *Monitoring / Hosts, Create host*. Zadali sme nasledovné údaje:

- ✓ Host name = *Xerox printer*

- ✓ Templates = *Printer Xerox WorkCentre 3220*
- ✓ Groups = *Network devices, SNMP devices*
- ✓ SNMP IP address = *192.168.88.197*
- ✓ SNMP version = *SNMPv3*
- ✓ Security level = *authPriv*
- ✓ Context name = *{ \$CONTEXT\_NAME }*
- ✓ Security name = *{ \$SECURITY\_NAME }*
- ✓ Authentication protokol = *SHA1*
- ✓ Authentication passphrase = *{ \$AUTH\_PASS }*
- ✓ Privacy protokol = *DES*
- ✓ Privacy passphrase = *{ \$PRIVACY\_PASS }*

V záložce *Macros* sme ku každému makru priradili hodnotu nasledovne:

- ✓ *{ \$AUTH\_PASS } = Xerox@123*
- ✓ *{ \$PRIVACY\_PASS } = DESxeroX.123.*
- ✓ *{ \$SECURITY\_NAME } = xerox-snmp*
- ✓ *{ \$CONTEXT\_NAME } = xerox*

Zariadenie sme pridali tlačidlom *Add*. To sa nám pridalo do tabuľky k ostatným zariadeniam. Po krátkom okamihu toto zariadenie bolo dostupné protokolom *SNMP*.

### 8.2.6 Vmware ESXi

Toto zariadenie sme konfigurovali tak, ako väčšinu zariadení v predchádzajúcich podkapitolách tejto práce, a to pomocou protokolu *SNMPv3*. Toto zariadenie sme konfigurovali prostredníctvom konzoly cez *ssh*, kde sme sa prihlásili administrátorskými prihlasovacími údajmi.

#### Esxi

V tejto časti budú zapísané len príkazy, ktorých cieľom bolo správne nastaviť protokol *SNMPv3*. V úvode bolo nutné získať MAC adresu zariadenia, aby sme mohli nastaviť jedinečnosť parametra *Engineid*.

Na úvod bolo potrebné zistiť MAC adresu zariadenia, ktorú sme si zobrazili príkazom:

```
# esxcfg-info | grep "Mac Address"
|----Mac Address.....00:e0:4c:3b:08:e1
```

V protokole *SNMP* sme nastavili nasledujúcimi príkazmi *Engineid* a autentifikačné protokoly.

```
# esxcli system snmp set -E=00e04c3b08e1
# esxcli system snmp set -x=AES128
# esxcli system snmp set -a=SHA1
```

Ďalej bolo potrebné vytvoriť komunitu *diplomka*, čo bol názov, ktorý sme použili aj pri ostatných zariadeniach.

```
# esxcli system snmp set --communities diplomka
```

Potrebné bolo zvoliť vhodné bezpečnostné heslá a prostredníctvom nich vygenerovať hash. Tieto hash boli obe použité pri konfigurácii používateľa *esxi-snmp*. V samom závere konfigurácie sme povolili protokol *SNMP* a konfiguráciu sme si overili výpisom v konzole.

```
# esxcli system snmp hash -r -A esxi@014 -X AESesxi-124Snmp
# esxcli system snmp set --users esxi-snmp/2ea-
edb3464f7ff290399c8620e5f06cf83a87c50/fc2e5b741670d8f020b0d50ca0fcd5696e7b37a5/pri
v
# esxcli system snmp set -e yes
# esxcli system snmp get
```

```
[root@ESXiServer:~] esxcli system snmp get
Authentication: SHA1
Communities: diplomka
Enable: true
Engineid: 00e04c3b08e1
Hwsrc: indications
Largestorage: true
Loglevel: warning
Notraps:
Port: 161
Privacy: AES128
Remoteusers:
Syscontact:
Syslocation:
Targets:
Users: esxi-snmp/2eaedb3464f7ff290399c8620e5f06cf83a87c50/fc2e5b741670d8f020b0d50ca0fcd5696e7b37a5/priv
V3targets:
[root@ESXiServer:~] █
```

Obrázok 8.30 Konfigurácia SNMP na zariadení ESXi, zdroj vlastný

## Zabbix

Vmware ESXi sme pridávali aj v nástroji Zabbix medzi zariadenia. Prešli sme v menu do časti *Monitoring / Hosts, Create host*, kde sme vyplnili nasledujúce údaje:

- ✓ Host name = *Vmware Esxi*
- ✓ Templates = *SNMP OS ESXi*
- ✓ Groups = *Servers, SNMP devices*
- ✓ SNMP IP address = *192.168.88.50*
- ✓ SNMP version = *SNMPv3*
- ✓ Security level = *authPriv*
- ✓ Security name = *{ \$SECURITY\_NAME }*

- ✓ Authentication protokol = *SHA1*
- ✓ Authentication passphrase = *{ \$AUTH\_PASS }*
- ✓ Privacy protokol = *AES128*
- ✓ Privacy passphrase = *{ \$PRIVACY\_PASS }*

V záložke *Macros* sme ku každému makru priradili hodnotu nasledovne:

- ✓ *{ \$AUTH\_PASS } = esxi@014*
- ✓ *{ \$PRIVACY\_PASS } = AESesxi-124Snmp*
- ✓ *{ \$SECURITY\_NAME } = esxi-snmp*
- ✓ *{ \$SNMP\_COMMUNITY } = diplomka*

Zariadenie sme pridali tlačidlom *Add*, čo pridalo zariadenie k ostatným do tabuľky.

V krátkom časovom okamihu toto zariadenie bolo dostupné protokolom *SNMP*.

Po pridání všetkých zariadení sme mali možnosť všetky zariadenia vidieť dostupné v tabuľke. Dostupnosť zariadení signalizoval zelený indikátor *SNMP* v stĺpci *Availability*.

Name ▲	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Mikrotik router	192.168.88.1:161	SNMP	class: network target: mikrotik	Enabled	Latest data	Problems	Graphs 11	Dashboards 1	Web
mikrotik switch	192.168.88.198:161	SNMP	class: network target: mikrotik	Enabled	Latest data	Problems	Graphs 7	Dashboards 1	Web
Synology NAS	192.168.88.194:161	SNMP		Enabled	Latest data	1	Graphs 14	Dashboards 2	Web
Vmware Esxi	192.168.88.50:161	SNMP		Enabled	Latest data	2	Graphs 2	Dashboards	Web
Xerox printer	192.168.88.197:161	SNMP		Enabled	Latest data	1	Graphs 1	Dashboards 1	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Enabled	Latest data	Problems	Graphs 24	Dashboards 4	Web

Displaying 6 of 6 found

Obrázok 8.31 Zariadenia z infraštruktúry monitorované protokolom *SNMP*, zdroj vlastný

## 8.2.7 Nastavenie emailov

Vždy bolo veľmi dôležité, aby bol administrátor informovaný o akýchkoľvek problémoch, ktoré sa v sieti vyskytli. Informáciu o probléme bolo možné doručiť administrátorovi vo viacerých platformách ako sú email, Slack, MS Teams a podobne. My sme zvolili overenú emailovú formu notifikácie. Pri konfigurácii sme použili školský účet a server od *Office 365*.

### Emailový server

V nástroji *zabbix* sme v hlavnom menu zvolili záložku *Administration* a podkategóriu *Media types*, v tabuľke sme vybrali možnosť *Email*. Údaje sme vyplnili nasledovne:

- ✓ Name = *Email*
- ✓ Type = *Email*
- ✓ SMTP server = *smtp.office365.com*
- ✓ SMTP server port = *587*



- ✓ SMTP helo = *smtp.office365.com*
- ✓ SMTP email = *t\_misutka@utb.cz*
- ✓ Connection security = *STARTTLS*
- ✓ Authentication = *Username and password*
- ✓ Vyplnili sme prihlasovacie údaje

The screenshot shows a web application interface for configuring email settings. The interface is divided into three tabs: 'Media type', 'Message templates 5', and 'Options'. The 'Options' tab is active. The form contains the following fields and options:

- Name:** Text input field containing 'Email'.
- Type:** Dropdown menu showing 'Email'.
- \* SMTP server:** Text input field containing 'smtp.office365.com'.
- SMTP server port:** Text input field containing '587'.
- \* SMTP helo:** Text input field containing 'smtp.office365.com'.
- \* SMTP email:** Text input field containing 't\_misutka@utb.cz'.
- Connection security:** Radio buttons for 'None', 'STARTTLS' (selected), and 'SSL/TLS'.
- SSL verify peer:** Checkbox, currently unchecked.
- SSL verify host:** Checkbox, currently unchecked.
- Authentication:** Radio buttons for 'None' and 'Username and password' (selected).
- Username:** Text input field containing 't\_misutka@utb.cz'.
- Password:** Password input field with masked characters.
- Message format:** Radio buttons for 'HTML' and 'Plain text' (selected).
- Description:** Large text area for additional information.
- Enabled:** Checkbox, currently checked.
- Buttons:** 'Update' (highlighted in blue), 'Clone', 'Delete', and 'Cancel'.

Obrázok 8.32 Konfigurácia emailov, zdroj vlastný

Konfiguráciu sme uložili tlačidlom *update*, čím sme sa vrátili do podkategórie *Media types*. Emailovú konfiguráciu sme si mali možnosť ihneď overiť, jednoducho tlačidlom *Test*, ktoré sa nachádzalo v tabuľke v stĺpci *Action*.

Vyplnili sme email prijímateľa, predmet správy a obsah správy sme nechali v predvolenom formáte. Testovací email sme odoslali tlačidlom *Test*. Úspešné obdržanie emailu je možné vidieť na nasledujúcom obrázku.



Obrázok 8.33 Testovací email z nástroja zabbix, zdroj vlastný

### Priradenie emailu

Po úspešnej emailovej konfigurácii bolo potrebné definovať používateľov v nástroji zabbix, ktorým bude emailová notifikácia doručená. Konfigurácia bola skrytá pod existujúcim administrátorským účtom, konkrétne pod záložkou *Media*.

Konfiguračnú stránku sme našli v hlavnom paneli *Administration / Users* a tam sme vybrali náš existujúci administrátorský účet *Admin*. Po zobrazení detailoch o používateľovi sme sa v hornej časti konfigurácie prepli na záložku *Media* a tlačidlom *Add* sme pridali tomuto účtu nové médium. Údaje o médiu sme vyplnili nasledovné:

- ✓ Type = *Email*
- ✓ Send to = *vlastný súkromný email* (emailových adries môže byť viac)
- ✓ When active = *1-7, 00:00-24:00*
- ✓ Use if severity = *povolené sme nechali všetky možnosti*
- ✓ Povolili sme možnosť *Enabled*

Médium bolo úspešne pridané k administrátorskému účtu tlačidlom *Add*.

### Trigger action

Pomocou akcie na priradený trigger sme mohli zabbixu povedať, čo sa má stať, ak sa objaví nová udalosť. Mohol sa napríklad spustiť nejaký skript, vytvoriť nový ticket, prípadne sa mohla odoslať emailová notifikácia, čo bol aj náš prípad.

Prešli sme v hlavnom navigačnom paneli do časti *Configuration / Actions / Trigger action*. Tu sa nachádzal už existujúci záznam s názvom *Report problems to Zabbix administrators*, kde úlohou tohto záznamu bolo informovať všetky existujúce administrátorské účty o vzniknutej udalosti prostredníctvom všetkým nakonfigurovaných médií.

Túto možnosť sme označili a tlačidlom *Enable* možnosť povolili. Ihneď po tejto konfigurácii sa informácia o vzniknutom probléme doručila do našej súkromnej emailovej schránky. Týmto krokom sme zároveň overili aj funkčnosť a požiadavky riešenia.

	Hlavné	Siete	Reklamy
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Resolved in 9m 0s: Zabbix server: Utilization of discoverer processes over 75% - Problem has been resolved at 22:07:35 on 2022.05.14 Problem name: Zabbix server: Utilization of di...	22:07
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Problem: Zabbix server: Utilization of discoverer processes over 75% - Problem started at 21:58:35 on 2022.05.14 Problem name: Zabbix server: Utilization of discoverer processes o...	21:58
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Problem: Synology NAS has been restarted (uptime < 10m) - Problem started at 21:45:43 on 2022.05.14 Problem name: Synology NAS has been restarted (uptime < 10m) Host: Synol...	21:45
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Resolved in 11m 10s: Synology NAS has been restarted (uptime < 10m) - Problem has been resolved at 21:42:13 on 2022.05.14 Problem name: Synology NAS has been restarted (upt...	21:42
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Resolved in 10m 0s: Zabbix server: Utilization of discoverer processes over 75% - Problem has been resolved at 21:38:35 on 2022.05.14 Problem name: Zabbix server: Utilization of d...	21:38
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Problem: Synology NAS has been restarted (uptime < 10m) - Problem started at 21:31:03 on 2022.05.14 Problem name: Synology NAS has been restarted (uptime < 10m) Host: Synol...	21:31
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Problem: Zabbix server: Utilization of discoverer processes over 75% - Problem started at 21:28:35 on 2022.05.14 Problem name: Zabbix server: Utilization of discoverer processes o...	21:28
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Resolved in 10m 26s: Synology NAS has been restarted (uptime < 10m) - Problem has been resolved at 21:26:13 on 2022.05.14 Problem name: Synology NAS has been restarted (upt...	21:26
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Problem: Synology NAS has been restarted (uptime < 10m) - Problem started at 21:15:47 on 2022.05.14 Problem name: Synology NAS has been restarted (uptime < 10m) Host: Synol...	21:15
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Resolved in 10m 0s: Synology NAS has been restarted (uptime < 10m) - Problem has been resolved at 21:10:43 on 2022.05.14 Problem name: Synology NAS has been restarted (upt...	21:10
<input type="checkbox"/> ☆ ➤	<b>l_misutka</b>	Resolved in 10m 0s: Zabbix server: Utilization of discoverer processes over 75% - Problem has been resolved at 21:09:35 on 2022.05.14 Problem name: Zabbix server: Utilization of d...	21:09

Obrázok 8.34 Doručené správy z nástroja zabbix do súkromnej emailovej schránky, zdroj vlastný

## 8.2.8 Kontrola dostupnosti zariadení

V požiadavkách riešenia bol jedným z bodov monitorovanie dostupností zariadení a služieb. My sme sa zamerali na monitoring zariadenia, aj keď monitorovanie služby je na úplne rovnakom princípe. V našej testovacej infraštruktúre bolo niekoľko kritických zariadení, kde by bolo vhodné monitorovať ich dostupnosť. V prípade výskytu nedostupnosti týchto kritických zariadení bolo nevyhnutné okamžite o tom informovať emailom administrátora. My sme sa zamerali na kontrolu dostupnosti zariadenia *Synology NAS*, čo je z nášho pohľadu určite kritický prvok v našej testovacej infraštruktúre.

Na konfiguráciu bolo potrebné nastaviť niekoľko dôležitých podmienok, ktoré nám zabezpečili zisťovanie dostupnosti zariadenia v pravidelných časových intervaloch prostredníctvom *ICMP* protokolu. Konfiguráciu emailov sme spravili v predchádzajúcej podkapitole, ktorú sme následne mohli použiť aj v tejto časti. Dôležité bolo poznamenať, že zariadenie *Synology NAS* bolo dostupné na IP adrese *192.168.88.194*.

### Discovery rule

V tomto kroku sme definovali pravidlo na zisťovanie dostupnosti zariadenia na IP adrese *192.168.88.194* prostredníctvom protokolu *ICMP*. V nástroji zabbix sme prešli v hlavnom menu do kategórie *Configuration* a zvolili podkategóriu *Discovery*. V zobrazenej tabuľke už bolo dostupné, ale nepovolené 1 pravidlo, ktorého účelom bolo zisťovanie všetkých zariadení v rozsahu *192.168.88.1-254*.

Nové pravidlo sme pridali tlačidlom *Create discovery rule*, kde sme vyplnili názov *nas discovery* s IP adresou *192.168.88.194* v časovom intervale *5m*. V časti *Checks* sme definovali protokol *ICMP ping* a ostatné parametre zostali v predvolenom stave. Pravidlo sme pridali Tlačidlom *Add*, čím sa pravidlo zaradilo k existujúcemu pravidlu do tabuľky.

\* Name: nas discovery

Discovery by proxy: No proxy

\* IP range: 192.168.88.194

\* Update interval: 5m

\* Checks: Type: ICMP ping, Actions: Edit, Remove, Add

vice uniqueness criteria: IP address

Host name: DNS name, IP address

Visible name: Host name, DNS name, IP address

Enabled: ☒

Add Cancel

Obrázok 8.35 Definícia pravidla na zisťovanie dostupnosti zariadenia NAS, zdroj vlastný

## Discovery action

Po konfigurácii pravidla bolo potrebné ešte nakonfigurovať akciu, ktorá bola úzko spätá s vytvoreným pravidlom. V hlavnom navigačnom paneli v kategórii *Configuration* sme prešli do podkategórie *Action / Discovery actions*, kde sme pridali novú akciu tlačidlom *Create action*.

V záložke *Action* sme vyplnili názov akcie *nas discovery action*, prepočet podmienok, samotné podmienky a povolili sme možnosť *Enabled*. Medzi podmienky sme zaradili IP adresu *192.168.88.194* a *Discovery status equals Down*.

Action Operations

\* Name: nas discovery action

Type of calculation: And A and B

Conditions:

Label	Name	Action
A	Host IP equals 192.168.88.194	Remove
B	Discovery status equals Down	Remove

Add

Enabled: ☒

\* At least one operation must exist.

Add Cancel

Obrázok 8.36 Definícia akcie pri zisťovaní dostupnosti zariadenia NAS, zdroj vlastný

V záložke *Operation* sme pridali novú operáciu tlačidlom *Add*, kde sme typ operácie zvolili *Send messege*, v časti *Send to users* sme pridali náš administrátorský účet *Admin* a vybrali sme možnosť odoslania správy len prostredníctvom emailu. Operáciu sme pridali tlačidlom *Add*.

**Operation details** ×

Operation Send message ▾

\* At least one user or user group must be selected.

Send to user groups

User group	Action
<a href="#">Add</a>	

Send to users

User	Action
Admin (Zabbix Administrator)	<a href="#">Remove</a>
<a href="#">Add</a>	

Send only to Email ▾

Custom message ☐

[Add](#) [Cancel](#)

Obrázok 8.37 Definícia operácie pri zisťovaní dostupnosti zariadenia NAS, zdroj vlastný

### 8.2.9 Vlastný trigger

V tejto časti sme vytvorili doplňujúce možnosti monitoringu tlačiarne, ktoré sme pridali do šablóny *Printer Xerox WorkCentre 3220*. Vytvorenie bolo nevyhnutné vzhľadom na stanovené požiadavky monitoringu tlačiarne, ktoré vyššie zmienená šablóna nepodporovala. Preto sme vytvorili monitorovanie 2 nových položiek, a na 1 z nich sme následne vytvorili *trigger*, ktorý informoval administrátora o nedostatku papierov v zásobníku 1.

Prvá položka, ktorú sme vytvorili slúžila na monitorovanie maximálneho počtu papierov v zásobníku 1. Druhá položka bola určená na sledovanie aktuálnej hodnoty v zásobníku 1.

### Vytvorenie itemov

Ako sme spomenuli v úvode tejto podkapitoly, vytvorili sme 2 nové položky v šablóne určenej na tlačiareň xerox. V navigačnom paneli sme zvolili možnosť *Configuration / Templates*, kde sme použili filter na vyhľadávanie šablón. Šablónu sme vyhľadali pomocou mena *printer*.

Zobrazili sme si detail šablóny, a v hornej časti sme klikli na záložku *Items* a v pravom hornom rohu sme klikli na tlačidlo *Create item*. Povinné údaje boli označené červenou hviezdikou. Pri vytváraní itemu, ktorým sme sledovali maximálnu hodnotu papiera v zásobníku číslo 1, sme použili nasledovné údaje:

Items

All templates / Printer Xerox WorkCentre 3220 Items 7 Triggers 2 Graphs 1 Dashboards 1 Discovery rules Web scenarios

Item Tags Preprocessing

\* Name Tray 1 Max Capacity

Type SNMP agent

\* Key tray.max.capacity [Select](#)

Type of information Numeric (unsigned)

\* SNMP OID .1.3.6.1.2.1.43.8.2.1.9.1.1

Units paper count

\* Update interval 1h

Custom intervals

Type	Interval	Period	Action
<b>Flexible</b>	Scheduling	50s	1-7,00:00-24:00 <a href="#">Remove</a>
<a href="#">Add</a>			

\* History storage period Do not keep history **Storage period** 30d

\* Trend storage period Do not keep trends **Storage period** 365d

Value mapping type here to search [Select](#)

Populates host inventory field -None-

Description

Enabled ☒

[Add](#) [Test](#) [Cancel](#)

Obrázok 8.38 Konfigurácia itemu na monitorovanie maximálneho množstva papiera v zásobníku 1, zdroj vlastný

Druhý item sme vytvorili na to, aby v pravidelných intervaloch 1m kontroloval aktuálny stav papiera v zásobníku 1. Tomuto itemu sme prideliť nasledovné hodnoty:

Items

All templates / Printer Xerox WorkCentre 3220 Items 9 Triggers 3 Graphs 1 Dashboards 1 Discovery rules Web scenarios

Item Tags 1 Preprocessing

\* Name

Type

\* Key

Type of information

\* SNMP OID

Units

\* Update interval

Custom intervals

Type	Interval	Period	Action
Flexible	Scheduling	50s	1-7,00:00-24:00
<input type="button" value="Remove"/>			

\* History storage period

\* Trend storage period

Value mapping

Populates host inventory field

Description

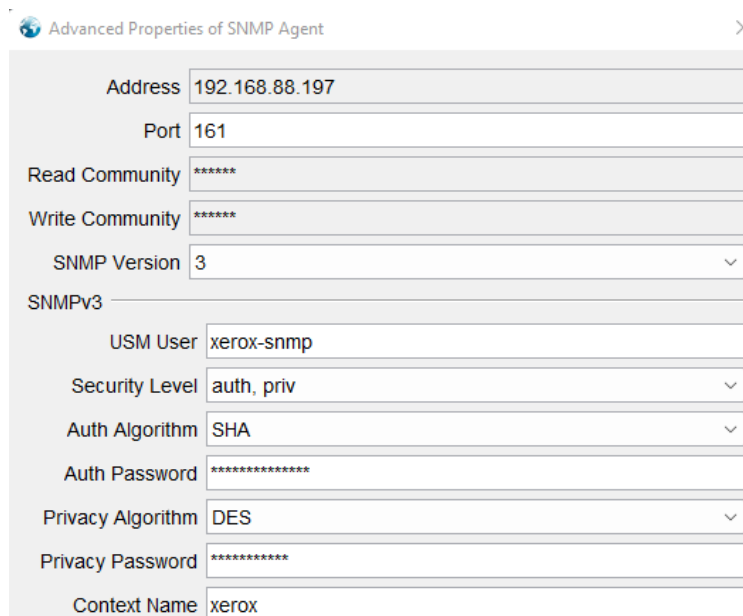
Enabled ☒

Obrázok 8.39 Konfigurácia itemu na monitorovanie aktuálneho množstva papiera v zásobníku 1, zdroj vlastný

## Získanie SNMP OID

Hodnoty, ktoré sme položkám pridali v parametri *Key* sme museli najskôr zistiť priamo pre náš typ tlačiarne zo zariadenia. Boli to tzv. hodnoty *SNMP OID*. Na získanie týchto hodnôt sme použili softvér *iReasoning MIB Browser* v OS Windows a dokumentáciu MIB. Dokumentácia bola dostupná na adrese <http://www.mibdepot.com/index.shtml?id=234049>. Z tabuľky sme si zobrazili dáta pre zariadenia xerox, a následne sme vybrali normu *RFC1579*, kde sa nachádzal popis položiek s názvom *prtInputMaxCapacity* a *prtInputCurrentLevel*, o ktoré sme mali záujem.

Pokračovali sme v programe *MIB Browser*, ktorý umožňoval sledovať *OID* hodnoty pomocou *SNMP API*. V nastaveniach sme zadali cieľovú IP adresu *192.168.88.197* a v časti *Operations* sme vybrali hodnotu *Walk*. Pomocou tlačidla *Advanced* sme doplnili konfiguráciu *SNMPv3*. Prehľadávanie sme začali Tlačidlom *Go*. Dôležité bolo ešte pred vyhľadávaním importovať normy *MIB* do softvéru. V navigačnom menu sme zvolili *File / Load MIBs*, kde sme vybrali všetky dostupné normy *RFC*.



Advanced Properties of SNMP Agent

Address: 192.168.88.197

Port: 161

Read Community: \*\*\*\*\*

Write Community: \*\*\*\*\*

SNMP Version: 3

SNMPv3

USM User: xerox-snmpp

Security Level: auth, priv

Auth Algorithm: SHA

Auth Password: \*\*\*\*\*

Privacy Algorithm: DES

Privacy Password: \*\*\*\*\*

Context Name: xerox

Obrázok 8.40 Konfigurácia SNMP agenta v softvéri MIB Browser, zdroj vlastný

Dáta sa nám zobrazili v tabuľke, kde sme vyhľadali záznamy, ktoré obsahovali názvy, ktoré sme identifikovali v dokumentácii. Po kliknutí na položku sa nám hodnoty *OID* zobrazili v hornej časti programu pod položkou *OID*, ktoré sme následne použili pri konfigurácii itemov v šablóne pre tlačiareň.

prtInputMediaDimXFeedDirChosen.1.2	82700	Integer
prtInputCapacityUnit.1.1	sheets (8)	Integer
prtInputCapacityUnit.1.2	sheets (8)	Integer
prtInputMaxCapacity.1.1	250	Integer
prtInputMaxCapacity.1.2	1	Integer
prtInputCurrentLevel.1.1	0	Integer
prtInputCurrentLevel.1.2	0	Integer
prtInputStatus.1.1	16	Integer

Obrázok 8.41 Hodnoty SNMP OID získané prostredníctvom softvéru MIB browser, zdroj vlastný

Naše vytvorené itemy boli pridané do šablóny určenej na tlačiareň. Viditeľné boli v dolnej časti tabuľky. Na základe týchto pridaných itemov, ktorých úlohou bolo monitorovať stav papiera v zásobníku číslo 1, sme mohli vytvoriť trigger pre prípad, že množstvo papiera v zásobníku klesne pod hodnotu 5.

<input type="checkbox"/>	Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
<input type="checkbox"/>	Cartridge toner level % - black	Triggers 2	black cartridge toner	30	7d	365d	Calculated	Enabled	Application: Consuma
<input type="checkbox"/>	Current cartridge toner level - black		ink black now	30	7d	365d	SNMP agent	Enabled	Application: Consuma
<input type="checkbox"/>	Max cartridge toner level - black		ink black max	30	7d	365d	SNMP agent	Enabled	Application: Consuma
<input type="checkbox"/>	Pages printed - total		Pages_printed_total	30	7d		SNMP agent	Enabled	Application: Pages pr...
<input type="checkbox"/>	Printer location	Triggers 2	printer location	1h	7d		SNMP agent	Enabled	Application: Printer inf...
<input type="checkbox"/>	Printer model	Triggers 2	model	1h	7d		SNMP agent	Enabled	Application: Printer inf...
<input type="checkbox"/>	Serial number	Triggers 2	serial number	1h	7d		SNMP agent	Enabled	Application: Printer inf...
<input type="checkbox"/>	Tray 1 current capacity		tray current capacity	1m	30d	365d	SNMP agent	Enabled	Application: Tray cure...
<input type="checkbox"/>	Tray 1 max capacity		tray max capacity	1h	30d	365d	SNMP agent	Enabled	Application: Tray max ca...

Displaying 9 of 9 found

Obrázok 8.42 Pridanie itemov do šablóny, zdroj vlastný



## Vytvorenie triggeru

V detailom zobrazení šablóny sme sa prepli do časti *Triggers* a v pravom hornom rohu sme klikli na tlačidlo *Create trigger*. Názov sme zvolili *Lack of papers in Tray 1* a následne sme v časti *Expressions* definovali podmienku, ktorou sme zabezpečili sledovanie poslednej aktuálnej hodnoty v zásobníku 1. Dôležitosť sme zvolili *Average*, pretože chýbajúci papier v tlačiarňi je značné obmedzenie v používaní zariadenia. *Trigger* sme pridali tlačidlom *Add*.

Triggers

All templates / Printer Xerox WorkCentre 3220 Items 9 Triggers 2 Graphs 1 Dashboards 1 Discovery rules Web scenarios

Trigger Tags Dependencies

\* Name: Lack of papers in Tray 1

Event name: Lack of papers in Tray 1

Operational data:

Severity: Not classified Information Warning **Average** High Disaster

\* Expression: last (/Printer Xerox WorkCentre 3220/tray.current.capacity)<5 Add

Expression constructor

OK event generation: Expression Recovery expression None

PROBLEM event generation mode: Single Multiple

OK event closes: All problems All problems if tag values match

Allow manual close: ☒

URL:

Description: Lack of papers in Tray 1. The printer won't print pages.

Enabled: ☒

Add Cancel

Obrázok 8.43 Vytvorenie triga v šablóne pre tlačiareň, zdroj vlastný

Po pridaní sa nám zobrazil trigger v tabuľke medzi ďalšími dvoma predvolenými.

Severity	Name	Operational data	Expression	Status	Tags
High	Empty cartridge toner - black		last (/Printer Xerox WorkCentre 3220/black cartridge toner)=0 and nodata (/Printer Xerox WorkCentre 3220/model,3w)=0 and nodata (/Printer Xerox WorkCentre 3220/serial number,3w)=0	Enabled	
Average	Lack of papers in Tray 1		last (/Printer Xerox WorkCentre 3220/tray.current.capacity)<5	Enabled	
Information	Low cartridge toner - black		last (/Printer Xerox WorkCentre 3220/black cartridge toner)>20 and nodata (/Printer Xerox WorkCentre 3220/model,3w)=0 and nodata (/Printer Xerox WorkCentre 3220/serial number,3w)=0	Enabled	
	Depends on: Printer Xerox WorkCentre 3220: Empty cartridge toner - black				

Displaying 3 of 3 found

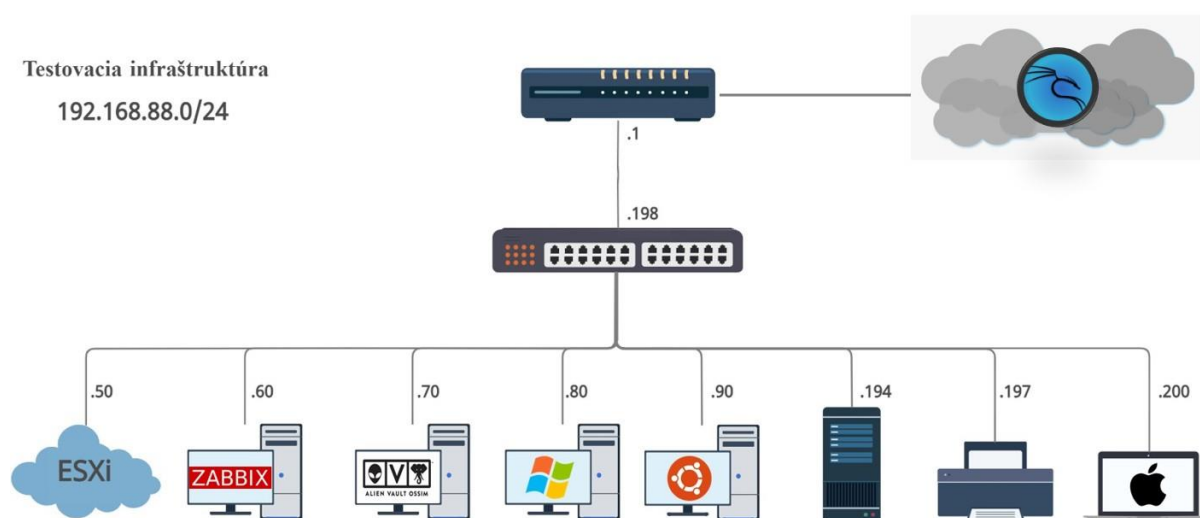
Obrázok 8.44 Trigger pridaný k ostatným v šablóne, zdroj vlastný

## 9. OVERENIE IMPLEMENTÁCIE

Implementáciu navrhnutého riešenia bolo na záver potrebné otestovať v testovacom segmente, čo bola v našom prípade testovacia infraštruktúra. V prípade objavených nedostatkov upraviť konfiguráciu tak, aby sme splnili stanovené požiadavky na detekciu zraniteľností. Na testovanie sme využili zariadenie s OS *Kali Linux*, z ktorého sme sa pokúsili útočiť na testovaciu infraštruktúru. Toto nové zariadenie bolo inštalované vo virtuálnom prostredí na našom vlastnom počítači s natovaným sieťovým rozhraním. Dôležitým faktom bolo, že toto zariadenie sa nachádza mimo rozsahu testovacej infraštruktúry a prístup do siete sme využili prostredníctvom VPN tunelu. V tomto stave sme boli schopní otestovať riešenie z externej strany internetu.

Testovali sme útok hrubou silou (*brute-force*) na koncové zariadenia v sieti či skenovaním ich portov. Dôležité bolo tieto útoky zachytiť v logoch, vytvoriť alarm a poslať email o vzniknutej udalosti administrátorovi. Návrh protiopatrení proti útoku nebolo cieľom tejto práce.

Novú testovaciu infraštruktúru sme zobrazili na obrázku nižšie. Vzhľadom na skutočnosť, že sme neboli schopní nakonfigurovať na zariadení *mikrotik switch* monitoring prevádzky prostredníctvom netflow, zachytiť útok skenovaním portov na L2 vrstve v internej sieti nebolo možné. Tým sme testovanie útoku skenovaním portov z internej siete vynechali.



Obrázok 9.1 Testovacia infraštruktúra na overenie implementácie, zdroj vlastný

V ďalšej časti tejto práce bol potrebné otestovať implementáciu nástroja zabbix, ktorého schopnosti sme využili na monitorovanie prevádzky na sieťových a kritických zariadeniach

v sieti. Monitorovať bolo potrebné vyťaženie a dostupnosť týchto zariadení, prípadne ich služieb. Tieto zariadenia sme monitorovali prostredníctvom protokolu *SNMP*, prevažne verzie 3.

## 9.1 Overenie detekcie zraniteľností

Ako bolo spomenuté v úvode, pri overení implementácie tohto nástroja sme použili zariadenie s OS *Kali Linux*. Z tohto zariadenia sme testovali 2 typy útokov.

Prvým útokom bolo skenovanie portov koncových zariadení aplikáciou *nmap*. Druhým útokom bol tzv. útok hrubou silou pomocou aplikácie *Hydra*, kde sme sa pokúsili na koncové zariadenie získať heslo na pripojenie cez protokol *ssh*.

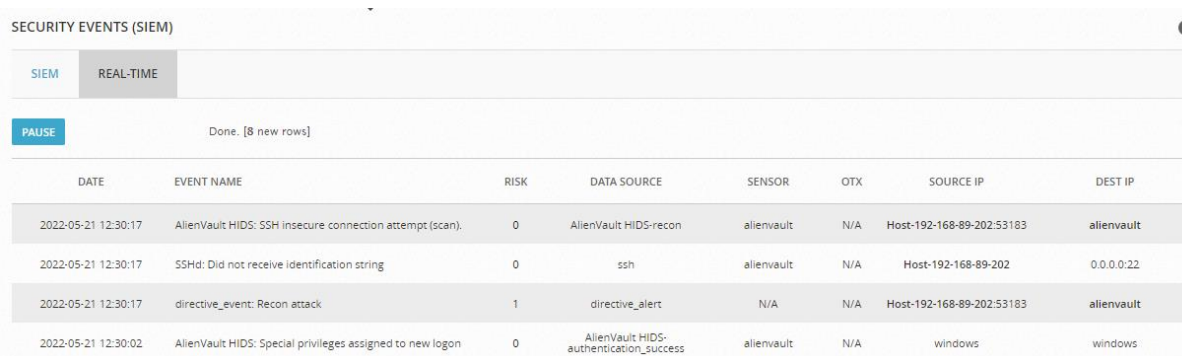
### 9.1.1 Skenovanie portov - nmap

Skenovanie sme mohli smerovať len na zariadenia, na ktorých sa nám poradilo nainštalovať a spustiť HIDS agentov. Z logov, ktoré sa posielali do nástroja AlienVault prostredníctvom remote log sme útok skenovaním portov neboli schopní zachytiť. Preto sme útok skenovaním portov smerovali len na zariadenia *alienvault*, *ubuntupc*, *windows* a *zabbix*.

V zariadení s Kali Linuxom sme si otvorili konzolu a pomocou nasledujúceho príkazu sme vykonali útok skenovaním portov na koncové zariadenie AlienVault.

```
# nmap 192.168.88.70
```

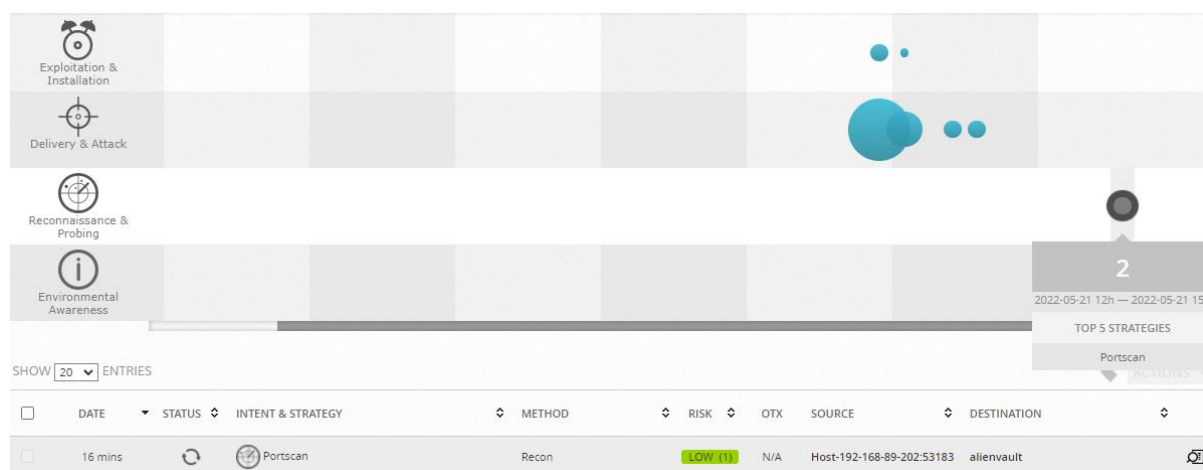
Ihneď sa nám v logoch zobrazila informácia o tom, že zariadenie s IP adresou *192.168.89.202* skenovalo porty zariadenia *alienvault*.



SECURITY EVENTS (SIEM)							
SIEM		REAL-TIME					
PAUSE		Done, [8 new rows]					
DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	CTX	SOURCE IP	DEST IP
2022-05-21 12:30:17	AlienVault HIDS: SSH insecure connection attempt (scan).	0	AlienVault HIDS-recon	alienvault	N/A	Host-192-168-89-202:53183	alienvault
2022-05-21 12:30:17	SSHD: Did not receive identification string	0	ssh	alienvault	N/A	Host-192-168-89-202	0.0.0.0:22
2022-05-21 12:30:17	directive_event: Recon attack	1	directive_alert	N/A	N/A	Host-192-168-89-202:53183	alienvault
2022-05-21 12:30:02	AlienVault HIDS: Special privileges assigned to new logon	0	AlienVault HIDS: authentication_success	alienvault	N/A	windows	windows

Obrázok 9.2 Logy so zachyteným skenovaním portov, zdroj vlastný

Z tejto udalosti sa vygeneroval alarm, ktorý bol zabezpečený konfiguráciou direktívy. Alarm bol dostupný v časti *ANALYSIS / ALARM*.



Obrázok 9.3 Vytvorený alarm po útoku skenovaním portov, zdroj vlastný

Rovnakým spôsobom sme chceli útočiť aj na ostatné zariadenia *zabbix*, *ubuntupc* a *windows*, avšak počas útokov sme zistili, že z neznámych príčin útok na týchto zariadeniach pomocou HIDS agentov nebol zachytený. Z neznámych príčin tento útok nebol zachytený v logoch zariadení a dôsledkom toho sa tieto logy neobjavili ani v logoch nástroja AlienVault.

Po konzultácii s vedúcim práce sme došli k záveru, že v konfigurácii by nemal byť problém a skúmanie či hľadanie príčiny, čo mohlo spôsobiť problém, by bolo časovo veľmi náročné. Principiálne sme riešenie sme overili útokom na zariadenie *alienvault*, čím môžeme povedať, že zadanie na detekciu útoku skenovaním portov bolo splnené.

### 9.1.2 Útok hrubou silou – brute-force

V zariadení Kali Linux sme spustili konzolu a pomocou aplikácie *Hydra* sme začali útočiť na zariadenie *ubuntupc*, na ktorom sme mali spusteného HIDS agenta a neskôr rovnakým spôsobom aj na zariadenie *ESXi*, odkiaľ sme dostávali logy do nástroja AlienVault prostredníctvom *remote log*. Do systémov sme sa snažili preniknúť prostredníctvom protokolu *ssh* a prihlasovacích údajov *root:root*. Pri tomto útoku sme mohli použiť slovníky, v ktorých by sa nachádzali mená a heslá, ktoré by sme použili namiesto *root:root*. Útok aplikáciou *hydra* sme spustili 100- krát pomocou cyklu *for*.

```
(kali@kali)-[~]  
$ for loop in {1..100}  
do  
hydra -l root -p root 192.168.88.90 ssh  
done
```

Obrázok 9.4 Brute force útok aplikáciou hydra spustený 100 krát v cykle for, zdroj vlastný

Po spustení útoku sme ihneď v logoch mali možnosť vidieť, že zariadenie s IP adresou *192.168.89.202* sa priebehu niekoľko desiatok sekúnd neúspešne prihlasovalo na zariadenie *macubuntu*.

DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	OTX	SOURCE IP	DEST IP
2022-05-21 15:20:43	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52872	ubuntupc
2022-05-21 15:20:41	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:20:17	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52853	ubuntupc
2022-05-21 15:20:15	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:19:51	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52837	ubuntupc
2022-05-21 15:19:49	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:19:27	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52820	ubuntupc
2022-05-21 15:19:25	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:19:01	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52799	ubuntupc
2022-05-21 15:18:59	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:18:35	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52782	ubuntupc
2022-05-21 15:18:33	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:18:09	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202:52748	ubuntupc
2022-05-21 15:18:07	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 15:17:43	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS- authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc

Obrázok 9.5 Logy z nástroja AlienVault počas brute force útoku, zdroj vlastný

Útok sme zároveň sledovali v konzole na zariadení s OS Kali Linux.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-21 08:57:35
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:1), ~1 try per task
[DATA] attacking ssh://192.168.89.90:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-21 08:57:39
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-21 08:57:39
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:1), ~1 try per task
[DATA] attacking ssh://192.168.89.90:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-21 08:57:42
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-21 08:57:42
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:1), ~1 try per task
[DATA] attacking ssh://192.168.89.90:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-21 08:57:45
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-21 08:57:45
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:1), ~1 try per task
[DATA] attacking ssh://192.168.89.90:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-21 08:57:48
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-21 08:57:48
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:1), ~1 try per task
[DATA] attacking ssh://192.168.89.90:22/
```

Obrázok 9.6 Progres útoku hrubou silou pomocou aplikácie hydra, zdroj vlastný

Po niekoľkých neúspešných pokusoch o prihlásenie sme očakávali, že sa v časti *ANALYSIS / ALARM* objaví nový alarm signalizujúci útok hrubou silou. Nič také sa však ani po 100 neúspešných pokusoch neudialo. Preto sme museli analyzovať dôvod, prečo sa tak nestalo.

## Analýza problému



V analýze tohto zisteného problému sme sa najskôr zamerali na existujúce vstavané direktívy alarmujúce na tento typ útoku. V predvolených direktívach zameraných na *BruteForce* útoky sme zistili, že v zariadeniach, na ktorých bol aplikovaný HIDS agent, je predpripravený alarm s číslom *EVENT TYPE 5712* a *5715*.

Následne sme teda prešli na analýzu zachytených udalostí po útoku aplikáciou *hydra* v časti *ANALYSIS / SECURITY EVENTS (SIEM)*, kde sme si pomocou filtra nechali zobrazit' všetky udalosti patriace do skupiny *AlienVault HIDS*. Zo zachytených záznamov sme zistili, že čísla typov udalostí boli *5720*, *5716* a *5503*. Z týchto skutočností sme zistili, že aktuálne predpripravené direktívy zamerané na *BruteForce* útoky nezachytávajú udalosti s týmito číslami. Preto bolo potrebné upraviť konfiguráciu pridaním novej direktívy, v ktorej tieto zistené skutočnosti budú zapracované.

## Úprava konfigurácie

V tejto časti vytvorili novú direktívu, pomocou ktorej bolo možné zachytiť brute force útok aplikáciou *hydra*.

Prešli sme do časti *CONFIGURATION / THREAT* a zvolili sme záložku *DIRECTIVES*. Pridali sme novú direktívu, ktorú sme nazvali *Brute force attack*. V časti *TAXONOMY* sme vyplnili parametre *Delivery & Attack*, *Bruteforce authentication* a metódu sme nazvali *Hydra* s prioritou 4. Názov pravidla sme zadali *Brute force authentication failed*, typ udalosti sme vybrali *ALIENVAULT HIDS-AUTHENTICATION\_FAILED*. Následne sme vybrali hodnoty, ktoré by sme chceli klasifikovať ako brute force útok.

Choose between Event Sub-Types Selection or Taxonomy

☒ Event Sub-Types ☐ Taxonomy

PLUGIN SIGNATURES		
8 items selected	Remove all	Add all
5503 - AlienVault HIDS: User login failed.	—	11502 - AlienVault HIDS: FTP Authentication failed.
5710 - AlienVault HIDS: Attempt to login using a non-existent user	—	14101 - AlienVault HIDS: VPN authentication failed.
5716 - AlienVault HIDS: SSHD authentication failed.	—	14202 - AlienVault HIDS: VPN authentication failed.
19111 - AlienVault HIDS: VMWare ESX authentication failure.	—	18125 - AlienVault HIDS: Remote access login failure.
19113 - AlienVault HIDS: VMWare ESX user authentication failure.	—	31205 - AlienVault HIDS: Admin authentication failed.
30108 - AlienVault HIDS: User authentication failed.	—	31315 - AlienVault HIDS: Web authentication failed.
30110 - AlienVault HIDS: User authentication failed.	—	50106 - AlienVault HIDS: Database authentication failure.
108011 - AlienVault HIDS: Authentication Failed for user	—	50512 - AlienVault HIDS: Database authentication failure.
		51003 - AlienVault HIDS: Bad password attempt.
		20000000 - AlienVault HIDS-authentication_failed: Generic event
		2000000000 - AlienVault HIDS-authentication_failed: Generic ev...

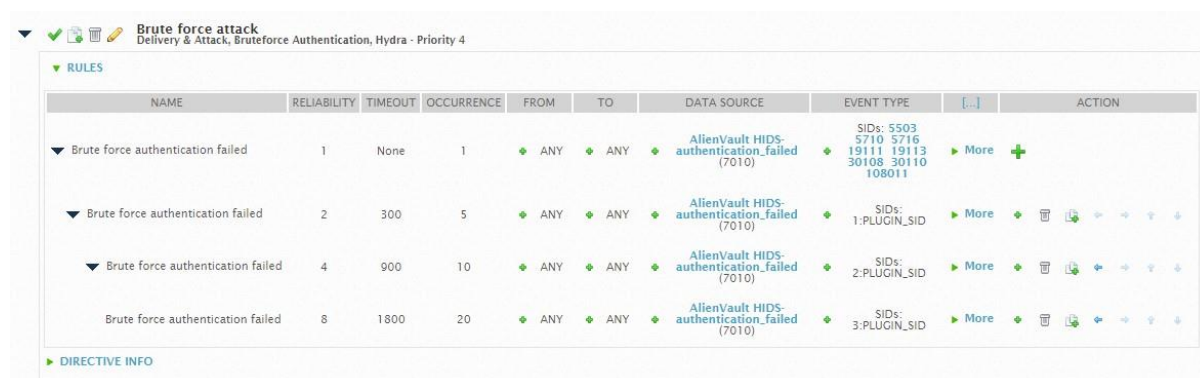
Empty selection means ANY signature

CANCEL BACK NEXT

Obrázok 9.7 Výber typov udalostí na klasifikovanie brute force útoku, zdroj vlastný

Zdrojové a cieľové *assets* sme nechali v predvolenej konfigurácii *ANY ANY*, čím sme zabezpečili klasifikáciu útoku na všetkých zariadeniach. Úvodnú spoľahlivosť sme definovali na úroveň *1*. Direktívu sme pridali tlačidlom *FINISH*.

Následne sme pridali záznamy s vyššou spoľahlivosťou klasifikácie útoku pri vyššom zaznamenaní neúspešných pokusov a prihlásenie časovým rozstupom.



Obrázok 9.8 Dodatočná konfigurácia pravidiel direktívy na brute force útok, zdroj vlastný

Na záver sme celú direktívu spustili obnovením všetkých direktív tlačidlom *Reload Directives*.

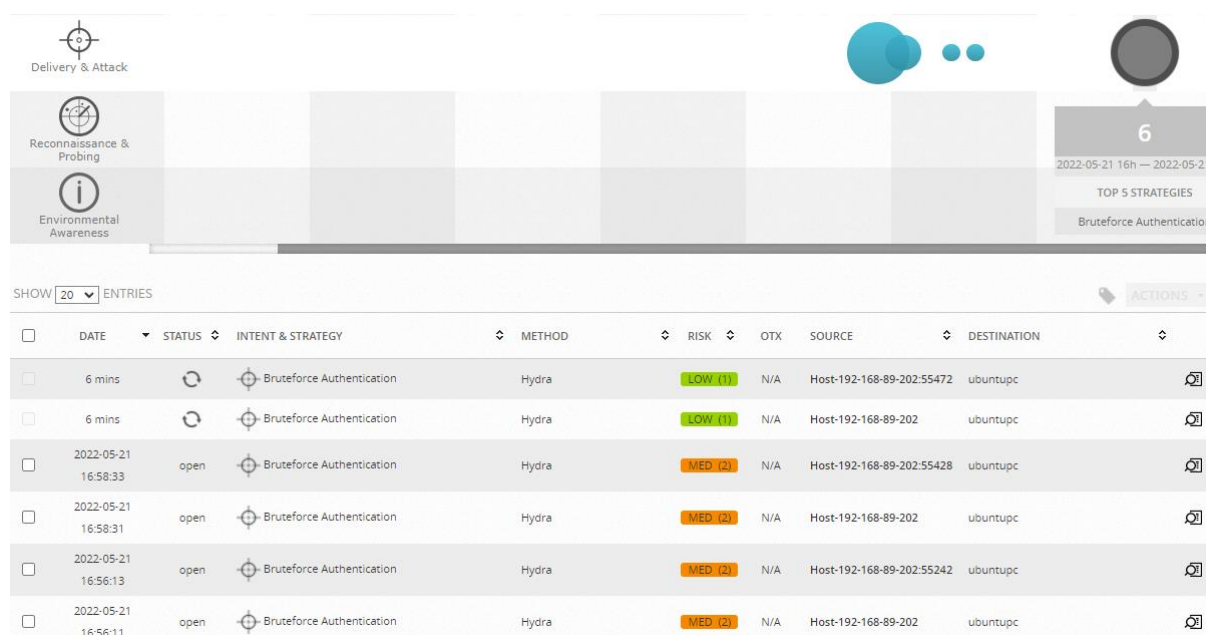
## Zopakovanie útoku

Útok sme zopakovali rovnakým spôsobom ako predtým pomocou aplikácie *hydra*. Útok sme rovnako spustili 100-krát za sebou. Po spustení útoku sme opäť mali možnosť vidieť pribúdajúce logy v nástroji AlienVault, ktorý zaznamenával neúspešné pokusy o prihlásenie na zariadenie *ubuntupc*. V tomto prípade už boli útoky klasifikované nami vytvorenou direktívou.

2022-05-21 16:56:15	AlienVault HIDS: SSHD authentication failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202:55244	ubuntupc
2022-05-21 16:56:13	AlienVault HIDS: SSHD authentication failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202:55242	ubuntupc
2022-05-21 16:56:13	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 16:56:13	directive_event: Brute force attack	2	directive_alert	N/A	N/A	Host-192-168-89-202:55242	ubuntupc
2022-05-21 16:56:11	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 16:56:11	directive_event: Brute force attack	2	directive_alert	N/A	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 16:56:09	AlienVault HIDS: Multiple SSHD authentication failures.	0	AlienVault HIDS-authentication_failures	alienvault	N/A	Host-192-168-89-202:55240	ubuntupc
2022-05-21 16:56:07	AlienVault HIDS: Multiple failed logins in a small period of time.	0	AlienVault HIDS-authentication_failures	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 16:56:07	AlienVault HIDS: SSHD authentication failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202:55238	ubuntupc
2022-05-21 16:56:03	AlienVault HIDS: SSHD authentication failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202:55236	ubuntupc
2022-05-21 16:56:03	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 16:56:01	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202	ubuntupc
2022-05-21 16:55:59	AlienVault HIDS: SSHD authentication failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202:55234	ubuntupc
2022-05-21 16:55:57	AlienVault HIDS: SSHD authentication failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202:55232	ubuntupc
2022-05-21 16:55:57	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	Host-192-168-89-202	ubuntupc

Obrázok 9.9 Zachytenie a klasifikovanie útoku nami vytvorenou direktívou, zdroj vlastný

V tomto prípade sa však podarilo útok klasifikovať a následne vytvoriť alarm, o ktorom sme boli informovaní aj prostredníctvom emailu.



Obrázok 9.10 Úspešne vytvorené alarmy počas útoku po upravení konfigurácie, zdroj vlastný

Vzhľadom na konfiguráciu direktívy a počet spustenia útoku až 100-krát bol zachytený a klasifikovaný až 6- krát. Zároveň týchto 6 zachytených útokov nám bolo doručených aj emailom, v ktorých môžeme vidieť, že alarmy boli vytvorené vo veľmi krátkom časovom rozmedzí.

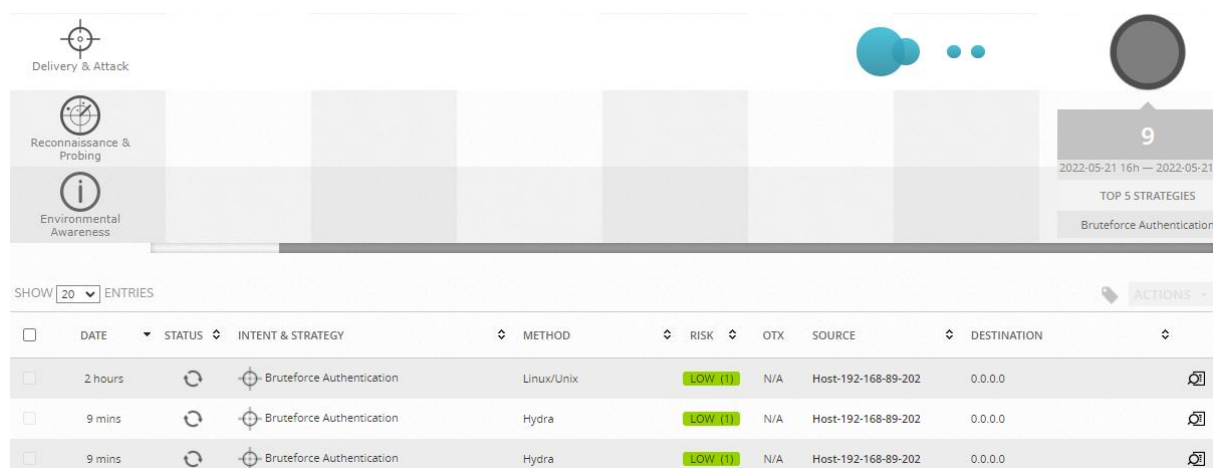
t_misutka	Event appears	High priority event appears to monitoring asset Date: 2022-05-21 16:59:27 [Europe/Prague], priority: 4, Risk: 1 Source IP: 192.168.89.202 : 55472 Destin: IP: 192.168.8...	16:59
t_misutka	Event appears	High priority event appears to monitoring asset Date: 2022-05-21 16:59:25 [Europe/Prague], priority: 4, Risk: 1 Source IP: 192.168.89.202 : 0 Destin: IP: 192.168.88.90 : ...	16:59
t_misutka	Event appears	High priority event appears to monitoring asset Date: 2022-05-21 16:58:33 [Europe/Prague], priority: 4, Risk: 2 Source IP: 192.168.89.202 : 55428 Destin: IP: 192.168.8...	16:58
t_misutka	Event appears	High priority event appears to monitoring asset Date: 2022-05-21 16:58:31 [Europe/Prague], priority: 4, Risk: 2 Source IP: 192.168.89.202 : 0 Destin: IP: 192.168.88.90 : ...	16:58
t_misutka	Event appears	High priority event appears to monitoring asset Date: 2022-05-21 16:57:11 [Europe/Prague], priority: 4, Risk: 1 Source IP: 192.168.89.202 : 55367 Destin: IP: 192.168.8...	16:57
t_misutka	Event appears	High priority event appears to monitoring asset Date: 2022-05-21 16:57:09 [Europe/Prague], priority: 4, Risk: 1 Source IP: 192.168.89.202 : 0 Destin: IP: 192.168.88.90 : ...	16:57

Obrázok 9.11 Klasifikovaný brute force útok doručený emailom, zdroj vlastný

## Útok na zariadenie ESXi

Útok na zariadenie ESXi s IP adresou 192.168.88.50, z ktorého sme dostávali logy do nástroja AlienVault prostredníctvom *remote logs*, sme previedli rovnakým spôsobom ako na zariadenie *ubuntupc*. Z nasledujúceho obrázka sme mohli vidieť, že útok sa podarilo rovnakým spôsobom klasifikovať a vyhodnotiť ako útok hrubou silou, ktorý prichádzal zo zariadenia s IP adresou 192.168.89.202. Ako cieľová IP adresa bola uvedená 0.0.0.0 a to z dôvodu, že zariadenie *ESXi* do logov nepridáva informáciu o cieľovom zariadení. Útok bol zaznamenaný dokonca viacerými direktívami, a to našou novo vytvorenou a aj predvolene vytvorenou.



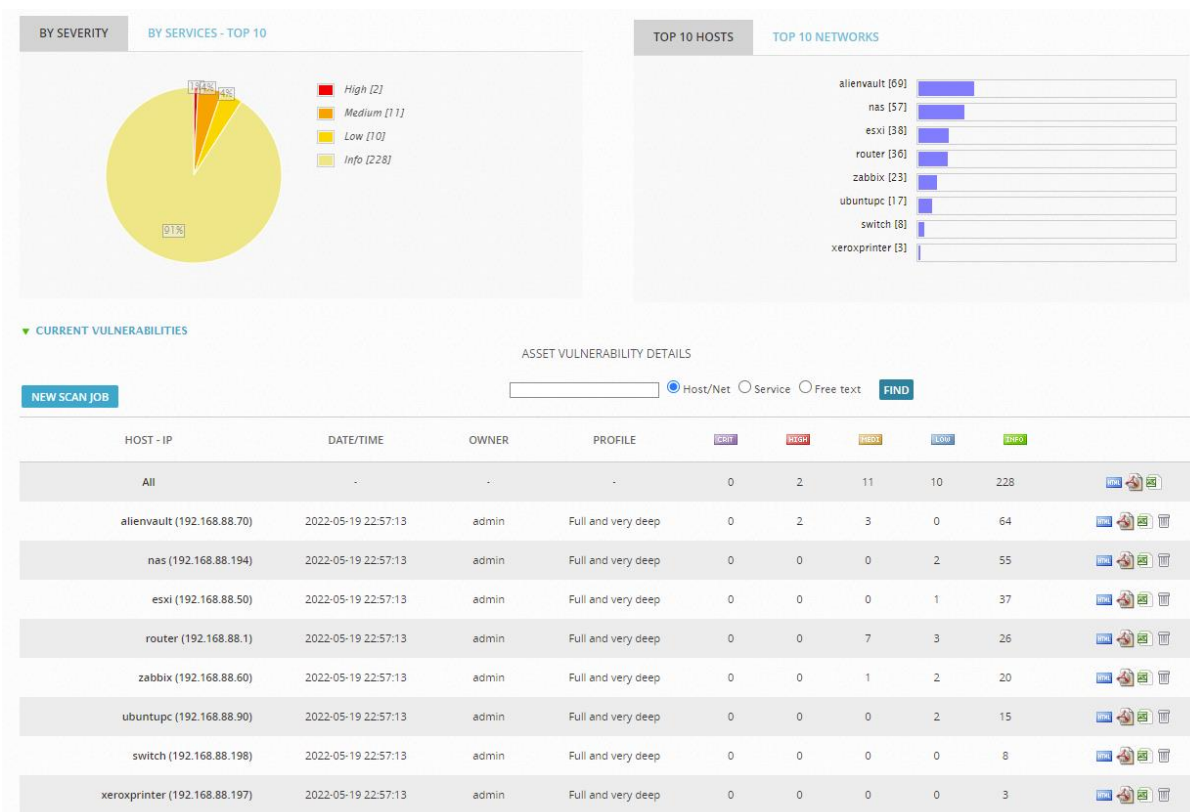


Obrázok 9.12 Zachytenie a klasifikácia brute force útoku na zariadenie ESXi, zdroj vlastný

### 9.1.3 Výsledky hľadania zraniteľností

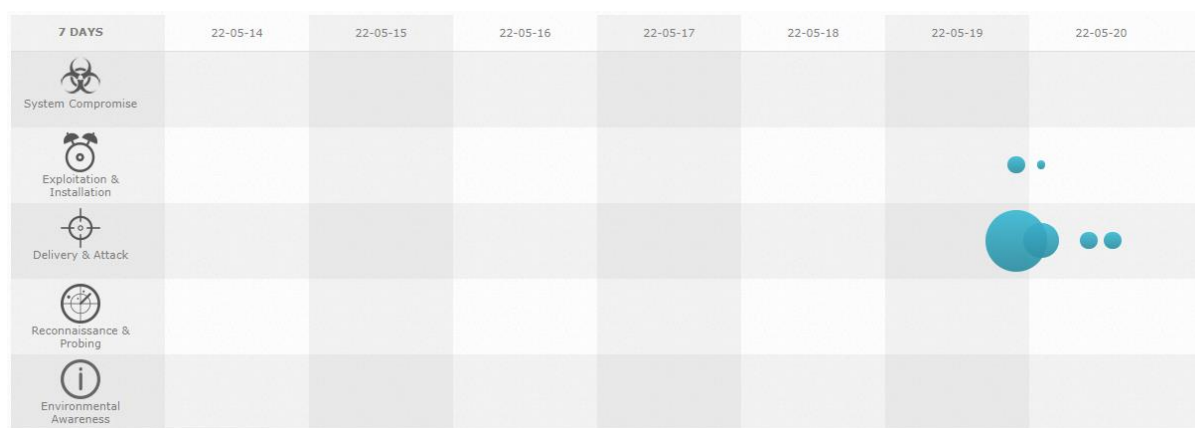
Hľadanie zraniteľností v sieti bolo zabezpečené 2 skenovaniami. Prvým skenovaním bolo úplné hlboké skenovanie cielené na celú testovaciu infraštruktúru a tým druhým skenovaním bolo úplné hlboké *ultimate* skenovanie cielené na serveri a sieťové prvky v sieti. Obe tieto skenovania trvali zhruba 80 minút a zraniteľnosti, ktoré boli objavené, boli veľmi podobné. Po ukončení skenovania sa nám zobrazil prehľadný report, kde sme mali možnosť vidieť, kde, koľko a aké dôležité zraniteľnosti boli objavené. Všetky tieto dáta boli zobrazené ako v tabuľkovej verzii, tak aj v stĺpcových a koláčových grafoch.

Detailný popis zraniteľností aj s odporúčaním, ako túto zraniteľnosť eliminovať, bolo možné vygenerovať aj v .pdf súbore prípadne si ho zobrazit prostredníctvom spôsobu *HTML* stránky. V týchto výsledkoch bolo možné vidieť, akým spôsobom sa dá zraniteľnosť zneužiť, akých OS sa to týka a podobne.



Obrázok 9.13 Výsledok skenovania zraniteľností určeného na všetky zariadenia, zdroj vlastný

Alarmy, ktoré boli vytvorené počas skenovania, môžeme pozrieť v časti *ANALYSIS / ALARMS*. Tabuľka spolu s farebne ohodnotenou prioritou prehľadne označovali dôležitosť a urgentnosť objavených zraniteľností. Objavené alarmy sú dostupné ako v tabuľkovej, tak aj v grafovej forme.

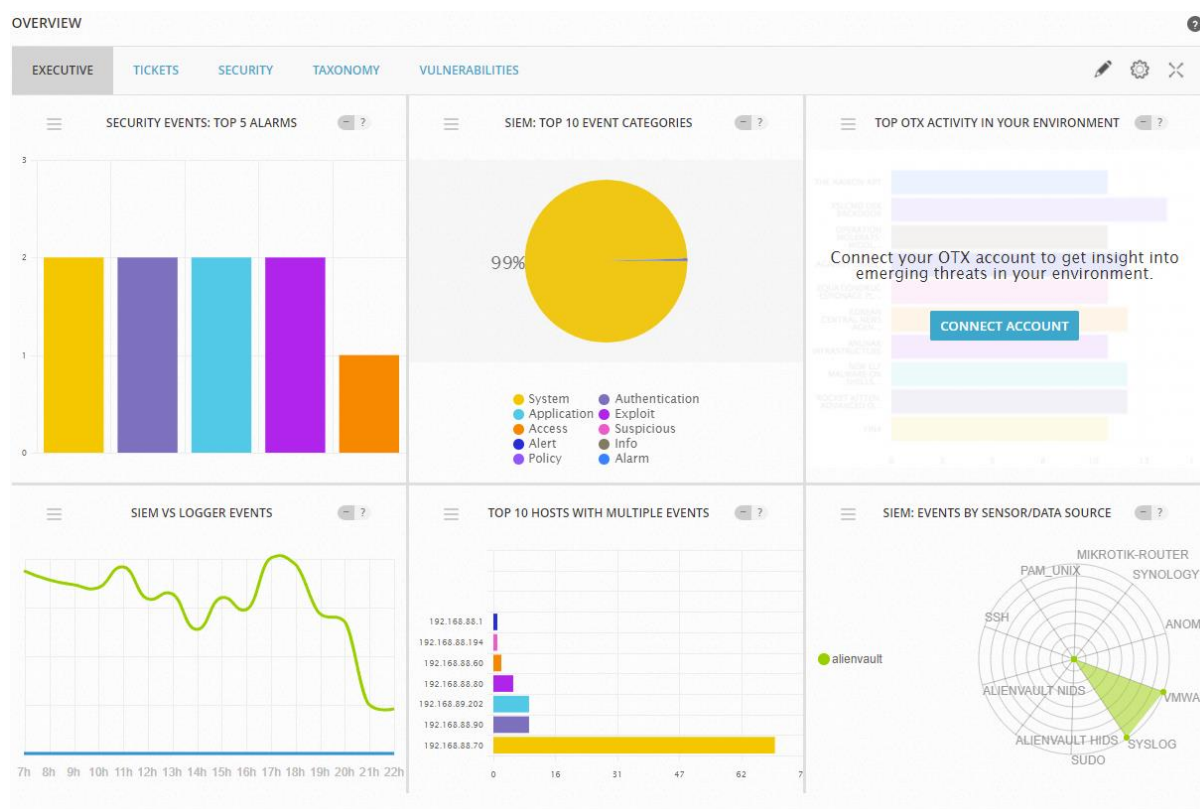


Obrázok 9.14 Grafické zobrazenie alarmov po hľadaní zraniteľností, zdroj vlastný

<input type="checkbox"/>	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION	
<input type="checkbox"/>	2022-05-20 12:55:30	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:56147	0.0.0.0:ssh	
<input type="checkbox"/>	2022-05-20 12:51:00	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:46371	ubuntupc	
<input type="checkbox"/>	2022-05-20 10:34:32	open	Bruteforce Authentication	Linux/Unix	CRITICAL (1)	N/A	alienvault	0.0.0.0	
<input type="checkbox"/>	2022-05-20 10:29:36	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:59525	ubuntupc	
<input type="checkbox"/>	2022-05-20 01:41:27	open	Bruteforce Authentication	Linux/Unix	CRITICAL (1)	N/A	alienvault	0.0.0.0	
<input type="checkbox"/>	2022-05-20 01:30:43	open	WebServer Attack	XSS	MED (2)	N/A	alienvault	ubuntupc	
<input type="checkbox"/>	2022-05-20 01:30:42	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	alienvault	ubuntupc	
<input type="checkbox"/>	2022-05-19 22:50:44	open	Bruteforce Authentication	Linux/Unix	MED (2)	N/A	alienvault	0.0.0.0	
<input type="checkbox"/>	2022-05-20 01:43:45	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:48287	alienvault	
<input type="checkbox"/>	2022-05-20 01:40:37	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:44779	0.0.0.0:ssh	
<input type="checkbox"/>	2022-05-19 22:46:11	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:55017	ubuntupc	
<input type="checkbox"/>	2022-05-19 22:44:51	open	WebServer Attack	XSS	MED (2)	N/A	alienvault	0.0.0.0	
<input type="checkbox"/>	2022-05-19 22:49:05	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:52381	0.0.0.0:ssh	
<input type="checkbox"/>	2022-05-19 22:44:33	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	alienvault	alienvault	
<input type="checkbox"/>	2022-05-19 22:36:59	open	WebServer Attack	XSS	MED (2)	N/A	alienvault	ubuntupc	
<input type="checkbox"/>	2022-05-19 22:36:59	open	WebServer Attack - SQL Injection	Attack Pattern Detection	MED (2)	N/A	alienvault	ubuntupc	
<input type="checkbox"/>	2022-05-19 22:36:48	open	Bruteforce Authentication	Linux/Unix	MED (2)	N/A	alienvault	0.0.0.0	
<input type="checkbox"/>	2022-05-19 22:22:02	open	Bruteforce Authentication	SSH	MED (2)	N/A	alienvault:47607	0.0.0.0	

Obrázok 9.15 Popis alarmov v tabuľkovej forme po hľadani zraniteľností, zdroj vlastný

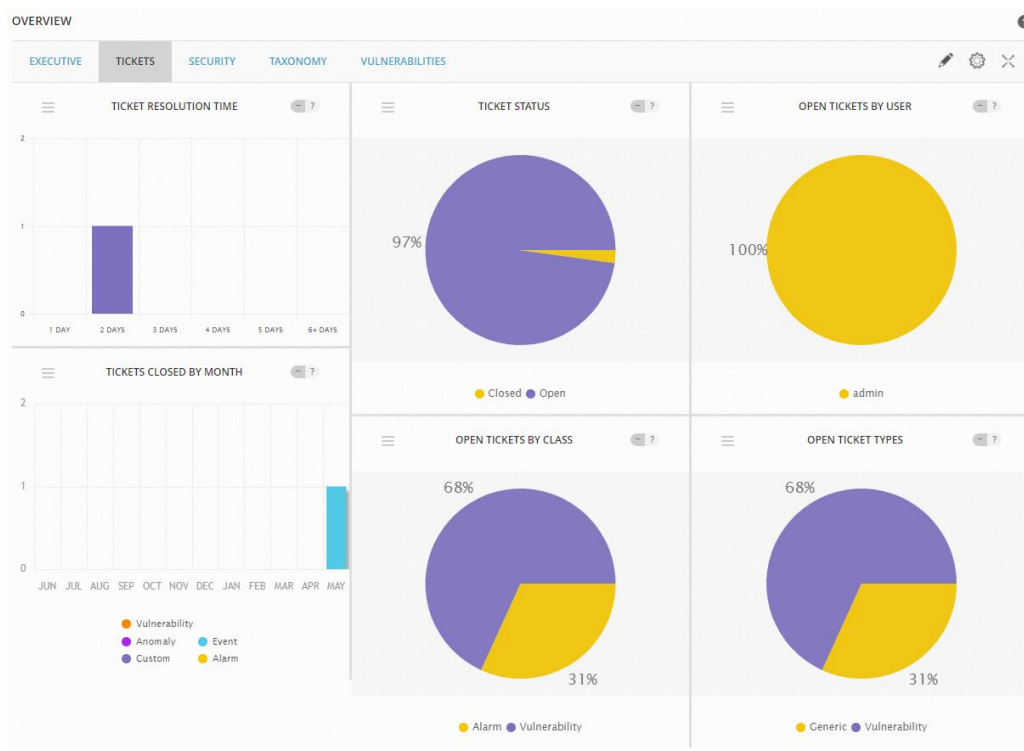
Zároveň sme mali možnosť vidieť, že po dokončení skenovania sa značne upravili aj grafy, ktoré boli dostupné v časti *DASHBOARD / OVERVIEW* v záložke *EXECUTIVE*.



Obrázok 9.16 Dashboard po skenovaní zraniteľností v sieti, zdroj vlastný

V tomto prehľadnom zobrazení sme mali možnosť vidieť niekoľko koláčových a stĺpcových grafov, ktoré zobrazovali najčastejšie sa vyskytujúce alarmy a udalosti, top 5 objavených najzávažnejších alarmov či aktuálny stav kombinácie logov s informáciami o *assetoch*, používateľoch, zraniteľnostiach a podobne.

V záložke *DASHBOARD / TICKETS* boli zobrazené tikety, ktoré boli vytvorené v dôsledku alarmov. Tikety boli zobrazené najmä prostredníctvom koláčových grafov. Zaujímavou časťou boli pre nás aj dáta v záložke *SECURITY*.



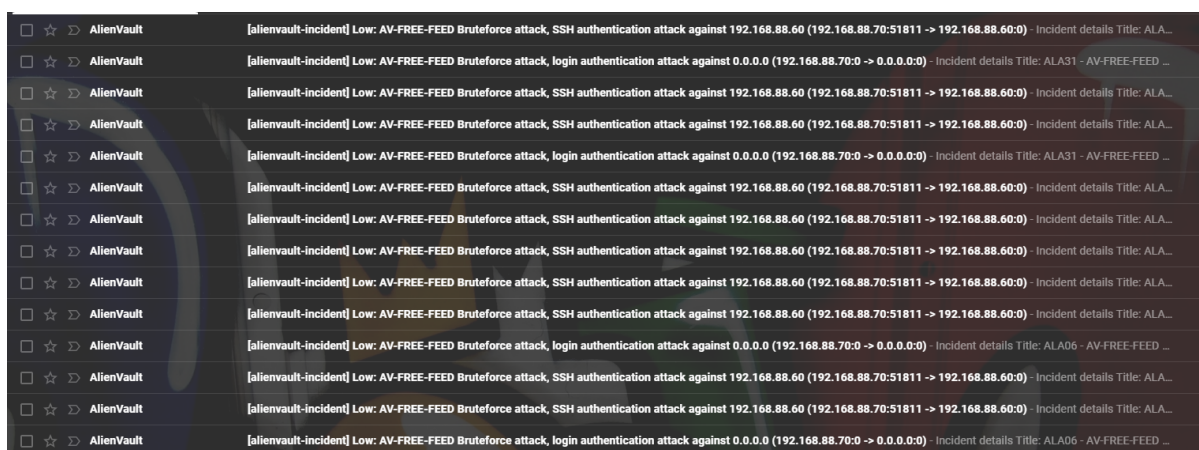
Obrázok 9.17 Koláčové grafy zobrazujúce štatistiky vytvorené tikety, zdroj vlastný



Obrázok 9.18 Prehľad dát zobrazených v grafoch, ktoré popisujú bezpečnosť, zdroj vlastný

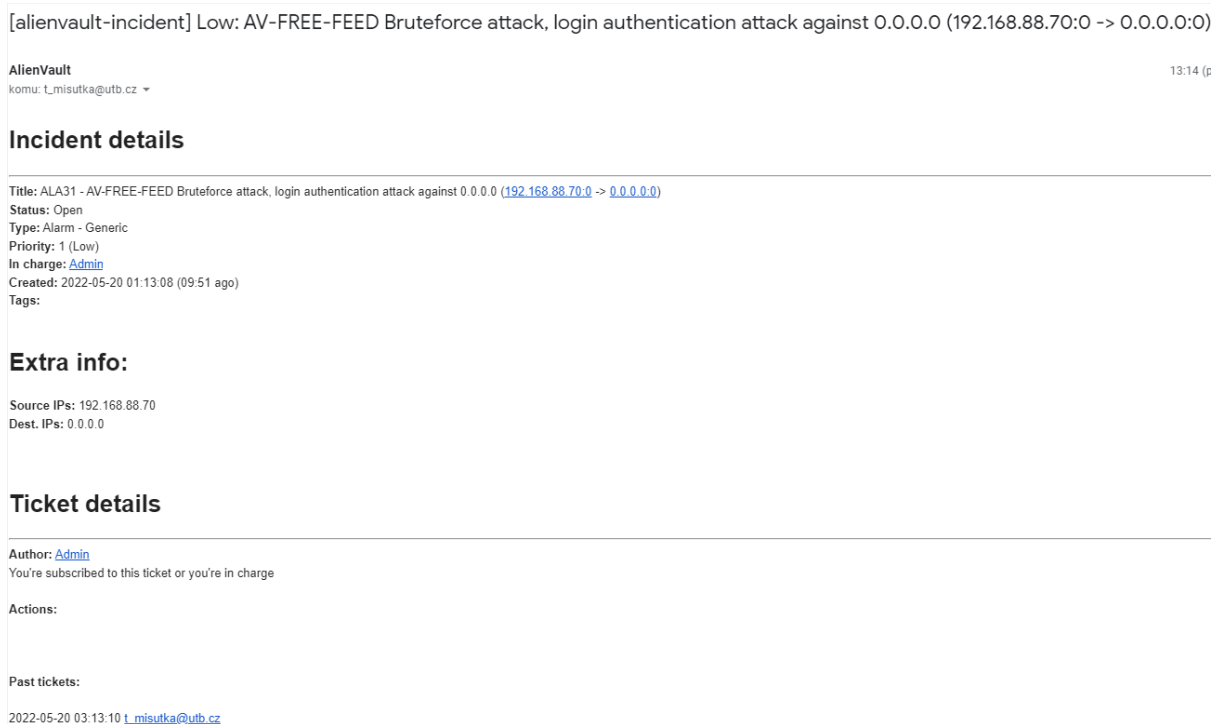
### 9.1.4 Overenie emailových notifikácií

V tejto časti sme si overili konfiguráciu notifikácií prostredníctvom emailov. Cieľom bolo pri novo vzniknutom alarme notifikovať administrátora prostredníctvom emailu, na ktorom sme použili školský účet *office365*. Na vygenerovanie alarmu sme použili jeden z nakonfigurovaných skenovaní zraniteľností v sieti. Všetky alarmy, ktoré sa počas skenovania objavili, boli doručené emailom, čo znamená, že konfigurácia bola prevedená úspešne.



Obrázok 9.19 Emailové notifikácie z nástroja AlienVault, zdroj vlastný

V detaile jedného z emailov sme mohli vidieť jeho konkrétnu štruktúru. Tá pozostávala z názvu incidentu, času vzniku, typu incidentu, priority, informácii o zdroji a cieľi incidentu a ďalšie.



Obrázok 9.20 Detail doručeného emailu z nástroja AlienVault, zdroj



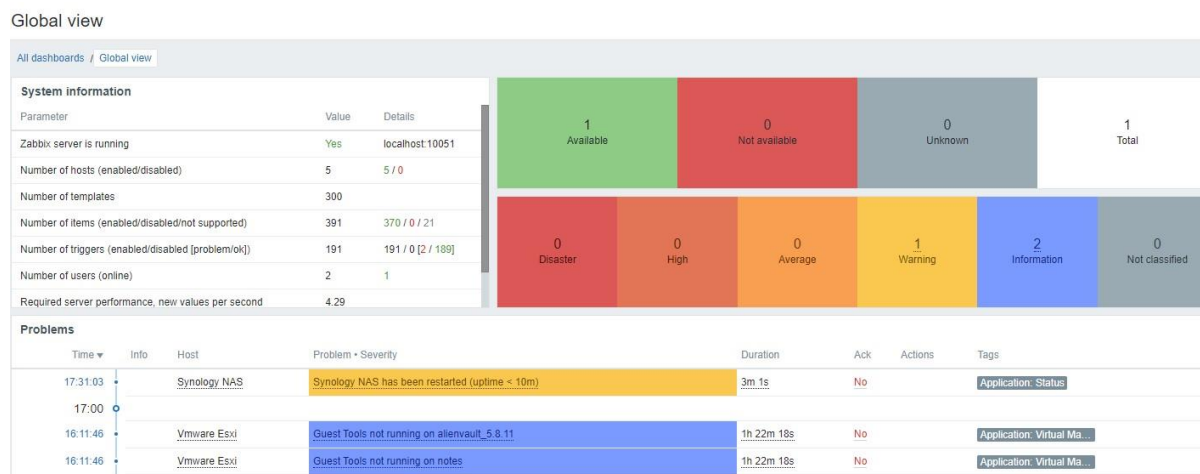
## 9.2 Overenie monitoringu nástrojom zabbix

V tejto časti sme overili funkčnosť implementácie nástroja zabbix. Jeho hlavnou úlohou bolo monitorovať vytťaženie a v určitých prípadoch aj dostupnosť zariadení v sieti prostredníctvom protokolu SNMP.

### 9.2.1 Signalizácia problémov

V tejto časti sme overili signalizáciu problémov, ktoré sa objavili na zariadeniach v testovacej infraštruktúre. Medzi problémy, ktoré sa zistili, boli napríklad notifikácie o zariadeniach. Tie boli monitorované menej ako 10 minút. Niektoré virtuálne zariadenia boli nedostupné, čo signalizovali nasledovné upozornenia.

Tieto problémy sa zobrazovali priamo v nástroji v časti *Monitoring / Dashboard*.



Obrázok 9.21 Dashboard signalizuje problémy zo zariadení, zdroj vlastný

V prípade, kedy by bolo problémov v sieti väčšie množstvo, zabbix poskytuje problémom vlastnú sekciu *Monitoring / Problems*, ktorá poskytuje možnosť použiť filter na rýchlejšie prehľadávanie a pohyb v problémoch. Dôležitou časťou medzi problémami je *Severity*, ktorá zobrazuje závažnosť problému a časť *Host* signalizuje, na ktorom zariadení sa problém vyskytol.

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
23:15:43	Warning		PROBLEM		Synology NAS	↓ Synology NAS has been restarted (uptime < 10m)	6m 40s	No		Application: Status
23:00										
16:11:46	Information		PROBLEM		Vmware Esxi	Guest Tools not running on alienvault_5.8.11	7h 10m 37s	No		Application: Virtual Ma
16:11:46	Information		PROBLEM		Vmware Esxi	Guest Tools not running on notes	7h 10m 37s	No		Application: Virtual Ma

Obrázok 9.22 Sekcia Problems zobrazuje objavené problémy s možnosťou filtrácie, zdroj vlastný

Zo zobrazených problémov sme mali možnosť zistiť, že dve virtuálne zariadenia v zariadení Vmware ESXi nie sú spustené. V prvej možnosti bola signalizácia zameraná na nástroj AlienVault, čo bol údaj správny, hoci v zariadení s názvom *notes* išlo o chybnú anomáliu, pretože toto zariadenie bolo vytvorené na zdieľanie prihlasovacích údajov.

## 9.2.2 Získavanie dát zo zariadení

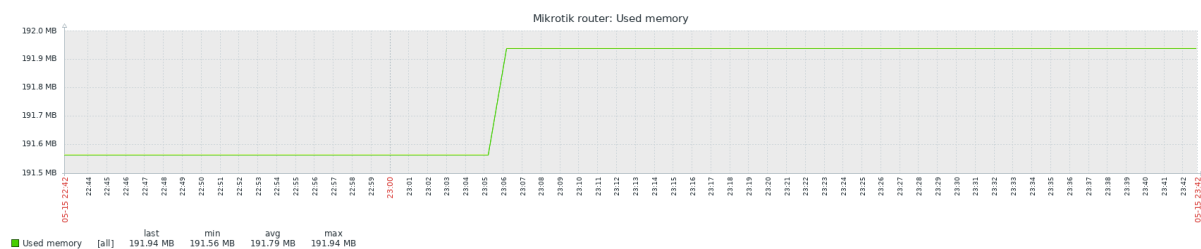
Dáta, ktoré boli získané zo zariadení, sme si mohli detailne prehliadať v časti *Monitoring / Latest data*. Dáta sa zobrazovali v prehľadnej tabuľke, kde sa nachádzali dáta o názve zariadenia, aktuálne monitorovanej položke, posledná získaná hodnota, tagy, dostupnosť grafu a podobne. Rovnako, ako aj iné časti nástroja zabbix bola aj ponuka filtrácie podľa rôznych možností.

Host	Name	Last check	Last value	Change	Tags	Info
<input type="checkbox"/> Mikrotik router	#1: CPU utilization	31s	0 %		component: cpu	Graph
<input type="checkbox"/> Mikrotik router	#2: CPU utilization	31s	0 %		component: cpu	Graph
<input type="checkbox"/> Mikrotik router	#3: CPU utilization	31s	0 %		component: cpu	Graph
<input type="checkbox"/> Mikrotik router	#4: CPU utilization	31s	0 %		component: cpu	Graph
<input type="checkbox"/> Synology NAS	/: Free inodes in %				component: storage filesystem:/	Graph
<input type="checkbox"/> Zabbix server	/: Free inodes in %	51s	92.5838 %		component: storage filesystem:/	Graph
<input type="checkbox"/> Synology NAS	/: Space utilization	22s	48.4513 %		component: storage filesystem:/	Graph
<input type="checkbox"/> Zabbix server	/: Space utilization	50s	43.8811 %	+0.005893 %	component: storage filesystem:/	Graph
<input type="checkbox"/> Zabbix server	/: Total space	49s	38.63 GB		component: storage filesystem:/	Graph
<input type="checkbox"/> Synology NAS	/: Total space	33s	2.28 GB		component: storage filesystem:/	Graph
<input type="checkbox"/> Synology NAS	/: Used space	33s	1.1 GB		component: storage filesystem:/	Graph
<input type="checkbox"/> Zabbix server	/: Used space	48s	16.08 GB	+2.2 MB	component: storage filesystem:/	Graph
<input type="checkbox"/> Synology NAS	/tmp: Free inodes in %				component: storage filesystem:/tmp	Graph
<input type="checkbox"/> Synology NAS	/tmp: Space utilization	21s	0.0496 %		component: storage filesystem:/tmp	Graph
<input type="checkbox"/> Synology NAS	/tmp: Total space	33s	1.9 GB		component: storage filesystem:/tmp	Graph
<input type="checkbox"/> Synology NAS	/tmp: Used space	33s	988 KB		component: storage filesystem:/tmp	Graph
<input type="checkbox"/> Synology NAS	/volume1: Free inodes in %				component: storage filesystem:/volume1	Graph
<input type="checkbox"/> Synology NAS	/volume1: Space utilization	20s	0.002039 %		component: storage filesystem:/volume1	Graph
<input type="checkbox"/> Synology NAS	/volume1: Total space	33s	7.21 TB		component: storage filesystem:/volume1	Graph
<input type="checkbox"/> Synology NAS	/volume1: Used space	33s	154.26 MB		component: storage filesystem:/volume1	Graph
<input type="checkbox"/> Vmware Esxi	Allocation units VMFS 3	29s	1048576		Application: Disk partit.	Graph
<input type="checkbox"/> Vmware Esxi	Allocation units VMFS 4	29s	1048576		Application: Disk partit.	Graph
<input type="checkbox"/> Synology NAS	Available memory	56s	3.44 GB	+2.08 MB	component: memory	Graph

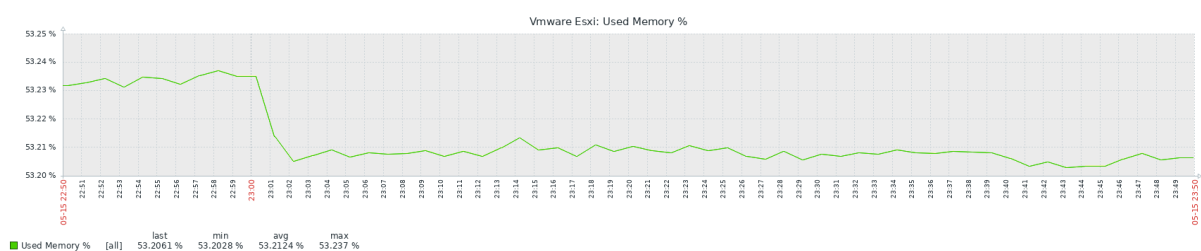
Obrázok 9.23 Získané dáta zo zariadení protokolom SNMP, zdroj vlastný



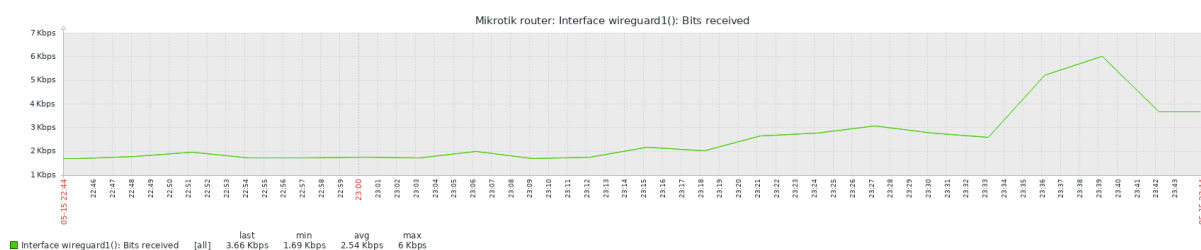
Grafy, ktoré boli dostupné z monitoringu zariadení sú zobrazené nižšie. Zamerali sme sa na zariadenia *mikrotik router* a *Vmware ESXi*, kde nás zaujímal stav pamäte oboch zariadení a na routri aj sieťová prevádzka na rozhraní pre VPN tunel. Narazili sme aj na problém, kde niektoré grafy neboli dostupné. Dôvodom bola nekompatibilita so zariadeniami.



Obrázok 9.24 Graf zobrazujúci použitie pamäte na zariadení mikrotik router, zdroj vlastný



Obrázok 9.25 Graf zobrazujúci percentuálnu časť použitia pamäte na Vmware Esxi, zdroj vlastný



Obrázok 9.26 Graf prijatých Bitov cez VPN na zariadení mikrotik router, zdroj vlastný

Dostupných dát bolo samozrejme ďaleko viac, zobrazené grafy vyššie boli hlavne ukážkou v možnostiach grafov nástroja zabbix.

### 9.2.3 Notifikácia o nedostupnosti

V tejto časti sme sa zamerali na overenie funkčnosti monitoringu a signalizácie administrátora prostredníctvom emailu. Signalizácia by prebehla v prípade, že zariadenie *Synology NAS* by nebolo dostupné.

Vzhľadom na fyzickú nedostupnosť k zariadeniu sme upravili podmienku nedostupnosti tak, aby nás informovala o dostupnosti zariadenia namiesto signalizácie o nedostupnosti. Časový interval bol nastavený na 5 minút, čo malo dôsledok, že v priebehu pár hodín sme mali

značne zaplnenú emailovú schránku. Funkčnosť však bola zachovaná, keďže sme vymenili len jednu z podmienok, ktorá bola práve opakom podmienky, ktorá kontrolovala nedostupnosť.

\* Name

Type of calculation Custom expression A and B

Label	Name	Action
A	Host IP equals 192.168.88.194	<a href="#">Remove</a>
B	Discovery status equals Up	<a href="#">Remove</a>
		<a href="#">Add</a>

Enabled ☒

\* At least one operation must exist.

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

Obrázok 9.27 Úprava podmienky na zisťovanie dostupnosti namiesto nedostupnosti, zdroj vlastný

Ako bolo spomenuté vyššie, podmienku sme zmenili iba na testovacie účely a po skončení testovacej fázy sme túto podmienku upravili do pôvodného stavu.

<input type="checkbox"/>	☆	➤	<b>Problem: Synology NAS has been restarted (uptime &lt; 10m)</b> - NOTE: Escalation canceled: action 'Report problems to Zabbix administrators' disabled. Last message sent: Problem star...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 57m 8s Device service name: *UNKNOWN*...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 57m 8s Device service name: ICMP ping D...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 52m 5s Device service name: *UNKNOWN*...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 52m 5s Device service name: ICMP ping D...
<input type="checkbox"/>	☆	➤	<b>Problem: Synology NAS has been restarted (uptime &lt; 10m)</b> - Problem started at 00:15:43 on 2022.05.16 Problem name: Synology NAS has been restarted (uptime < 10m) Host: Syno...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 47m 3s Device service name: *UNKNOWN*...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 47m 3s Device service name: ICMP ping D...
<input type="checkbox"/>	☆	➤	<b>Resolved in 11m 0s: Synology NAS has been restarted (uptime &lt; 10m)</b> - Problem has been resolved at 00:11:43 on 2022.05.16 Problem name: Synology NAS has been restarted (upti...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 42m 3s Device service name: *UNKNOWN*...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 42m 3s Device service name: ICMP ping D...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 37m 0s Device service name: *UNKNOWN*...
<input type="checkbox"/>	☆	➤	<b>Discovery: UP 192.168.88.194</b> - Discovery rule: nas discovery Device IP: 192.168.88.194 Device DNS: Device status: UP Device uptime: 12h 37m 0s Device service name: ICMP ping D...

Obrázok 9.28 Informovanie administrátora o dostupnosti zariadenia Synology NAS, zdroj vlastný

## 9.2.4 Overenie funkčnosti triggeru

Pri overení konfigurácie vlastného triggra sme očakávali, že ak sme postupovali v konfigurácii správne, mal by nás informovať o nedostatku papiera v tlačiarňi. Ihneď po nasadení trigra do šablóny a získaní aktuálnej hodnoty papiera v zásobníku bol vytvorený problém dôležitou *Avarage*, ktorý signalizoval nedostatok papiera v tlačiarňi. Týmto overením môžeme tvrdiť, že sme splnili požiadavky na monitoring tlačiarne. Úlohou šablóny, ktorá bola aplikovaná na tlačiarňi, bolo taktiež monitorovať hladinu tonera v tlačiarňi a v prípade nízkej hladiny tonera upozorniť na túto skutočnosť vytvorením problému. Rovnako aj túto skutočnosť je možné vidieť na nasledujúcom obrázku.

Time ▼	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
23:13:23	Average		PROBLEM		Xerox printer	Lack of papers in Tray 1	1m 9s	No	Application: Tray cure	
23:00:43	Warning	23:11:13	RESOLVED		Synology NAS	↓ Synology NAS has been restarted (uptime < 10m)	10m 30s	No	Application: Status	
23:00										
12:33:25	Information		PROBLEM		Xerox printer	↓ Low cartridge toner - black	10h 41m 7s	No	Application: Consuma...	Application: Printer inf...
Today										
2022-05-15 16:11:46	Information		PROBLEM		Vmware Esxi	Guest Tools not running on alienvault_5.8.11	1d 7h 2m	No	Application: Virtual Ma...	
2022-05-15 16:11:46	Information		PROBLEM		Vmware Esxi	Guest Tools not running on notes	1d 7h 2m	No	Application: Virtual Ma...	

Obrázok 9.29 Zoznam problémov obsahujúci problém vyvolaný vlastným triggrom, zdroj vlastný

## 10. VYHODNOTENIE RIEŠENIA

V závere práce bolo vhodné celkové riešenie vyhodnotiť, či bolo zadanie splnené a na aké problémy v súvislosti s konfiguráciou sme narazili.

Z hľadiska nástroja AlienVault OSSIM môžeme konštatovať, že zadanie bolo splnené, pretože sme si navrhnuté riešenie zároveň aj otestovali. Dokázali sme zachytiť útok skenovaním portov, aj keď len na jednom zariadení a na hľadanie príčiny, prečo sme neboli úspešní aj pri zvyšných zariadeniach nám nezvýšil čas, principiálne sme však zadanie splnili. Úspešnejší sme boli pri zachytení útoku hrubou silou, aj keď sme museli konfiguráciu počas testovacej fázy najskôr doplniť. Problémy, na ktoré sme narazili počas konfigurácie v tomto nástroji, boli spojené hlavne s menšou nestabilitou alebo objavenými chybami nástroja, kedy sme neboli schopní dokončiť určitú konfiguráciu alebo nástroj nečakane vyčerpal celú pridelenú pamäť a prestal byť dostupný. Kvôli týmto skutočnostiam sme museli nástroj niekoľkokrát preinštalovať, čo nás značne spomaľovalo vo vytváraní riešenia. Za malý nedostatok môžeme hodnotiť aj nedokonalú dokumentáciu, ktorá bola zlúčená pre našu verziu AlienVault OSSIM spolu s platenou verziou AlienVault USM. Zo získaných výsledkov však môžeme konštatovať, že zadanie bolo splnené a celkovo môžeme zvolený nástroj aj na vzniknuté problémy ohodnotiť veľmi pozitívne.

Naopak pri nástroji zabbix sme nenarazili na žiadnu nestabilitu systému alebo objavenú a neočakávanú chybu, ktorá by nám znemožnila postupovať v implementácii riešenia. Veľkou prednosťou tohto nástroja bola hlavne flexibilita, prehľadná dokumentácia, ktorá nám značne uľahčila implementáciu riešenia. Taktiež veľkou prednosťou tohto nástroja je grafické spracovanie, ktoré je veľmi užívateľsky prívetivé. Prevádzkový monitoring týmto nástrojom dokonale splnil požiadavky, a v testovacej fáze sme nenarazili na žiaden problém. Preto sme tento nástroj ohodnotili rovnako veľmi pozitívne, ako to bolo aj v prípade nástroja AlienVault OSSIM.

## ZÁVER

Detekcia zraniteľností a monitorovanie sieťovej prevádzky by sa mali stať neoddeliteľnou, a neustále sa zlepšujúcou súčasťou každej spoločnosti.

Z prieskumu nástrojov, ktorému sme venovali pozornosť v teoretickej časti tejto práce sme mohli vidieť, že v súčasnosti sa na trhu aktuálne nachádza nemalé množstvo nástrojov. V kombinácií správneho nástroja na detekciu zraniteľností a nástroja na prevádzkové monitorovanie siete môžeme vytvoriť plnohodnotné sledovanie sieťovej aktivity.

Cieľom tejto práce bolo navrhnúť a implementovať riešenie na detekciu zraniteľností a jej prevádzkový monitoring. Po analýze nástrojov sme dospeli k výberu dvoch vhodných kandidátov na implementáciu riešenia. O toto riešenie mala záujem externá firma, preto sme v spolupráci s ňou stanovili detailnejšie body zadania. V spolupráci s nimi sme pripravili v ich infraštruktúre testovací segment, kde sme mali možnosť navrhnuté riešenie implementovať a následne ho celé overiť. Počas implementácie sme narazili na niekoľko drobných problémov v nástroji AlienVault, ktoré môžu byť odstránené hlbšou analýzou problému logovania HIDS agentov.

Zo získaných výsledkov z praktickej časti môžeme konštatovať, že navrhnuté riešenie použitím nástroja AlienVault OSSIM a nástroja Zabbix sme splnili všetky požadované body, ktoré boli pridelené tejto práci.

## ZOZNAM POUŽITEJ LITERATÚRY

- [1] Dan Daniels, What is Network Infrastructure?, 06.03.2019, [cit. 21.04.2022], [online], dostupné na internete: <https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure/>
- [2] NÚKIB, 2022, [cit. 22.04.2022], [online], dostupné na internete: <https://nukib.cz/cs/o-nukib/>
- [3] NBÚ, Kybernetická bezpečnost, 10.04.2019, [cit. 22.04.2022], [online], dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html>
- [4] Digital Defense Inc, What Are The Most Common Types Of Network Vulnerabilities, 2022, [cit. 26.04.2022], [online], dostupné na internete: <https://www.digitaldefense.com/blog/what-are-the-most-common-types-of-network-vulnerabilities/>
- [5] Jason Firsch, Common Types Of Network Security Vulnerabilities In 2022, 23.09.2021, [cit. 26.04.2022], [online], dostupné na internete: <https://purplesec.us/common-network-vulnerabilities/>
- [6] Sam Cook, Malware statistics and facts for 2022, 18.02.2022, [cit. 28.04.2022], [online], dostupné na internete: <https://www.comparitech.com/antivirus/malware-statistics-facts/>
- [7] Purplesec, 2021, [cit. 29.04.2022], [online], dostupné na internete: <https://purplesec.us/resources/cyber-security-statistics/>
- [8] Avtest, Malware, 2022, [cit. 30.04.2022], [online], dostupné na internete: <https://www.av-test.org/en/statistics/malware/>
- [9] ESET, Ransomware, 2022, [cit. 30.04.2022], [online], dostupné na internete: <https://www.eset.com/sk/ransomware/>
- [10] Trellix, What is Ransomware, 2022, [cit. 30.04.2022], [online], dostupné na internete: <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html>
- [11] Portia Linao, How ransomware spreads: Uncovering infections methods, 01.02.2022, [cit. 30.04.2022], [online], dostupné na internete: <https://www.officesolution-sit.com.au/blog/how-ransomware-spreads#:~:text=Aside%20from%20attachments%2C%20phishing%20emails,network%20and%20infect%20other%20data>
- [12] MXTOOLBOX, What is Email Phishing?, 11.01.2018, [cit. 30.04.2022], [online], dostupné na internete: <https://blog.mxtoolbox.com/2018/01/11/what-is-email-phishing/comment-page-1/>
- [13] Jareth, How ransomware spreads: 9 most common infection methods and how to stop them, 19.12.2019, [cit. 30.04.2022], [online], dostupné na internete:

<https://blog.emsisoft.com/en/35083/how-ransomware-spreads-9-most-common-infection-methods-and-how-to-stop-them/>

[14] Jan Kopriva, SANS ISC InfoSec Forums, 31.10.2019, [cit. 30.04.2022], [online], dostupné na internetu: <https://isc.sans.edu/forums/diary/EML+attachments+in+O365+a+recipe+for+phishing/25474/>

[15] imperva, Malvertising, 2021, [cit. 01.05.2022], [online], dostupné na internetu: <https://www.imperva.com/learn/application-security/malvertising/>

[16] Antonio Challita, The four most popular methods hackers use to spread ransomware, 08.03.2022, [cit. 01.05.2022], [online], dostupné na internetu: <https://www.itpropertal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/>

[17] Michael Kan, Ransomware Hits Research Facility After Student Installs Pirated Software, 06.05.2021, [cit. 01.05.2022], [online], dostupné na internetu: <https://www.pcmag.com/news/ransomware-hits-research-facility-after-student-installs-pirated-software>

[18] ška, mos, iDNES.cz, ČTK, Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty, 13.03.2020, [cit. 01.05.2022], [online], dostupné na internetu: [https://www.idnes.cz/brno/zpravy/brno-nemocnice-fakultni-nemocnice-kyberneticky-utok.A200313\\_071531\\_brno-zpravy\\_bur](https://www.idnes.cz/brno/zpravy/brno-nemocnice-fakultni-nemocnice-kyberneticky-utok.A200313_071531_brno-zpravy_bur)

[19] ČTK, Kyberútok způsobil brněnské fakultní nemocnici škody v desítkách milionů korun, 17.04.2020, [cit. 01.05.2022], [online], dostupné na internetu: <https://zpravy.aktualne.cz/domaci/kyberutok-zpusobil-brnenske-fakultni-nemocnici-skody-v-desit/r~2608ab6c808411ea9d470cc47ab5f122/>

[20] Petr Čačík, CI Oddělení systému FN Brno, 12.-13.3.2020, [cit. 01.05.2022], [online], dostupné na internetu: [https://www.cacio.cz/Frontend/Webroot/uploads/files/2022/02/3\\_kyberneticky\\_utok\\_na\\_fn\\_brno360.pdf](https://www.cacio.cz/Frontend/Webroot/uploads/files/2022/02/3_kyberneticky_utok_na_fn_brno360.pdf)

[21] Michal Kovář, Daniela Tauberová, Kyberútok na olomoucký magistrát , agendy úřadů jsou mimo provoz, 07.04.2021, [cit. 02.05.2022], [online], dostupné na internetu: [https://olomoucky.denik.cz/zpravy\\_region/kyberutok-magistrat-olomouc-hacker-napadeni-2021.html](https://olomoucky.denik.cz/zpravy_region/kyberutok-magistrat-olomouc-hacker-napadeni-2021.html)

[22] Petra Špičková, Kriminalisté odložili případ kyberútoku na olomouckou datovou síť, 17.02.2022, [cit. 02.05.2022], [online], dostupné na internetu: <https://ct24.ceskatelevize.cz/regiony/3443586-kriminaliste-odlozili-pripad-kyberutoku-na-olomouckou-datovou-sit>

[23] Jana Magdoňová, Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné, 22.05.2021, [cit. 02.05.2022], [online], dostupné na internetu:

[https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ranso-mware-avaddon\\_2105221133\\_ako](https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ranso-mware-avaddon_2105221133_ako)

[24] ČTK, Národní knihovnu v noci napadli hackeři, pro veřejnost je uzavřena, 19.5.2021, [cit. 02.05.2022], [online], dostupné na internetu: <https://prazsky.denik.cz/zlociny-a-so-udy/narodni-knihovna-hacker-kyberutok-knihy-pujcka-databaze.html>

[25] Národní knihovna České republiky, Kybernetický útok na Národní knihovnu ČR, 22.02.2022, [cit. 02.05.2022], [online], dostupné na internetu: [https://www.cacio.cz/Frontend/Webroot/uploads/files/2022/02/2\\_kyberneticky\\_utok\\_na\\_nk\\_cr-aktualizace359.pdf](https://www.cacio.cz/Frontend/Webroot/uploads/files/2022/02/2_kyberneticky_utok_na_nk_cr-aktualizace359.pdf)

[26] Zoznam/nia, Hackeri napadli slovenskú televíziu: Odstavili vysielanie... Rieši to polícia v troch štátoch!, 23.11.2020, [cit. 02.05.2022], [online], dostupné na internetu: <https://www.topky.sk/cl/100313/2010133/AKTUALNE-Hackeri-napadli-slovensku-televiziu-Odstavili-vysielanie---Riesi-to-policia-v-troch-statoch->

[27] Dan Milmo, Russia unleashed data-wiper malware on Ukraine, say cyber experts, 24.02.2022, [cit. 02.05.2022], [online], dostupné na internetu: <https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts>

[28] Dan Milmo, Russia unleashed data-wiper malware on Ukraine, say cyber experts, 24.02.2022, [cit. 02.05.2022], [online], dostupné na internetu: <https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts>

[29] Threat Intelligence Team, HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine, 04.03. 2022, [cit. 02.05.2022], [online], dostupné na internetu: <https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/>

[30] Jonathan Greig, Government and researchers keep US attention on Russia's cyber activity in Ukraine, 28.04.2022, [cit. 02.05.2022], [online], dostupné na internetu: <https://therecord.media/government-and-researchers-keep-us-attention-on-russias-cyber-activity-in-ukraine/>

[31] Daryna Antoniuk, A deeper look at the malware being used on Ukrainian targets, 21.04.2022, [cit. 02.05.2022], [online], dostupné na internetu: <https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/>

[32] Michael Dereviashkin, NEW ANALYSIS: THE CADDYWIPER MALWARE ATTACKING UKRAINE, 05.04.2022, [cit. 03.05.2022], [online], dostupné na internetu: <https://blog.morphisec.com/caddywiper-analysis-new-malware-attacking-ukraine>

[33] ESET, IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine, 04.03.2022, [cit. 03.05.2022], [online], dostupné na internetu: <https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/>



- [34] UNITRENDS, How Ransomware Works, 2022, [cit. 03.05.2022], [online], dostupné na internete: <https://www.unitrends.com/solutions/ransomware-education>
- [35] AT&T Business, AlienVault OSSIM is Trusted by Thousand of Security Professionals in 140 Countries, 2022, [cit. 05.05.2022], [online], dostupné na internete: <https://cybersecurity.att.com/products/ossim>
- [36] Greenbone Networks GmbH, OpenVAS Vulnerability Assessment Scanner, 2022, [cit. 05.05.2022], [online], dostupné na internete: <https://www.openvas.org/>
- [37] New Net Technologies LLC, GREENBONE SECURITY MANAGER (GSM), 2022, [cit. 05.05.2022], [online], dostupné na internete: <https://www.newnettechnologies.com/greenbone-security-manager.html>
- [38] ITperfection.com, What is NESSUS and How Does it Work?, 2020, [cit. 06.05.2022], [online], dostupné na internete: <https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scanning-security-data-windows-unix-linux/>
- [39] Nagios.org, What is Nagions?, 2022, [cit. 08.05.2022], [online], dostupné na internete: <https://www.nagios.org/about/>
- [40] David Taylor, Nagios Tutorial, What is Nagios Tool? Architecture & Installation, 30.04.2022, [cit. 08.05.2022], [online], dostupné na internete: <https://www.guru99.com/nagios-tutorial.html>
- [41] Educba, What is Zabbix?, 2022, [cit. 10.05.2022], [online], dostupné na internete: <https://www.educba.com/what-is-zabbix/>
- [42] Rajesh Kumar, What is Zabbix and use of it?, 23.05.2021, [cit. 10.05.2022], [online], dostupné na internete: <https://www.devopsschool.com/blog/what-is-zabbix-and-use-of-it/>

**ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK**

ACL	Access Control List
API	Application Programming Interface
C&C	Command & Control
CPU	Central Processing Unit
DDoS	Distributed Denial-of-Service
DLL	Dynamic-link Library
DoS	Denial-of-Service
FQDN	Fully Qualified Domain Names
HDD	Hard Drive Disk
HIDS	Host Instruction Detection System
HTML	Hypertext Markup Language
IoT	Internet of Things
IP	Internet Protocol
LTS	Long-Term Support
NAS	Network-attached storage
NBÚ	Národní Bezpečnostný Úřad
NÚKIB	Národní Úřad pre Kybernetickú a Informačnú Bezpečnosť
NVT	Network Vulnerability Test
OID	Object Identifier
OpenVAS	Open Vulnerability Assessment Scanner
OS	Operating System
OSI	Open System Interconnection
OSSIM	Open-Source Security Information Management
OTX	Open Threat Exchange

---

PC	Personal Computer
PDF	Portable Document Format
PE	Portable Executable
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RFC	Replication Factor C
SIEM	Security Information and Event Management
SMB	Server Message Block
SOC	Security Operations Center
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
UX	User Experience
VPN	Virtual Private Network
WMI	Windows Management Instrumentation

## ZOZNAM OBRÁZKOV

Obrázok 2.1 Infraštruktúra spoločnosti, zdroj vlastný .....	17
Obrázok 3.1 Nárast malvéru počas obdobia od roku 2009 až 2018, zdroj [7] .....	20
Obrázok 3.2 Aktuálne hodnoty vzoriek malvérov za posledných 5 rokov, zdroj [8] .....	21
Obrázok 3.3 Ukážka infikovanej prílohy s využitím platobnej brány PayPal, zdroj: [12] .....	23
Obrázok 3.4 Falošná URL adresa, kde útočník vyzýva svoju obeť na okamžité prihlásenie sa do platobnej brány PayPal, zdroj: [14] .....	24
Obrázok 4.1 Úvodná stránka v nástroji AlienVault OSSIM, zdroj vlastný .....	34
Obrázok 4.2 Dáta zachytené prostredníctvom SIEM v nástroji AlienVault OSSIM, zdroj vlastný .....	35
Obrázok 4.3 Správa a aplikácia agentov na koncové zariadenia v nástroji AlienVault OSSIM, zdroj vlastný .....	35
Obrázok 4.4 Možnosti reportov v nástroji AlienVault OSSIM, zdroj vlastný .....	36
Obrázok 4.5 Všeobecné konfiguračné možnosti v nástroji AlienVault OSSIM, zdroj vlastný .....	36
Obrázok 4.6 Progres skúšobného skenovania v nástroji AlienVault OSSIM, zdroj vlastný ...	37
Obrázok 4.7 Výsledok skúšobného testu zraniteľností v nástroji AlienVault OSSIM, zdroj vlastný .....	37
Obrázok 4.8 Dashboard po spustení nástroja Greenbone, zdroj vlastný .....	39
Obrázok 4.9 Prehľad výsledkov zraniteľností v nástroji Greenbone, zdroj vlastný .....	39
Obrázok 4.10 Možnosti správy certifikátov v nástroji Greenbone, zdroj vlastný .....	40
Obrázok 4.11 Detaily zraniteľností NVTs dostupné v nástroji Greenbone, zdroj vlastný .....	40
Obrázok 4.12 Progres skúšobného skenovania zraniteľností v nástroji Greenbone, zdroj vlastný .....	41
Obrázok 4.13 Výsledok skúšobného skenovania zraniteľností v nástroji Greenbone, zdroj vlastný .....	42
Obrázok 4.14 Úvodná stránka nástroja Nessus, zdroj vlastný .....	43
Obrázok 4.15 Možnosti sledovania stavu skenera v nástroji Nessus, zdroj vlastný .....	44
Obrázok 4.16 Progres skúšobného skenovania zraniteľností v nástroji Nessus, zdroj vlastný .....	44
Obrázok 4.17 Výsledok skúšobného skenovania zraniteľností v nástroji Nessus, zdroj vlastný .....	45
Obrázok 5.1 Graf zobrazujúci princíp, ktorým pracujú plugíny v nástroji Nagios, zdroj [40] .....	48
Obrázok 5.2 Úvodná obrazovka nástroja Nagios, zdroj vlastný .....	49

Obrázok 5.3 Kategória v nástroji Nagios, ktorá zobrazuje objavené problémy v službách, zdroj vlastný .....	50
Obrázok 5.4 Report vytvorený na základe histórie alarmov v nástroji Nagios, zdroj vlastný	50
Obrázok 5.5 Bezpečnosť a autentifikácia medzi komponentami zabbix-u, zdroj [42].....	52
Obrázok 5.6 Dashboard ako úvodná obrazovka nástroja zabbix, zdroj vlastný .....	53
Obrázok 5.7 Zachytenie posledných monitorovaných dát nástrojom zabbix, zdroj vlastný ...	54
Obrázok 5.8 Prehľad využívania hardvérových prostriedkov v nástroji zabbix, zdroj vlastný .....	54
Obrázok 5.9 Report z monitoringu dostupnosti zariadenia zabbix server, zdroj vlastný .....	55
Obrázok 5.10 Ponuka konfigurácie rôznych sociálnych médií v nástroji zabbix, zdroj vlastný .....	56
Obrázok 5.11 Voľne dostupné šablóny na rôzne zariadenia a služby v nástroji zabbix, zdroj vlastný .....	57
Obrázok 6.1 Testovacia inštalácia v externej spoločnosti, zdroj vlastný .....	60
Obrázok 7.1 Úvodná obrazovka inštalácie AlienVault, zdroj vlastný .....	63
Obrázok 7.2 Sieťová konfigurácia v vo vlastnej infraštruktúre AlienVault, zdroj vlastný .....	63
Obrázok 7.3 Vytvorenie hesla pre používateľa root – AlienVault, zdroj vlastný.....	64
Obrázok 7.4 AlienVault - vytvorenie účtu admin pomocou grafického rozhrania, zdroj vlastný .....	65
Obrázok 7.5 Ubuntu sieťové nastavenia vo vlastnej infraštruktúre, zdroj vlastný .....	66
Obrázok 7.6 Konfigurácia databázy serverovej časti zabbix, zdroj vlastný .....	67
Obrázok 7.7 Konfigurácia databázy cez management zabbix-u, zdroj vlastný .....	68
Obrázok 7.8 Zabbix - zmena predvolených administrátorských údajov, zdroj vlastný .....	69
Obrázok 8.1 Pridanie testovacej siete v nástroji ALIENVAULT, zdroj vlastný .....	72
Obrázok 8.2 Pridanie zariadení do nástroja AlienVault, zdroj vlastný.....	73
Obrázok 8.3 Pridanie zariadení do skupín, zdroj vlastný .....	73
Obrázok 8.4 Konfigurácia HIDS agentov v nástroji AlienVault, zdroj vlastný .....	74
Obrázok 8.5 Generovanie binárneho súboru pre inštaláciu HIDS agenta s OS Windows, zdroj vlastný .....	75
Obrázok 8.6 Konfigurácia IP adresy HIDS servera na zariadeniach s OS Linux, zdroj vlastný .....	76
Obrázok 8.7 Zobrazenie unikátneho kľúča HIDS agenta pre zariadenie zabbix, zdroj vlastný .....	76
Obrázok 8.8 Priradenie unikátneho kľúča HIDS agenta do zariadenia, zdroj vlastný .....	77

Obrázok 8.9 Konfigurácia posielania logov na vzdialený server zo zariadenia router, zdroj vlastný .....	79
Obrázok 8.10 Pravidlá na posielanie logov na vzdialený server na zariadení router, zdroj vlastný .....	80
Obrázok 8.11 Konfigurácia posielania vzdialených logov na zariadení Synology NAS, zdroj vlastný .....	81
Obrázok 8.12 Monitoring dostupnosti zariadení je v stave UP, zdroj vlastný .....	82
Obrázok 8.13 Monitoring dostupnosti portov na zariadení nas, zdroj vlastný .....	83
Obrázok 8.14 Konfigurácia Email Relay, zdroj vlastný .....	84
Obrázok 8.15 Konfigurácia akcie, ktorá vyvolá odoslanie emailu, zdroj vlastný .....	85
Obrázok 8.16 Konfigurácia politiky pre kritické zariadenie Synology NAS, zdroj vlastný ...	86
Obrázok 8.17 Konfigurácia politiky na serveri, ktorá zabezpečí odoslanie emailu, zdroj vlastný .....	87
Obrázok 8.18 Konfigurácia pravidelného prehľadávania testovacej infraštruktúry, zdroj vlastný .....	88
Obrázok 8.19 Konfigurácia pravidelného skenovania kritických zariadení, zdroj vlastný .....	90
Obrázok 8.20 Povolenie netflow na zariadení mikrotik router, zdroj vlastný .....	91
Obrázok 8.21 Konfigurácia odoslania netflow zachytený na routri, zdroj vlastný .....	92
Obrázok 8.22 Konfigurácia senzoru na prijímanie netflow z routra, zdroj vlastný .....	93
Obrázok 8.23 Prijímanie sieťovej prevádzky z routra cez netflow, zdroj vlastný .....	93
Obrázok 8.24 Top 10 zdrojových zariadení zachytených prostredníctvom netflow, zdroj vlastný .....	94
Obrázok 8.25 Konfigurácia direktívy na vytvorenie alarmu pri útoku skenovaním portov, zdroj vlastný .....	95
Obrázok 8.26 Konfigurácia SNMP na zariadení mikrotik router, zdroj vlastný .....	97
Obrázok 8.27 Konfigurácia SNMP na zariadení mikrotik switch, zdroj vlastný .....	98
Obrázok 8.28 Konfigurácia SNMPv3 na zariadení Synology NAS, zdroj vlastný .....	100
Obrázok 8.29 Konfigurácia SNMP na tlačiarni Xerox, zdroj vlastný .....	101
Obrázok 8.30 Konfigurácia SNMP na zariadení ESXi, zdroj vlastný .....	103
Obrázok 8.31 Zariadenia z infraštruktúry monitorované protokolom SNMP, zdroj vlastný	104
Obrázok 8.32 Konfigurácia emailov, zdroj vlastný .....	105
Obrázok 8.33 Testovací email z nástroja zabbix, zdroj vlastný .....	106
Obrázok 8.34 Doručené správy z nástroja zabbix do súkromnej emailovej schránky, zdroj vlastný .....	107

Obrázok 8.35 Definícia pravidla na zisťovanie dostupnosti zariadenia NAS, zdroj vlastný.	108
Obrázok 8.36 Definícia akcie pri zisťovaní dostupnosti zariadenia NAS, zdroj vlastný .....	108
Obrázok 8.37 Definícia operácie pri zisťovaní dostupnosti zariadenia NAS, zdroj vlastný .	109
Obrázok 8.38 Konfigurácia itemu na monitorovanie maximálneho množstva papiera v zásobníku 1, zdroj vlastný.....	110
Obrázok 8.39 Konfigurácia itemu na monitorovanie aktuálneho množstva papiera v zásobníku 1, zdroj vlastný.....	111
Obrázok 8.40 Konfigurácia SNMP agenta v softvéri MIB Browser, zdroj vlastný .....	112
Obrázok 8.41 Hodnoty SNMP OID získané prostredníctvom softvéru MIB browser, zdroj vlastný .....	112
Obrázok 8.42 Pridanie itemov do šablóny, zdroj vlastný .....	112
Obrázok 8.43 Vytvorenie trigra v šablóne pre tlačiareň, zdroj vlastný .....	113
Obrázok 8.44 Trigger pridaný k ostatným v šablóne, zdroj vlastný .....	113
Obrázok 9.1 Testovacia infraštruktúra na overenie implementácie, zdroj vlastný .....	114
Obrázok 9.2 Logy so zachyteným skenovaním portov, zdroj vlastný .....	115
Obrázok 9.3 Vytvorený alarm po útoku skenovaním portov, zdroj vlastný .....	116
Obrázok 9.4 Brute force útok aplikáciou hydra spustený 100 krát v cykle for , zdroj vlastný .....	116
Obrázok 9.5 Logy z nástroja AlienVault počas brute force útoku, zdroj vlastný.....	117
Obrázok 9.6 Progres útoku hrubou silou pomocou aplikácie hydra, zdroj vlastný .....	117
Obrázok 9.7 Výber typov udalostí na klasifikovanie brute force útoku, zdroj vlastný .....	118
Obrázok 9.8 Dodatočná konfigurácia pravidiel direktívy na brute force útok, zdroj vlastný	119
Obrázok 9.9 Zachytenie a klasifikovanie útoku nami vytvorenou direktívou, zdroj vlastný	119
Obrázok 9.10 Úspešne vytvorené alarmy počas útoku po upravení konfigurácie, zdroj vlastný .....	120
Obrázok 9.11 Klasifikovaný brute force útok doručený emailom, zdroj vlastný.....	120
Obrázok 9.12 Zachytenie a klasifikácia brute force útoku na zariadenie ESXi, zdroj vlastný .....	121
Obrázok 9.13 Výsledok skenovania zraniteľností určeného na všetky zariadenia, zdroj vlastný .....	122
Obrázok 9.14 Grafické zobrazenie alarmov po hľadaní zraniteľností, zdroj vlastný .....	122
Obrázok 9.15 Popis alarmov v tabuľkovej forme po hľadaní zraniteľností, zdroj vlastný ...	123
Obrázok 9.16 Dashboard po skenovaní zraniteľností v sieti, zdroj vlastný .....	124
Obrázok 9.17 Koláčové grafy zobrazujúce štatisticky vytvorené tikety, zdroj vlastný.....	125

Obrázok 9.18 Prehľad dát zobrazených v grafoch, ktoré popisujú bezpečnosť, zdroj vlastný .....	125
Obrázok 9.19 Emailové notifikácie z nástroja AlienVault, zdroj vlastný .....	126
Obrázok 9.20 Detail doručeného emailu z nástroja AlienVault, zdroj .....	126
Obrázok 9.21 Dashboard signalizuje problémy zo zariadení, zdroj vlastný.....	127
Obrázok 9.22 Sekcia Problems zobrazuje objavené problémy s možnosťou filtrácie, zdroj vlastný .....	128
Obrázok 9.23 Získané dáta zo zariadení protokolom SNMP, zdroj vlastný.....	128
Obrázok 9.24 Graf zobrazujúci použitie pamäte na zariadení mikrotik router, zdroj vlastný .....	129
Obrázok 9.25 Graf zobrazujúci percentuálnu časť použitia pamäte na Vmware Esxi, zdroj vlastný .....	129
Obrázok 9.26 Graf prijatých Bitov cez VPN na zariadení mikrotik router, zdroj vlastný ....	129
Obrázok 9.27 Úprava podmienky na zisťovanie dostupnosti namiesto nedostupnosti, zdroj vlastný .....	130
Obrázok 9.28 Informovanie administrátora o dostupnosti zariadenia Synology NAS, zdroj vlastný .....	130
Obrázok 9.29 Zoznam problémov obsahujúci problém vyvolaný vlastným triggrom, zdroj vlastný .....	131



## **ZOZNAM TABULIEK**

Tabuľka 1 Zoznam pluginov, ktoré sa aplikovali na jednoltivé zariadenia, zdroj vlastný ..... 78

## **ZOZNAM PRÍLOH**

Príloha A: Diplomová práca vo formáte .pdf.

Príloha B: Export konfigurácie z nástroja AlienVault

Príloha C: Export konfigurácie z nástroja Zabbix