Návrh praktické úlohy pro potřeby kybernetické laboratoře

Bc. Matěj Križan

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Matěj Križan**
Osobní číslo:	**L22416**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Rizikové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Návrh praktické úlohy pro potřeby kybernetické laboratoře**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Identifikujte vhodné oblasti výcviku pro potřeby kybernetické bezpečnosti.
3. Detailně navrhněte obsah laboratorní úlohy.
4. Ověřte aplikovatelnost navržené laboratorní úlohy.

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

Seznam doporučené literatury:

1. BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. *Cybersecurity Essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.
2. EVANS, Lester. *Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, the Internet of Things + an Esential Guide to Ethical Hacking for Beginners*. USA: Lester Evans, 2019. ISBN 9781794647237.
3. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8. Dostupné také z: https://knihy.nic.cz/files/edice/cybersecurity.pdf.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2023**
Termín odevzdání diplomové práce: **26. dubna 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou 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);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 26.4.2024

Jméno a příjmení studenta: Bc. Matěj Križan

.....
podpis studenta

ABSTRAKT

Cílem práce bylo navrhnout praktickou úlohu pro potřeby kybernetické laboratoře. V této navržené úloze jde o nalezení hesla. Docíleno je toho za pomoci nástroje Hydra. V práci je zmíněno, jak vytvořit silné heslo a jak pracovat s nástrojem Hydra včetně postupu. Postup v práci je vypsán krok po kroku. Dále je zde zmíněno, co za rizika vychází z procvičování této navržené úlohy. Práce obsahuje i alternativní způsob, jak nástroj Hydra zprovoznit a použít. V práci je vypsána i možnost zavedení úlohy do výuky a vysvětleny termíny, které byly použity v úloze nebo jsou potřeba znát při jejím procvičování.

Klíčová slova: Hydra, heslo, útok hrubou silou, operační systém, kybernetická bezpečnost, hacking, etický hacking

ABSTRACT

The goal of the work was to design a practical task for the needs of a cybernetics laboratory. In this suggested task the objective is to find the password. This is achieved with the help of Hydra tool. In this thesis it is mentioned how to create a strong password and how to work with Hydra tool including the procedure. The procedure in the thesis is listed step by step. Furthermore, it is mentioned what are the risks involved in practicing this proposed task. The thesis also includes an alternative way to get the Hydra tool working and how to use it. The thesis also describes the possibility of introducing the task into the classroom and explains the terms that have been used in the task or are needed to know when practicing it.

Keywords:Hydra, password, brute force attack, operating system, cybersecurity, hacking, ethical hacking

Zde bych chtěl poděkovat panu Ing. Petru Svobodovi, Ph.D. za provedené konzultace, cenné rady a nápady. Dále bych chtěl poděkovat všem, kteří mě podporovali při tvorbě práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V současné době se stále narůstajícím vývojem technologií, se většina věcí přesouvá do kyberprostoru. Z tohoto důvodu je potřeba poukázat na nebezpečí, které hrozí při jeho používání. Nebezpečí hrozící do jisté míry každé osobě je úzce spojeno s hesly, které si u svých účtů vytvářejí. Znát postup útočníka je velmi pomocná informace pro osoby, které si chtějí zvýšit bezpečnost svého hesla. Práce tedy obsahuje informace o heslech a nástroje používané na zjištění hesla, mimo jiné i základní informace o kyberprostoru, kybernetické bezpečnosti, operačních systémech a kryptografii, která blízce souvisí s hesly. Cílem diplomové práce je navrhnout úlohu pro potřeby kybernetické laboratoře. Téma úlohy bylo probráno s vedoucím práce. Po výběru z možností byl jejich počet snížen a stačilo vybrat možnost, která bude nejlépe zapadat k studijnímu oboru a zároveň bude užitečná. Vybraným návrhem tedy bylo za použití aplikací a příkazového řádku zprovoznit Kali Linuxa použít nástroj nazývaný Hydra, o kterém je pojednáváno z velké části diplomové práce. V současné době příkazový řádek Kali Linux a nástroj Hydra využívají nejčastěji hackeři, hobbisté a osoby začínající s hackingem.

Problematika hesel je neustále řešena a jejich bezpečnost je zlepšována, a to hlavně za pomoci podmínek, které jsou pro tvorbu hesla na určitých webových stránkách neustále přísnější (např. minimální počet znaků byl dříve zhruba 6 a dnes je to 8), ale závisí na každé webové stránce a jejím nastavení.

V současné době stále slýcháme z médií o ztrátě finančních prostředků z účtů způsobem sociálního inženýrství, která jsou nejčastější formou zjištění přihlašovacího jména a hesla. O hackerských útocích se v médiích skoro nemluví, protože to není zajímavé téma, ale mělo by se o tom více mluvit, aby byli lidé více opatrnější při tvorbě hesla.

Snad poznatky z diplomové práce pomohou lidem, zvláště starší generaci, kteří nejsou tak dobře neznají nebezpečí, které může slabé heslo pro zabezpečení účtů přinést.

Pevně věřím, že diplomová práce vytvoří přínos do blízké budoucnosti tím, že se lidstvo naučí bezpečně využívat kybernetických technologií, naučí se tvořit silnější a bezpečnější hesla pro zabezpečení všech svých účtů. Zároveň si díky této diplomové práci mohou odzkoušet pohled ze strany hackera, kterému se v dnešní době daří díky kreativnímu myšlení a schopnostem programování nabourat do účtů osob a organizací skrze zjištění hesla.

CÍL PRÁCE A POUŽITÉ METODY

V této kapitole je představen hlavní cíl práce a následně její specifické dílčí cíle. To, čím se bude práce zabývat, je vymezeno materiály, které jsou v ní obsaženy. Tato kapitola také pojednává o jednotlivých metodách pro zpracování diplomové práce, které autor použil a kterými se řídil.

Hlavní cíl:

- Navrhnout praktickou úlohu pro potřebu výuky v rámci kybernetické laboratoře Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Dílčí cíle:

- Pojednat o souvisejících teoretických východiscích práce.
- Identifikovat vhodnou praktickou úlohu a vytvořit její zadání.
- Zpracovat příkladový postup k naplnění zadání.
- Pojednat o souvisejících teoretických východiscích práce.
- Identifikovat vhodnou praktickou úlohu a vytvořit její zadání.
- Zpracovat příkladový postup k naplnění zadání.

Použité metody v diplomové práci

- Literární rešerše – metoda použita v teoretické části při hledání a výběru zdrojů diplomové práce.
- Analýza– metoda použita v praktické části, kapitole Posouzení rizik vycházejících z úlohy v podobě checklist, what if a FMEA metod.
- Dedukce– metoda byla použita ve více částích práce, ale nejvíce v kapitolách Počáteční kroky diplomové práce, Konzultace a Možnost zavedení do výuky.

I. TEORETICKÁ ČÁST

1 KYBERPROSTOR

Kyberprostor označuje virtuální počítačový svět, konkrétně elektronické médium, které se používá k usnadnění online komunikace. Kyberprostor obvykle zahrnuje rozsáhlou počítačovou síť tvořenou mnoha celosvětovými počítačovými podsítěmi, které využívají protokol TCP/IP („Transmission Control Protocol over Internet“) k usnadnění komunikace a výměny dat.

Kyberprostor umožňuje uživatelům sdílet informace, vzájemně komunikovat, vyměňovat si názory, hrát hry, účastnit se diskusí nebo společenských fór, podnikat a vytvářet intuitivní média a mnoho dalších činností.

Termín kyberprostor původně představil William Gibson ve své knize Neuromancer z roku 1984. V pozdějších letech Gibson tento termín kritizoval a označil ho za "sugestivní a v podstatě nesmyslný". Přesto se tento termín stále hojně používá k označení jakéhokoli zařízení nebo funkce, které jsou spojeny s internetem. Lidé tímto termínem označují všechny možné druhy virtuálních rozhraní, která vytvářejí digitální realitu.

Jeden ze způsobů, jak hovořit o kyberprostoru, souvisí s využíváním globálního internetu k různým účelům, od obchodu po zábavu. Všude tam, kde zúčastněné strany zřizují virtuální prostory pro své schůzky, se setkáváme s existencí kyberprostoru. Dalo by se říci, že všude, kde se používá internet, vzniká kyberprostor. Hojné využívání stolních počítačů i chytrých telefonů k přístupu na internet znamená, že v praktickém (a zároveň poněkud teoretickém) smyslu kyberprostor roste.

Dalším ukázkovým příkladem kyberprostoru jsou online herní platformy, které jsou inzerovány jako masivní online ekosystémy pro hráče. Tyto velké komunity, kde hrají všichni společně, vytvářejí své vlastní kyberprostory, které existují pouze v digitální sféře, a nikoli ve fyzickém světě.

Pro skutečné uvážení toho, co kyberprostor znamená a co to je, je třeba si uvědomit, co se stane, když tisíce lidí, kteří se mohli v minulosti sejít ve fyzických místnostech, aby hráli hru, to místo toho dělají tak, že se každý dívá do zařízení z míst, která jsou od sebe vzdálená. Když provozovatelé her vyzdobí rozhraní tak, aby bylo atraktivní a přitažlivé, v jistém smyslu vnášejí do kyberprostoru interiérový design (Rouse, 2023).

1.1 Kybernetická bezpečnost

Kybernetická bezpečnost odkazuje obecně na schopnost kontrolovat přístup k síťovým systémům a informacím, které obsahují. Jestliže jsou ovládací prvky kybernetické bezpečnosti účinné, je kybernetický prostor považován za spolehlivou, odolnou a důvěryhodnou digitální infrastrukturu. Tam, kde kontroly kybernetické bezpečnosti chybí, jsou neúplné nebo nesprávně navržené, je kyberprostor považován za divoký západ digitálního věku. Dokonce i ti, kteří pracují v oblasti bezpečnosti, budou mít na kybernetickou bezpečnost odlišný pohled v závislosti na aspektech kyberprostoru, se kterými osobně přicházejí do styku. Nechť je systémem fyzické zařízení (budova) nebo soubor komponent kyberprostoru, úkolem odborníka v oblasti bezpečnosti, který je tomuto systému přidělen, je plánovat a připravit se na možný útok a jeho následky (Bayuk et al, 2022, s. 1).

Mezinárodní telekomunikační unie ("The International Telecommunication Union", ITU) definuje kybernetickou bezpečnost jako "soubor nástrojů, politik, bezpečnostních koncepcí, bezpečnostních opatření, pokynů, přístupů k řízení rizik, opatření, školení, nejlepších postupů, záruk a technologií, které lze použít k ochraně kybernetického prostředí a majetku organizace a uživatelů". Aktiva organizace a uživatele zahrnují připojená počítačová zařízení, personál, infrastrukturu, aplikace, služby, telekomunikační systémy a celek přenášených a/nebo uložených informací v kybernetickém prostředí. Kybernetická bezpečnost se snaží zajistit dosažení a udržení bezpečnostních vlastností aktiv organizace a uživatele proti odpovídajícím bezpečnostním rizikům v kybernetickém prostředí." Podle ITU obecné bezpečnostní cíle kybernetické bezpečnosti zahrnují dostupnost, integritu a důvěrnost (Kshetri, 2022, s. 9).

1.1.1 Triáda CIA

Triáda CIA je základním principem v oblasti bezpečnosti informací. Tento nástroj slouží k tomu, aby pomohl odborníkovi v oblasti informační bezpečnosti přemýšlet o tom, jak nejlépe chránit data organizace.

Důvěrnost: Má co do činění s tím, zda jsou informace označeny za tajné nebo soukromé. Je třeba využít mechanismy, jako je šifrování, které způsobí, že data budou nepoužitelná, pokud by k nim byl získán přístup neoprávněným způsobem.

Integrita: Souvisí s tím, zda jsou informace uchovávány v přesné podobě a jsou pravdivé. Informace by neměly být měněny neoprávněným jednáním a měla by být zavedena taková ochranná opatření, která umožní včas zjistit neoprávněné změny.

Dostupnost: To souvisí se zajištěním toho, aby informace byly k dispozici, když jsou potřeba. Tato úroveň řízení může být dosažena zavedením různých nástrojů, od záložních baterií v datovém centru až po distribuci obsahu v cloudové síti. (Death, 2017)

Každé písmeno v triádě CIA reprezentuje základní princip v oblasti kybernetické bezpečnosti. Důležitost bezpečnostního modelu hovoří sama za sebe: Důvěrnost, integrita a dostupnost jsou považovány za tři nejdůležitější pojmy v oblasti informační bezpečnosti.

Zohlednění těchto tří principů společně v rámci modelu triády je vodítkem pro tvorbu a vývoj bezpečnostních politik organizací. Při vyhodnocování potřeb a případů použití pro potenciální nové produkty a technologie pomáhá tento model triády organizacím klást cílené otázky o tom, jaká je hodnota poskytovaná v těchto třech klíčových oblastech (CIA triad, 2023).

1.1.2 Kybernetický útok

Kybernetický útok může provést jediný hacker nebo skupina hacktivistů (slovní spojení hackerů a aktivistů), stejně jako celá organizace. Útoky mohou být součástí státem sponzorované kybernetické války s politickými motivy nebo kyberterorismu různých nestátních aktérů a teroristických skupin. Hackeři se obvykle snaží vylákat peníze a požadují za ně výkupné, které se v zájmu ochrany identity platí nejlépe v Bitcoinech (kryptoměna).

Sofistikovanost kybernetických útoků v poslední době vzrostla a nyní představují větší hrozbu pro národní bezpečnost. Útoky mohou být vedeny z různých důvodů, včetně sabotáže, špionáže, krádeže, podvodu, hacktivismu a dalších (Kybernetický útok, 2022).

Existuje více typů definice kybernetického útoku. Všechny definice vystihují kybernetický útok, ale jsou jinak frázovány, proto jich je zde uvedeno více pro lepší pochopení.

Definice:

Jakýkoli druh škodlivé činnosti, která se pokouší shromáždit, narušit, znehodnotit nebo zničit prostředky informačního systému nebo samotné informace.

Útok prostřednictvím kyberprostoru, cílený na využívání kyberprostoru společností za účelem narušení, znefunkčnění, zničení nebo škodlivého ovládání výpočetního prostředí/infrastruktury; nebo zničení integrity dat či odcizení kontrolovaných informací.

Pokus o získání neoprávněného přístupu k systémovým službám, zdrojům nebo informacím či pokus o narušení integrity, dostupnosti nebo důvěrnosti systému.

Akce prováděné prostřednictvím počítačových sítí s cílem narušit, odepřít, znehodnotit nebo zničit informace uchovávané v počítačích a počítačových sítích nebo samotné počítače a sítě. Poznámka: V rámci DoD, Joint Publication 3-13, "Information Operations", bylo 27. listopadu 2012 schváleno odstranění termínů a definic útoku na počítačovou síť (CNA), obrany počítačové sítě (CND), zneužití počítačové sítě a operací v počítačové síti (CNO) z JP -1-02, "Department of Defense Dictionary of Military Terms and Associated Terms". Tento termín a definice již nejsou v JP 1-02 publikovány. Tato publikace je základním terminologickým zdrojem při přípravě korespondence, včetně dokumentů týkajících se zásad, strategie, doktrín a plánovacích dokumentů. Termíny se již nepoužívají ve vydáních aktualizovaných v rámci DoD. JP 1-02 po vydání JP 3-12 "Cyberspace Operations" uvádí nové termíny a definice, jako jsou kyberprostor, operace v kyberprostoru, nadřazenost v kyberprostoru, obranná odezvová akce v kyberprostoru, obranné operace v kyberprostoru, operace v informační síti ministerstva obrany a útočné operace v kyberprostoru (NIST, 2024).

1.2 Kybernetická hrozba

Termín " cyber" jako předpona se datuje od roku 1940 a poprvé byl použit v konceptu "cybernetics", který se týkal komunikačních a řídicích rozhraní mezi živými bytostmi a stroji. Od tohoto data se termín hojně používá v souvislosti s futuristickými technologiemi (Lee, 2023, s. 3).

V padesátých letech bránilo rozvoji kybernetiky nepříznivé politické prostředí v Československu. V důsledku toho se zájemci o toto téma mohli stýkat pouze v soukromých debatních skupinách. Stálými účastníky těchto "kybernetických kroužků" byli docent A. Svoboda, profesor J. Charvát a profesor V. Vondráček, který byl v té době přednostou psychiatrické kliniky na pražské lékařské fakultě. Díky uvolnění politických poměrů vyústila iniciativa této skupiny v roce 1958 v ustavení Komise pro kybernetiku Československé akademie věd. Tato skupina se později v roce 1966 přejmenovala na

Československou kybernetickou společnost (Historie výpočetní techniky v Československu).

Hrozby lze nalézt v tradičních oblastech jako je země, moře a vzduch. Tyto hrozby jsou různorodé povahy, od nepřátelských protivníků, kteří se snaží způsobit újmu, přes nepříznivé povětrnostní podmínky, které mohou poškodit lodě nebo letadla, až po prosté geografické prvky, jako jsou horská pásma, která mohou blokovat cesty.

V tomto ohledu se kyberprostor neliší. V této nové oblasti mohou působit nepřátelští aktéři, operace mohou omezovat fyzické vlastnosti infrastruktury a softwarové instalace se mohou měnit stejně často jako počasí (Lee, 2023, s. 4).

Kybernetická bezpečnostní hrozba je škodlivá činnost spáchaná s cílem zničit, ukrást nebo narušit data, kritické systémy a digitální život obecně. Příkladem těchto rizik jsou počítačové viry, útoky malwaru, narušení dat a útoky typu Denial of Service (DoS). S rostoucí závislostí na technologiích tato nebezpečí v oblasti kybernetické bezpečnosti pokročila a stala se více rozšířenými, což představuje značné riziko pro osoby a podniky. Pochopení rizik kybernetických hrozeb je prvním krokem k obraně před nimi.

Mezi běžné původce kybernetické hrozby patří:

Kriminální organizace

Organizované skupiny hackerů se snaží proniknout do organizací za účelem finančního zisku. Tito aktéři kybernetických hrozeb využívají phishing, spam, spyware a malware k vydírání, krádežím soukromých informací a online podvodům, které jsou řízeny jako korporace, s velkým počtem zaměstnanců, kteří vyvíjejí nástroje útoku a provádějí útoky.

Národní státy

Nepřátelské země mohou podnikat kybernetické útoky proti místním společnostem a institucím s cílem narušit komunikaci, vyvolat nepokoje a způsobit škody.

Teroristická organizace

Teroristé provádějí kybernetické útoky s cílem zničit nebo zneužít kritickou infrastrukturu, ohrozit národní bezpečnost, narušit ekonomiku a způsobit občanům újmu na zdraví.

Nečestní interní pracovníci

Zaměstnanci s oprávněným přístupem k firemním aktivům zneužívají svá oprávnění ke krádežím informací nebo poškozování elektronických aktiv za účelem ekonomického nebo

osobního zisku. Těmito vnitřními hrozbami mohou být zaměstnanci cílové organizace, smluvní partneři, dodavatelé nebo společníci (Preyproject, 2024).

1.2.1 Phishing

Phishing je velmi běžná forma útoku, při níž se používají různé techniky, jak přimět lidi k vyzrazení osobních nebo jiných důvěrných informací. Slovo "phishing" je odvozeno od běžného anglického slova "fishing", které pěkně popisuje to, co útočník ("phisher") dělá (tj. loví informace). Stejně jako když jde člověk na ryby, potřebuje nějakou návnadu, o které si myslí, že se na ni oběť chytí. Nejčastěji je tato návnada zaslána v e-mailu nebo textové zprávě, která případně obsahuje škodlivou přílohu nebo odkaz na škodlivou webovou stránku, ale phishing může probíhat také prostřednictvím sociálních sítí, jako jsou Facebook, Twitter a LinkedIn.

Návnada se musí zdát pro oběť atraktivní nebo dokonce nezbytná. Může jít například o zprávu, jako je jedna z následujících:

- Vyhráli jste cenu v loterii,
- musíte aktualizovat svou kreditní kartu,
- můžete získat peníze zpět od daňového úřadu,
- můžete si zahrát novou vzrušující online hru,
- musíte podniknout kroky, aby vám hackeři nevyprázdnili bankovní účet,
- váš šéf by chtěl znát vaše připomínky k nějakému tématu,
- musíte si přečíst důležitou zprávu,
- odesílatel by s vámi rád navázal spolupráci o něčem, co by vás mohlo zajímat.

Je dobře známo, že mnoho phishingových útoků se snaží přimět lidi, aby prozradili své uživatelské jméno a heslo do počítačového systému nebo na webovou stránku, která vyžaduje přihlášení. Když se takové útoky ve firmě podaří, může se stát, že pracovníci IT podpory firmy budou muset přimět všechny uživatele, aby si změnili svá hesla. Jak to mohou udělat tak, aby se uživatelé nedomnívali, že jde jen o další phishingový útok, při kterém jsou žádáni o zadání svých uživatelských jmen a hesel (Sharp, 2023, s. 35)?

1.2.2 Sociální inženýrství

Sociální inženýrství ("Social Engineering", SE) je do značné míry mylně chápáno, což vede k mnoha rozdílným názorům na to, co sociální inženýrství je a jak funguje. To vedlo k situacím, kde někteří mohou považovat sociální inženýrství za pouhé lhaní za účelem podvodu s triviálními předměty zdarma, jako je pizza nebo získání sexuálního uspokojení; jiní si myslí, že sociální inženýrství se odkazuje pouze na nástroje, které používají zločinci nebo podvodníci, nebo že se snad jedná o vědu, jejíž teorie lze rozdělit na části nebo složky a studovat je. Nebo je to možná dávno ztracené mystické umění, které dává praktikujícím schopnost používat mocné mentální triky jako kouzelník nebo iluzionista.

Sociální inženýrství je používáno každý den běžnými lidmi v každodenních situacích. Sociální inženýrství používá dítě, které se snaží dosáhnout svého v uličce se sladkostmi, nebo zaměstnanec, který chce dostat přidáno. K sociálnímu inženýrství dochází i ve státní správě nebo v marketingu malých firem. Bohužel se vyskytuje i v případech, kdy zločinci, podvodníci a podobní lidé obelstí lidi, aby jim poskytli informace, které je činí zranitelnými vůči zločinům. Jako kterýkoli jiný nástroj, ani sociální inženýrství není dobré nebo zlé, ale je to prostě nástroj, který má mnoho různých využití.

Platí zde staré hackerské přísloví “knowledge is power” ("znalost je síla"). Čím více znalostí a pochopení člověk má o nebezpečích a hrozbách sociálního inženýrství a každý spotřebitel a firma může mít, a čím více jsou jednotlivé scénáře útoků rozebrány, tím snazší bude se před těmito útoky chránit, zmírnit je a zastavit. Právě zde se projeví síla všech těchto znalostí (Hadnagy, 2022, s. 1-2).

1.2.3 Další časté typy hrozeb

Malware

Malware je také známý jako malicious code (" zlomyslný kód") nebo malicious software ("zlomyslný software"). Malware je program vložený do systému za účelem narušení důvěrnosti, integrity nebo dostupnosti dat. Je prováděn tajně a může ovlivnit vaše data, aplikace nebo operační systém. Malware se stal jednou z nejvýznamnějších vnějších hrozeb pro systémy. Malware může způsobit rozsáhlé škody a narušení provozu a vyžaduje obrovské úsilí v rámci většiny organizací.

Podle šíření

V práci jsou uvedeny tři typy šíření – viry, červy, trojské koně.

Viry

Viry jsou vytvořeny tak, aby zaznamenávaly, poškozovaly nebo mazaly data v zařízení a bránily tak jeho běžnému provozu. Často oklamou uživatele, aby otevřeli škodlivé soubory a mohli se tak šířit do dalších zařízení.

Červi

Červ se replikuje a k šíření po síti využívá bezpečnostních chyb v přílohách e-mailů, textových zprávách, aplikacích pro sdílení souborů, platformách sociálních médií, sdílených síťových úložištích a přenosných discích. V závislosti na druhu červa může změnit nastavení zabezpečení, znemožnit přístup k souborům nebo ukrást důvěrná data.

Trojské koně

Trojské koně spoléhají na to, že si je uživatelé neúmyslně stáhnou, protože napodobují skutečné soubory nebo aplikace. Po stažení mohou:

- Stáhnout a nastavit další škodlivý software, jako jsou červi nebo viry.
- použít podvodné kliknutí na napadeném zařízení;
- sledovat stisknuté klávesy a navštívené webové stránky;
- předávat data (hesla, přihlašovací údaje a historii prohlížení) z napadeného zařízení zlovolnému hackerovi;
- předat napadené zařízení kyberzločinci (Microsoft, 2024).

Podle efektu

V diplomové práci je uvedeno šest efektů – spyware, ransomware, CATO, MITM, DDoS, cryptojacking.

Spyware

Spyware, škodlivý software určený k narušení soukromí, se také stal pro organizace velkým problémem. Ačkoli se škodlivý software narušující soukromí používá již mnoho let, v poslední době se stal mnohem běžnějším. Spyware napadá mnoho systémů za účelem sledování osobních aktivit a provádění finančních podvodů.

Ransomware

Ransomware brání nebo omezuje uživatelům přístup k jejich systému prostřednictvím škodlivého softwaru. Ransomware požaduje zaplacení výkupného pomocí online platebních metod, aby získal zpět přístup k systému nebo datům. Online platební metody obvykle zahrnují virtuální měny, například Bitcoiny. Ransomware je jednou z nejrozšířenějších metod útoků.

Corporate Account Takeover (CATO)

CATO je krádež podnikatelského subjektu, kdy se kybernetičtí zloději vydávají za podnik a odesílají neoprávněné bankovní a automatizované platební transakce. Neoprávněné finanční prostředky jsou zasílány na účty kontrolované kyberzločincem (Mass.gov, 2024).

Man-in-the-middle

Útok MITM (man-in-the-middle) je typ kybernetického útoku, při kterém útočník zachytí a případně změní komunikaci mezi dvěma stranami bez jejich vědomí. Útočník se postaví mezi odesílatele a příjemce a stává se tak "prostředníkem" v tomto procesu.

DDoS

Útok DDoS (Distributed Denial of Service) je zákeřný pokus o narušení normálního fungování počítačové sítě, služby nebo webové stránky tím, že je zahltí přívalem nelegálního provozu. Při útoku DDoS je použito více kompromitovaných zařízení nebo systémů, které generují obrovský objem požadavků nebo datových paketů směrem k cíli, zahlcují jeho zdroje a znemožňují jeho dostupnost pro legitimní uživatele (NordLayer, 2023).

Cryptojacking

S rostoucí popularitou kryptoměn se těžba mincí stala výnosnou činností. Těžaři mincí těží kryptoměny pomocí výpočetního výkonu zařízení. Tyto druhy malwarových infekcí často začínají přílohou e-mailu, která se pokouší nainstalovat malware, nebo webovou stránkou, která využívá chyby prohlížeče nebo prostředků počítače k infikování zařízení malwarem.

Těžaři mincí využívají složité matematické výpočty ke krádeži výpočetních zdrojů, které jim umožňují vyrábět nové měny a udržovat knihu blockchain. K ukradení relativně skromných částek kryptoměn však těžba mincí vyžaduje velký výpočetní výkon počítače. Z tohoto důvodu kyberzločinci často spolupracují ve skupinách, aby zvýšili a rozdělili výnosy (Microsoft, 2024).

2 OPERAČNÍ SYSTÉMY

Co je to operační systém? Dalo by se říct, že je to to, co je mezi člověkem a hardwarem, ale to by se týkalo prakticky veškerého softwaru. Takže by se dalo říct, že je to software, který se nachází mezi softwarem a hardwarem. Znamená to ale, že knihovna, která byla získána na nějaké webové stránce, je součástí operačního systému? Pravděpodobně bude vhodné, aby definice operačního systému nebyla tak obsáhlá. Takže je možno říci, že je to ten software, na kterém závisí téměř všechno ostatní. To je sice stále nejasné, ale pak se tento termín používá v celém odvětví poněkud mlhavě.

Možná bude lepší popsat, co má operační systém vlastně dělat. Z pohledu programátora poskytují operační systémy užitečné abstrakce základních funkcí hardwarových prvků. Protože tyto prvky může využívat mnoho programů najednou, je operační systém také zodpovědný za správu toho, jak jsou tyto prvky sdíleny.

Přesněji řečeno, mezi typické hardwarové prvky, pro které operační systém poskytuje příslušné funkce, patří:

- Procesory,
- paměť RAM (paměť s náhodným přístupem, někdy označovaná jako primární úložiště, primární paměť nebo fyzická paměť),
- disky (specifický druh sekundárního úložiště),
- síťové rozhraní,
- displej,
- klávesnice,
- myš (Doeppner, 2022, s. 2).

2.1 Microsoft Windows

Microsoft Windows, počítačový operační systém (OS) vyvinutý společností Microsoft Corporation pro provoz osobních počítačů (PC). Operační systém Windows, který jako první obsahoval grafické uživatelské rozhraní (GUI) pro počítače kompatibilní s IBM, brzy ovládl trh s osobními počítači. Přibližně 90 % osobních počítačů používá některou z verzí systému Windows (Microsoft Windows: operating systém, 2024).

2.2 Linux

Operační systém linux se stal jedním z nejrozšířenějších operačních systémů, který si oblíbili výzkumníci, vývojáři aplikací i koníčkáři. V současné době se operační systém Linux nachází v různých počítačových prostředích, od mobilních telefonů až po satelity.

Systémem Linux má k dispozici mnoho různých verzí, lze tedy lehce zmást osoby, které se neorientují v dané problematice. Při prohlížení balíčků Linuxu je možno nalézt pojmy jako distribuce, LiveDVD a GNU, které mohou snadno zmást.

Ačkoli se o operačním systému Linux obvykle mluví jen jako o "Linuxu", ve skutečnosti tvoří kompletní systém Linux několik částí. Systém Linux má čtyři hlavní části:

- Jádro Linuxu („The Linux kernel“),
- nástroje GNU („The GNU utilities“),
- uživatelské rozhraní,
- aplikační software.

Každá z těchto čtyř částí má v systému Linux specifickou úlohu. Ačkoli každá z těchto částí sama o sobě není příliš užitečná, dohromady tvoří to, co lidé označují jako "Linux" (Blum, 2023, s. 1-2).

2.3 Subsystém Windows pro Linux

Subsystém Windows pro Linux ("Windows Subsystem for Linux", WSL) je funkce systému Windows, která umožňuje spustit prostředí Linux v počítači se systémem Windows bez nutnosti používat samostatný virtuální počítač nebo dual booting. WSL je navržen tak, aby poskytoval bezproblémové a produktivní prostředí pro vývojáře, kteří chtějí používat současně Windows i Linux (Microsoft, 2023).

3 KRYPTOGRAFIE

Definice, které jsou zde uvedeny, jsou v oblasti kryptografie univerzální, takže se s nimi lze setkat při auditu nebo jiném hodnocení různých technologií a systémů v této oblasti nebo při přezkoumávání právních nebo regulačních norem pro organizaci klienta. Právní předpisy mohou často obsahovat slangové výrazy týkající se šifrování a dešifrování a také algoritmů apod.

Plaintext (Čistý text)

Plaintext označuje jakoukoli informaci, která existuje před zpracováním v kryptografickém systému. V tomto případě se čistým textem rozumí informace, která neprošla procesem šifrování a nebyla transformována do jiné podoby. Může se jednat o binární informace, například ty, které se nacházejí ve spustitelných a datových souborech v systému.

Ciphertext (Šifrovaný text)

Ciphertext je výsledek, který získáte, když do systému vstoupí čistý text, se kterým se pracuje a který se transformuje. Šifrovaný text je ze své podstaty něco, co by nemělo být snadné rozluštit, pokud člověk nerozumí systému a nezná konkrétní kombinace nebo sekvence použité k přeměně čistého textu v šifrovaný text. Pokud se hovoří o pojmech čistý a šifrovaný text v kontextu procesu šifrování a dešifrování, lze čistý text převést na šifrovaný text pomocí šifrování, zatímco šifrovaný text lze převést zpět na čistý text pomocí procesu dešifrování.

Algorithm (Algoritmus)

Aby bylo možné přejít z čistého textu na šifrovaný text nebo šifrovaný text z čistého textu, je třeba použít něco, čemu se říká algoritmus. Algoritmus si můžete představit jako vzorec popisující postup kroků, který vyjadřuje, co je třeba udělat a v jakém pořadí, aby bylo dosaženo požadovaného výsledku. Algoritmus poskytuje konzistentní a opakovatelnou řadu kroků, které lze provést k dosažení libovolného požadovaného výsledku, který zamýšlel tvůrce systému. Ve funkci pentestera (testovatel průniku) je nutné seznámit se s mnoha různými názvy a typy algoritmů, abyste pochopili, k řešení, jakých výzev je každý z nich vhodný.

Klíč

Jednou z věcí, za kterou je algoritmus zodpovědný, je definování tzv. klíče, přesněji řečeno oblasti klíče. Při diskusi o algoritmu a převodu z čistého textu na šifrovaný text nebo

šifrového textu na čistý text rychle zjistíte, že pouhá znalost algoritmu vás sama o sobě příliš daleko nedostane. Dobrý algoritmus totiž definuje různá nastavení, která lze použít na jakoukoli informaci převáděnou z jednoho formátu do druhého. Ve skutečnosti je přesnější říci, že algoritmus definuje všechna možná nastavení, která lze použít pro převod z jednoho formátu do druhého, ale algoritmus vám neřekne, jaká konkrétní nastavení k zašifrování dané informace dotyčný použil (Oriyano, 2017).

3.1 Hashing

Hashovací funkce jsou jednoduše funkce, které přijímají vstupy určité délky a komprimují je do krátkých výstupů stanovené délky. Klasické použití hashovacích funkcí je v datových strukturách, kde je lze použít k sestavení hashovacích tabulek, které umožňují vyhledávání při ukládání množiny prvků.

Na nejzákladnější úrovni poskytuje hashovací funkce způsob, jak mapovat dlouhý vstupní řetězec na kratší výstupní řetězec, který se někdy nazývá digest. Hlavním požadavkem je zabránit kolizím neboli dvěma vstupům, které se mapují na stejný digest. Hashovací funkce odolné proti kolizím mají mnohostranné využití.

Kromě toho se hashovací funkce staly v kryptografii všudypřítomné a často se používají ve scénářích, které vyžadují mnohem silnější vlastnosti, než je odolnost proti kolizi. Stalo se běžným modelovat kryptografické hashovací funkce, aby byly "zcela nepředvídatelné" (tzv. "random oracles").

Hašovací funkce jsou zajímavé tím, že se na ně lze dívat jako na něco mezi světem private-key (soukromých klíčů) a public-key (veřejných klíčů) v kryptografii (Katza Lindell, 2022, s. 153).

3.2 Klasifikace a abstrakce kryptografie

Symetrická kryptografie neboli kryptografie s tajným klíčem (secret-key cryptography). Je použito pouze jedno tajemství. Pokud toto tajemství zná více účastníků, nazývá se sdílené tajemství (Wong, 2021, s. 19).

Soukromý klíč, je známý také jako tajný klíč (Loshin, 2021).

Asymetrická kryptografie neboli kryptografie s veřejným klíčem (public-key cryptography). Účastníci mají asymetrický pohled na tajemství. Někteří budou například znát veřejný klíč, zatímco někteří budou znát veřejný i soukromý klíč (Wong, 2021, s. 19).

4 HESLA

Heslům je vhodné věnovat větší pozornost, protože jsou stále nejčastěji používaným způsobem ověřování uživatelů. Heslo, které uživatel zadá, se porovnává s heslem, které již do systému zadal při registraci.

Tím se dostáváme k prvnímu problému, a to, jak heslo v systému uložit, aby se k němu útočník nedostal ani v nepravděpodobném případě, že získá přístup do systému. Riziko představuje také oprávněný správce systému, protože má přístup k celému systému a může potenciálně přečíst hesla uživatelů a zneužít je.

V minulosti byla hesla v systémech mnohdy uchovávána v původní čitelné podobě a některé systémy se tento problém snažily řešit šifrováním hesel. Pokud se však útočníkovi podařilo do systému nabourat, získal přístup nejen k zašifrovaným heslům, ale obvykle i k šifrovacímu klíči. Z důvodu této zjevné zranitelnosti se rozšířily hashovací funkce.

Následující vlastnosti hashovacích metod je předurčují k tomu, aby byly vhodné pro tvorbu otisků (hashů) hesel:

- Jedná se o jednocestné funkce, což znamená, že matematické techniky nelze použít k obnovení původního textu z hashe,
- jakákoli malá změna textu na vstupu funkce povede k radikálně odlišnému výstupu (dva otisky stejného textu, které byly jen nepatrně změněny, budou vypadat zcela odlišně),
- je téměř nemožné najít dva vstupy, které by daly stejný výstup,
- nezáleží na tom, jak velký je soubor vstupních dat, výstup funkce má vždy stejnou délku.

Při volbě vyhovující hashovací funkce lze vycházet ze základních standardů pro kryptografické algoritmy, jak jsou uvedeny ve vyhlášce o kybernetické bezpečnosti.

Při přihlášení je nejprve vygenerován hash uživatelova hesla, který je následně porovnán s uloženou hodnotou. Je-li zjištěno, že hashe jsou totožné, je uživatel ověřen na základě znalostí, které má (tzn. „něco zná“).

V současné době rozlišujeme několik útoků na hesla. Heslo může být:

1) zachyceno z fungování na počítačové síti,

2) z uživatele vymámeno sociálním inženýrstvím (např. phishingovým útokem aj.),

3) pořízeno z počítačového systému za užití malwaru (např. pomocí keylogeru aj.),

4) uhádnuto,

5) „lámáno“.

Útočník, který se podílí na on-line prolomení, zadá několik hesel a čeká, až je počítačový systém ověří. Takový typ útoku je obvykle poměrně pomalý a útočník se vystavuje nebezpečí, že bude odhalen správcem v záznamu, pokud se pokusí o příliš mnoho přihlášení ze stejné IP adresy nebo se objeví příliš mnoho účtů (Kolouch a Bašta, 2019, s. 464-465).

4.1 Správa hesel

Hesla jsou pro uživatele velkou nepříjemností. Většina uživatelů si pamatuje pouze jedno nebo dvě hesla, a pokud každé přihlášení vyžaduje jedinečné schéma nebo ověřovací faktor, mohou to prostě vzdát a neúčastnit se.

Správci musí vyvažovat potřebu zabezpečení a ochotu uživatelů dodržovat požadavky na silná hesla. Téměř vždy se objeví nespokojenost, ale tato rovnováha musí být stanovena a vynucována. Nespokojenost bude mnohem větší, pokud bude uživatelův účet kompromitován.

Aplikace pro správu hesel mohou být použity ke zmírnění potíží uživatelů s hesly. Tyto aplikace běží na počítačích a mobilních zařízeních a zapamatují si autentizační parametry uživatele, takže si je uživatelé nemusí pamatovat. Při použití těchto aplikací se sice všechna hesla uživatele umístí za jedno ověřovací heslo, ale toto heslo je uloženo na soukromějším zařízení, ke kterému má uživatel přístup pod kontrolou.

Tento systém s jediným přístupovým údajem může být bezpečnější použitím náročného hesla; naštěstí se většina uživatelů dokáže naučit jediné bezpečné heslo. Správci hesel obvykle navrhují dlouhá a bezpečná hesla, která lze použít a která si není možné zapamatovat. To může být skvělé řešení, dokud správce hesel vždy funguje, ačkoli ne každá aplikace nebo brána bude s těmito systémy pracovat příhodně (Brooks et al., 2018, s. 538-539).

4.2 Ověřování

Zabezpečení na všech úrovních vždy zahrnuje určitý typ procesu ověřování. Je nutné si pamatovat, že ověřování je jednoduše způsob, jak určitým způsobem zjistit identitu

uživatele. Zcela jistě bude žádoucí ověřit externí uživatele, kteří chtějí přistupovat k dané síti, a zpravidla bude žádoucí ověřit i interní uživatele, kteří se vydávají na neznámá místa v internetu.

Uživatelé mohou být ověřováni tak, že jsou požádáni o zadání uživatelského jména a hesla, zkoumáním jejich MAC adresy nebo podle jejich síťové adresy, pokud mají přidělenou statickou IP adresu. Lze použít kombinaci různých faktorů a stále častěji se do schématu ověřování zapojují i další faktory, které nesouvisejí se sítí v ověřovacím procesu. Pokud jsou do sítě vpuštěni neověřovaní uživatelé, nemáte možnost sledovat jejich aktivity.

Po ověření uživatele je obvykle třeba určit jeho oprávnění, což v podstatě zahrnuje prostředky, ke kterým má ověřený uživatel přístup, a akce, které může provádět. Často jsou tato osvědčení a oprávnění uložena v nějaké databázi, ale někdy jsou ověření uložena v jednoduchých textových souborech. Zajištění ochrany těchto souborů a databází je kritickým aspektem zabezpečení sítě.

Poté, co byl uživatel ověřen a autorizován, je třeba jeho činnosti evidovat pomocí nějakého typu zaznamenávání. Jedná se o často přehlížený koncept související s ověřováním. Zaznamenávání je však klíčovou součástí procesu zajištění bezpečnosti, protože zabezpečení nikdy není čistě preventivní činností. Administrátoři musí čas od času procházet záznamy, aby vyhodnotili, k jakým událostem v jejich sítích došlo, mohlo dojít nebo ještě může dojít, a také komu se to stalo (Brooks et al., 2018, s. 536).

4.2.1 Jednofaktorové ověřování

Mělo by být jasné, že nejznámější metodou ověřování je určitě ověřování heslem. Může to být tak jednoduché, jako když uživatele vyzvete k zadání hesla a nic jiného. Běžně se s tím setkáváme, když se uživatelé bezdrátové sítě připojují k přístupovému bodu. Uživatel si může prohlédnout dostupné přístupové body ve svém okolí a pak mu stačí zadat heslo nebo ověřovací klíč, aby se mohl připojit. Jedná se o jednofaktorové ověřování a představuje nejnižší dostupnou úroveň zabezpečení.

Jednofaktorové ověřování může být vhodné pro omezení přístupu ke zdrojům, ale může být obtížnější ověřit totožnost konkrétního uživatele. Může být také dostačující pro přístup hostů v rezidenční síti, ale vyjadřuje to určitou důvěru v tyto uživatele, protože nyní mohou přistupovat k síti a jejímu připojení k internetu s téměř stejným přístupem jako vlastník.

Je možné nakonfigurovat omezení, ale v určitém okamžiku budou mít uživatelé přístupové možnosti, které zvýší odpovědnost správce. Když je tato odpovědnost příliš velká, je třeba najít jiný způsob ověřování. Pokud jsou hesla součástí bezpečnostního plánu, je nutné zvážit také zásady týkající se těchto hesel. Slabé heslo může být dostačující pro domácí sítě, ale každá firma by měla mít přísné zásady týkající se kvality hesel a možná i historie hesel (Brooks et al., 2018, s. 537).

4.2.2 Více faktorové ověřování

Dvou faktorové ověřování zahrnuje žádost o ověření pomocí druhé, odlišné metody. Jedním faktorem je například něco fyzického nebo co má uživatel v držení, jako např:

▶ Klíč RFID

▶ klíč USB

▶ přejetí karty

Dalším faktorem je nějaká fyzická vlastnost, jako např:

▶ Otisky prstů nebo naskenovaná duhovka.

▶ Vyslovená fráze, analýza hlasu uživatele.

Různé použité faktory lze rozlišit jako jeden z následujících:

▶ Něco, co znáte (heslo nebo PIN).

▶ Něco, co máte (fyzický token nebo karta).

▶ Něco, co jste (fyzická charakteristika, např. otisk prstu).

Příkladem dvou faktorového ověřování je vlastnictví bankovní karty a znalost kódu PIN. Pokud nelze provést ověřování pomocí nějakého fyzického atributu, lze jako druhý faktor použít identifikátor, který není snadno uhodnutelný. Pokud jsou obě složky obtížně uhodnutelné, je pravděpodobnost úspěchu útoku hrubou silou výrazně nižší než u jednofaktorového ověřování nebo u kombinace e-mailu a hesla.

Do přihlašovací sekvence lze přidávat další faktory ověřování, které zvyšují bezpečnost tím, že je stále méně pravděpodobné, že útok bude úspěšný. S náročnějšími přihlašovacími sekvencemi však budou uživatelé nespokojeni a uchýlí se k zapisování přihlašovacích údajů na lepicí papírky a do stolních kalendářů nebo prostě nebudou službu používat. To je obrovská výzva pro každého tvůrce webových stránek nebo bezpečnostního inženýra, u

kterého je spokojenost uživatelů problémem. Když jsou uživatelé dostatečně nespokojeni, najdou způsob, jak obejít systém zabezpečení (Brooks et al., 2018, s. 537-538).

4.3 Hrozby pro hesla

Hlavní hrozbou pro heslo je lenost uživatele, která ho často odradí od dodržování pokynů pro správu hesel. Krádež hesla je jednou z hlavních příčin útoků DDoS a mnoha dalších krádeží dat a finančních podvodů.

Podle nejnovějšího výzkumu provedeného v roce 2018 bylo zjištěno, že velké množství lidí používá velmi obecná hesla, jako jsou 123456, 12345678 a abc123. Tato hesla lze při zadávání velmi snadno uhodnout a vyzvědět pohledem.

Bezpečnostní průzkum WatchGuard za 2. čtvrtletí 2018 zjistil, že více než 1 700 lidí pracujících ve vládních a vojenských organizacích Austrálie používá heslo "123456"! Mezi další slabá hesla, která tito státní zaměstnanci používali, patřila "password" (544 lidí), "linkedin" (405 lidí) a "12345678" (120 lidí). Všechna tato hesla jsou ze skupiny nejméně spolehlivých a nejsnadněji uhodnutelná hesla na světě. Mnoho organizací a bezpečnostních společností již zařadilo tato hesla na černou listinu, která se nesmí používat.

Používání slabých hesel je velmi náchylné k riziku snadné krádeže. Snadná hesla by se proto nikdy neměla používat. Hesla v čistém textu jsou ke krádeži ještě náchylnější.

Mezi hlavní hrozby krádeže hesel patří následující:

- Odposlech,
- odhadnutí hesla,
- prolomení hesla pomocí počítačového softwaru,
- offline prolamování hashů,
- techniky kybernetického útoku na obnovu nebo reset hesla,
- použití stejného hesla na více účtech,
- používání výchozích hesel systému,
- škodlivý software v počítači, například sniffery a keyloggery,
- zneužití zadních vrátek,
- škodlivé pluginy,

- phishing (Thakur a Pathan, 2020, s. 122-123).

4.4 Kritéria pro dobré heslo

Zjednodušeně řečeno, dobré heslo je takové, které nelze zapomenout, ale které nikdo jiný (člověk ani počítač) není schopen uhodnout. Za tímto jednoduchým popisem se skrývají dva spletité, vzájemně propojené problémy:

Odhadnutelnost: Většina lidí má nerealistickou představu o tom, co znamená "uhodnutelné" heslo. Lze si představit, že heslo ninjaboy si s danou osobou nikdo nespojí, ale počítač, který právě používá, by na to přišel dřív, než by dokončil psaní této věty. Kdyby člověk, který o dané osobě ví všechno, by její hesla nikdy neuhádl, sofistikované prolamující algoritmy je však mohou odhalit, pokud nebudou podniknuty kroky k jejich zmaření. Aby se tomuto riziku předešlo, měla by být hesla mnohem složitější, než se může zdát.

Zapamatovatelnost: Pokud si heslo nelze zapamatovat, je k ničemu. S rostoucí složitostí hesla (a tedy i jeho silou) má jeho zapamatovatelnost tendenci klesat. Je potřeba si připustit, že iYb48nzJ#;sEoR je sice výrazně silnější než ninjaboy, ale zrovna nepřijde na mysl.

Vytvoření zapamatovatelných a zároveň nezapamatovatelných hesel, a nejen jednoho či dvou, ale potenciálně stovek hesel se může zdát jako neřešitelný problém.

Tento vágní pojem odhadnutelnosti kvantifikujme. V běžné řeči slovo entropie znamená neuspořádanost, nahodilost nebo nepředvídatelnost. Osoby zabývající se kryptografií používají termín entropie k označení matematické aproximace složitosti hesla na základě metody použité k jeho vytvoření. Heslo s vyšší entropií je pro člověka (a hlavně pro stroj) hůře uhodnutelné. Pro hesla je tedy vyšší entropie velmi dobrá věc.

Když je teď vysvětleno, proč jsou potřeba hesla s vysokou entropií, jak je lze získat? Možná bude překvapivé, že pokud jde o entropii hesla, slovo "složité" nemusí nutně znamenat "komplikované". K vysoké entropii vede více než jedna cesta. Když to trochu zjednodušeně shrneme, hlavními faktory, které ovlivňují entropii hesla, jsou jeho délka, velikost sady znaků a náhodnost.

Délka: Například čtyřznakové heslo, ve kterém jsou všechny znaky tvořeny malými anglickými písmeny. Je známo, že pro každý znak existuje 26 možných hodnot, takže celkový počet možností je 26 × 26 × 26 × 26, tedy 456 976. Když se přidá další písmeno,

vynásobí se tento celkový počet opět 26, což je 11 881 376 možných voleb a tak dále. Prodloužení hesla, byť jen o jeden znak tedy exponenciálně zvyšuje jeho entropii, protože k jeho uhodnutí bude potřeba v průměru o tolik více pokusů. Zvětšení délky je nejjednodušší a nejefektivnější způsob, jak zvýšit entropii hesla.

Sada znaků: Pokračování stejného příkladu, co když heslo může obsahovat jak velká, tak malá písmena? Nyní existuje 52 možných hodnot pro každý slot, takže čtyřznakové heslo má 7 311 616 variant (52 × 52 × 52 × 52) a pětiznakové heslo má 380 204 032 variant. To je obrovský nárůst oproti počtu, který lze získat, když každý znak může mít pouze 26 možných hodnot. Pokud se k tomu přidají číslice od 0 do 9, vznikne 62 možností pro každý znak. Přidáním tuctu interpunkčních znamének vznikne 74 možností, čímž se počet možností pro pětiznakové heslo zvýší na 2 219 006 624. (Nicméně je nutné si uvědomit, že počítač dokáže zkontrolovat všechny dvě miliardy těchto hesel za méně než jednu sekundu!)

Z toho plyne ponaučení, že čím větší počet možných znaků musí počítač vyzkoušet pro každé místo v hesle, tím déle trvá jeho uhodnutí. Proto mnoho webů vyžaduje, aby se používala velká a malá písmena, číslice a interpunkční znaménka a aby byl cílový soubor znaků co největší.

Náhodnost: Heslo kůň je, jedním z 11 881 376 možných hesel na 5 znaků psaných malými písmeny. Přesto je jeho entropie mnohem nižší (zhruba 9 bitů) než u jiného pětimístného hesla, například dcxuw (zhruba 17 bitů). To proto, že dalším faktorem ovlivňujícím entropii je náhodnost, a dcxuw je náhodné, zatímco kůň nikoli.

Pro účely této úvahy je náhodnost chápána jako "absence rozeznatelného vzoru". Slovníková slova se řídí vzory. Stejně tak vyslovitelné řetězce, které nejsou slovy (například glavondi), i když tyto vzory jsou jemnější. Ale jak bylo zdůrazněno dříve, software pro prolamování hesel dokáže rozpoznat nejrůznější další schémata, kterých by si náhodný lidský pozorovatel nikdy nevšiml, včetně nejběžnějších metod konstrukce zdánlivě náhodných hesel.

Vytvořit skutečně náhodné řetězce je pro člověka téměř nemožné a obtížné je to i pro počítač. Většina řetězců, které počítač vytváří, je pseudonáhodná, což znamená, že je do značné míry, ale ne dokonale nepředvídatelná. Jsou však vždy náhodnější, a tedy lépe přispívají k entropii hesla než cokoli, co by člověk sám vymyslel (Kissell, 2023).

Tabulka 1 Rychlosti zjištění hesla (Antivirové centrum, 2023)

Počet znaků	Pouze čísla	Malá písmena	Malá a velká písmena	Čísla, malá a velká písmena	Čísla, malá a velká písmena, speciální znaky
4	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
5	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
6	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
7	okamžitě	okamžitě	1 s	2 s	4 s
8	okamžitě	okamžitě	28 s	2 min	5 min
9	okamžitě	3 s	24 min	2 h	6 h
10	okamžitě	1 min	21 h	5 dní	2 týdny
11	okamžitě	32 min	1 měsíc	10 měsíců	3 roky
12	1 s	14 h	6 let	53 let	226 let
13	5 s	2 týdny	332 let	3 tis. let	15 tis. let
14	52 s	1 rok	17 tis. let	202 tis. let	1 mil. let
15	9 min	27 let	898 let	12 mil. let	77 mil. let
16	1 h	713 let	46 mil. let	779 mil. let	5 mld. let
17	14 h	18 tis. let	2 mld. let	48 mld. let	380 mil. let
18	6 dní	481 tis. let	126 mld. let	2 bil. let	26 bil. let

5 HACKING

Hacking je termín používaný jak těmi, kdo píší kód, tak těmi, kdo jej zneužívají. Přestože tyto dvě skupiny hackerů mají různé konečné cíle, obě skupiny používají podobné techniky řešení problémů. A protože porozumění programování pomáhá těm, kteří zneužívají, a porozumění zneužívání pomáhá těm, kteří programují, mnoho hackerů se věnuje oběma činnostem. Zajímavé hackerské postupy lze nalézt jak v technikách používaných k psaní elegantního kódu, tak v technikách používaných ke zneužívání programů. Hacking je vlastně jen hledání chytrého a proti intuici orientovaného řešení problému.

Hacky nalezené v programových zneužití se obvykle zabývají používáním pravidel počítače způsobem, který nikdy nebyl zamýšlen, k dosažení zdánlivě zázračných výsledků, které jsou obvykle zaměřeny na obcházení bezpečnosti. Hacky vyskytující se při psaní programů jsou podobné v tom, že také využívají pravidla počítače novými a vynalézavými způsoby, ale konečným cílem bývá dosažení co nejpůsobivějšího a nejlepšího způsobu splnění daného úkolu (Erickson, 2022).

V nejširším slova smyslu je hacking neoprávněná úprava produktu, která umožňuje jeho nezamýšlené použití. Například u automobilu mohou být hacknuty směrové blinkry, aby umožňovaly vysílání zpráv v Morseově abecedě. Trpný rod tam není jen proto, aby se angličtinářům dělala pěna u úst; hacknout auto může opravdu každý. To by bylo možné, protože výrobcem automobilu byl vytvořen propracovaný softwarový balík a zabudován do automobilu, který má shodou okolností také spoustu děr a způsobů, jak se do něj nabourat (Evans, 2019, s. 107-108).

5.1 Etický hacking

Jak si mnoho osob představuje hackery? Nosí v interiéru sluneční brýle a mikiny s kapucí a píší na klávesnici rychleji, než oko dohlédne? Pijí Jolt Colu, zatímco se snaží "hacknout Gibsona"? Se vší pravděpodobností by člověk nikdy nepoznal skutečného hackera, který by ho potkal na ulici. Mohla by to být jen nějaká uhrovitá holka, která se na výzvu nabourala do multimilionové společnosti. Jak ukazuje tato kniha, není nic jednoduššího než se stát hackerem a může se jím nakonec stát každý. Trik spočívá v tom, že se člověk stane etickým hackerem, a může jím být kdokoliv. Trik spočívá v tom, že se stane etickým hackerem, což je speciální druh hackera, který dělá, co může, aby z produktů a služeb vytěžil maximum užitku, ale nezneužívá a nezneužívá ostatní.

Etický hacking se dělí na dvě základní kategorie: white hat (bílí klobouk) a black hat (černý klobouk) hacking. Názvy pocházejí z westernů, kde divák snadno pozná padoucha a hrdinu podle jejich klobouků. White hat hacking má za cíl prozkoumat počítačový systém a podívat se na něj zevnitř z pouhé zvědavosti, ale může zahrnovat i hackery najaté společností k testování jejích systémů a uživatele, které rozčilují drobná omezení softwaru, který používají.

Black hat hacking je zákeřný, prováděný s úmyslem způsobit škodu. Například s cílem ukrást informace o kreditních kartách nebo znemožnit odezvu konkurenčních stránek. Metafora s kloboukem jde hlouběji, protože ukazuje, že tentýž hacker si může vyměnit roli stejně snadno jako vyměnit klobouk.

V některých případech se hranice mlží a uživatelé jsou nuceni použít kombinaci "white hat" a "black hat" hackingu, jen aby byl software použitelný. Jedním z významných příkladů byl prohlížeč Mozilla Firefox, který poskytl uživatelům robustní rámec pro programování malých kousků kódu zvaných pluginy, které prohlížeči přidávaly další funkce. Existovaly doslova tisíce pluginů, které Mozilla nazývala "doplňky", pro nejrůznější účely, což dávalo každému uživateli možnost přizpůsobit si svou verzi Firefoxu. Vše šlo skvěle, dokud se někteří černí hackeři nerozhodli do těchto pluginů schovat trojské koně, malware, který umožňuje skrytý přístup k infikovanému počítači, a Mozilla se rozhodla zpřísnit, jak mohou být používány (Evans, 2019, s. 107, 29-30).

5.2 Kali linux

Kali Linux (dříve známý jako BackTrack Linux) je open-source distribuce Linuxu založená na Debianu, která je určena pro pokročilé penetrační testování a bezpečnostní audit. Toho dosahuje tím, že poskytuje běžné nástroje, konfigurace a automatizační prostředky, které umožňují uživateli soustředit se na úkol, který je třeba splnit, nikoli na okolní činnosti.

Kali Linux obsahuje oborově specifické modifikace a také několik stovek nástrojů zaměřených na různé úkoly v oblasti informační bezpečnosti, jako je penetrační testování, bezpečnostní výzkum, počítačová forenzní analýza, reverzní inženýrství, management zranitelností a Red Team testování.

Kali Linux je multiplatformní řešení, které je přístupné a volně dostupné profesionálům v oblasti informační bezpečnosti i nadšencům (Kali, 2023).

5.2.1 Funkce Kali Linux

Obsahuje více než 600 nástrojů pro penetrační testování: Po přezkoumání všech nástrojů, které byly součástí BackTracku, bylo vyřazeno velké množství nástrojů, které buď zkrátka nefungovaly, nebo duplikovaly jiné nástroje, které poskytovaly stejné nebo podobné funkce. Podrobnosti o tom, co je součástí, jsou uvedeny na webu Kali Tools.

Bezplatné ("as in beer" myšleno, jako „dar, tudíž nebude stát peníze na pořízení“) a vždy budou: Kali Linux je stejně jako BackTrack zcela zdarma a vždy bude. Za Kali Linux nebude muset nikdy, nikdo platit.

Git tree s otevřeným zdrojovým kódem: Vývojáři jsou odhodlaní do vývojového modelu a jejich vývojový strom je dostupný pro všechny. Veškerý zdrojový kód, který je součástí Kali Linuxu, je k dispozici všem, kteří chtějí balíčky upravit nebo přebudovat podle svých specifických potřeb.

V souladu s FHS: Kali dodržuje Filesystem Hierarchy Standard, což uživatelům Linuxu umožňuje snadno najít binární soubory, podpůrné soubory, knihovny atd.

Široká škála podpory bezdrátových zařízení: Pravidelným kamenem úrazu linuxových verzí byla podpora bezdrátových rozhraní. Kali Linux byl vytvořen tak, aby podporoval co nejvíce bezdrátových zařízení, což umožňuje jeho správný provoz na široké škále hardwaru a zajišťuje kompatibilitu s mnoha USB a dalšími bezdrátovými zařízeními.

Vlastní jádro, opravené pro injektování: Jako testeři průniku vývojový tým často potřebuje provádět posouzení bezdrátových sítí, takže naše jádro obsahuje nejnovější opravy pro injektování.

Vyvinuto v zabezpečeném prostředí: Tým Kali Linuxu se skládá z malé skupiny jednotlivců, kteří jsou jediní, jimž je svěřeno schvalování balíčků a interakce s repositáři, přičemž vše probíhá pomocí několika bezpečných protokolů.

Balíčky a repositáře opatřené GPG signaturami: Každý balíček v systému Kali Linux je označen podpisem jednotlivých vývojářů, kteří jej vytvořili a schválili, a následně jsou balíčky podepsány i v repositářích.

Podpora více jazyků: Přestože penetrační nástroje jsou většinou napsány v angličtině, bylo zajištěno, aby Kali obsahovalo skutečnou vícejazyčnou podporu, která umožní více uživatelům pracovat v jejich rodném jazyce a najít nástroje, které potřebují pro svou práci.

Plně upravitelné: Jelikož je jasné, že ne každý bude souhlasit s našimi designovými rozhodnutími, bylo umožněno odvážnějším uživatelům přizpůsobit si Kali Linux podle svých představ, a to až do úrovně jádra.

Podpora ARMEL a ARMHF: Vzhledem k tomu, že jednodeskové systémy na bázi ARM, jako jsou mimo jiné Raspberry Pi a BeagleBone Black, jsou stále populárnější a cenově dostupnější, bylo jasné, že podpora ARM v Kali musí být co nejrobustnější a musí obsahovat plně funkční instalace pro systémy ARMEL i ARMHF. Kali Linux je k dispozici na široké škále zařízení ARM a má repositáře ARM integrované s hlavní distribucí, takže nástroje pro ARM jsou aktualizovány ve spojení se zbytkem distribuce (Kali, 2023).

5.2.2 Hydra

Hydra, kterou vyvinula hackerská skupina "The Hacker's Choice", je silný a flexibilní nástroj pro použití hrubé síly, který používají penetrační testeři a etičtí hackeři. Je určen k prolamování hesel pro různé síťové služby, mezi které patří například telnet, FTP, HTTP, HTTPS, SMB a databáze. Hydra je známá svou schopností paralelního prolamování přihlašovacích údajů, což umožňuje navázat více spojení současně. Tato paralelizace výrazně zkracuje dobu potřebnou k prolomení hesla (Trent, 2023).

V podstatě se jedná o předinstalovaný nástroj, pokud v nějakém případě není nainstalován nebo uživatel pracoval s jinými verzemi distribuce, tak lze nainstalovat individuálně (Educba, 2023).

5.2.3 Útoky hrubou silou

Útoky hrubou silou ("brute-force attacks") jsou považovány za nejprimitivnější typ kybernetického útoku. Nevyžadují mnoho inteligence. Stačí útočit na cíl znovu a znovu, pokaždé mírně změnit nebo zvýšit jednu hodnotu, dokud se nedosáhne úspěchu. Pokud nejsou použity žádné obranné ovládací prvky blokující všechny pokusy, jedná se o jedinou metodu kybernetického útoku, která zaručuje, že nakonec zvítězí.

Hádání hesel hrubou silou je jedním ze způsobů, jak uhodnout hesla. Osoba, která hádá hesla hrubou silou a nezná povolenou minimální délku cílového hesla, by začala například písmenem A, a když by to nefungovalo, zkusila by písmeno B a tak dále, dokud by nevyzkoušela všechna písmena, číslice a symboly z možného seznamu znaků a nedospěla by k výsledku. Pak by osoba hádající heslo hrubou silou zkusila AA, pak AB, pak AC a tak

dále, přičemž by opět prošla všechny možné znaky na druhé pozici. Postupné přidávání dalších znaků na každou pozici, zkoušení všech možných kombinací, jednu po druhé, až nakonec nalezne správnou kombinaci znaků, které tvoří cílové heslo. Není překvapivé, že metoda hrubou silou získávání hesel nebo čehokoli, co souvisí s kybernetickým prostředím, je poměrně pomalá. Počítačem automatizované hádání se může zdát velmi rychlé, ale ve srovnání s pokročilejšími metodami je hádání hrubou silou stále relativně pomalé.

Většina útočníků i při hádání hesel ráda přidává do hádání trochu inteligence a doufá, že bude úspěšná rychleji. Osoby pokoušející se uhodnout heslo pravděpodobně vědí, že většina lidí tvoří hesla na základě svého rodného jazyka a přirozeného tvarosloví tohoto jazyka. Některé znaky, jako například samohlásky "a", "e", "i" a "o", budou v průměru používány mnohem častěji než souhlásky. Obvykle většina hesel začíná souhláskou, po které následuje samohláska. Pokud jsou uživatelé nuceni používat velké znaky, obvykle to bude velká souhláska na pozici prvního znaku. Pokud jsou nuceni používat číslice, obvykle zvolí 1 nebo 2 a budou na konci hesla nebo v jeho blízkosti. Při použití trochy inteligence útočníci zjistí, že většinu hesel (a PIN kódů) lze prolomit rychleji s menším počtem pokusů než pomocí metody hrubé síly (Grimes, 2020, s. 295-296).

6 DÍLČÍ ZÁVĚR

Teoretická část je sestavena z mnoha různých zdrojů. Těmito zdroji jsou nejen knihy, ale i internetové zdroje. Při shromažďování zdrojů byly získány nové vědomosti, které napomohli s nasměrováním se a praktickým použitím nástrojů a aplikací uvedenými v diplomové práci.

Teoretická část rozdělena na pět hlavních kapitol se svými podkapitolami. Úvod do problematiky je nazván kyberprostor. V této kapitole je kybernetická bezpečnost, kde jsou zmíněny pojmy, které mohou být užitečné pro neznalého čtenáře této práce. Nejvíce užitečnými pojmy této části jsou pojmy pod bodem kybernetická hrozba jako jsou phishing a sociální inženýrství. Jelikož je práce zaměřena na navrženou úlohu, ve které tyto pojmy hrají velkou roli.

Další kapitolou jsou operační systémy, kde jsou zmíněny pouze operační systémy, co budou použity v následující části (praktické) a nástroj díky kterému je možno použít oba operační systémy na jednom počítači. Jeden z operačních systémů bude použit jako aplikace.

Následuje kapitola o kryptografii s termínem hashing a klasifikací a abstrakcí kryptografie. Hashing je úzce spojen s hesly. Klasifikace a abstrakce kryptografie je zde pro doplnění hashingu.

Pátou kapitolou jsou hesla. Tato kapitola se zabývá správou hesla, typy ověřování, hrozbami pro hesla a kritériem pro dobré heslo. Nejdůležitější roli zde hrají kritéria pro dobré heslo, neboť jedním z přínosů této práce by měla být informovanost ohledně bezpečnosti hesla.

Hacking, jakož to poslední tedy šestá kapitola obsahuje etický hacking, operační systém Kali Linux a jeho funkce, nástroj Kali Linuxu Hydra pro zjišťování hesel a útoky hrubou silou (takzvané „brute force attacks“).

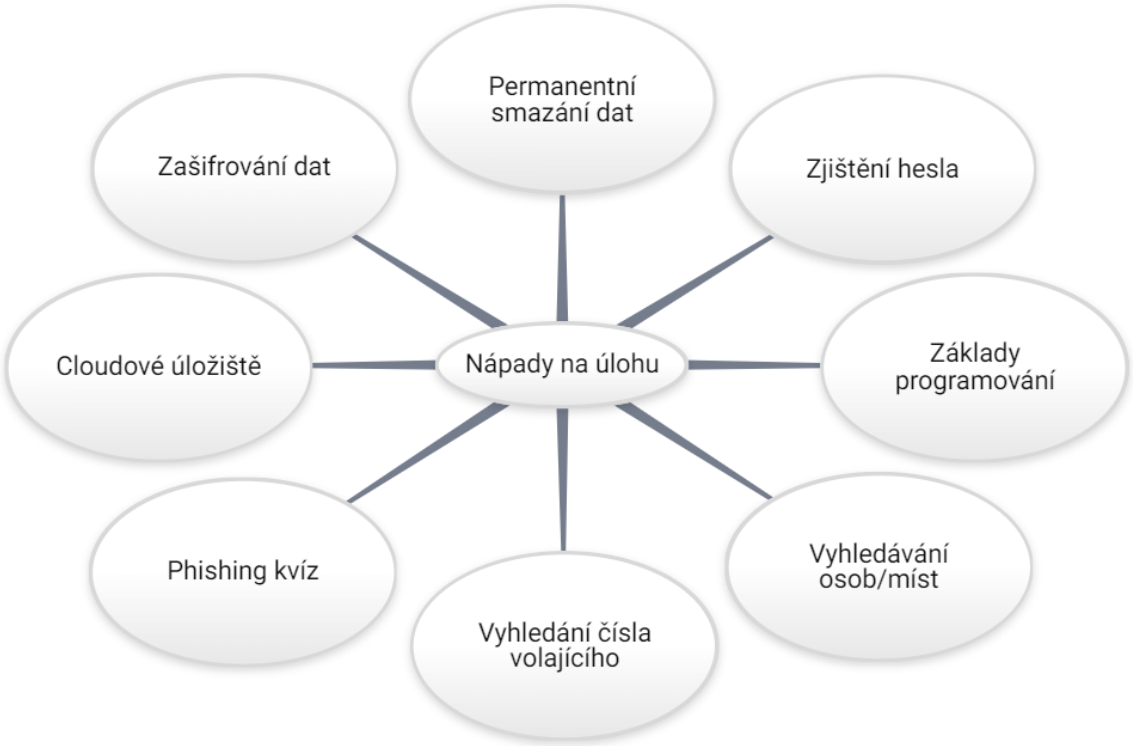
II. PRAKTICKÁ ČÁST

7 POČÁTEČNÍ KROKY DIPLOMOVÉ PRÁCE

V počátečních krocích diplomové práce bylo, samozřejmě po tématu, potřeba vymyslet obsah. Jinými slovy to, čím se tato práce bude zabývat a bude její náplní.

Prvním potřebným krokem byla domluva s vedoucím práce na předpokládaném obsahu a vymyšlení prvotních návrhů. Bylo zjištěno, že od obou stran, tedy jak od strany studenta, tak od strany vedoucího práce, jsou podobné představy o tom, jakou práce bude mít náplň. První konzultace vznesla malé množství nápadů na náplň diplomové práce, jak již lze poznat z názvu práce, tak se jednalo o vymyšlení, který z návrhů bude vybrán jako navržená úloha. Bylo potřeba úlohu strukturalizovat tak, aby zapadla svou náplní do výuky a zároveň přinesla co nejvíce užitku.

Nápadů bylo relativně málo, ale přinesly by studentům vědomosti, které by mohli využít různým způsobem. Těmito nápady byly zašifrování hesla pomocí aplikace Veracrypt; permanentní smazání dat z disku počítače aplikací Eraser; zjištění hesla na OS Kali Linux za pomoci nástroje Hydra; cloudové úložiště z pohledu tvorby a funkcí; základy programování jednodušeji pochopitelnou cestou her, které se soustředí na učení programování (těmito hrami jsou Elevator Saga, CodeCombat, Human Resource Machine); phishing kvíz, který zprostředkovává na internetu Google; vyhledávání osob nebo míst skrze „Open Source Intelligence“ (OSINT) a jako poslední vyhledání čísla volajícího skrze nástroj PhoneInfoga.



Obrázek 1 Nápady na úlohu (myšlenková mapa)

8 PROCVIČENÍ NAVRŽENÝCH ÚLOH

Navržené úlohy byly předem procvičeny na osobním počítači obsahujícím operační systém Microsoft Windows, který je určen pro domácí použití. Každá z úloh trvala delší čas z důvodu seznámení se s programem, webem nebo nástrojem. Následně byla vybrána jedna z následujících úloh.

Zašifrování dat

Operační systém od Microsoft Windows má své vlastní šifrování, které lze zapnout v nastavení a používat jej. Pro úlohy byl zvolen program Veracrypt více důvodů. Prvním a také hlavním důvodem pro použití aplikace Veracrypt je možnost sdílení dat mezi jinými operačními systémy na kterých je nainstalován Veracrypt. Druhým důvodem je dostupnost aplikace, což zde představuje možnost stažení na známé operační systémy jako je již zmíněný Windows, Linux ale také macOS. Dále v dostupnosti hraje roli cena, kde Veracrypt je zdarma ke stažení (a následné instalaci). Veracrypt byl stažen z oficiálních stránek Veracryptu a následně nainstalován. Z důvodu malé důvěry správnosti překladu a lepší orientace byla vybrána možnost instalace v anglickém jazyce.

Při spuštění aplikace se otevře okno, ve kterém jsou ukázány disky (popsány velkými písmeny s dvojtečkou). V oknu byla vybrána možnost „create volume“. Tato možnost vytvoří úložný prostor. V průběhu vytváření se aplikace dotáže na možnosti, kde si uživatel vybere možnost, která je pro něj užitečná. Pro potřebu úlohy byla vybrána možnost vytvoření zašifrovaného souboru. Dále byly vybrány možnosti „standart volume“, výběr uložení (plocha), šifrování (AES) a použit nejlepší možný hash (SHA-512) algoritmus, zvolena velikost (1 GB), nastaveno heslo, nastavení formátu (nechán předem vybraný). Tímto byla tvorba úložného prostoru dodělána a bylo potřeba do něj vložit nějaká data na zašifrování.

Pro tento účel byl vytvořen soubor s pár řádky textu. Následně byl nahrán úložný prostor, který byl pár minut zpět vytvořen, vybrán disk, zadáno heslo pro jeho otevření a otevřela se složka. Tato složka byla dočasně vytvořena jako vybraný disk. Soubor s textem byl vložen do dočasné složky. Složka byla zavřena a v programu Veracrypt zrušeno její nahrátí (tzn. disk zmizel ze složky „Tento počítač“. V tuto chvíli bylo již vše splněno a soubor byl zašifrován. Jediné, co bylo potřeba bylo zapamatovat si heslo pro další použití a přístupu k souboru.

Zjištění hesla na Virtuálním počítači

Odzkoušeno bylo více možností, jak úlohu provést. První odzkoušení bylo na virtuálním počítači. Toto provedení znamenalo stažení programu pro provoz virtuálního počítače. Použitý program se nazývá VirtualBox (celým názvem „Oracle VM VirtualBox“). V programu pro použití virtuálního počítače je potřeba počítač „vytvořit“, tzn. z počítače na kterém je provozován VirtualBox nastavit parametry, které vymezí maximální zatížení reálného počítače. Vymezením maximálního zatížení je zde myšleno, jak použití dostupné paměti počítače pro uložení dat, tak nastavení parametrů pro „funkčnost“ počítače (těmito parametry jsou velikost operační paměti, počet procesorů). Dále bylo potřeba navštívit internetové stránky poskytovatele operačního systému Kali Linux pro stažení instalačního balíčku. Zde byl vybrán klasický instalační balíček („Installer Images“) s nejnovější verzí. Klasický balíček byl vybrán z důvodu použití aplikace VirtualBox a umístění operačního systému právě na vytvořený virtuální počítač, tak aby bylo možné používat Kali Linux jako kdyby byl na reálném zařízení. Dále se instalační soubor nahrál do virtuálního počítače skrze funkci, kterou VirtualBox obsahuje. Instalační soubor se zde otevřel a byl nainstalován v pár krocích, kde si uživatel mohl zvolit z předem určených možností. Následně bylo potřeba si založit profil na operačním systému Kali Linux z důvodu jeho používání (stejný systém používání profilu jako u operačního systému Microsoft Windows, tzn. vytvoření přihlašovacího jména a hesla, kterým se pak uživatel přihlašuje).

Celé prostředí bylo tedy připraveno k použití nástroje, který operační systém Kali Linux obsahuje. Dříve tento nástroj nebyl v základním balíčku, ale již pár let jej verze operačního systému Kali Linux obsahují. Nástrojem použitým v úloze je Hydra. Tento nástroj slouží k zjišťování hesel uživatelů služeb (zkušení hackeři, kteří mají zlomyslné záměry s dostatečným odhodláním naleznou údaje u jakýchkoli služeb, které mají databázi v elektronické podobě). Je možnost Hydru stáhnou i manuálně, například pokud by nefungovala v nainstalované verzi nebo by osoba chtěla využít pouze Hydru, tzn. byla by vybrána taková verze osobou, která neobsahuje nástroje operačního systému Kali Linux. Nainstalovaná verze obsahovala nástroje, tudíž nebylo potřeba instalovat soubory navíc.

Tato verze obsahovala více možností, jakým způsobem spustit nástroj. Nástroj lze spustit ve velmi podobném typu prostředí jako například windows powershell, WSL nebo příkazový řádek. To znamená že jsou zde pouze příkazové řádky, kde se píšou určené příkazy na vyvolání akce. Druhou možností je spustit nástroj, tak aby se v něm dalo jednoduše orientovat. Tento typ spuštění otevře okno, ve kterém jsou informace

uspořádány a je potřeba znatelně méně znalostí nebo zkušeností než u předchozí možnosti. Okno je děláno na podobný způsob jako je například okno „vlastnosti“, které se otevře přes kliknutí pravým tlačítkem na soubor a vybráním řádku s názvem vlastnosti (nebo zkratkou Alt + Enter).

V obou případech je potřeba mít nainstalován operační systém Kali Linux na virtuálním počítači a mít jej zpuštěný. Podle prvotního nastavení při instalaci operačního systému Kali Linuxu je potřeba zvolit, jak prostředí bude vypadat. V případě výběru možnosti prostředí, které svým stylem připomíná prostředí více verzí Microsoft Windows, což je možnost s názvem Xfce neboli základní prostředí plochy Kali. Spodní lišta neboli panel, na který jsou uživatelé windowsů zvyklí se v tomto případě nachází na horní části obrazovky. Panel funguje podobně jako na windowsech.

Při výběru první možnosti bylo potřeba rozkliknout levé horní tlačítko s logem Kali Linuxu a vybrat z nástrojů Hydru, která se otevře jako příkazový řádek. Jinou možností, která je o trochu lepší z pohledu jistoty bylo otevřít příkazový řádek a zadat příkaz „sudo hydra“ pro otevření hydry s oprávněním jako na windowsech administrátorovo oprávnění. Zde bylo potřeba zadat heslo účtu uživatele virtuálního počítače. Dále bylo potřeba zadat příkazy pro uvedení stránky, jména účtu a hesla účtu, na které se bude útočit. Jméno již je známé, proto se vyplnilo napřímo s příkazem „-l uživatel“. Na místo uživatele se dosadilo název profilu a dále se zadalo heslo pod příkazem „-P hesla.txt“. Zde byl vytvořen soubor obsahující hesla, která mohou být použita k přihlášení. Jedno heslo ze souboru je správné a zbytek je špatný neboli nesprávné. Dále se vyplnil cíl, na který se bude útočit. Cílem je zde internetová stránka, tudíž lze zadat celé URL stránky s příkazem. Příkaz je zde „module, tzn. například www.názevstránky.com/login.

Zjištění hesla za pomoci WSL

V prvním kroku bylo potřeba nainstalovat Windows Subsystem for Linux (WSL). Tato instalace byla velmi snadná, protože je to produkt Microsoftu, tudíž na počítači používajícím operační systém Microsoft Windows stačilo zadat do příkazového řádku, který byl otevřen zkratkou „okna + R“ (windows + R) a napsáno do pole cmd (zkratka pro „command line“), příkaz pro spuštění. Do příkazového řádku se pak napsalo „wsl --install“ a potvrdilo se pár vyskakujících oken pro změny v počítači. Po krátké instalaci, jejíž průběh šel pozorovat v příkazovém řádku, jedna z posledních zpráv v příkazovém řádku byla operace proběhla úspěšně. Dále bylo potřeba restartovat počítač a proběhl zde „reboot“.

Po restartu a přihlášení se do počítače se otevřel program Ubuntu ve kterém bylo psáno, že se instalace dokončuje. V obou programech (WSL i Ubuntu bylo potřeba zadat heslo a jméno pro potvrzování akcí. Pro použití Linuxových nástrojů bylo dále potřeba stáhnout Linux aplikaci. Lze stáhnout pouze nástroje bez potřeby Linuxu, ale Hydra se nezobrazila na počítači, kde byla instalace provedena. Stažení Linuxu lze provést více způsoby. Prvním způsobem je instalace přes příkazový řádek. U této možnosti bylo potřeba znát příkaz pro stažení. Druhou možností je otevřít Microsoft Store a do vyhledávače napsat Kali Linux. Vybráním Kali Linux v aplikaci a kliknutím na „získat“ se nainstaluje Kali Linux skrze Microsoft Store. Pro snadnější instalaci byla vybrána druhá možnost.

Po instalaci bylo potřeba otevřít aplikaci a zadat heslo a jméno pro potvrzování akcí. Z důvodu nefunkčnosti některých příkazů v příkazovém řádku bylo potřeba odzkoušet více příkazů, které by tuto chybu mohly opravit. Těmito příkazy byly „sudo apt-get update“, „sudo apt-get upgrade“. Po odzkoušení těchto příkazů bylo zjištěno, že nebyla žádná změna, tudíž problém přetrval. Po delším hledání byl nalezen příkaz „kali-tweaks“, díky kterému se dalo dostat do nastavení úložišť a změnit jednu z možností. Po této změně bylo možné pokračovat dále, protože byl problém vyřešen.

Pro lepší orientaci v prostředí Kali Linuxu byl zadán příkaz „sudo apt install -y kali-win-kex“, který umožnil záměnu příkazového řádku za okno, které vypadá podobně jako plocha na počítači s operačním systémem Microsoft Windows.

Po seznámení se s oknem byla vysunuta lišta (podobná dříve nazývané liště „Start“ na počítači používajícím operační systém Microsoft Windows) a vybrán nástroj Hydra. Oproti verzi nainstalované na virtuálním počítači zde nebyla možnost výběru z grafického zobrazení nástroje Hydra a příkazového řádku nástroje Hydra. Z tohoto důvodu byl spuštěn příkazový řádek s nástrojem Hydra.

Po otevření příkazového řádku se objevily instrukce k nástroji a zároveň byl nástroj přednastaven pro lehčí použití (tzv. hydra-wizard). Dále stačilo postupovat podle požadovaných kroků (tzn. zadávat požadované informace, soubory atd.).

Permanentní smazání dat

Je více možností, jak smazat data, ale permanentní smazání je obtížné z pohledu neobnovitelnosti dat (tzn. data nebude možné po smazání obnovit). Pro pleší pochopení je potřeba uvést, jak jsou data na počítači smazána. Když uživatel smaže data, tak dojde k tomu, že se ta data označí a systém je považuje za přepsatelná. Tato přepsatelná data se

následně ukazují jako volné místo na disku. Při označení jsou data přeměněna na jiná data, z kterých při klasickém otevření tohoto souboru by z něj obyčejný člověk nic nezjistil. Existují programy na obnovu dat, které použijí stejný algoritmus jako při jejich smazání, ale v tomto případě pro obnovu. Z tohoto důvodu jsou aktuálně dvě nejlepší možnosti, jak smazat data, kterých se osoba chce zbavit do takové míry, aby již nešly obnovit. První možnost je zničení disku. Tato možnost je dobrá, pokud na disku byly citlivé data nebo data s utajovanými informacemi. Konkrétním komponentem, který je potřeba zničit je tmavá destička, ze které by data šli obnovit. Pokud se osoba rozhodne, že nechce z jakýchkoli důvodů zničit disk, tak nastává čas pro druhou možnost. Druhou možností je použití lepšího algoritmu (v tomto případě je algoritmem myšleno více přepsání dat). Pro tento typ smazání dat je dobré použít program s názvem Eraser. Program je dostupný na internetu zdarma.

Pro potřeby úlohy byl stažen a nainstalován program Eraser. Aplikace lze použít více způsoby. Oba způsoby byly odzkoušeny. Prvním způsobem bylo kliknutí pravým tlačítkem myši na soubor, který byl vytvořen pro smazání. Následné vybrání řádku s názvem aplikace Eraser, kde se rozbalily možnosti a bylo vybráno odstranit. Druhá možnost je klasickým stylem odstraňování (tzn. buď kliknutím na soubor a zmáčknutím tlačítka delete na klávesnici nebo vybráním pravým tlačítkem myši a odstranit). V obou možnostech bylo poté potřeba otevřít aplikaci Eraser a vybrat soubor, který byl určen na smazání. Dále se vybrala lokace odkud se bude soubor mazat (v tomto případě „Koš“), možnost typu smazání (US DOD 5220.22-M) a zvolena možnost smazání ihned.

Cloudové úložiště

Jelikož obsahem této úlohy je práce s cloudovými úložišti, tak na operačním systému nezáleží, protože přístup ke cloudovému úložišti je přes internet. Byly vybrány tři rozdílná úložiště, ale všechny tři jsou dostupné do určité části zdarma. Těmito úložišti jsou Google drive, Mega a TeraBox. Pro použití všech tří cloudových úložišť je potřeba se zaregistrovat. Každé z úložišť nabízí jiné možnosti, co se ukládání týče.

První částí úlohy byla registrace (registrace je zdarma a účty by zůstaly studentům i nadále). Po zaregistrování bylo možné se dostat do rozhraní, které fungovalo jako hlavní stránka po přihlášení. Zde byla lišta s více možnosti a tlačítka na přidání souboru. Jak je již zmíněno ohledně možností úložiště, tak každé úložiště ve výsledku bylo použito pro jiný účel. Například do TeraBoxu lze uložit malý počet souborů se znatelnou velikostí (až do jednoho terabytu).

Nahrávání souborů bylo velmi jednoduchou záležitostí, neboť všechny úložiště mají tlačítko, přes které lze soubory nahrát. Úložiště také obsahují možnost tvorby složek, kde bylo potřeba stejně jako na ploše složku pojmenovat a dále se dala používat.

Velkým plusem cloudových úložišť je možnost sdílení souborů. Tato funkce nebyla zkoušena, ale je velmi užitečná jak pro domácí účely, tak pracovní.

Základy programování

Vzdělávací hry jsou jednoduchou možností, jak osoby je hrající něco naučit a zároveň zabavit. Pro tuto úlohu byly vybrány vzdělávací hry Elevator Saga, Human Resource Machine a CodeCombat.

Elevator Saga je volně dostupná a bez registrace v prohlížeči a úkolem hrající osoby je dostat pasažéry na nebo z podlaží. Při této úloze je potřeba využít hodně logického myšlení a zároveň přemýšlet jako programátor na napsání příkazů. Úloha byla procvičena do 8 kola. Prvních pár kol se opakovalo z pohledu příkazů, ale nabývaly stále na obtížnosti. Příkazy byly psány způsobem příkazových řádků. Kolo šlo pokaždé zpustit znovu a opravit chybu, která se objevila nebo zapřemýšlet, kde chybí část příkazů, aby bylo kolo splněno.

Další úlohou byl CodeCombat. Tato hra je taktéž volně dostupná a bez registrace na internetu zdarma, ale pouze do určité úrovně. S registrací hra odzkoušena nebyla, ale je zde nabízena i možnost pro založení skupinového prostředí, které založí vyučující a žáci se přes kód napojí. Hra nabídne více možností (programovacích jazyků) ve kterých lze hrát. Po zpuštění bylo potřeba tedy vybrat programovací jazyk a postavu pro započnutí. Jak již bylo tedy zmíněno CodeCombat je vhodný pro školy, kde vyučující distribuuje kód (neboli klíč). Hra progresivně naučila pohyb objektem (zde vybraná postava) po hrací ploše a následné akce postavy (vizuálně doprovázeno pro jednoduché zjištění chyb).

Poslední navrženou hrou bylo Human Resource Machine. Tato hra je placená, ale bylo možné sehnat legální kopii této hry skrze Epic games v období Vánoc. Z důvodu tvorby diplomové práce byl pro účel použití ve školním prostředí založen profil na Epic games, který obsahuje pouze tuto hru. Účet byl založen pouze za účelem předání škole, tudíž pokud bude vedoucí práce mít zájem, tak účet bude předán i s emailem, který byl za účelem tvorby profilu vytvořen. Ve hře Human Resource Machine jde o přenášení a počítání boxů s čísly za pomoci slov, které zde představují příkazy. Zde také narůstá obtížnost s postupem úrovní. Tato hra nebyla odzkoušena, ale bylo o ní zjištěno dostatečné množství informací pro její navržení.

Phishing kvíz

U této úlohy, stejně jako u předešlých, je irelevantní, na kterém operačním systému je prováděna. Phishing kvíz od googlu jako návrh pro úlohu byl vybrán z důvodu jeho velmi dobrého zpracování a pro informovanost studentů, která má za účel přispět nejen při studiu, ale i v zaměstnání a běžném životě. Phishing kvíz byl odzkoušen až od poslední možnosti neboli při odzkoušení byl Phishing kvíz dokončen. Z phishing kvízu byly získány nové vědomosti a zjištěno, jakým způsobem phishing funguje v praxi.

Vyhledávání osob nebo míst

Byly zde použity nástroje, které společně spadají pod název OSINT. Jelikož tyto nástroje jsou skrze webové stránky, tak na operačním systému počítače zde nezáleží. Pro procvičení byly použity dříve pořízené fotky.

V první možnosti byly použity vyhledávače, které mohou hledat obrázky zpětně (tzn. vyhledávat lokaci podle obrázku). Nejlepšími vyhledávači byly Google, Microsoft Bing, TinEye a Yandex. Před vyhledáváním bylo potřeba obrázky posoudit a z pozadí a okolí zjistit, kde by foto mohlo být pořízeno.

První obrázek byl vyhledáván ve vyhledávačích podle obrázku a doplněn vyhledáváním ze stránek s podobnými obrázky. Vyhledávače navrhly mnoho podobných obrázků, ale každý byl z jiného místa. Proto bylo potřeba obrázek upravit skrze jeho ořezání a přiblížení pro nalezení podobnosti ve výsledcích. Při nalezení podobnosti byly otevřeny stránky s již zmíněnou podobností a prohledány, zda lokace odpovídá.

Druhý obrázek byl stylem „selfie“, proto zde bylo potřeba použít „Cleanup.pictures“ pro smazání objektu (zde osoba) před klíčovými prvky, díky kterým lze nalézt lokaci. Zbytek postupu byl stejný jako u předchozí metody.

Pro třetí obrázek byly použity nápisy, které jsou používány pro označení. Konkrétně tím nápisem byla část názvu hotelu. Při nalezení hotelu se správnými budovami v okolí šlo poznat, kde bylo foto pořízeno.

Čtvrté foto bylo pořízeno v krajině bez budov, které by se dali použít pro lehké nalezení. Ve fotu bylo zachyceny části dětského hřiště, les a zvířat ze dřeva. Díky těmto částem bylo lehčí nalézt lokaci. Skrze Google Earth byly nalezeny hřiště a bylo vzato v potaz, že foto bylo pořízeno v České republice. Stačilo již jen najít hřiště s lesem a dřevěnými zvířaty.

Dále se skrze obrázky potvrdilo, že je to správná lokace a díky Google Earth se dala odhadnou přibližná pozice fotografa.

Další, tedy páté foto bylo nalezeno skrze „Meta Data“. Pro toto hledání byla použita webová stránka „Forensically“. Stačilo zde nahrát obrázek a zakliknout Meta Data záložku. Ta vypsala data obrázku a hlavními daty byly GPS data. Dále se zaklikla záložka „Geo Tags“ a díky GPS datům bylo nalezeno téměř přesné místo, kde bylo foto pořízeno.

Vyhledání telefonního čísla

Stejně jako u předchozí úlohy na operačním systému zde nezáleží, protože nástroje jsou používány skrze webové stránky. Jedním z prvních pár kroků bylo potřeba otevřít Google cloud konzoly, přes kterou se bude používat nástroj na hledání telefonního čísla. Dalším z kroků spadajících mezi prvních pár bylo otevřít „Github“ stránku nástroje PhoneInfoga. Při sjetí níže na této stránce byly vypsány informace. Skrze kliknutí na dokumentaci, začínáme (Getting Started) a následně na instalaci (Installation) byly nalezeny příkazy na použití nástroje skrze „Docker“. Zde se zkopíroval příkaz „docker pull sundowndev/phoneinfoga:latest“. Dále se vrátilo k Google cloud konzoli (při použití vyhledávače nalezena jako „Google Cloud Platform“) a vybrána možnost „Activate Cloud Shell“ ve vrchní liště v pravém rohu. Do konzole se vložil zkopírovaný příkaz a klikl Enter (na klávesnici) pro potvrzení. Chvíli se počkalo a po dokončení se zadal příkaz „docker run -it -p 8080:8080 sundowndev/phoneinfoga serve -p 8080“. Dále se v liště konzole vybralo tlačítko „Web Preview“ a v základu po vysunutí možností by měl být port 8080, pokud je jiný tak lze přepsat skrze „Change port“ nebo změnit v příkazu. Z předchozího příkazu byla tedy vyvolána stránka na portu 8080 s nahraným nástrojem PhoneInfoga. Na tuto stránku bylo nejjednodušší se dostat přes stejné tlačítko, kterým je „Web Preview“ a přes rozbalenou lištu vybrat „Preview on port 8080“. Tato možnost tedy otevřela stránku v novém okně a zde stačilo již jen zadat číslo, které bylo hledáno z jakéhokoliv důvodu. Dále tedy byly vypsány informace o čísle a nabídnuty možnosti vyhledání. Jelikož bylo použito osobní číslo, tak jedinou možností bylo použít „Googlesearch“ (jedna z možností nástroje, který použil přichystaný příkaz) na vyvolané stránce a pokusit se jej najít zde.

8.1 Posouzení úloh

Všechny typy úloh jsou vhodné pro získání znalostí a/nebo informací, které lze aplikovat do budoucího pracovního nebo soukromého života. V navržených úlohách phishing kvíz,

základy programování a cloudové úložiště nebude dostatečná přidaná hodnota, tudíž dále nejsou brány v potaz.

Úlohy vyhledávacího typu, což jsou vyhledávání osob nebo míst (OSINT) a vyhledávání telefonního čísla plně nesedí do studijního programu, který je na fakultě nastaven pro obor Rizikové inženýrství, tudíž i přes to že jsou užitečné, tak jejich navržení dává menší smysl než u zbytku navržených úloh. Přesto je třeba zmínit, že zacházení s OSINT prostředky je velmi užitečná zkušenost. PhoneInfoga je již méně užitečná, ale mohou se vyskytnou případy, kdy osoba potvrdí přijetí hovoru a na druhém konci se osoba nepředstaví, položí otázky nebo začne mluvit a následně se vyptává na jméno toho, kdo zvedl hovor.

Jelikož velkým rizikem jak pro firmu, tak i jednotlivce může být nedostatečná bezpečnost v oblasti zařízení, která se mohou napojit na internet, tak byly vybrány návrhy na úlohu spojené se zajištěním právě psané oblasti bezpečnosti. Těmito navrženými úlohami jsou zašifrování dat, zjištění hesla (obě varianty, tzn. WSL a VirtualBox) a permanentní smazání dat.

9 KONZULTACE

Následovala konzultace o navrhovaných úlohách s vedoucím práce. Obě strany předložily své návrhy. Původní doporučení se zaměřila na úlohy, které by bylo možné splnit v prostředí kybernetické laboratoře. Bylo navrženo osm úloh. Mezi navržené úlohy patřily i úlohy uvedené na obrázku "Nápady na úlohu" (obrázek 1). Bylo také zjištěno, že několik úloh bylo již dříve splněno. Zejména nemělo smysl navrhovat zašifrování dat a permanentní smazání dat, protože již byly používány.

Na zbývající úlohy mají zpracovatel i vedoucí práce poměrně podobné názory. Tyto názory se velmi podobají informacím v předchozí části (Posouzení úloh).

9.1 Výběr z odsouhlasených

Po návrhu následoval výběr úloh. Úlohy, které byly odstraněny (tzn. zašifrování dat a permanentní smazání dat) již nebyly brány v potaz. Výměnou názorů se možnost výběru snížila na tři. Těmito úlohami, které byly vhodné a odsouhlasené se staly zjištění hesla (Hydra), phishing kvíz od Googlu a vzdělávací hry, které podporují programovací jazyk Python a který se v nich lze určitým způsobem naučit. Po další domluvě byl vybrán nástroj Hydra neboli návrh úlohy zjištění hesla. Pro tuto úlohu bylo nutné zjistit, jakým způsobem by mohla být provedena. Z diskuze vzešlo, že díky procvičení virtuálního počítače by bylo možné ji navrhnout na virtuální počítač, ale preferovanou možností je naučit studenty dalším věcem, což znamenalo stažení programu WSL a následné nastavení a spuštění aplikací včetně nástroje Hydra.

10 POTŘEBNÉ ČINNOSTI, NÁSTROJE A APLIKACE PRO PROVEDENÍ NAVRŽENÉ ÚLOHY

Pro navrženou úlohu je potřeba mnoho činností, nástrojů a aplikací, které je potřeba si připravit předem nebo během úlohy. Její zpracování bez postupu vyžaduje mnoho znalostí. Níže jsou uvedeny činnosti a nástroje potřebné ke splnění návrhu úlohy, což je úzce spojeno s jejím vypracováním.

10.1 Činnosti

Níže jsou uvedeny všechny činnosti, které jsou potřeba k provedení úlohy. Jedná se o následující činnosti – nalezení a použití příkazů; restart a reboot; tvorba souboru.

10.1.1 Nalezení a použití příkazů

První z činností je nalezení a správné použití příkazů, které budou v průběhu úlohy použity v příkazových řádcích, webových stránkách a nástrojích. Příkazy pro webové stránky jsou velmi snadné, protože jejich používání je již předdefinováno v pravém kliknutí myší na zobrazenou webovou stránku nebo načtení webové stránky a použití příkazového řádku. Při první možnosti (pravé kliknutí myši) se zvolí „Prozkoumat“ a nalezne se zde adresa stránky. V možnosti s příkazovým řádkem je zadán příkaz „ping“ díky kterému je nalezena odezva stránky společně s její adresou. Dále příkazů do příkazových řádků pro potřeby úlohy je mnoho a jsou použity ve více příkazových řádcích. Je potřeba začít v příkazovém řádku Microsoft Windows nebo použít jeho alternativu „Windows PowerShell“. U těchto dvou příkazových řádků na výběru nesejde, neboť jsou téměř identické a je to pouze otázka preference pro potřeby úlohy. Následně jsou příkazy zadávány do příkazového řádku operačního systému „Kali Linux“. Program „Ubuntu“, který byl nainstalováno v navržené úloze je pouze jako prostředník pro „Kali Linux“ a není zde potřeba zadávat žádná příkazy pouze pokud je osoba (v tomto případě žák) dotázána na nastavení jména a hesla, tak je potřeba tyto informace zadat. Následně jsou příkazy psány do příkazového řádku nástroje Hydra, kde se odehrává hlavní část navržené úlohy, díky které vznikne výstup z úlohy. Příkazy pro každou z částí jsou níže zmíněny v ukázce postupu.

10.1.2 Restart a reboot

Další potřebnou činností byl restart počítače nebo lépe řečeno „reboot“ počítače. Před započnutím navržené úlohy je potřeba se dostat do BIOS části používaného počítače. Je to

potřeba z důvodu vypnuté virtualizace. Do BIOS části se lze dostat více možnostmi, ale nejsnadnější možností je restart a mačkání tlačítka „Delete“ na klávesnici. Zde bylo potřeba následně nalézt možnost povolení virtualizace a následně v prostředí počítače po provedení změny lze najít ve správci úloh, zda tato změna byla uložena. Druhý restart nebo tedy „reboot“ byl po instalaci WSL, kde byl nainstalován operační systém „Ubuntu“ jako program do počítače. Skrze příkazový řádek je osoba vyzvána k provedení akce „reboot“ pro dokončení instalace.

10.1.3 Tvorba souboru

Nedílnou součástí pro potřeby navržené úlohy byla tvorba souboru ve formátu textového souboru. Tento soubor je pojmenován „hesla.txt“, kde koncovka značí formát souboru. Tvorba souboru byla jednoduchá, ale tvorba kontextu v souboru byla již těžší. Zde bylo potřeba použít kreativní myšlení společně se zkušenostmi a informacemi získanými z tvorby navržené úlohy. V souboru je dvanáct řádků, které obsahují potencionální hesla k profilu, na který je proveden útok. Tato hesla bylo potřeba navrhnout tak, aby při použití programu nebylo spotřebováno mnoho času kvůli čekání na výsledek z „brute force“ metody. Navrhnutí takových hesel znamenalo použití malého množství zásad, které jsou dále uvedeny v checklistu níže. Soubor je následně potřeba nahrát na webové stránky, pro potřeby navržené úlohy. Tato potřeba je z důvodu jednoduchého vložení souboru do režimu okna v aplikaci operačního systému Kali Linux, neboť úloha bude s velkou pravděpodobností přidána do školních „moodle“ stránek.

10.2 Nástroje a aplikace

V průběhu úlohy je použito větší množství nástrojů, z tohoto důvodu jsou zde uvedeny. Jedná se o následující nástroje a aplikace – Příkazový řádek nebo Windows Powershell, Windows Subsystems for Linux, Ubuntu, Kali Linux a Hydra.

10.2.1 Příkazový řádek nebo Windows PowerShell

Prvním použitým nástrojem je příkazový řádek nebo „Windows PowerShell“. Teno nástroj je v počítačích obsahujících operační systém Microsoft Windows již v základu. Příkazový řádek mají i jiné systémy, ale Windows PowerShell je pouze v počítačích používajících operační systém Micrsoft Windows. Zde byl zadán pouze jeden příkaz po povolení virtualizace a tímto příkazem je „wsl --install“.

10.2.2 Windows Subsystems for Linux

Druhým použitým nástrojem je WSL. Tento nástroj je v podobě příkazového řádku a jeho hlavní účel je zprostředkování použití aplikací a nástrojů, které jsou v operačním systému Linuxu používány nebo předem nainstalovány. Pro dokončení instalace WSL je potřeba provést „reboot“ počítače.

10.2.3 Ubuntu

Jakožto jednou z verzí operačního systému Linux je Ubuntu, tak je právě tento operační systém nainstalován v podobě aplikace a jeho účelem je zprostředkovat možnost používání Linuxových aplikací společně s WSL. Tyto dvě aplikace jsou v navržené úloze vzájemně používány pro dosažení právě použití nástrojů a aplikací Linuxu, jak je již zmíněno v části WSL.

10.2.4 Kali Linux

Kali Linux je nainstalován skrze Microsoft Store jako aplikace. Důvodem, proč není použit příkaz v příkazovém řádku pro stažení je ten, že v Microsoft Strore aplikaci je aktuální verze Kali Linuxu, který je používán skrze WSL. Kali Linux je spuštěn jako příkazový řádek, ale příkazem pro změnu na režim okna se z něj stane něco velmi podobného ploše na operačním systému Microsoft Windows. Tento příkaz je tedy zadán pro příjemnější prostředí pro nástroj Hydra.

10.2.5 Hydra

Hydra je hlavní nástroj v navržené úloze. Tento nástroj je v již zmíněné aplikaci Kali Linux. Nejlepší možností, jak nástroj spustit je přes „sudo hydra“ příkaz. Tento nástroj v navržené úloze slouží k „brute force“ metodě útoku na kolonky s přihlašovacími údaji a následně je použit při útoku na webové stránky. Tento útok je proveden přes vyhledání adresy stránky a její zadání do nástroje. Dále je zde použit soubor hesla.txt, který obsahuje hesla a nástroj je prozkouší řádek po řádku, aby zjistil, které heslo je pro přihlášení použito.

11 ODZKOUŠENÍ ÚLOHY

Z důvodu nedostatku času byly úlohy odzkoušeny pouze na osobním počítači obsahujícím operační systém Microsoft Windows a který je určen pro domácí použití.

Teoretická příprava na odzkoušení vybrané navržené úlohy

Po procvičení úlohy předem byly získány vědomosti, které pomohly s vyzkoušením. Těmito vědomostmi jsou postup, informace o příkazech zadávaných do řádků, průběh instalací a akce pro postup správné instalace.

Bylo potřeba si nachystat všechny webové stránky a dokumenty, které byly potřeba ke stažení a instalaci. Těmito byly stránky pro stažení WSL, Kali Linuxu, VirtualBoxu. Odkazy s dokumentací byly informace k instalaci WSL, návod instalace Kali Linuxu za použití WSL, dokumentace ke spuštění Kali Linuxu graficky, dokumentace k nástroji Hydra. Po zjištění chyby, která nastala po spuštění příkazového řádku Kali Linux následná dokumentace k opravě chyby.

Praktická příprava na odzkoušení vybrané navržené úlohy

Navržená úloha zabrala hodně času, který byl hlavně v podobě čekání na dokončení instalací a změn v systému. V části počítače s názvem BIOS bylo potřeba změnit nastavení pro umožnění zapnutí virtuálního počítače. Dále bylo potřeba nainstalovat program VirtualBox. Program byl stažen z oficiálních stránek a nainstalován. V programu bylo potřeba nastavit parametry virtuálního počítače, které úzce souvisely s parametry reálného počítače z pohledu výkonu a úložného místa. Dále bylo potřeba do virtuálního počítače nahrát instalační soubor operačního systému Kali Linux. Tento soubor byl stažen z oficiálních stránek. Bylo zde na výběr z mnoha možností, ale byla stažena obyčejná instalace i přes možnost stažení instalace pro virtuální počítače. Obyčejná instalace byla zvolena z důvodu plného seznámení se s Kali Linuxem. Dále pro typ navržené úlohy bez virtuálního počítače byla stažena aplikace WSL, která po instalaci potřebovala „reboot“ systému. Tato akce vyžadovala restart počítače. Po restartu byla přidána aplikace Ubuntu. Ubuntu je ve své podstatě verze Linuxu (konkrétně otevřená distribuce, která je založena na distribuci Debianu). Dále bylo potřeba stáhnout Kali Linux. Pro tuto akci byl zvolen postup přes Microsoft Store. Z aplikace Microsoft Store byl nainstalován Kali Linux. Po otevření příkazového řádku Kali Linux byly zadány příkazy pro takzvaný „Win-KeX“. Tyto příkazy zpřístupnili možnost grafického zobrazení Kali Linux stejným způsobem, jako Microsoft Windows zobrazuje plochu počítače. V této části se vyskytl problém se

síťovými úložišti, ale byl vyřešen. V obou typech možnosti postupu (virtuální počítač a za pomoci WSL) bylo v tento moment již vše připraveno.

11.1 Řešení problémů (stránky, program)

Při chybě, která se vyskytla v postupu s WSL v prostředí příkazového řádku Kali Linux bylo potřeba odzkoušet více postupů, protože při hledání řešení bylo nalezeno více odpovědí, které byly okomentovány, že problém vyřešily. První odzkoušenou odpovědí na to, jak vyřešit problém, bylo přepsat data v umístění „/etc/apt/sources.list“. Přepsána byla všechna data a přidána další pro možnost přenosu dat z jiných úložišť, která Kali Linux poskytuje. Tato možnost byla bez kladného výsledku. Změna nezměnila výsledek a bylo potřeba využít další možnosti. Další odpovědí byla stejná situace jako v předchozí odpovědi, ale bylo přidáno pár kroků. Těmito kroky bylo přidat příkazy, které se pokusily chybu opravit. Příkazy pro pokus o opravu byly „sudo apt-get update“, „sudo apt-get upgrade“. Provedené změny neměly žádný dopad na vyřešení stále trvajícího problému. Ve chvíli, kdy byly odpovědi od ostatních uživatelů se stejnou chybou prozkoušeny a jiné možnosti nebyly nalezeny, tak bylo potřeba experimentovat z vlastních zkušeností a dostupných informací. V dokumentaci o síťových úložištích byl nalezen příkaz „kali-tweaks“. Tento příkaz otevřel tabulku s možnostmi. Díky tabulce bylo zjištěno, že je možno získat balíčky od komunity. Tato možnost byla zakliknuta, provedla se aktualizace a vylepšení za pomoci příkazů „sudo apt-get update“ a „sudo apt-get upgrade“. Po dokončení příkazů bylo zkontrolováno, zda nastavení v „kali-tweaks“ příkazu zůstalo stejné. Následně byla funkčnost vyzkoušena znovu a chyba se již nevyskytla. Dále tedy bylo možné pokračovat se příkazy, následným spuštěním a odzkoušením nástroje Hydra.

Dalším problémem, který se vyskytl, byla tvorba webové stránky pro potřeby navržené úlohy. Prvním problémem bylo vytvořit stránku, která by byla provozována přes zprostředkovatele, aby se na ni šlo dostat odkudkoli (samozřejmě s připojením k internetu). Tento problém byl vyřešen nalezením více zprostředkovatelů, kteří poskytovali zároveň tvorbu stránek. Další tentokrát zásadní problém se vyskytl při tvorbě stránek. Žádná z webových stránek nenabízela možnost registrace a přihlášení jako jednu z možností základního zdarma balíčku. Na některé z webových stránek byl zaslán email s dotazem ohledně přihlašování a přizpůsobení nastavení, které nebylo uvedeno v možnostech nastavení stránky. Tímto nastavením bylo maximální počet pokusů o přihlášení. Na email

nebyla poskytnuta zpětná vazba, tudíž bylo potřeba se obrátit na vedoucího práce, který dříve nabídl možnost tvorby těchto stránek na fakultě.

12 MOŽNOSTI PROVEDENÍ ÚLOHY

Jak již bylo zmíněno dříve je zde více možností, jak úlohu provést. Jednou možností je za použití virtuálního počítače a druhou možností je za použití softwaru s názvem „Windows Subsystem for Linux“ (zkratka WSL). Při znalostech založení virtuálního počítače je velmi jednoduché přichystat operační systém Kali Linux na právě zmíněném virtuálním počítači. Zdlouhavější metodou je zde za použití softwaru WSL, protože samotná příprava pro použití operačního systému Kali Linux potřebuje mnoho předchozích kroků a čekání na instalace a restart počítače. Tímto je potřeba následně vybrat možnost, která bude zasazena do výuky podle časových možností.

12.1 Doporučení

Zde je potřeba vzít v potaz, že nastavení virtuálního počítače bylo již studenty vyzkoušeno, což představuje jednodušší a rychlejší přípravu pro navrženou úlohu. Z tohoto pohledu by se navržená úloha dala zvládnout i v časovém napětí, kdy by se možnost bez virtuálního počítače stihnout nedala.

Navržená úloha s použitím virtuálního počítače by tedy byla vhodná při nedostatku času a případně po několika pokusech naučit studenty WSL metodou s příkazovým řádkem, které nedopadly podle očekávání. Očekáváním zde může být přesně stanovený výstup práce a čas do kdy má být práce odevzdána nebo jiné kritérium, které je potřeba naplnit. Pokud například studenti budou bezradní nebo se bát zadávání příkazů do příkazového řádku, tak to může mít velký dopad na časové zpracování. Z tohoto důvodu by bylo vhodné použít metodu s virtuálním počítačem, kde lze spustit hydra v režimu okna, které vypadá podobně jako okno „vlastnosti“, které lze otevřít přes kliknutí pravým tlačítkem myši na soubor. Toto okno je sympatičtější pro osoby, které se špatně orientují v příkazovém řádku nebo se bojí, co by zadání špatného příkazu nebo správného příkazu o kterém nic nevědí mohlo provést. Okno je velmi jednoduše vytvořeno a stačí zde do kolonek zadat informace, které jsou zde požadovány. Stručně řečeno tato metoda s virtuálním počítačem je vhodná při nedostatku času, schopností, vědomostí, „odvahy“ a orientaci v příkazovém řádku, ale získají se zde vědomosti a poznatky o nástroji Hydra v operačním systému Kali Linux a bezpečnosti hesla.

Navržená úloha s použitím softwaru WSL je vhodná pro distribuci vědomostí mezi žáky. Pokud bude vybrána tato možnost, tak s velkou pravděpodobností bude potřeba přidělit úloze více než dvě hodiny rozvrhového času (bráno jako celkový čas semináře v rozvrhu, a

ne jako dva dvouhodinové semináře). Určitě se najdou výjimky, které by navrženou úlohu zvládly ve dvou hodinách rozvrhového času, ale takových pravděpodobně moc nebude. Záleží také na výbavě, což je zde hlavně hardware počítače. Čím výkonnější počítač a internet bude, tím rychleji bude možno navrženou úlohu zvládnout. Jelikož je nedílnou součástí navržené úlohy práce s příkazovým řádkem, tak je potřeba vypsat zadávané příkazy. Zároveň je použito více příkazových řádků skrze procházení navržené úlohy od začátku až do konce. Těmito příkazovými řádky jsou „obyčejný“ příkazový řádek (ten co je již v počítačích s operačním systémem Microsoft Windows), WSL příkazový řádek, Ubuntu příkazový řádek a Kali Linux příkazový řádek. V případě příkazového řádku Kali Linux je možné podle postupu rozdělit příkazový řádek na dvě části. Těmito částmi jsou myšleny před použitím grafického rozhraní Kali Linux a po použití grafického rozhraní Kali Linux za pomoci příkazu „sudo apt install -y kali-win-kex“ neboli po instalaci Win-KeX. Tímto příkazem lze otevřít grafické rozhraní, které vypadá jako plocha u počítačů s operačním systémem Microsft Windows. Díky předchozím akcím jsou žáci učeni, jak nainstalovat software na otevření Linuxových aplikací na počítačích s operačním systémem Microsoft Windows a zároveň se naučí lépe zacházet s příkazovými řádky. Stručně řečeno tato úloha je vhodná pro získání nových poznatků a vědomostí ohledně příkazových řádků, bezpečnosti hesla, nástroje Hydra v operačním systému Kali Linux a o Kali Linuxu jako takovém (ať už v podobě příkazového řádku nebo grafického prostředí).

Z předchozích odstavců je tedy doporučena možnost, kde je použito WSL. Důvodem tohoto doporučení je získání více informací a zkušeností i za cenu delšího zpracování.

13 TVORBA POSTUPU

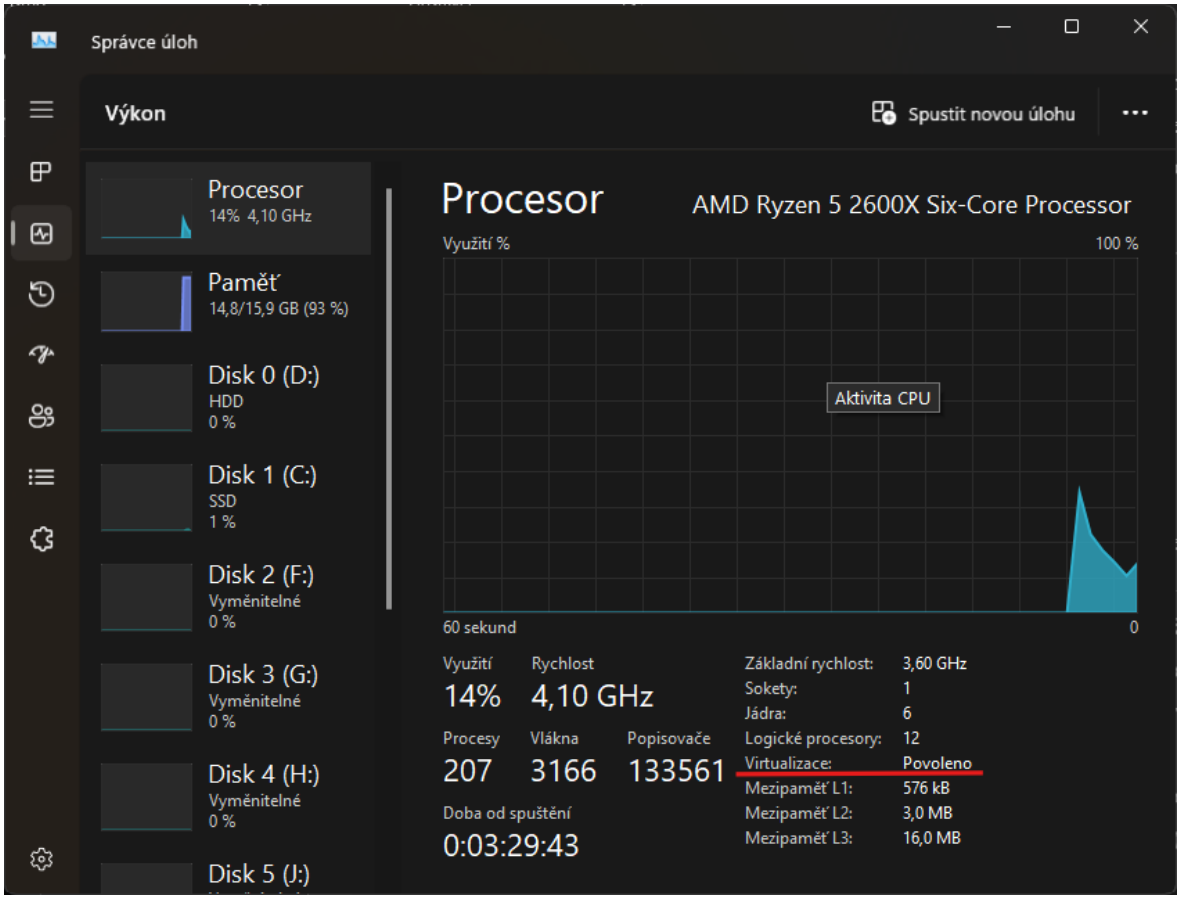
Postup byl tvořen po procvičení navržené úlohy a po odzkoušení na osobním počítači obsahujícím operační systém Microsoft Windows a který je určen pro domácí použití. V rámci této navržené úlohy bylo při tvorbě postupu potřeba projít jednotlivé kroky a uvědomit si, jak byly tyto kroky provedeny. Kroky bylo potřeba zaznamenat, aby bylo možné vytvořit postup. Ke krokům byly doplněny informace, které pomohly v postupu nebo dávají dodatkovou informaci.

13.1 Ukázka postupu

Postup by mohl vypadat, jak je uvedeno níže. Případně je možno jej upravit podle potřeby. Některé kroky nebudou doplněny obrázky z důvodu dřívějšího procvičení (tudíž dřívější instalace bez dokumentování). Část postupu byla pro potřeby obrázků vytvořena znovu, proto některé obrázky mají jiné údaje v určitých místech, něž ostatní.

13.1.1 Povolení virtualizace v prostředí BIOS

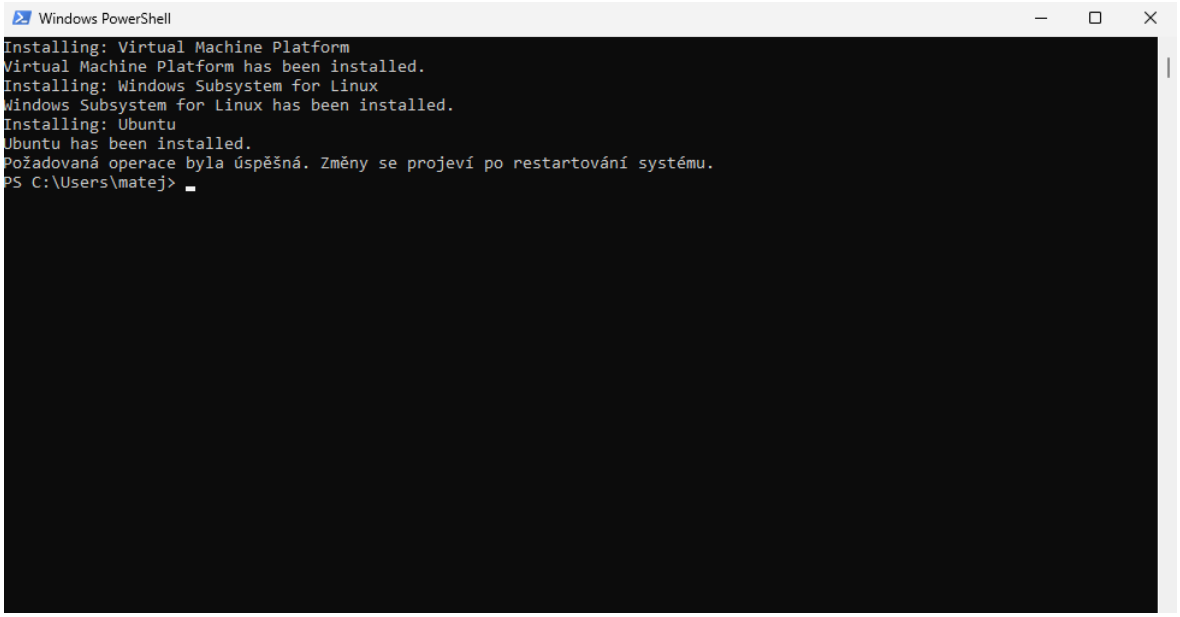
Prvním krokem je dostat se do BIOS a změnit nastavení. Nastavení, které je měněno je povolení virtualizace. Do BIOS se lze dostat buď přes klikání tlačítka „Delete“ (většina používá tlačítko „Delete“, ale je možné, že je pro tuto akci jiné tlačítko, a to lze zjistit při startu počítače) na klávesnici nebo přes nastavení („Spuštění s upřesněným nastavením“). Nastavení ohledně virtualizace se může nacházet pod různými názvy v nastavení, neboť to každý BIOS, který má rozdílné výrobce, má trochu jinak. Lze zjistit skrze správce úloh, zda toto nastavení je povoleno (v záložce výkon) a WSL právě tuto možnost může vyžadovat. Software WSL lze používat pouze na verzi Windows nižší než 2004 (sestavu 19041 a vyšší), ostatní (tzn. nižší) verze nejsou podporovány.



Obrázek 2 Virtualizace ve Správci úloh

13.1.2 Instalace WSL

Druhým krokem je nainstalovat WSL na počítač, který obsahuje operační systém Microsoft Windows (Toho bylo dosaženo díky nalezené dokumentaci obsahující instalaci WSL). Za pomoci windows + R (okna + R) nebo skrze vyhledávač v levém spodním rohu se otevře příkazový řádek a vepíše se příkaz „wsl --install“. Po kratším čekání na dokončení instalace je osoba vybídnuta k rebootu počítače, pokud instalace proběhla úspěšně.



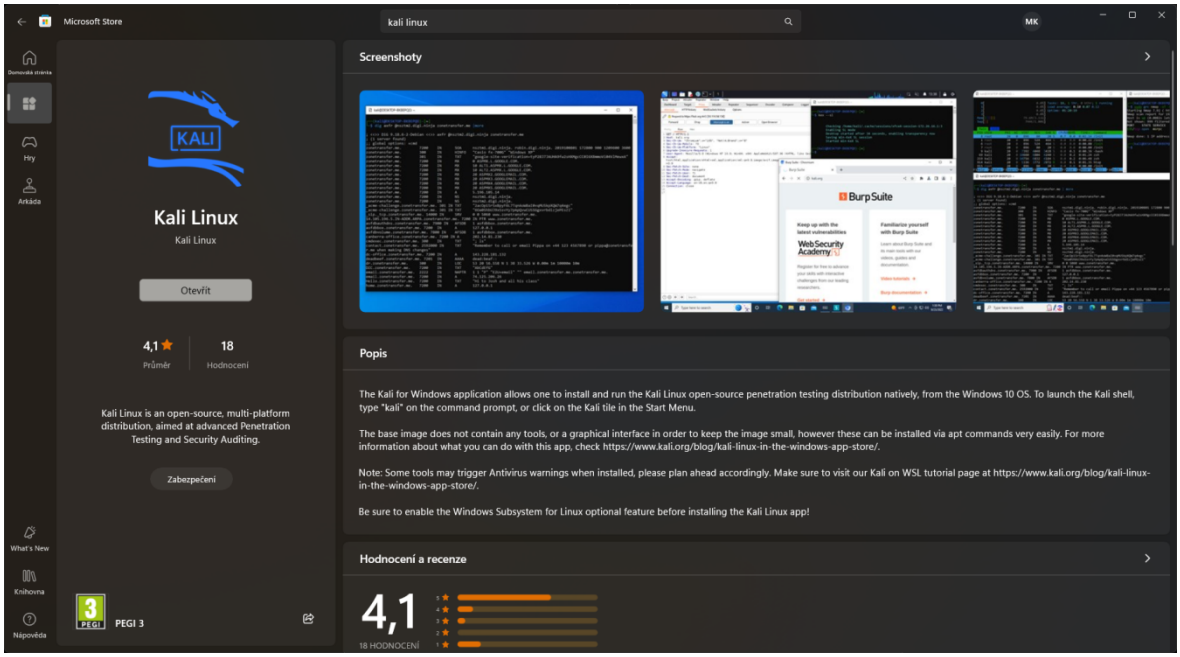
Obrázek 3 Instalace WSL

13.1.3 Reboot počítače

V třetím kroku je počítač restartován, aby bylo možné aplikovat změny. Tento restart potrvá delší dobu (podobně jako aplikování nové aktualizace systému) právě z důvodu změn. Po dokončení restartu a přihlášení se do systému počítače je přidána nová aplikace s názvem Ubuntu. Tato aplikace se sama otevře po přihlášení, pokud ne tak ji je možné najít mezi nově přidanými aplikacemi (levé spodní tlačítko okna nebo tlačítko na klávesnici okna).

13.1.4 Instalace aplikace Kali Linux

Čtvrtým krokem je vyhledání Kali Linuxu v aplikaci Microsoft Store. Skrze vyhledávač se vyhledá Kali Linux, rozklikne a klikne se získat (v levé liště). Aplikace se nainstaluje a následně lze používat.



Obrázek 4 Kali Linux v Microsoft Store aplikaci

13.1.5 Nachystání aplikace Kali Linux

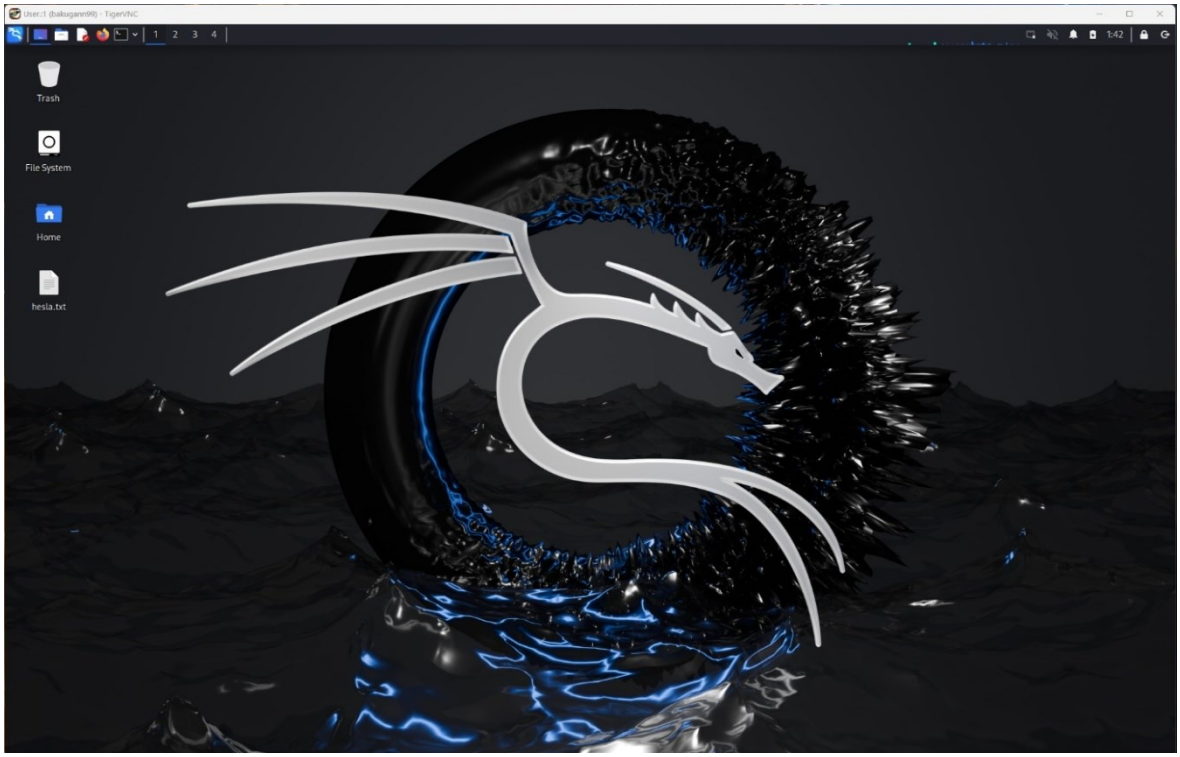
V pátém kroku se otevře nainstalovaná aplikace, kterou je Kali Linux. Tato aplikace vypadá jako příkazový řádek a při prvním zpuštění bude potřeba chvíli počkat na dokončení instalace. Po dokončení instalace aplikace požaduje vytvoření jména a hesla. Jakmile je jméno a heslo vytvořeno, tak je aplikace připravena k použití.

13.1.6 Instalace Win-KeX

Šestým krokem je instalace Win-KeX. K tomuto kroku je využit příkazový řádek Kali Linux. Do příkazového řádku je vepsán příkaz „sudo apt install -y kali-win-kex“ (sudo funguje podobně jako správce). Po zadání příkazu je potřeba zadat heslo (které je vytvořeno při prvním spuštění). V tomto kroku se čeká nejdéle ze všech kroků, ale pokud je počítač starší nebo méně výkonný, tak se čeká nejdéle na reboot.

13.1.7 Výběr režimu

V sedmém kroku je se nabízí možnost výběru ze tří podporovaných režimů Win-KeX. Pro účely navržené úlohy stačí „Window Mode“ (režim okna). Tento režim je spuštěn příkazem „kex --win -s“ v příkazovém řádku Kali Linuxu. Po zadání příkazu se objeví Kali Linux v režimu okna a již je v něm možno provádět akce. V otevřeném okně se otevře webová stránka školního Moodlu (předpokládá se, že zde je úloha zadána) a je ze zadání stažen soubor „hesla.txt“.

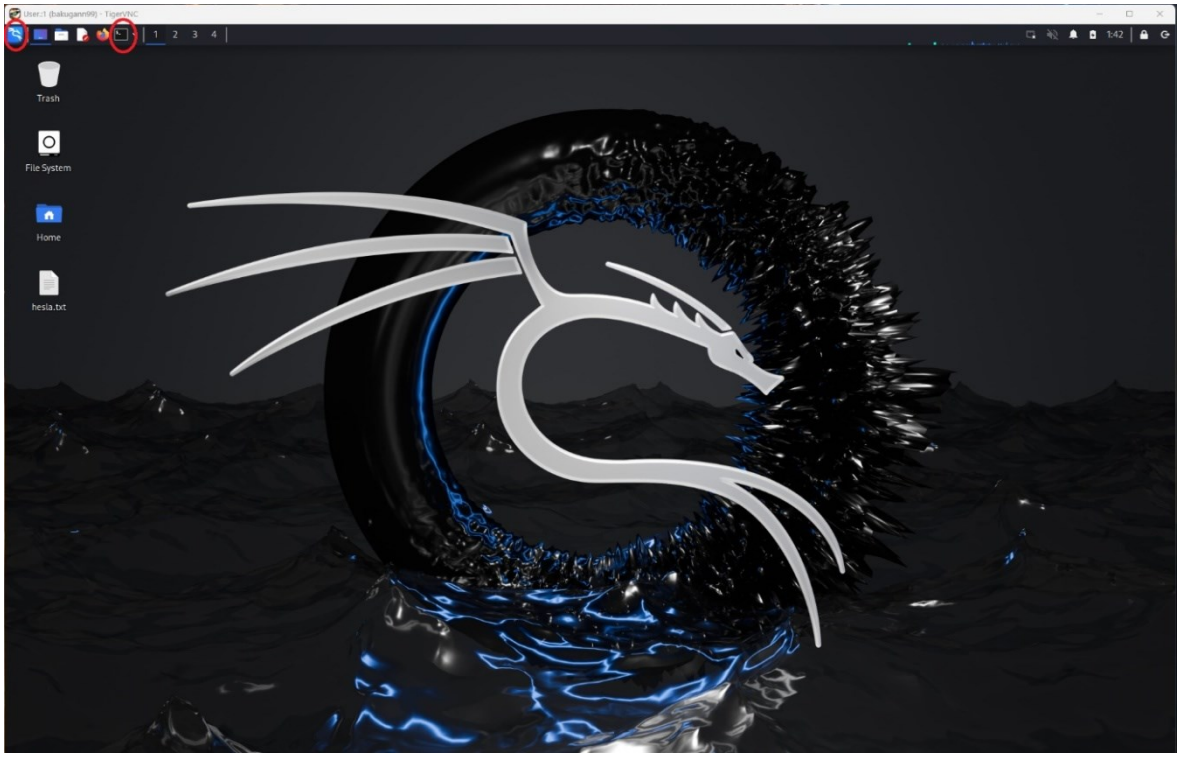


Obrázek 5 Kali Linux v režimu okna (s již přidaným souborem hesla)

13.1.8 Nástroj Hydra

Osmým krokem je otevřít nástroj Hydra. Tento nástroj se nachází ve vysunovací liště v pravém horním rohu. Lišta obsahuje vyhledávač pro jednodušší přístup k nástrojům. Nástroj je otevřen kliknutím na řádek s názvem nástroje.

Druhou možností, jak otevřít nástroj Hydra v prostředí Kali Linuxu je přes otevření příkazového řádku, který je i v grafickém prostředí (režimu okna). Tato možnost je s většími pravomocemi díky příkazu „sudo hydra“. Po zadání příkazu je uživatel vyzván pro zadání dříve stanoveného hesla.



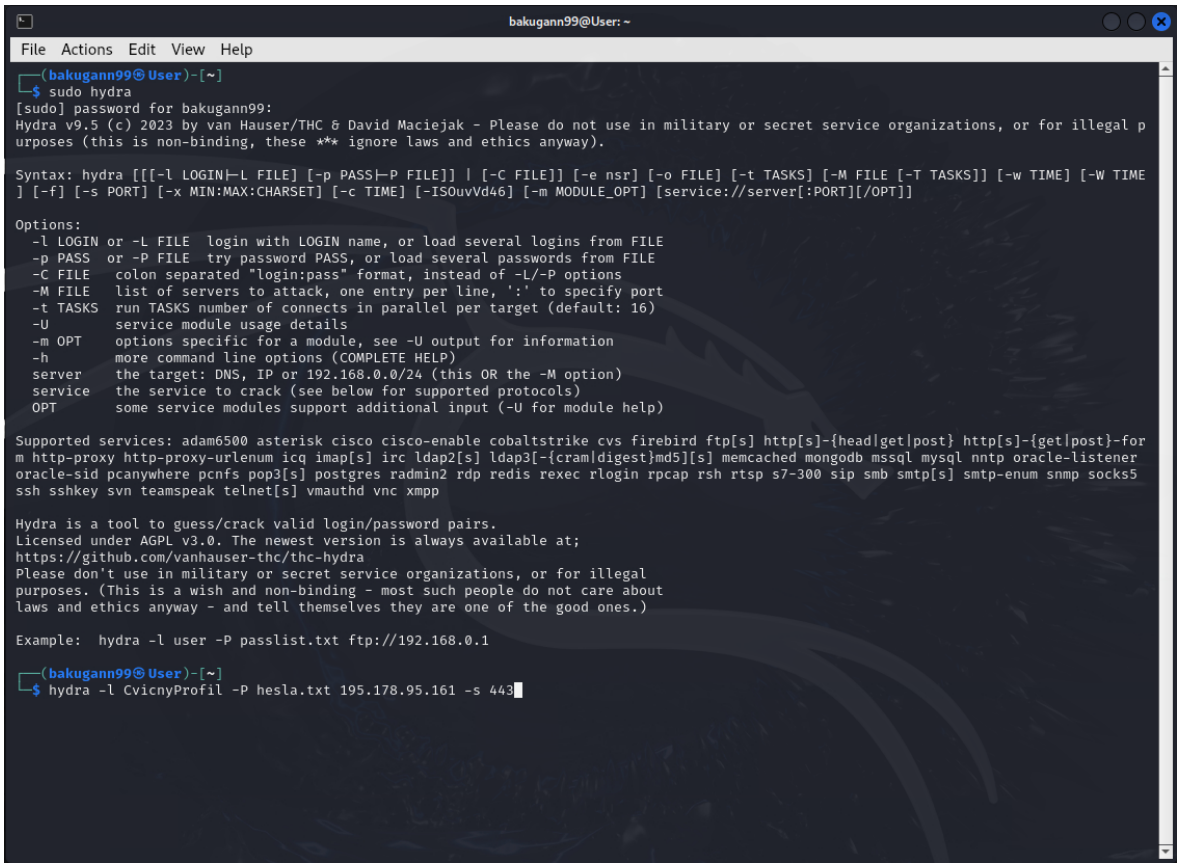
Obrázek 6 Možnosti pro otevření nástroje Hydra

13.1.9 Nalezení adresy

Devátým krokem je nalezení webové stránky, na kterou se bude útočit. Tyto webové stránky jsou specifikovány až při zadání pro studenty, ale webovými stránkami jsou stránky vytvořené zaměstnanci fakulty pro potřeby navržené úlohy. Jakmile se studenti dostanou k stránce s přihlašovacími údaji, tak jsou dvě možnosti provedení zjištění adresy webové stránky. První možností, velmi snadnou je otevřít příkazový řádek a zadat příkaz „ping“. Tento příkaz slouží pro zjištění odezvy webové stránky. Za příkaz „ping“ je vložena adresa webové stránky bez „www“ (například seznam.cz). Příkaz se pokusí zjistit jaká je odezva této stránky a zároveň vypíše její číselné přiřazení (tyto čísla jsou uvedena v DNS). Druhou možností je použít „Prozkoumat“. Tento příkaz je v prohlížeči, když je kliknuto pravým tlačítkem v prostředí webové stránky (jeden z posledních řádků při pravém kliknutí). V pravé liště, která se otevře je potřeba překliknout na „Network“ a znovu načíst stránku. Po novém načtení se zde vypíší data. Většinou chtěnou částí je první položka ve sloupci „Name“. Tato položka při levém kliknutí na ni vypíše informace. Pokud zde není „Remote Address“ v části „Request URL“, tak je potřeba přejít na další položku (tato položka má většinou při najetí na ni stejné URL, jako v horní části prohlížeče) ve sloupci. Jakmile je adresa nalezena, tak je možno ji použít v dalším kroku. Adresa je nalezena oběma kroky, takže nezáleží na tom, který je použit.

13.1.10 Útok nástrojem

V desátém kroku se útočí „brute-force“ metodou na stránky s přihlašovacím polem. Do zapnutého nástroje hydra je vypsán příkaz, který je ve vrchní části nástroje vysvětlen. Tímto příkazem je například „hydra -l CvicnyProfil -P hesla.txt 195.178.95.161 -s 443“ tento příkaz je k útoku na veřejně dostupné webové stránky Moodle školy s přihlašovacím polem (pouze ukázkový příkaz, nenalezne žádný výsledek při zadání do nástroje, tento příkaz nebyl prakticky odzkoušen). V příkazu malé l znamená přesné přihlašovací jméno a velké P soubor s hesly (proto hesla.txt). Jsou i jiné možnosti pro pokračování příkazu, ale z důvodu malého obsahu hesel a jednoduchého nalezení adresy je zvolena právě tato verze. Po zadání příkazu nástroj zjistí, které heslo se shoduje a vypíše výsledek.



Obrázek 7 Prostředí nástroje hydra s již zadaným příkazem (bez jeho potvrzení)

14 MOŽNOST ZAVEDENÍ DO VÝUKY

Ideální možností, kdy tuto úlohu použít je po odzkoušení práce s příkazovým řádkem předem, a to ať už v jiné úloze nebo ve volném čase studenta. Úlohu je vhodné umístit ke konci studia, ale pravděpodobně je jedno zda konce bakalářského nebo navazujícího magisterského studia. Úloha může být procvičována způsobem s použitím WSL nebo s použitím virtuálního počítače. Je doporučeno nástroj Hydra v navržené úloze zapínat pomocí příkazu „sudo hydra“. Při nedostatku času je možné ji přidat k úloze tvorby virtuálního počítače, která je již zavedena. Navržená úloha má také možnost být z velké části pozměněna. Možnost měnit části úlohy ji dělá flexibilní natolik, že při sdílení informací mezi studenty je možno zaměnit některé z částí a úloha poskytne stále velmi podobné znalosti.

14.1 Vyhodnocení

Navržená úloha je velkou výzvou s velkým přínosem informací. Za pomoci navržené úlohy si studenti mohou uvědomit nebezpečí, které plyne z jednoduchosti hesel a sociálního inženýrství. Díky sociálnímu inženýrství lze sestavit soubor hesel, podobný jako je v úloze. V průběhu úlohy je použito více aplikací s příkazovými řádky, tudíž je potřeba se orientovat do kterého příkazového řádku se zadávají které z příkazů. Jsou uvedeny dvě možnosti, jak navrženou úlohu provést (WSL a VirtualBox) pro lepší možnost variability a pokud by nastaly nějaké faktory, které jednu možnost udělají nedostupnou, tak lze použít zmíněná druhá možnost. Dále díky možnosti pozměnit úlohu (například změnit vybrané heslo), tak že výsledek bude sice jiný, ale průběh zůstane zachovalý z navržená úlohy dělá velmi užitečnou úlohu při sdílení informací mezi studenty (například jak zní heslo). Z procvičení navržené úlohy plyne riziko jejího zneužití, proto při navržení úlohy není v postupu zmínka, jak je možné tento nástroj zneužít a zároveň je postup tvořen tak, aby úlohu bylo možné procvičit pouze jako útok na webovou stránku, která nemá zabezpečení, jaké většina webových stránek v dnešní době obsahuje. Poskytnutí informací k procvičení navržené úlohy je tedy klíčové a navržená úloha by v budoucnu neměla obsahovat informace, které ji mohou dělat zneužitelnou.

14.2 Objasnění, proč zrovna tato úloha

Navržená úloha má potenciál přispět studentům ve všech oblastech, neboť je založení účtu na internetu (na kterékoliv webové stránce) v dnešní době možno brát za nutnost. I starší

osoby mají účty na webových stránkách (nejčastěji email) a je potřeba znát riziko špatného zabezpečení i když se heslo jeví jako dobrá možnost, tak je potřeba dbát na jeho komplexnost. Skrze navrženou úlohu si odzkoušejí, jak rychle lze takové jednoduché heslo zjistit a je třeba doufat, že pokud již nemají komplexní hesla, tak je začnou používat. Zároveň tato úloha přiblíží studenty k představě termínu „hacker“ neboť si odzkoušejí práci s příkazovými řádky a hackerským nástrojem. V obou směrech je potřeba navyšovat informovanost a praktické úlohy jsou velmi efektivní, protože si to osoby (v tomto případě studenti) odzkoušejí a odnesou si více znalostí než z teoretického výkladu. Díky možnosti vytvořit vlastní stránku pro toto použití je fakulta velmi dobrým místem, kde právě tuto úlohu vyzkoušet. Navržená úloha zároveň je jednou z preferovaných úloh, které byly navrženy a velmi dobře zapadá do studia na fakultě. Z navržených úloh je pravděpodobně nejtěžší na provedení, ale zároveň poskytuje mnoho nových informací.

15 POSOUZENÍ RIZIK VYCHÁZEJÍCÍCH Z ÚLOHY

Rizika jsou úzce spojená se získáním hesla osoby blízce souvisí s tvorbou hesla, které osoba použije (viz. obrázek 1). Z tohoto důvodu většina stránek používá něco na styl checklistu. Dále budou posouzena rizika samotné úlohy.

15.1 Rizika hesel

Rizika u hesel jsou hlavně od hackerů nebo osob používajících sociální inženýrství (bez schopností hackera). Dalším částí rizik plyne od osoby zakládající si heslo. Těmito riziky mohu být například vyzrazení hesla nebo jeho zapomenutí. Právě z nátlaku neetických hackerů je potřeba vytvářet takové checklisty. Tyto checklisty se budou postupně vyvíjet společně s kreativními pokusy hackerů. Každá osoba tedy používá nějakou formu checklistu ať už z donucení nebo samostatně sestavený.

U samostatně sestaveného checklistu je potřeba zavést požadavky, které se již používají a přidat další požadavky, které vypadají, že pomohou k bezpečnosti hesla. Níže je uvedena ukázka, jak takový checklist může vypadat.

Tabulka 2 Checklist hesla (vyplněna pro negativní dopad)

Otázka	Ano	Ne
Obsahuje heslo více než 8 znaků?		X
Jsou v hesle použita velká písmena?		X
Jsou v hesle použita malá písmena?		X
Jsou v hesle použita čísla?		X
Jsou v hesle použity speciální znaky (+, @, ?, /, € atd.)?		X
Jsou v hesle použita slova v infinitivu (lze je nalézt v slovníku)?	X	
Jsou slova v hesle pouze v rodném jazyce?	X	
Obsahuje heslo slovo, které lidé při interakci s vámi jsou schopni zjistit z vašeho života?	X	
Obsahuje heslo slovo, které by mohly blízké osoby uhodnout?	X	
Je v hesle nahrazeno písmeno číslem (J0s3f)?	X	
Obsahuje heslo číslice pouze na začátku nebo konci?	X	

Otázka	Ano	Ne
Je heslo vygenerováno některým z generátorů hesel?	X	

Skrze příklad, kterým je tabulka checklistu, lze zjistit, jak dobré heslo osoba použila. Většinou webové stránky s přihlašovacími údaji požadují jako odpověď „Ano“ na prvních pět otázek. Ostatní otázky jsou zde pro větší bezpečnost hesla a na webových stránkách je nelze plně zavést, protože si osoba může zvolit jinou lokalitu nebo případně použít VPN, pokud by byla nucená lokace a díky tomu použít slova v infinitivu. Podobným způsobem lze přistoupit i k ostatním otázkám. Ideální heslo by bylo použít něco, co není slovo, které se vyskytuje v daném jazyce a zároveň je propleteno čísly a speciálními znaky.

Následuje „Tabulka 3 What if k checklist tabulce (tabulka 2)“ pro účely tabulky jsou brány odpovědi, tak že mají negativní dopad (například „Obsahuje heslo více než 8 znaků?“ s odpovědí „Ne“).

Tabulka 3 What if k checklist tabulce (tabulka 2)

Pořadové číslo	Příčina	Následek	Návrh opatření k minimalizaci (preventivní, nápravné)	Poznámka
1	Lenost, neschopnost, malá kreativita, neznalost	Nízká bezpečnost hesla s možností prolomení v rámci minut	Použití důvěryhodného správce hesel (program), na papírek napsat a řádně schovat	Řádné schování neznamená v šuplíku u počítače nebo hůře ze spodní části klávesnice
2	Lenost, neznalost	Nízká bezpečnost hesla	Použití velkých písmen, změna hesla	S větší variací znaků narůstá čas potřebný na prolomení

Pořadové číslo	Příčina	Následek	Návrh opatření k minimalizaci (preventivní, nápravné)	Poznámka
3	Neznalost, lenost	Nízká bezpečnost hesla	Použití malých písmen, změna hesla	S větší variací znaků narůstá čas potřebný na prolomení
4	Lenost, neznalost	Nízká bezpečnost hesla	Použití čísel, změna hesla	S větší variací znaků narůstá čas potřebný na prolomení
5	Lenost, neschopnost, malá kreativita, neznalost	Nízká bezpečnost hesla	Použití speciálních znaků, změna hesla	S větší variací znaků narůstá čas potřebný na prolomení
6	Lenost, neschopnost, malá kreativita, neznalost	Lehce odhadnutelné od cizích hackerů	Nepoužívat slova v infinitivu, změna hesla	Použít slova v jakémkoli jiném stylu než infinitivu nebo lépe pozměnit celá slova
7	Lenost, neschopnost, neznalost	Lehce odhadnutelné při zjištění rodného jazyka	Použít slovo z jiného jazyku nebo slovo pozměnit; změna hesla	Stejný případ je světový jazyk

Pořadové číslo	Příčina	Následek	Návrh opatření k minimalizaci (preventivní, nápravné)	Poznámka
8	Lenost, malá kreativita, neznalost, jednoduchost, sociální inženýrství	Lehce odhadnutelné od hackerů a ostatními osobami, které provedou interakci	Dávat si pozor na odpovědi a konverzaci, která by mohla odhalit heslo; nepoužívat slova z běžné konverzace a ze zájmových aktivit; změna hesla	Nepoužívat slova, která lze zjistit pouze z dokumentů o osobě (termíny z pracovního odvětví atd.)
9	Lenost, zaváhání, malá kreativita, neznalost, jednoduchost, sociální inženýrství	Lehce odhadnutelné od blízkých osob	Dávat si pozor na odpovědi a konverzaci, která by mohla odhalit heslo; nepoužívat slova z běžné konverzace a ze zájmových aktivit; změna hesla	
10	Lenost, malá kreativita	Lehce odhadnutelné s nízkou bezpečností	Pozměnit slovo jiným způsobem, než přeměnit písmena na čísla a přidat čísla; změna hesla	S narůstající četností se tato možnost stala očekávanou
11	Lenost, neschopnost, malá kreativita, neznalost	Lehce odhadnutelné s nízkou bezpečností	Používat čísla mezi slovy nebo lépe mezi písmeny, změna hesla	
12	Lenost, neschopnost, malá kreativita, neznalost	Nízká bezpečnost hesla	Získat inspiraci, ale vytvořit vlastní heslo; změna hesla	Velká šance, že nepozměněné heslo bude v souboru s hesly hackerů

Některé informace z tabulky je potřeba rozvést. Těmito informacemi jsou:

- V prvním řádku neschopnost, kterou se myslí neschopnost zapamatovat si dlouhé heslo a neznalost jako neznalost nebezpečí spojeného s použitím krátkého hesla.
- Ve třetím řádku neznalost a lenost, jako špatně pochopená informace ohledně bezpečnosti za použití velkých písmen a lenost z pohledu použití klávesy „Caps Lock“ pro jednodušší zadávání.
- V osmém řádku jednoduchost jako použití jednoduchého slova nebo slovního spojení jako heslo, zájmové aktivity se zde myslí nejen jako sporty a hobby, ale také jako často vyhledávaná témata atd.
- V devátém řádku zaváháním je zde myšleno nejistota vyslovení právě toho slova, které je použito v heslu nebo se vyhýbání použití tohoto slova, jednoduchostí je myšleno použití velmi jednoduchého hesla, které bude možno zjistit skrze zaváhání nebo velmi časté používání skupiny výrazů nebo propagování některé ze zájmových aktivit.

Jak lze z výše uvedených tabulek vidět je potřeba hesla stále zdokonalovat a ideální možností by bylo je i měnit za určitý čas. Slabé heslo tedy představuje velkou hrozbu pro jeho uživatele, kdy lze zjistit za pomoci podpůrných nástrojů a nástrojů jako je Hydra pro účely zjištění hesla. Slabé heslo se může velmi rychle stát silný po změně. Změna musí být velká pro takové heslo, aby se z něj stalo velmi silné heslo. Sociální inženýrství hraje při zjišťování hesla velkou roli a nesmí se na něj zapomenout. Tato metoda je velmi nebezpečná pro osoby, které se s ní ještě nesetkali nebo si nedávají pozor na otázky které jsou kladeny a nedokážou si spojit souvislosti. Další velkou roli zde hraje zapomenutí hesla. Kdyby bylo heslo tak silné, že by bylo prolomeno až za několik staletí, ale bylo zapomenuto během pár sekund, nemá význam. Pro osoby, které si silná hesla nedokážou zapamatovat je zde mnoho správců hesel. U správců hesel, ale nastává problém s důvěryhodností zachování hesla pouze pro osobu, která si jej zde uložila. Také je potřeba zadat heslo pro vstup do správce hesel, tudíž alespoň jedno heslo je potřeba si zapamatovat. Jinou možností je zapsání hesla na papírek, ale zde je velké nebezpečí jeho nalezení, proto se nedoporučuje tento způsob použít v pracovním prostředí. V domácím prostředí je to možné, ale jeho uschování může být problém. Doporučením je zde tedy použití něčeho, co zní osobě jako slovo z důvodu lepšího zapamatování a jeho poupravení

přidáním čísel a znaků (například I5ND73EBO$D1, kde je použito něco, co zní jako slovo tzn. INDEBOD).

15.2 Rizika pro úlohu

Jelikož je tato práce zaměřena na návrh úlohy pro potřeby kybernetické laboratoře, tak je zde potřeba v první řade určit rizika, která jsou přímo spjata s úlohou, konkrétně s jejím průběhem při vypracování a zadání v hodině. S tímto samozřejmě souvisí i její příprava. Jelikož je úloha navržena pro podmínky kontrolovaného prostředí, tak zde nebude řešen dopad nastavení prostředí, ve kterém se úloha bude procvičovat. Z tohoto pohledu jsou zde zmíněny části, které by šli považovat jako součást již zmíněného prostředí, ale jsou přímo použity pro potřeby navržené úlohy, proto jsou zahrnuty v analytické části. Následující tabulky jsou tvořeny pro potřeby navržené úlohy, které nelze považovat za nejlepší možné z pohledu účinnosti, neboť úloha ještě nebyla odzkoušena v již zmíněném prostředí, přesto jsou svým způsobem významné a mohou poskytnout nápovědu nebo směr na který se zaměřit při jejich následné úpravě.

15.2.1 Klasifikace významu

Klasifikace významu je uvedena v intervalu od 1 do 10 včetně. Jinak řečeno je v hodnocení zahrnuto i počáteční číslo 1 a koncové číslo 10. Tabulka byla vytvořena na základě předchozích zkušeností a přizpůsobena úloze.

Tabulka 4 Význam

Význam	Následky	Klasifikace
Žádný význam	Minimální následky s téměř nulovým negativním dopadem	1
Nízký význam	Následky jsou znatelné, ale nečiní závažný problém	2-4
Střední význam	Následky je třeba řešit a jejich nevyřešení způsobí negativní dopad	5-6
Velký význam	Následky je třeba urgentně řešit a mohou způsoby velký negativní dopad	7-9

Význam	Následky	Klasifikace
Nepřijatelný význam	Nenavratitelný negativní dopad	10

15.2.2 Klasifikace výskytu

Klasifikace výskytu je uvedena v intervalu od 1 do 10 včetně. Jinak řečeno je v hodnocení zahrnuto i počáteční číslo 1 a koncové číslo 10. Tabulka byla vytvořena na základě předchozích zkušeností a přizpůsobena úloze.

Tabulka 5 Výskyt

Výskyt	Četnost	Klasifikace
Téměř nikdy	1 z 10 000	1
Nízký	1 z 7 500	2
	1 z 5 000	3
	1 z 2 500	4
Střední	1 z 1 000	5
	1 z 500	6
Vysoký	1 z 100	7
	1 z 50	8
	1 z 20	9
Téměř jistý	1 ze 2	10

15.2.3 Klasifikace odhadnutelnosti

Klasifikace odhadnutelnosti je uvedena v intervalu od 1 do 10 včetně. Jinak řečeno je v hodnocení zahrnuto i počáteční číslo 1 a koncové číslo 10. Tabulka byla vytvořena na základě předchozích zkušeností a přizpůsobena úloze.

Tabulka 6 Odhadnutelnost

Odhadnutelnost	Komentář	Klasifikace
Skoro jistá	Na první pohled lze odhadnout chybu při zvýšené pozornosti	1
Vysoká	Nalezení chyby po specifické akci	2-4
Střední	Chyba nalezena po jejím hledání	5-6
Nízká	Chyba nalezena po zdlouhavém hledání soustředěném na určitou část	7-9
Skoro nemožná	Téměř nelze odhadnout chybu	10

15.2.4 Failure Mode and Effect Analysis (FMEA)

Tuto metodu lze nalézt pod českým názvem „analýza možného výskytu a vlivu vad“. Metoda je často zpracovávána pro systémy, výrobky, procesy, a služby. Jelikož návrh úlohy má blízko k návrhu systému nebo procesu, tak je metoda velmi sympatickou možností pro potřeby práce. Tato metoda je pravděpodobně nejlepší metodou pro potřeby práce z metod, které byly vyučovány. Metoda byla upravena pro potřeby práce a je doplněna komentáře pod tabulkou.

Tabulka 7 FMEA (upravena pro potřeby DP)

prvek	Možná vada	Možná příčina	Možné následky	Význam	Výskyt	Odhadnutelnost	Rizikové číslo	Doporučená opatření
Student	Špatný cíl útoku	Zadání nesprávných údajů při práci s Hydrou	Neetické použití (bráno jako kriminální aktivita)	9	6	1	54	Kontrola vyučující při zadávání příkazů v Hydře
	Špatný postup úlohou	Nepozornost, uspěchanost	Nedodělání úlohy, zdržení ostatních, neetické použití	5	5	3	75	Tučně vyznačit části textu pro navýšení pozornosti, po dodělání určitých části kontrola vyučujícím
	Špatná instalace aplikací	Nepozornost, nenásledování postupu,	Zdržení ostatních, reinstalace aplikací	2	4	2	16	Ukázka, obrázky v postupu
Webová stránka	Zahlcení serveru pro potřeby úlohy	Přílišné opakování v rámci krátkého času	„Denial of Service“ (tzv. DoS útok)	5	2	5	50	Rozdělení do menších skupin, změna nastavení webové stránky

Vyučující	Nesprávný výběr hesla	Nepozornost, brzké pořadí hesla v souboru	Znemožnění provedení úlohy, postup úlohou urychlen	2	3	3	18	Kontrola před zadáním úlohy studentům, změna pořadí hesel
Počítač	Špatná verze Microsoft Windows	Znemožnění instalace WSL	Konec úlohy, změna úlohy	10	1	2	20	Potřeba použití druhé možnosti (virtuální počítač), nahradit úlohu

15.2.5 Komentář k FMEA

Z analýzy je znatelně poznat, že největším rizikem je zde špatný postup úlohou. Důvodem je zde výskyt, protože je brán celkový počet studentů s předpokladem, že v jedné třídě je zhruba 30 žáků. Rizikové číslo je zde tedy největší (75). Druhým největším rizikem je špatný cíl útoku. Jelikož je adresa, na kterou je útočeno zadávána do příkazového řádku a v příkazovém řádku je relativně malá velikost písma, tak společně s velkým počtem čísel za sebou je možné, že se student přepíše v jednom z čísel. Zde hraje velkou roli jak výskyt, tak význam, kde význam je na hodně vysoké úrovni právě kvůli legálním problémům, které by z toho mohly vzniknout. U nesprávného výběru hesla je to potřeba brát jako použití studenty, a ne na počet změn, neboť by zde vzniklo číslo, které by pokazilo ohodnocení a tím pádem by minimálně tento řádek ztratil smysl. Ke všem rizikům jsou přidány doporučená opatření, které mají za cíl výrazně snížit výskyt.

ZÁVĚR

Problematika hesel zadávaných na zabezpečení účtů je v dnešní době narůstajícího používání kybernetických technologií velmi složitá. Stále častěji v médiích slýcháme o kybernetickém útoku ať na fyzické osoby, firmy, různá zařízení i na různé instituce. Tyto útoky mohou být různého typu. Například jak již v diplomové práci zmíněný DDoS útok, Ransomware nebo za pomoci nástrojů útok hrubou silou na hesla účtů, které je podrobněji zpracováno v diplomové práci jakožto návrh na praktickou úlohu.

V teoretické části je uveden kyberprostor pro seznámení se s termínem. Zabývám se zde důležitými pojmy spadajícími pod kybernetickou bezpečnost jako je Triáda CIA a kybernetický útok. Následně zde spadá i kybernetická hrozba, která je dále rozvedena o pojmy Phishing, sociální inženýrství a další méně podstatné hrozby z pohledu diplomové práce. Následuje téma Operační systémy, jako nejznámější a často používaný Microsoft Windows, dále méně známý Linux a software pro zprovoznění Linuxových nástrojů nazývaných subsystém Windows pro Linux (Windows Subsystém for Linux). Dalším tématem je Kryptografie, která je úzce spojena s hesly z důvodu používání hashovacích algoritmů, které jsou zde uvedeny jako pojem pod zmíněnou kapitolou. Jedná se o formu zabezpečení, díky které lze poznat, zda byla provedena změna třetí stranou. Poslední témata v teoretické části, jako je Hesla a Hacking jsou rozebírána více dopodrobna z důvodu potřebných znalostí do praktické části diplomové práce.

V praktické části je navržena úloha k procvičování v prostředí kybernetické laboratoře na Fakultě logistiky a krizového řízení UTB ve Zlíně. Úlohy byly procvičovány na osobním počítači v domácím prostředí. Jednalo se o tyto úlohy, jako zašifrování dat, zjištění hesla na virtuálním počítači, zjištění hesla za pomoci WSL, permanentní smazání dat, cloudové úložiště, základy programování, Phishing kvíz, vyhledávání osob a míst a vyhledávání telefonního čísla. První sekce praktické části byla ukončena posouzením úloh a navržení vedoucímu diplomové práce. Pro provedení navržené úlohy byly využity potřebné činnosti, nástroje a aplikace, které jsou popsány v další části diplomové práce. Všechny úlohy byly vyzkoušeny jak teoreticky, tak prakticky s následným řešením vzniklých problémů. Úlohy byly vyzkoušeny za použití virtuálního PC a softwaru WSL. Následuje ukázka postupu doporučenou možností, kterou je WSL. Na základě vyzkoušených postupů je navržena možnost, jak zavést úlohu do výuky. Následuje vyhodnocení, ve kterém je zmíněno, jakým

způsobem úloha pomůže. Dále okomentováno, proč jsem vybral tuto úlohu. Posledním tématem jsou analytické metody pro potřeby této diplomové práce.

Přínosem práce je informovanost čtenáře a studentů, kteří budou procvičovat tuto praktickou úlohu.

Domnívám se, že cíle této práce byly naplněny. Kde hlavním cílem této práce bylo navrhnout praktickou úlohu pro potřeby kybernetické laboratoře. Po konzultaci s vedoucím práce bylo navrženo spoustu návrhů k vypracování této diplomové práce. Po konzultaci bylo vybráno pouze jedno téma, kterému jsem se věnoval dopodrobna.

Na závěr lze říct, že je velmi důležité dbát na sílu hesla, které osoby používají. Tyto hesla blízce souvisí s každodenním životem. V současné době všichni používají hesla, jedno jestli mladí či dříve narození, a to stejná jak na zabezpečení telefonu, mailu bankovního účtu. Neinformovanost v oblasti kybernetické bezpečnosti občanů vede k problémům v životě.

SEZNAM POUŽITÉ LITERATURY

BAYUK, Jennifer L.; HEALEY, Jason; ROHMEYER, Paul; SACHS, Marcus; SCHMIDT, Jeffrey et al. Cyber security policy guidebook. USA: Wiley, 2022. ISBN 9781118027806.

BLUM, Richard. Linux Fundamentals. 2nd ed. USA: Jones & Bartlett Learning, 2023. ISBN 9781284254884.

BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. Cybersecurity Essentials. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.

CIA triad (confidentiality, integrity and availability). Online. TechTarget. 2023. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [cit. 2024-03-20].

Cyber Attack. Online. NIST. C2024. Dostupné z: https://csrc.nist.gov/glossary/term/cyber_attack. [cit. 2024-03-20].

DEATH, Darren. Information Security Handbook. Velká Británie: Packt Publishing, 2017. ISBN 1788478835.

DOEPPNER, Thomas W. Operating Systems In Depth: Design and Programming. USA: Wiley, 2022. ISBN 0471687235.

ERICKSON, Jon. Hacking: The Art of Exploitation. USA: No Starch Press, 2022. ISBN 9781593270070.

EVANS, Lester. Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, the Internet of Things + an Esential Guide to Ethical Hacking for Beginners. USA: Lester Evans, 2019. ISBN 9781794647237.

GRIMES, Roger A. Hacking Multifactor Authentication. USA: Wiley, 2020. ISBN 9781119650799.

HADNAGY, Christopher. Social Engineering: The Art of Human Hacking. USA: Wiley, 2022. ISBN 9780470639535.

Kali Linux Hydra. Online. Educba. C2024, 15.2.2023. Dostupné z: https://www.educba.com/kali-linux-hydra/. [cit. 2024-03-21].

KATZ, Jonathan a LINDELL, Yehuda. Introduction to modern cryptography. 2nd ed. London: CRC Press/Taylor & Francis, 2022. ISBN 9781466570276.

KISSELL, Joe. Take Control of Your Passwords. 4th ed. Canada: alt concepts, 2023. ISBN 9781990783302.

Know the types of cyber threats. Online. Mass.gov. 2024. Dostupné z: https://www.mass.gov/info-details/know-the-types-of-cyber-threats. [cit. 2024-03-20].

KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8. Dostupné také z: https://knihy.nic.cz/files/edice/cybersecurity.pdf.

KSHETRI, Nir. Cybersecurity Management: An Organizational and Strategic Approach. Kanada: University of Toronto Press, 2022. ISBN 1487504969.

Kybernetický útok (kyberútok). Definice, typy, následky a prevence. Online. Legislativa. 13.09.2022. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok. [cit. 2024-03-20].

LEE, Martin. Cyber Threat Intelligence. USA: Wiley, 2023. ISBN 9781119861744.

LOSHIN, Peter. Private key. Online. TechTarget. 2021. Dostupné z: https://www.techtarget.com/searchsecurity/definition/private-key. [cit. 2024-03-20].

Mastering Modern Cybersecurity Threats: Your Essential Guide. Online. Preyproject. 2024. Dostupné z: https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them. [cit. 2024-03-20].

Microsoft Windows: operating system. Online. In: Britannica. 2024, 19.3.2024. Dostupné z: https://www.britannica.com/technology/Microsoft-Windows. [cit. 2024-03-20].

MICROSOFT. Types of malware. Online. C2024. Dostupné z: https://www.microsoft.com/en-us/security/business/security-101/what-is-malware. [cit. 2024-04-19].

MICROSOFT. What is the Windows Subsystem for Linux? Online. MICROSOFT. Learn. 2023, 29.11.2023. Dostupné z: https://learn.microsoft.com/en-us/windows/wsl/about. [cit. 2024-03-20].

Most common types of cyberattacks in 2023. Online. NordLayer. 2023. Dostupné z: https://nordlayer.com/blog/most-common-types-of-cyber-attacks/?gad_source=1. [cit. 2024-03-20].

ORIYANO, Sean-Philip. Penetration testing essentials. Hoboken, NJ: Sybex, 2017. ISBN 9781119235330. Dostupné také z: https://proxy.k.utb.cz/login?url=https://onlinelibrary.wiley.com/doi/book/10.1002/9781119419358.

Počátky kybernetiky v Československu. Online. Historie výpočetní techniky v Československu. Dostupné z: https://www.historiepocitacu.cz/pocatky-kybernetiky-v-csr.html. [cit. 2024-03-20].

ROUSE, Margaret. Cyberspace. Online. In: Techopedia. 2023. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace. [cit. 2024-03-20].

SHARP, Robin. Introduction To Cybersecurity: A Multidisciplinary Challenge. Springer, 2023. ISBN 3031414624.

THAKUR, Kutub a PATHAN, Al-Sakib Khan. Cybersecurity Fundamentals: A Real-World Perspective. USA: CRC Press, 2020. ISBN 0367476487.

Tipy pro firemní politiku hesel: Tabulka. Online. In: Antivirové centrum. 2023, 4.8.2023. Dostupné z: https://www.antivirovecentrum.cz/aktuality/tipy-pro-firemni-politiku-hesel.aspx. [cit. 2024-03-21].

TRENT, ROD. Using Kali Linux and Hydra for Attack Testing and Alert Generation. Online. RodTrent substack. C2024, 15.9.2023. Dostupné z: https://rodtrent.substack.com/p/using-kali-linux-and-hydra-for-attack. [cit. 2024-03-21].

What is Kali Linux? Online. Kali. C2024, 4.11.2023. Dostupné z: https://www.kali.org/docs/introduction/what-is-kali-linux/. [cit. 2024-03-20].

WONG, David B. Real World Cryptography. Manning, 2021. ISBN 9781617296710.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
ARM	Advanced RISC Machines
ARMEL	Typ procesoru
ARMHF	Typ procesoru
CATO	Krádež podnikatelského subjektu
cmd	Command line
CNA	Útok na počítačovou síť
CND	Obrana počítačové sítě
CNO	Operace v počítačové síti
DDoS	Distributed Denial-of-Service
DoD	Department of Defense
FHS	Filesystem Hierarchy Standard
FTP	File Transfer Protocol
GNU	Operační systém podobný Unixu
GPG	GNU Privacy Guard
GUI	Grafické uživatelské rozhraní
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IBM	International Business Machines Corporation
IP	Protokol pro propojení sítí
ITU	Mezinárodní telekomunikační unie
MAC	Media Access Control
OS	Operační systém
OSINT	Open Source Intelligence

PIN	Osobní identifikační číslo
RAM	Paměť s náhodným přístupem
RFID	Identifikace na rádiové frekvenci
SE	Sociální inženýrství
SHA-512	Secure Hash Algorithm
SMB	Blokace zpráv na serveru
TCP	Protokol řízení přenosu
Triáda CIA	Důvěrnost, integrita a dostupnost
US DOD 5220.22-M	Vysoce uznávaný standard pro mazání dat
USB	Univerzální sériová sběrnice
WSL	Windows Subsystem for Linux
www	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ZADÁNÍ ÚLOHY NA MOODLE

Odevzdání:

Práci odevzdává každý v týmu ve formátu názvu "Příjmení_Hydra". Typ odevzdávaného souboru – PDF.

Zadání:

Úkol je zaměřen na zjištění hesla vybraného subjektu v souladu s platnou směrnicí NIS2. Je zpracováván samostatně. Cílem je zjištění hesla za pomoci postupu a následná dokumentace kroků. Dokumentaci je doporučeno zpracovat v typu souboru Dokument Microsoft Word.

Dokument bude obsahovat jak text, tak i obrázky. V dokumentu budou zaznamenány všechny klíčové informace a jeho postup bude chronologický.

Subjekt:

Předem určená stránka v lokální síti fakulty.

Rozsah:

Počet stran je minimálně 2, ale je potřeba uvést všechny klíčové kroky s obrázky (tzn. stran bude s velkou pravděpodobností více).

Obsah práce, struktura:

Práce nebude obsahovat „Teoretickou část“, pouze část „Praktickou“. Nebudou zde tedy uvedeny teoretické základy problematiky. Předpokládaná struktura:

1. Nastavení virtualizace.
2. Instalace WSL.
3. Dokončení instalace Ubuntu.
4. Instalace aplikace Kali Linux
5. Příprava Kali Linux (od prvního zapnutí, až po zprovoznění vybraného režimu Win-KeX)
6. Práce s nástrojem Hydra

Průběžné odevzdávání:

Studenti po každém cvičení odevzdávají soubor do Moodlu s korektním pojmenováním a inkrementálním verzováním, tedy např.: Příjmení_Hydra_v1

Staré verze jsou přitom zachovávány.

Hodnocení:

Úloha bude hodnocena na základě úspěšného splnění. Hodnocení bude formou splněno nebo nesplněno. Při chybě bude k odevzdané úloze přidán komentář na Moodlu, kde je úloha odevzdána.