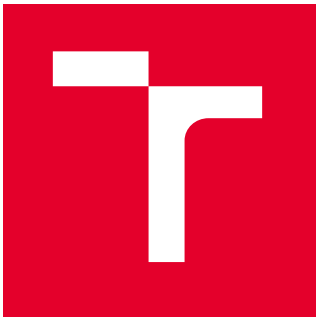


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

APLIKACE NA STAVBU A ZOBRAZOVÁNÍ VEKTORŮ ÚTOKŮ POMOCÍ METOD SOCIÁLNÍHO INŽENÝRSTVÍ

SEMESTRÁLNÍ PRÁCE

SEMESTRAL THESIS

AUTOR PRÁCE

AUTHOR

Bc. Jan Kašpar

VEDOUCÍ PRÁCE

SUPERVISOR

JUDr. Mgr. Jakub Harašta, Ph.D.

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Semestrální práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Jan Kašpar ***ID:*** 211796

Ročník: 2 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Aplikace na stavbu a zobrazování vektorů útoků pomocí metod sociálního inženýrství

POKYNY PRO VYPRACOVÁNÍ:

V rámci práce student vytvoří aplikaci na stavbu a zobrazování vektorů útoků pomocí metod sociálního inženýrství. Cílem je vytvoření aplikace, která umožní namodelování vektorů útoků, jejich přiřazení členům týmu, a vložení dalších vhodných detailů. Aplikace musí umožnit práci se související smluvní dokumentací a generování dílčích a celkových zpráv o průběhu útoků.
V rámci semestrálního projektu bude vytvořen základ technického řešení aplikace a budou demonstrovány základní funkce.

DOPORUČENÁ LITERATURA:

podle pokynů vedoucího práce

Termín zadání: 1.10.2022 ***Termín odevzdání:*** 12.12.2022

Vedoucí práce: JUDr. Mgr. Jakub Harašta, Ph.D.
Konzultant: Daniel Hejda

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

KAŠPAR, Jan. *Aplikace na stavbu a zobrazování vektorů útoků pomocí metod sociálního inženýrství*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2030, 50 s. Semestrální práce. Vedoucí práce: JUDr. Mgr. Jakub Harašta, Ph.D

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Bc. Jan Kašpar
VUT ID autora:	211796
Typ práce:	Semestrální práce
Akademický rok:	2029/30
Téma závěrečné práce:	Aplikace na stavbu a zobrazování vektorů útoků pomocí metod sociálního inženýrství

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

Obsah

Seznam obrázků

Úvod

V této době je kladen velký důraz na zabezpečení počítačové infrastruktury. Tato diplomová práce se zaměřuje na nejslabší článek v tomto zabezpečení a to na lidský faktor za pomocí využití metod sociálního inženýrství. Využitím těchto metod může dojít k získání citlivých informací prostřednictvím internetu nebo fyzické komunikace s obětí.

V teoretické části práce je vysvětleno co je sociální inženýrství. Kapitola 1.2 je věnována autentizaci se zaměřením na autentizaci znalostí, pro vysvětlení toho, čeho se útočníci snaží zmocnit. V kapitole 1.3 jsou popsány formy sociálního inženýrství, kde jsou popsány hrozby spojené s používáním sociálních sítí a komplikace, které mohou nastat při kompromitaci účtu na sociální síti nebo e-mailu. Kapitola 2 se věnuje popisu technik využívající sociální inženýrství s uvedenými příklady jak může být technika použita a jsou zde popsány typy škodlivých kódů, mezi kterými je dobré rozlišovat. V kapitole 3 je popsán rozdíl mezi penetračním testováním a Red Teamingem, uvedeny typy týmů a jejich funkce. Zároveň je zde popsáno zabezpečení objektu s překážkami, které je nutné překonat pro vniknutí do objektu a uvedena metodika Cyber Kill Chain pro vysvětlení aktivit, kterých chtějí testeři dosáhnout. Poslední kapitola teoretické části se věnuje legislativě, ve které jsou popsány zákony, a uvedeny příklady porušení těchto zákonů, se kterými se lze setkat při sociálním inženýrství.

Praktická část této práce se věnuje vývoji aplikace pro Red Team testery. V kapitole 5.1 jsou popsány frameworky používané při vývoji aplikace. Kapitola 5.2 popisuje již vytvořené funkce aplikace a jejich použití. Zároveň je zde uvedeno jakým způsobem bude aplikace zajišťovat dodržení právních předpisů identifikovaných v kapitole 4. A jsou uvedeny funkce, které budou implementovány v navazující diplomové práci.

Cílem této práce je vytvoření aplikace pro Red Teaming, kde dojde k propojení technické a právnické složky. Tato aplikace zajistí, že testování bude probíhat v souladu s právními předpisy a po technické stránce bude možné dohledat jak bylo testování provedeno společně s příslušnou dokumentací a prezentací výsledků. Tato aplikace bude sloužit k testování zaměstnanců ve firmách za účelem zjištění nedostatků v zabezpečení.

1 Teoretická část studentské práce

V této části bude popsáno, co je a čím se vyznačuje sociální inženýrství, princip autentizace se zaměřením na autentizaci pomocí znalosti a formy sociálního inženýrství v dnešní době.

1.1 Sociální inženýrství

Sociální inženýrství neboli sociotechnika je metoda manipulace s lidmi, díky které lze získat důvěrné informace nebo informace, které mohou být i jinak prospěšné pro sociotechnika (útočníka). Pro úspěšný útok pomocí sociálního inženýrství je velmi důležitý předpoklad, že oběť je držena v nevědomosti. Tedy když je použita nějaká metoda sociálního inženýrství, tak oběť neví, že se stala cílem útoku a informace ve většině případů dobrovolně vydá.

V současné době jsou nejvíce rozšířeny bezkontaktní metody sociálního inženýrství. To znamená, že útočník není v přímém kontaktu s obětí, ale využívá ke komunikace jiné prostředky. Nejvíce rozšířeným prostředkem je internet, kde převládá metoda phishing. Dále lze využít kontaktních metod sociálního inženýrství, kde je oběť s útočníkem v přímém kontaktu. U těchto metod je využíván mobilní telefon, a to ve formě SMS zpráv nebo hovoru. Nebo v dnešní době velmi rozšířené a používané sociální sítě, kde se útočník může vydávat za jinou osobu nebo se pokusit přisvojit profil osoby, kterou oběť zná a důvěřuje jí. Na stejném principu je možné také využít e-mail. Při využití kontaktních metod jsou velmi důležité schopnosti sociotechnika, především jeho přesvědčovací schopnosti, díky kterým si u oběti vybuduje důvěru.

Sociotechnici využívají těchto metod, protože je mnohem jednodušší přelstít člověka k vydání informací, jako je heslo nebo jiné údaje, které mohou být pro útok prospěšné, než aby se pokoušeli překonat zabezpečení systému. Zabezpečení systému může totiž být velmi sofistikované a v některých případech i neprolomitelné. Při úspěšném použití některé z metod sociálního inženýrství oběť informace sama vydá a není tak nutné útočit přímo na software zabezpečení a pokoušet se ho prolomit pomocí hrubé síly nebo slovníkových útoků. Informace, které oběť poskytne, nemusejí vždy souviset s hesly nebo osobními údaji, ale mohou to být informace o čase výměny služeb na vrátnici, principu zabezpečení objektu apod.

Sociální inženýrství je nejvíce využíváno k získání osobních údajů jako jsou hesla do přihlašovacího sytému firmy, čísla bankovních účtů apod. Může ale také být využito k získání informací, které nemusí s osobními údaji vůbec souviset a jejich získání může utvořit celistvý obraz, díky kterému může být později veden úspěšný útok přímo na infrastrukturu. Zabezpečení počítačových systémů (pokud jsou správně

nastaveny) je v dnešní době na velmi dobré úrovni. Při použití vhodných asymetrických a symetrických šifer je matematicky dokázáno, že není možné toto zabezpečení prolomit v polynomiálním čase. Z toho vyplývá, že nejslabším článkem v zabezpečení systému je a vždycky bude člověk neboli lidský faktor. Ať je zabezpečení jakkoliv silné, pokud zaměstnanec má své heslo napsané na papírku pod klávesnicí, tak se stává zbytečným.[1, 2, 3, 4]

1.2 Autentizace

Samotná autentizace je klíčovým prvkem při ochraně informačních systémů před neoprávněným přístupem. Způsoby autentizace mohou být klasifikovány podle použitých prvků, jako jsou znalosti, předměty, biometrika, průkazy nebo činnosti. Mezi nejčastěji používané metody autentizace patří autentizace znalostí, která využívá sdíleného tajemství mezi uživatelem a systémem. Tento typ autentizace je však také nejčastěji cílem útoků pomocí sociálního inženýrství.

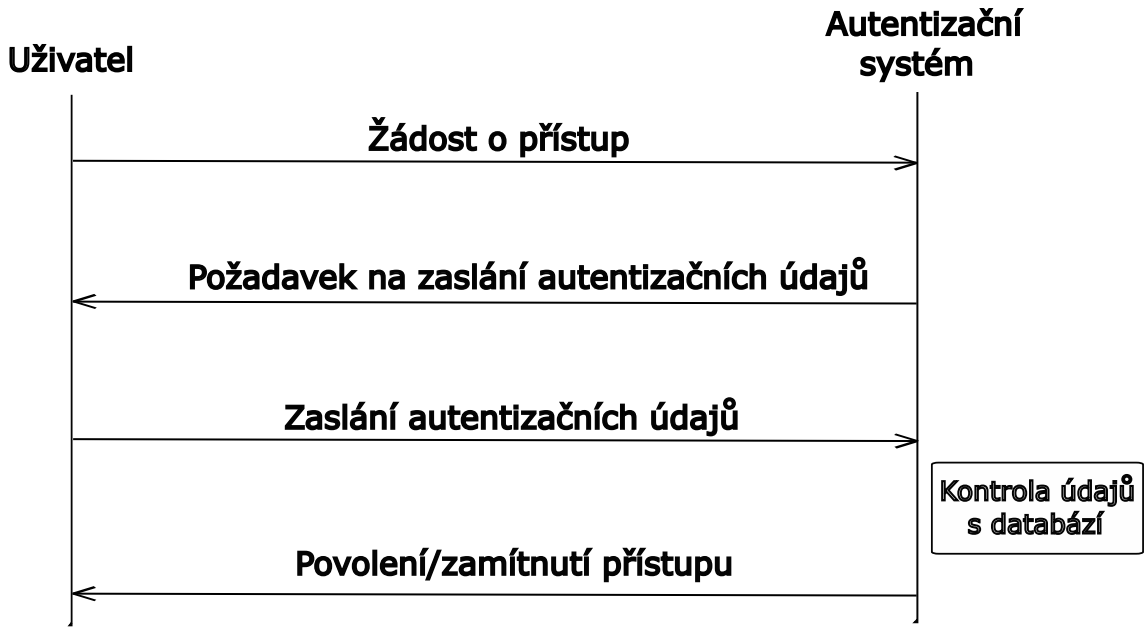
Útočníci mohou použít phishingové e-maily nebo jiné triky, aby získali autentizační údaje od uživatelů a následně získali neoprávněný přístup do systému. Vzhledem k tomu, že autentizace znalostí je nejrozšířenější autentizační metodou, je důležité brát v úvahu různé možnosti útoků a zvážit, zda by neměly být použity i jiné metody autentizace, jako je například autentizace biometrikou.

Kromě toho může být autentizace významným prvkem v sociálním inženýrství, zejména pokud uživatelé používají stejné nebo podobné autentizační údaje pro více systémů. V tomto případě může útočník získat údaje od jednoho systému a použít je pro útoky na další systémy, což zvyšuje celkové riziko bezpečnosti. Je tedy důležité, aby uživatelé používali silná hesla a změnili je pravidelně, aby minimalizovali riziko úspěšného útoku.

V kontextu sociálního inženýrství je třeba klást důraz na vzdělávání a povědomí o nebezpečích phishingu a dalších triků používaných útočníky. Dobrá autentizace může být klíčem k ochraně citlivých informací a dat, ale musí být použita ve správném kontextu a s vědomím rizik a možností útoků.[5, 6]

1.3 Formy sociálního inženýrství v současnosti

Sociální inženýrství se dělí na 2 podoby. S první formou se lze setkat na internetu, tedy bez fyzického kontaktu, kdy útočník sbírá informace o zájmové osobě online. Útočník může zahájit komunikaci s obětí pomocí dnes velmi používaných sociálních sítí nebo prostřednictvím e-mailu.



Obr. 1.1: Autentizace znalostí

Výhodou sociálních sítí pro útočníka je, že se lidé cítí v online prostředí bezpečně, a tak je jednodušší získat potřebné informace. Spoustu informací lze zjistit přímo z profilu oběti na sociální síti. S druhou formou sociálního inženýrství, tedy kontaktní formou, je těžší se setkat, protože pro její provedení a dosažení cíleného je zapotřebí zkušený sociotechnik s dobrou znalostí lidského chování a neverbální komunikace.

1.3.1 Sociální sítě

Sociální sítě jsou v dnešní době nejrozšířenější a nejpopulárnější službou pro zprostředkování komunikace mezi lidmi. Jedná se o nejsnazší a nejrychlejší způsob, jak komunikovat s přáteli na dálku, sdílet fotky a videa, polohu a vyměňovat informace. Všechny tyto informace mají pro útočníka velkou cenu a dají se zneužít v jeho prospěch. Ze sdílených fotografií lze navíc pomocí metadat vyčíst další užitečné informace jako místo a čas pořízení. Většina sociálních sítí umožňuje uživatelům nastavit, kdo bude mít přístup k informacím na jejich profilu a tím zamezit zneužití informací pro nežádoucí osoby. Je důležité zmínit, že tyto sociální sítě také zálohují komunikaci, takže pokud útočník získá přístup k účtu, může získat zprávy od počátku založení účtu. Z důvodu rozšířenosti sociálních sítí jsou také velmi často cílem útoku.

Pokud útočník získá přístup k profilu, nic mu nebrání zahájit komunikaci se spřátelenými kontakty a do zprávy vložit podvodnou stránku, odkaz na malware nebo požádat o peníze na specifický účet. Proto je dobré se vždy zamyslet, jaký odkaz bude rozkliknut, i když přijde od osoby, kterou známe a které věříme. Informace,

které jsou získány přístupem na profil oběti, lze dále využít například k vydírání (lechtivá fotografie) a to majitele profilu nebo osoby, která ji poslala.

1.3.2 E-mail

E-mail je často cílem útoků sociálních inženýrů. Pokud útočník získá autentizační údaje k e-mailu, může tak jednoduše získat i přístup k sociálním sítím (vyzkoušení stejného hesla, nahlášení zapomenutého hesla apod.) Pokud se mu tedy podaří získat přístup, může poté zahájit komunikaci se všemi kontakty oběti a rozesílat podvodné e-maily s odkazy a škodlivými přílohami.

Takový e-mail může obsahovat odkaz na stránku, kde se stáhne škodlivý software, který umožní útočníkovi přístup do počítače. Nebo podvodnou stránku, kde oběť zadá citlivé údaje, které tak útočník získá. Rozesílání takových e-mailů není vždy pravidlem, útočník může navázat komunikaci s jinou osobou, od které chce zjistit informace za použití identity oběti. Takové zprávy spoléhají na lidskou důvěřivost a zvědavost. Při obdržení pošty od někoho známého je větší šance, že oběť klikne na odkaz, než když by stejný e-mail přišel od někoho cizího.[1, 7]

V první kapitole bylo vysvětleno co je a čím se vyznačuje sociální inženýrství a z jakých důvodů je výhodnější jeho použití před klasickými metodami na prolomení zabezpečení. Byl popsán princip autentizace se zaměřením na metodu autentizace pomocí znalostí, na kterou bude mířená praktická část. A uvedeny možné typy útoků na tento princip autentizace a formy sociálního inženýrství používané v této době s ohledem na využití těchto forem v praktické části.

2 Techniky sociálního inženýrství

Tato kapitola se věnuje technikám sociálního inženýrství neboli praktikám, které jsou využívány pro zjištění citlivých informací. Aplikace, která bude vytvořena v rámci praktické části této práce, bude pracovat především s technikami vishing a phishing, které lze uskutečnit i s malým množstvím informací o oběti. Ostatní techniky jsou uvedeny z důvodu podobnosti výše zmíněným praktikám a jejich možnosti využití pro zisk informací nebo snazšího získání důvěry u oběti.

Hlavní myšlenka sociálního inženýrství je přinutit osobu, která zná heslo, k jeho vydání než se obtěžovat s používáním hrubé síly na prolomení hesla. Jako výhodu lze navíc brát, že při dobře vedeném útoku si oběť vůbec nemusí uvědomit, že vyzradila citlivé informace útočníkovi. Tento fakt lze pokládat za nejnebezpečnější rys problematiky sociálního inženýrství. Pokud je někomu ukradena/ztracena kreditní karta, nejběžnější reakce bude danou kartu zablokovat, aby nemohlo dojít k jejímu zneužití. Ale když je použito sociální inženýrství pro zisk informací, oběť se nemusí dozvědět o tom, že byla „okradena“ o informace. Sociotechnika je tedy velmi často nejjednodušší a nejlevnější způsob, jak ohrozit bezpečnost počítačové infrastruktury.

Sociální inženýrství je technika útoku, která využívá lidské chyby a nedostatky, aby se dostala k důvěrným informacím nebo získala přístup k chráněným systémům. Útočník využívá přesvědčivých technik, jako jsou vydávání se za jinou osobu, vytváření falešných důvodů, emotivní manipulace a sociálního tlaku, aby donutil oběť udělat něco, co by normálně neudělala. V případě útoku pomocí sociálního inženýrství může být obtížné zjistit, kdo je skutečným útočníkem, protože často se využívají anonymní metody, jako jsou anonymní e-mailové účty nebo falešné identity na sociálních sítích. To ztěžuje identifikaci útočníka a ztěžuje práci orgánům činným v trestním řízení.

Mezi časté metody útoků pomocí sociálního inženýrství patří vydávání se za jinou osobu, například za pracovníka banky, IT technika, nebo údržbáře, a žádání o přístup k důvěrným informacím, jako jsou hesla nebo bankovní údaje. Další metody zahrnují phishing útoky prostřednictvím e-mailů nebo textových zpráv, které se snaží přesvědčit oběť o odeslání citlivých informací. [8]

2.1 Pretexting

Pretexting, také známý jako Blagging, je metoda, při které útočník používá předem vytvořený a fiktivní scénář, aby přesvědčil oběť, aby mu poskytla citlivé informace nebo provedla činnost, která bude pro útočníka užitečná.

Aby tato metoda byla úspěšná, musí útočník připravit a shromáždit informace, které bude používat ve scénáři. Tyto informace mohou zahrnovat jméno, adresu,

datum narození, telefonní číslo a veřejně zveřejněné příspěvky, které oběť sdílela na sociálních sítích a dalších platformách.

Pokud útočník z těchto příspěvků zjistí, že oběť měla špatnou zkušenost s bankou, může se vydávat za zaměstnance této banky a zavolat oběti, aby ji upozornil na možné ohrožení jejího účtu. Pokud útočník disponuje výše uvedenými informacemi, bude pro oběť snazší mu uvěřit a poskytnout další informace, jako například číslo účtu nebo heslo. Útočník může také použít techniku "spoofing"telefonního čísla, aby vzbudil v oběti větší důvěru.

V každém případě je pro úspěšné provedení této metody klíčové dobře připravit a koordinovat scénář a sbírat informace o oběti předem.[9]

2.2 Caller ID Spoofing

Tato metoda se často využívá v kombinaci s pretextingem a nazývá se spoofing. Spoofing spočívá v nahrazení čísla volajícího za číslo důvěryhodné osoby, například banky nebo policie. Útočník zavolá oběti a představí se jako pracovník banky, přičemž hovor jde přímo z banky oběti nebo se tak alespoň pro oběť jeví. Tím je oběť přesvědčena, že opravdu hovoří s pracovníkem banky a nemusí mít podezření. Výhodou spoofingu je, že pokud oběť zavolá zpět, skutečně se dovolá do své banky. Nicméně, spoofování čísel není jednoduché a často se využívají externí firmy, které mají potřebnou techniku a schopnosti, ale za úplatu.[10]

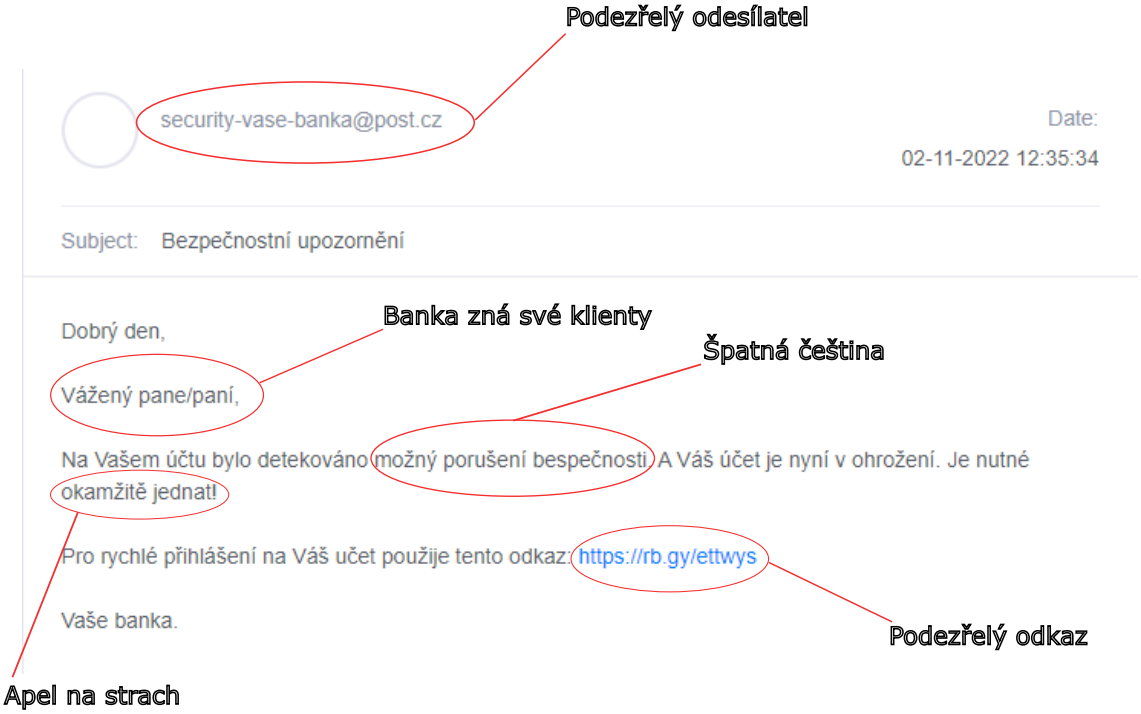
2.3 Phishing

Phishing je velmi využívaná metoda pro zjištění hesel pomocí internetových stránek.

Útočník vytvoří internetovou stránku, která se tváří jako legitimní stránka banky. Často je tato stránka provázána s oficiální stránkou pro vytvoření větší důvěry. Pokud tedy oběť klikne na nějaký odkaz na stránce, je přesměrována na legitimní stránku banky. Při vložení údajů do podvodné stránky jsou všechny informace poslány útočníkovi a zároveň může dojít k přihlášení do internetového bankovnictví pomocí vložených údajů, které útočník přesměruje na legitimní stránku. Oběť se na takovéto stránky nejčastěji dostane kliknutím na odkaz v e-mailu, který vypadá jako zpráva od banky s vymyšleným scénářem jako je možné napadení účtu s nutností změnit heslo.

Phishing je nebezpečný v tom, že uživatelé klikají na odkazy bez rozmyslu. Útočníci spoléhají na strach oběti, při oznámení o napadení účtu nebude člověk reagovat tak, jak by reagoval v normální situaci a na odkaz bez rozmyslu klikne. Prevencí

proti phishingu je kontrolovat, kam daný odkaz doopravdy vede a zamyslet se nad tím, zda se opravdu jedná o zprávu z banky.



Obr. 2.1: Příklad podvodného e-mailu

2.4 Spear phishing

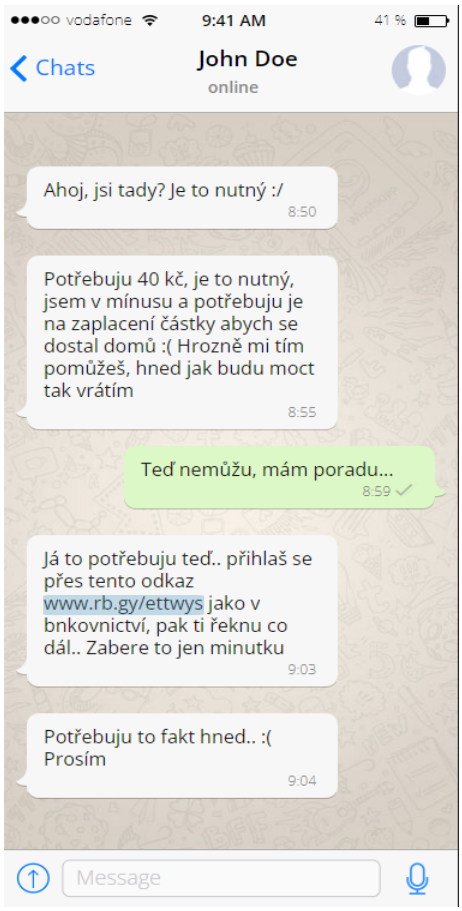
Je velmi podobná metoda získávání informací jako phishing s tím rozdílem, že phishing není cílen na určenou osobu, ale je rozesílán masivně. Oproti tomu spear phishing je mířen přímo na konkrétní osobu. Z toho vyplývá, že je nutný propracovanější scénář, a proto je tato metoda více nebezpečná než obyčejný phishing.

2.5 Smishing

Je forma phishingu provedená pomocí SMS zpráv. Pro oběť je snazší stát se obětí smishingu, protože lidé jsou více náchylní věřit SMS zprávám než zprávám, které přijdou přes e-mail. Při phishingu je také potřeba znát e-mail oběti, který může mít jakoukoliv délku a znění.

Oproti tomu smishing může být rozeslán masivně pomocí náhodně generovaných čísel. V ČR mají operátoři předvolbu a o to je jednodušší se trefit na nějaké číslo. Lze také použít mířený smishing na zájmovou osobu, ale zde je nutné již znát její telefonní číslo nebo se zmocnit účtu osoby, kterou má zájmová osoba již v kontaktech

a vydávat se za ní. Tyto mířené zprávy často obsahují prosbu o zaslání malé částky pro osobu v nouzi nebo přeposlání kódů, které přijdou oběti na zařízení. Zprávy obsahují odkaz na podvodnou stránku jako při phishingu.



Obr. 2.2: Mířený smishing

2.6 Vishing

Stejně jako smishing využívá mobilní telefon, ale zde již útočník přijde do kontaktu s obětí přes mobilní hovor. Při vishingu je vytvořen věrohodný scénář pomocí informací, které byly o oběti získány. Poté je uskutečněn hovor, kde se útočník může představit jako nový pracovník firmy, který zapomněl své heslo a nutně se potřebuje vzdáleně přihlásit do systému. IT pracovník firmy se bude snažit kolegovi pomoci a heslo mu může vyzradit.

2.7 Pharming

Název této metody je odvozen z anglických slov phishing a farming. Jedná se o podvod podobný phishingu, kde je oběť přesměrována na falešné stránky, kde jsou odcizeny citlivé údaje. Pharmingové útoky mohou být provedeny 2 způsoby. Při prvním útočník odešle oběti e-mail obsahující virus nebo trojského koně. Škodlivý kód poté pozmění soubory na hostitelském počítači takovým způsobem, že pokud oběť zadá adresu například své banky, bude přesměrována na falešné stránky. Tento způsob pharmingu je označován jako „pharming založený na malwaru“. Druhý způsob je založen na útoku zvaném DNS poisoning. DNS - Domain Name Systém, neboli systém doménových jmen je používán k překladu názvů domén na IP adresu. Pro uživatele je jednodušší si zapamatovat název domény jako www.vutbr.cz než její IP adresu 147.229.2.90. Tímto útokem lze infikovat DNS server tak, aby přepsal své údaje o IP adrese a tím odkazoval oběti na podvodné stránky.[11]

2.8 Quid Pro Quo

Quid Pro Quo neboli v doslovném překladu „něco za něco“ je technika využívaná prostřednictvím internetu, hovoru nebo přímého kontaktu. Útočník může aktivně obvolávat zaměstnance firmy s tím, že se jedná o pracovníka IT, který potřebuje vzdálený přístup k počítači oběti, aby aktualizoval software na novější verzi.

Pokud mu oběť takový přístup udělí například pomocí TeamVieweru nebo jiné aplikace pro vzdálený přístup, útočník může nainstalovat zadní vrátka, a tak se kdykoliv připojit na počítač. Útočník také může vyčkávat, až za ním oběť sama přijde se žádostí o pomoc. Pro takový typ útoku se používá scareware 2.14. Oběť zavolá na číslo uvedené na upozornění o možném infikování počítače a nutnosti ihned jednat. Útočník poté předstírá, že je pracovník technické podpory a potřebuje vzdálený přístup na počítač.

Tento typ útoku je velmi běžný a jsou pro něj vytvořeny „scam centra“, kde pracují operátoři používající předem připravený scénář. Oběti vysvětlí, že jejich počítač byl napaden a potřebuje okamžitou pomoc, jinak budou útočníci schopni získat všechny osobní údaje a přístup do internetového bankovnictví. Oběť je tak často vedena na stránku, kde si za finanční obnos zakoupí „antivirový program“ pro odstranění škodlivého softwaru na zařízení. Quid pro Quo lze použít i v přímém kontaktu s obětí.

2.9 Watering hole

Tento typ útoku není úplně běžný a je vysoce cílený na jednu osobu. Jméno této techniky bylo odvozeno od predátorů čekajících u napajedla pro svou kořist. Útočník čeká na specifickou událost, která bude obětí provedena, aby mohl zaútočit. Jak již bylo řečeno, tato technika je vysoce cílená, a proto je také nutná příprava.

Jako příklad lze uvést web donáškové služby, ze které si oběť objednává jídlo. Tuto informaci může zjistit pomocí trashingu. Poté se může pokusit najít zranitelnost na webu dodavatele a potom, co si oběť objedná jídlo, pomocí zranitelnosti dostat škodlivý software do zařízení oběti.

2.10 Baiting

Je metoda útoku, která spoléhá na lidskou zvědavost. Útočník umístí paměťové zařízení (USB, CD) na místě, kde ho někdo najde. Zařízení má na sobě často lákavé označení jako „prémie březen“, oběť samozřejmě chce zjistit, jakou dostane prémii a jako dostanou její kolegové, a tak vloží zařízení do počítače. Tím však dojde k aktivaci skriptu, který na počítači nainstaluje malware nebo keylogger. Oběť se tak nedozví, kolik dostane peněz, ale ještě kompromituje zařízení. Známým případem baitingu je USB disk s programem, který zpozdil jaderný program Iránu o 2 roky.[17]

2.11 Trashing

Metoda Trashing se využívá pro získávání citlivých informací, jako jsou hesla, čísla kreditních karet, adresy, telefonní čísla a další údaje, které jsou důležité pro útočníka. Útočník hledá tyto informace ve vyhozených dokumentech, které lidé vyhazují do běžného odpadu. Tyto dokumenty mohou být například účetní doklady, výpis z bankovního účtu, obálky s osobními údaji a další podobné dokumenty.

2.12 Tailgating a piggybacking

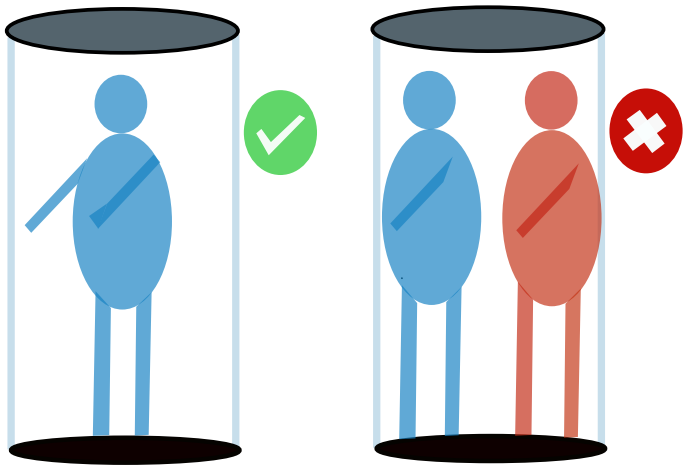
Tyto metody využívají fyzického kontaktu s obětí, nikoliv však pro získání citlivých informací, ale pro vpuštění do zabezpečené oblasti. Tyto techniky se používají hlavně ve velkých firmách, kde není možné znát všechny zaměstnance.

Tailgating spočívá v následování oběti do zabezpečené zóny v jejím závěsu. Nejčastěji pomocí karty oběť otevře dveře a útočník vstoupí hned za ní, protože on sám kartu nevlastní.

Piggybacking funguje na podobném principu, útočník předstírá, že kartu nechal doma, a tak poprosí zaměstnance venku, zda by mu nemohl otevřít svojí kartou.

Tailgating je tedy nevědomé vpuštění osoby do objektu a piggybacking vědomé vpuštění osoby do objektu.[1]

Proti tomuto typu útoku se lze bránit politikou firmy. Firma Google po svých zaměstnancích vyžaduje, aby do zabezpečené oblasti vstupovali jednotlivě. Tedy pokud je nutné k otevření dveří přiložit kartu, tak zaměstnanec kartu přiloží, otevře dveře, vstoupí, a zavře je, i když hned za ním stojí někdo jiný. Druhou metodou je dvojí ověření. Před vstupem do místnosti je box pouze pro jednu osobu. Pokud se v boxu nachází více osob, systém nedovolí dveře otevřít ani po přiložení platné karty. Pokud je všechno v pořádku, osoba vstoupí do zabezpečené místnosti a další osoba může vstoupit do boxu.



Obr. 2.3: Box proti tailgatingu

2.13 Shoulder surfing

Metoda Shoulder surfing spočívá v pozorování člověka při zadávání citlivých údajů jako jsou hesla nebo čísla platebních karet, a to bez jeho vědomí. Tento útok se často provádí v místech s vysokou koncentrací lidí, jako jsou vlakové stanice, letiště nebo veřejné prostory s počítači, kde útočník může snadno zahlédnout a zapamatovat si klíčové informace.[8, 12]

2.14 Typy škodlivých kódů

Útočníci mohou používat různé typy škodlivých kódů pro získání informací o oběti, získání kontroly nad počítačem nebo přinucení oběti vykonat nějakou činnost. Tyto

druhy kódů lze souhrnně označit jako škodlivé kódy. Pro pochopení názvosloví jednotlivých druhů škodlivých kódů byly tyto kódy popsány níže.

1. Virus – jedná se o kód se schopností replikace, bývá přiložen jako část přílohy souboru, kde po jeho spuštění dojde k replikaci kódu bez uživatelského vědomí. Jsou využívány k vytváření škodlivých akcí na uživatelském zařízení jako je vytěžování disku počítače, infikování dat nebo vytvoření „zombie“ PC. Zombie počítače mohou být poté aktivovány na dálku a mohou přes ně být vedeny útoky nebo je počítač pouze využit jako výpočetní síla pro DDos útok.
2. Trojský kůň – je částí legitimního softwaru bez schopnosti replikace. Je využíván jako nástroj pro připojení k infikovanému počítači, ke změně nebo destrukci dat nebo k narušení výkonosti zařízení.
3. Spyware – špionážní program ke zjištění dění na zařízení, může být použit k legitimní činnosti jako je kontrola zaměstnanců v práci, ale útočníky je často využit pro krádež osobních dat. Jako příklad spyware lze uvést keylogger.
4. Scareware – je podvodná taktika s cílem vystrašit oběť, může být šířen pomocí e-mailu nebo pomocí vyskakovacích reklam při navštívení některých stránek. Při otevření odkazu je oběť přesměrována na stránky, kde mohou být další typy škodlivých kódů. Nejčastější obsah scarewaru je oznámení o infikování počítače virem a nutnosti rychle jednat.
5. Adware – existují dva typy adwaru, první je neškodný v podobě aplikace, která nabízí levné hry zákazníkům a profituje z jejich prodeje. Druhým typem je speciální typ spywaru, který nabízí konkrétní reklamy. Například při použití webového prohlížeče pro vyhledání dárku pro 5leté děti se poté na sociálních sítích začnou objevovat reklamy související s vyhledávanou tématikou.
6. Ransomware – škodlivý kód, který po spuštění zašifruje všechny soubory na zařízení, oběť tak ztratí přístup k veškerým datům. Tento kód není používán k získání informací o oběti, ale pomocí technik sociálního inženýrství je spuštěn na zařízení oběti. Ta je poté vyzvána k zaplacení „výkupného“ pro odemčení veškerých dat. Pro platbu jsou v současné době používány kryptoměny, pro jejich pseudoanonymitu, nejčastěji bitcoin. Po odeslání požadované částky útočníci data odemknou, v případě, že by po zaplacení data nebyla dešifrována, uživatelé zasaženi stejným ransomwarem by věděli, že nemá cenu výkupné platit, což je špatné pro „byznys“. Nejznámějším ransomwarem je WannaCry.
7. Worm – jedná se o speciální druh viru se schopností replikace a šíření na další zařízení přes počítačovou síť. Stejně jako virus dokáže vytvořit zadní vrátka na zařízení, zpomalit jeho výkonnost nebo může omezit rychlost přenosu po síti.[13, 14, 15]

Obr. 2.4: WannaCry Ransomware [16]

V této části byly popsány techniky sociálního inženýrství hojně využívané v dnešní době společně s uvedením některých možných scénářů útoků a možností obrany, podle kterých lze vidět, že sociální inženýrství není jen prostřednictvím internetu, ale dá se aplikovat i pomocí fyzického kontaktu. Tyto obecně popsané metody lze aplikovat na netušící oběti, avšak hlavně při fyzickém kontaktu je nutná improvizace útočníka. Tyto metody je dobré znát pro jejich odhalení. V praktické části budou využity především metody phishing a vishing. Zároveň byly popsány typy škodlivých kódů využívaných pro získání kontroly nad zařízením nebo pro manipulaci s obětí, mezi kterými je dobré rozlišovat.

Obr. 2.5: Scareware na webové stránce

3 Red Teaming

Cílem této práce je vytvoření aplikace pro Red Teaming. Z toho důvodu je nutné vědět o co se jedná, jaké jsou rozdíly oproti penetračnímu testování, jaké subjekty figurují při testování zabezpečení a jaké jsou aktivity, kterých je třeba během testování dosáhnout.
Jako červený tým lze označit skupinu lidí, kteří se snaží zlepšit jak fyzické tak kybernetické zabezpečení firmy prostřednictvím útoků na danou instituci, stejným způsobem jako by byl veden útok hackerskou skupinou.

3.1 Penetrační testování vs Red Teaming

Při testování bezpečnosti sítě jsou často zaměňovány pojmy penetrační testování a Red Teaming. I když tyto metody používají podobné principy, každá se liší svým přístupem.

Penetrační testování je metoda testování zabezpečení, která umožňuje organizacím zjistit úroveň zabezpečení sítí, platforem, hardwaru, aplikací a dalších systémů v předem definovaném rozsahu s cílem identifikovat zranitelnosti. Pro tento účel se používají penetrační testeři, kteří postupují podle jasně definované metodiky, například OWASP, PTES nebo OSSTMM. Tyto testy nejsou skryté a správci ICT příslušné organizace o nich vědí, případně se na nich mohou podílet.

Na druhé straně Red Teaming je aktivita, která se snaží co nejvíce napodobit chování útočníků, kteří by se mohli pokusit získat přístup do sítě. Tato metoda testování zabezpečení se zaměřuje nejen na kybernetické, ale také na fyzické zabezpečení a využívá také sociálního inženýrství. Cílem Red Teamingu není pouze identifikovat zranitelnosti, ale také ověřit, jak organizace reaguje na hrozby a jak úspěšně může bránit svá aktiva. Testování je často prováděno skrytě a testovací tým má k dispozici dokumenty, které dokazují, že provádí testování zadané firmou a jsou oprávněni v objektu pobývat. Tyto dokumenty jsou v případě odhalení předloženy ochrance objektu, ale někdy i tak může dojít k nechtěným incidentům.

Red Teaming se také používá pro trénink interních týmů v reakci na dané události a hodnotí se správnost zvoleného postupu v souladu s incident response planem[1]. Při této metodě se také často používá MITRE ATTACK a MITRE DEFENSE pro identifikaci hrozeb a návodů na zajištění bezpečnosti. MITRE ATTACK popisuje útoky a taktiky používané útočníky, zatímco MITRE DEFENSE poskytuje návody na zajištění bezpečnosti pro obranu proti těmto útokům. Tyto frameworky mohou být použity pro identifikaci hrozeb a vytvoření lepšího incident response plánu. Při

[1]Incident response plan (IRP) je dokument, který popisuje postupy, kroky a odpovědnosti při reakci na kybernetický útok nebo jinou bezpečnostní událost.

testování zabezpečení se často používají společně s jinými metodami jako jsou penetrační testování a Red Teaming.

Je důležité si uvědomit, že penetrační testování a Red Teaming jsou dvě různé metody testování zabezpečení, které mohou být použity v různých situacích a mají odlišné cíle.

3.2 Typy týmů

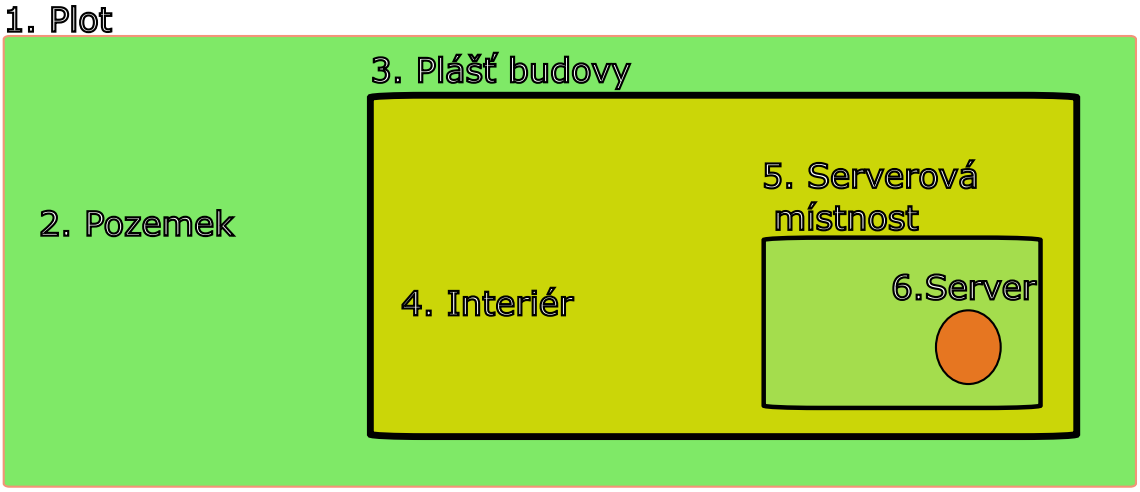
Testování zabezpečení pomocí Red Teamingu si lze představit jako hru na kočku a myš, ve které jsou 3 týmy - červený, modrý a bílý.

1. Červený tým - Tým útočníků, kteří mají za úkol napadnout organizaci a získat určený cíl. Často se jedná o informace, přístupové údaje nebo data, která mohou být použita pro škodlivé účely. Červený tým se snaží využít všech dostupných technik a postupů, aby byl útok úspěšný.
2. Modrý tým - Obranný tým, jehož úkolem je chránit organizaci před útoky. Tento tým je složen z odborníků na zabezpečení sítě a IT infrastruktury, kteří mají za úkol identifikovat a odvrátit útoky. Modrý tým také sleduje bezpečnostní události a incidenty a zajišťuje reakci na ně. Tyto týmy jsou často označovány jako Security Operations (SOC) či Cyber Defense Centrum (CDC).
3. Bílý tým - Tým organizátorů testování, kteří určují pravidla a cíle útoku. Bílý tým zajišťuje koordinaci a komunikaci mezi červeným a modrým týmem. Tento tým také zajišťuje transparentnost a dokumentaci všech kroků v rámci testování a poskytuje zprávu s výsledky.

3.3 Zabezpečení objektu

Red Team testeři provádějí i testování fyzického zabezpečení objektu s cílem nepovoleného vstoupení do objektu nebo areálu firmy pro zisk vlajky. Získání fyzického přístupu do objektu není vždy jednoduché (pokud neexistuje někdo, kdo nám dovnitř pomůže). Je totiž nutné překonat množství zabezpečení. Jednotlivé vrstvy zabezpečení popisuje obrázek níže kde je jako příklad uveden server, ke kterému by testeři chtěli získat fyzický přístup. Pro získání přístupu k serveru je nutné většinou překonat 6 linií překážek.

1. Překonání plotu
2. Průchod přes pozemek
3. Průnik pláštěm budovy



Obr. 3.1: Zabezpečení objektu

4. Průchod interiérem
5. Vstup do místnosti se serverem
6. Napojení na server

Při překonávání linií 1–5 může být útočník odhalen pomocí detektorů (pohybu, tepla, tříštění skla, otřesů), které automaticky spustí poplach, nebo kamer připojených na vrátnici obsluhovaných pověřenou osobou. U větších firem se lze setkat s liniemi 1-6 a u menších s 3-6, když firma sídlí například v centru bez pozemku.

Překonání všech linií nepozorovaně může být časově náročné a existuje velké riziko odhalení útočníka. Proto je mnohem jednodušší využít techniky sociálního inženýrství a do objektu být vpuštěn ostrahou objektu (falešná zabezpečovací firma), pokusit se o tailgaiting a vstoupit do objektu neautorizovaně, získat přístup do firemní sítě pomocí zadních vrátek nebo pomocí phishingové kampaně.[2][5]

3.4 Cyber Kill Chain

Stejně jako existují metodiky pro penetrační testování - OWASP, OSSTMM, atd., tak existují i různé frameworky pro Red Teaming. V této části bude popsán framework Cyber Kill Chain (CKC), který se oproti ostatním frameworkům vyznačuje svou přímočarostí. Součástí CKC je 7 aktivit, které je nutné vykonat Red Teamem pro splnění úspěšného útoku. Tyto aktivity se naopak Blue Team snaží narušit.

[2]Citlivé informace se mohou nacházet na serveru, který je od sítě odpojen a je k němu nutné získat fyzický přístup.

Těmto aktivitám předchází vymezení cíle, kterého má být dosaženo a jaké techniky mohou být použity. Po těchto aktivitách následuje konečná zpráva, kde je popsáno jak byl proveden útok, i v případě, že nebyl úspěšný a navrženo opatření.

Aktivity obsažené v CKC jsou následující:

1. Reconnaissance (Průzkum) - Sběr informací pro provedení útoku. O této aktivitě více pojednává kapitola 3.4.1
2. Weaponization (Vyzbrojení) - Vytvoření vektoru útoku na míru, může se jednat o virus, malware, červa, apod.
3. Delivery (Doručení) - Spuštění útoku, především se jedná o phishingové e-maily.
4. Exploitation (Zneužití) - Spuštění kódu na zařízení, který byl doručen v předchozím kroku. Může se jednat buď o špatné zabezpečení sítě nebo o lidskou chybu.
5. Installation (Instalace) - Instalace malwaru nebo backdooru pro zajištění přístupu.
6. Command and Control (Velení a řízení) - Navázání komunikace směrem ven ze sítě pro využití nainstalovaného malwaru, tak aby mohl být ovládán Red Teamem. Pro toto řízení se používají především protokoly DNS a HTTP pro jejich nenápadnost. V tuto chvíli útočník může postupovat dále sítí, rozšiřovat backdoor na další zařízení či eskalovat svoje práva pro dosažení cíle.
7. Actions on Objectives (Akce týkající se cílů) - Podnikání kroků k získání vlajky, tedy dosažení cíle, který byl stanoven v zadání.

3.4.1 Reconnaissance - Průzkum

Stejně jako při plánování vyloupení banky je velice nutná příprava a stejně je tomu tak i při útoku realizovaného Red Teamem. Jsou využívány veřejně dostupné i neveřejné zdroje pro zjištění co nejvíce informací o cíli. K získání těchto informací jsou používány sociální sítě jako Facebook, Instagram, Twitter, LinkedIn, techniky Open-source intelligence (OSINT) a další nástroje.

Součástí průzkumu je i zjištění informací o zaměstnancích. Tyto informace jsou buď poskytnuty White Teamem nebo je nutné je zjistit jiným způsobem. Zároveň jsou zjišťovány služby a technologie používané ve firmě. [18, 19]

Sběr konkrétních informací

Při útoku na organizaci není útok prováděn na organizaci samotnou, ale pouze na individuální pracovníky.

Zdrojem informací pro útok podle OSINT jsou: [20]

1. Veřejně dostupné databáze
   (a) Soudní záznamy
   (b) Politické příspěvky
   (c) Profesionální licence a registrace
2. Sociální sítě
   (a) Metadata
   (b) Charakter osoby
   (c) Frekvence přidávání příspěvků
   (d) Navštívená místa
   (e) Přítomnost na sociálních sítích
3. Používání internetu
   (a) E-mail
   (b) Přezdívky
   (c) Registrované domény
   (d) IP adresa
4. Bydliště
5. Mobilní stopa
   (a) Telefonní číslo
   (b) Typ zařízení
   (c) Nainstalované aplikace
   (d) Administrátorská oprávnění
6. Informace za zaplacení

V této kapitole bylo vysvětleno co je Red Teaming a jeho rozdíly oproti penetračnímu testování. Byly popsány funkce červeného, modrého a bílého týmu. Byly vysvětleny aktivity obsažené ve frameworku Cyber Kill Chain s důrazem na nejdůležitější část zjišťování informací a bylo popsáno zabezpečení objektu. V praktické části budou nejvíce využity aktivity 1. a 3. z CKC.

4 Legislativa

Jak již bylo zmíněno v předchozí kapitole, Red Teaming je činností, která vyžaduje velkou opatrnost a dodržování platných zákonů a nařízení. Tato kapitola se zaměřuje na právní rámec, který se týká sociálního inženýrství a souvisejících aktivit. V České republice neexistuje žádná zvláštní legislativa pro sociální inženýrství, ale to neznamená, že by se tato činnost nemusela řídit určitými normami a principy. V této kapitole budou přiblíženy platné zákony a nařízení, které mohou být aplikovány na Red Teaming a sociální inženýrství obecně. Zároveň se tato kapitola zaměřuje na konkrétní paragrafy, které je nutné dodržovat, aby nedošlo k porušení zákona.

4.1 Občanský zákoník

Zákon č. 89/2012 Sb. občanský zákoník
§ 2586 Dílo
Pro provádění aktivit spojených s Red Teamingem je nutné mít vytvořenou smlouvu o dílo, která definuje základní parametry projektu a zajišťuje, že práce bude provedena v souladu s platnými zákony a obecnými ustanoveními, které jsou v této kapitole dále rozebrány.

Smlouva o dílo je základním právním nástrojem, kterým se zhotovitel zavazuje k vytvoření určitého díla a zadavatel k zaplacení za provedenou práci. V oblasti IT a bezpečnosti, včetně Red Teamingu, je smlouva o dílo běžně používaná.

V rámci Red Teamingu slouží smlouva o dílo k jasně definovaní cílů projektu a k stanovení konkrétních výsledků, kterých má být dosaženo. V smlouvě se specifikují například požadované testy, rozsah práce a termíny pro doručení výsledků.

Důležité je rovněž stanovit v smlouvě podmínky a termíny platby za provedenou práci. To zajišťuje, že zhotovitel bude motivován k dokončení práce včas a v souladu se specifikacemi. Smlouva o dílo taktéž chrání obě strany před možnými nedorozuměními a sporovými situacemi.

Výsledkem smlouvy o dílo v Red Teamingu je jasně definovaný projekt s konkrétními cíli a výsledky, což umožňuje zhotoviteli plánovat a organizovat práci efektivně a zajišťuje, že zadavatel bude mít výsledky, které odpovídají jeho požadavkům.

§ 86
Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o

jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.[21]

S tímto paragrafem se lze setkat nejčastěji při kontaktní formě sociálního inženýrství, kdy se útočník snaží získat informace pomocí rozhovoru s obětí. Jako příklad lze uvést scénář, kdy se útočník uchází o pozici vrátného a tak se jako zájemce baví s pracovníkem ostrahy, kde se pomocí rozhovoru snaží získat potřebné informace (pauza na kafe, střídání směn apod.). Při takovém rozhovoru ale může být složité si zapamatovat všechny informace, obvzlášť pokud je pracovník velmi sdílný, a proto je možné rozhovor nahrát, čímž se útočník dopouští trestného činu. Pro vyhnutí spáchání trestného činu je možné se vydávat za zaměstnance novin a přímo informovat oběť o tom, že rozhovor bude nahrán. Pokud oběť udělí souhlas, není spáchán trestný čin.

4.2 Trestní Zákoník

K trestné činnosti **Zákona č. 40/2009 Sb. Zákon trestní zákoník,** je vztaženo mnoho zákonů, legislativ, nařízení a ustanovení. V této podkapitole budou vypsány trestné činy a obecná ustanovení a k nim uvedeny příklady, se kterými je možné se setkat při sociálním inženýrství.

4.2.1 Obecná ustanovení

§ 29 Nutná obrana
(1) Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvající útok na zájem chráněný trestním zákonem, není trestným činem.
(2) Nejde o nutnou obranu, byla-li obrana zcela zjevně nepřiměřená způsobu útoku.

Tento paragraf se nevztahuje přímo na útočníky, ale na osoby, které se starají o infrastrukturu pod útokem. Pokud je například veden útok na firemní server a není možné ho zastavit jiným způsobem (např. ukončením spojení nebo uvedením IP na blacklist), může být na útočníka použita reakce, tzv. **Hack Back**. Protože se bude jednat o nutnou obranu, nebude to trestný čin. Nicméně nutná obrana musí být úměrná nebo mírně větší než přicházející útok, jinak se nejedná o nutnou obranu. Pro lepší pochopení nepřiměřené obrany je uveden příklad z jiného prostředí. Když je osoba napadena pěstmi, použití automatické zbraně by bylo nepřiměřené obraně.

§ 30 Svolení poškozeného

(1) Trestný čin nespáchá, kdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny.
(2) Svolení podle odstavce 1 musí být dáno předem nebo současně s jednáním osoby páchající čin jinak trestný, dobrovolně, určitě, vážně a srozumitelně; je-li takové svolení dáno až po spáchání činu, je pachatel beztrestný, mohl-li důvodně předpokládat, že osoba uvedená v odstavci 1 by tento souhlas jinak udělila vzhledem k okolnostem případu a svým poměrům.

Tento paragraf je uveden z důvodu Red Teamingu popsaného v kapitole 3, kdy je nutné mít vytvořenou smlouvu se zadavatelem. Nebo při soutěžích, kde firmy svolí k útoku na jejich služby za cílem zvýšení bezpečnosti. Pokud je takové svolení uděleno, útočníci nepáchají trestnou činnost, pokud nepřekročí rozsah toho, co jim bylo povoleno. Bez tohoto paragrafu by nebylo možné provádět penetrační testování sítě bez možných právních následků.

§ 120 Uvedení někoho v omyl a využití něčího omylu prostřednictvím technického zařízení
Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do dat uložených v počítačovém systému nebo na nosiči informací, zásahu do programového nebo technického vybavení počítačového systému nebo provedením jiné operace v počítačovém systému, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.

S tímto paragrafem se lze setkat například při technice Quid pro Quo 2.8, kdy se útočník připojí pomocí vzdálené plochy na počítač po přesvědčení zaměstnance, že se jedná o správce sítě, který na něho potřebuje nutně přístup nebo při kontaktní formě, kdy je mu umožněn pod falešnou záminkou přístup na počítač. Pokud by poté bylo nějak manipulováno s daty, jedná se o trestný čin.

4.2.2 Trestné činy

§ 182 Porušení tajemství dopravovaných zpráv
(1) Kdo úmyslně poruší tajemství

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu dat do počítačového systému, z něj nebo v jeho

rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková data, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.
(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo

b) takového tajemství využije.

Samotné čtení zpráv, které nebyly určeny pro nás jako příjemce, je trestné, pokud k tomu nebyl udělen souhlas. Pomocí phishingu může být zjištěno heslo, které může být využito pro přístup na e-mail. Čtením zpráv v této e-mailové schránce je porušení tohoto paragrafu. Stejně tak lze tento paragraf uplatnit i na sociální sítě nebo SMS. Typickým způsobem, jakým se tento zákon porušuje, je sniffing, tedy zachytávání komunikace v síti, což umožňuje získat citlivé informace nejen o provozu, ale i o obsahu..

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

(1) Kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, dat uložených v počítačovém systému nebo na nosiči informací anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.
(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 v úmyslu získat pro sebe nebo pro jiného majetkový nebo jiný prospěch, způsobit jinému škodu nebo jinou vážnou újmu, anebo ohrozit jeho společenskou vážnost.

Tento paragraf se při použití technik sociálního inženýrství příliš často neuplatňuje, neboť pro splnění jeho podmínek je nutné zveřejnit získaný obsah zpráv. Nicméně, je uveden z důvodu možnosti využití technik sociálního inženýrství pro získání hesla nebo přístupu k informacím. Například hackeři mohou zveřejnit obsah zpráv politika, aby odhalili jeho lži před veřejností.

§ 209 Podvod

(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo pro-

padnutím věci.

Jako příklad lze uvést scénář využívající pretexting, také známý jako "blagging"2.1. Pachatel se vydává za ředitele společnosti nebo jinou důvěryhodnou osobu s odpovídajícími pravomocemi, aby navázal kontakt. Pod touto záminkou kontaktují zaměstnance firmy s tím, že jim byl zadán úkol od jejich nadřízeného, aby je přiměli k předání citlivých informací nebo k účasti na jiných útočných aktivitách.

Druhým příkladem mohou být podvodné e-shopy, které nabízejí brigády, kde je náplní práce zakládání účtů. Pachatelé poté přeposílají výdělky z nelegálních aktivit na tyto účty, aby byli hůře vystopovatelní. Tento druh útoku je znám jako "money muling"[22]

§ 230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Kdo zasáhne do počítačového systému nebo nosiče informací tím, že

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží nebo přenese data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítačového systému nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.

Tento paragraf se týká neoprávněného přístupu k počítačovému systému a zásahu do počítačového systému nebo nosiče informací, což zahrnuje mnoho aktivit, které jsou obvykle označovány jako hacking. Mezi takové aktivity patří například narušení, změna nebo smazání dat, přenos dat a podobně. Často se prověřuje, zda bylo překonáno zabezpečení systému a zda byly získány informace o oběti. Pod tuto kategorii spadají také kybernetické útoky, jako jsou DDoS útoky nebo zašifrování dat na zařízení pomocí ransomware.[22]

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části nebo k neoprávněnému zásahu do počítačového systému nebo nosiče informací, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, v úmyslu, aby jej bylo užito ke spáchání trestného činu porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b) nebo c) nebo trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 odst. 1 nebo 2, bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.

Tento paragraf se zabývá trestnými činy souvisejícími s opatřením a přechovávání přístupových zařízení a hesel k počítačovému systému. Mezi typické příklady patří neoprávněné získání přístupových údajů pomocí technik sociálního inženýrství 2, jejich přechovávání a použití pro neoprávněný přístup k počítačovému systému nebo k datům v něm uloženým. Legální opatření hesla samo o sobě není trestným činem, dokud není zjištěno, že bude použito pro neoprávněný přístup k počítačovému systému.

§ 232 Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítačového systému nebo jiného technického zařízení pro zpracování dat,a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci.[23]

Paragraf § 232 se vztahuje na případy neoprávněného zásahu do počítačového systému nebo nosiče informací z nedbalosti. Tento paragraf je významný zejména v oblasti Red Teamingu, kdy jsou testovány zabezpečovací mechanismy počítačových

systémů. Pro splnění trestného činu musí být porušena povinnost vyplývající ze zaměstnání, povolání nebo smlouvy a musí dojít k zavinění z nedbalosti, tedy zapomenutí nebo přímé ignorování povinností, což vede ke škodě. Hlavně se jedná o případy, kdy ICT správci, administrátoři nebo právě Red Team testeři neplní své povinnosti a tím způsobují škodu.

V této kapitole byly vypsány zákony týkající se sociálního inženýrství a paragrafy, které je možné při jeho praktikování porušit. V praktické části bude vytvořena aplikace, která zajistí, že nedojde k porušení těchto paragrafů při testování za pomocí Red Teamingu.

5 Výsledky studentské práce

Praktická část této práce se věnuje vývoji aplikace pro vytváření a zobrazování vektorů útoků za pomocí metod sociálního inženýrství. Tato aplikace bude sloužit pro potřeby Red Teamingu a měla by usnadnit testování zaměstnanců. Zároveň bude vytvořeno programové řešení, které by mělo zajistit, že testování bude probíhat v souladu s právem, v rozsahu a za použití technik, které budou stanoveny zadavatelem v smlouvě o dílo.

5.1 Využité frameworky

Tato kapitola se věnuje popisu využitých frameworků a knihoven použitých při vytváření aplikace.

5.1.1 Python

Programovací jazyk, ve kterém je aplikace napsaná, je Python. Jedná se o vysokoúrovňový, objektově orientovaný programovací jazyk s dynamickou sémantikou. Jeho syntaxe je jednoduše naučitelná, čímž z něho činí velice atraktivní jazyk pro vývoj aplikací, vytváření skriptů nebo spojovací jazyk pro propojení existujících komponent. Jazyk Python je volně dostupný a šiřitelný. Zároveň obsahuje debugger, který je napsán v jazyce Python, určený pro odladění kódu a rychlé kontroly proměnných pro nalezení chyb[24].

5.1.2 Pycharm

Jedná se o integrované vývojové prostředí (IDE) pro programovací jazyk python, které poskytuje velkou škálu základních nástrojů pro programátory píšící v pythonu. Pycharm poskytuje pohodlné prostředí pro produktivní vývoj aplikací psaných v Pythonu. Programovací prostředí bylo vytvořeno českou společností JetBrains a je podporováno na operačních systémech Windows, Linux a macOS. Od roku 2013 lze získat volně dostupnou (open-source) verzi[25] .

5.1.3 SqLite

Jedná se o knihovnu napsanou v jazyce C, která je součástí vývojového prostředí Pycharm. Tato knihovna implementuje rychlý, samostatný a vysoce spolehlivý databázový stroj SQL, který je nejpoužívanější databázový stroj na světě. V současné době se používá více než 1 bilión databázi SQL. Zdrojový kód SQLite je volně dostupný komukoliv pro libovolné účely[26].

5.1.4 Tkinter

Je knihovna, která je součástí jazyku Python, určená pro vytváření grafického rozhraní (GUI), stejně jako je uživatel zvyklý v prostředí Windows. Tato knihovna je jednoduchá k používání a určená především pro začátečníky v oblasti grafického programování.

5.2 Vývoj aplikace

Aplikace vytvářená v této práci by měla umožňovat základní funkce jako je vytvoření uživatele, vytvoření scénáře pro útok, který bude používán jako některá z metod sociálního inženýrství, zadávání úkolů skupinám nebo jednotlivci, výpis zpráv o provedeném testování, a to buď částečných nebo úplných a další funkce, které budou podporovat funkci a užitečnost aplikace. V semestrální části této práce bylo vytvořeno grafické rozhraní aplikace a základní funkce - vytvoření uživatele, vytvoření scénáře a načtení scénáře.

5.2.1 Vytvoření uživatele

Stejně jako ve všech ostatních aplikacích, které obsahují uživatele, je zapotřebí ukládat do databáze jejich autentizační údaje pro přihlášení do aplikace. Pro vytvoření takové databáze byla použita knihovna SQLite.

Oprávnění pro vytváření uživatelských účtů by neměl mít k dispozici každý uživatel, především z bezpečnostních důvodů. Z toho důvodu takovou možnost má pouze administrátor, který má na rozdíl od ostatních uživatelů více možností v aplikaci. Po přihlášení do aplikace jako administrátor má k dispozici více položek než běžný uživatel, mezi tyto položky patří správa uživatelů v systému.

Samotné vytvoření nového uživatele probíhá jednoduchým způsobem a to je zadáním nového přihlašovacího jména a hesla. Pokud nedojde ke shodě s již vytvořeným uživatelem, který je v databázi pod stejným jménem, je vytvořen nový uživatel, který může po přihlášení využívat všech možností aplikace jako ostatní uživatelé. Administrátor má možnost také uživatele po zadání jeho jména odstranit z databáze, změnit heslo uživatele v případě, že ho uživatel zapomene a vyhledávat uživatele v databázi. Všechny tyto funkce jsou ošetřeny výjimkami a v případě, že by některá z nich nastala, je na to administrátor upozorněn.

5.2.2 Vytváření scénářů

Vytváření scénářů pro útok je stěžejní částí aplikace. Stejně jako při vytváření uživatele jsou scénáře ukládány do databáze vytvořené v SQLite. Možnost vytvořit scénář

pro útok mají všichni uživatelé, avšak pouze administrátor je může odstranit. Pro vytvoření scénáře je nutné splnit několik podmínek a to je zadání názvu nového scénáře a zvolení o jakou praktiku se bude jednat (vishing, phishing).

V současném stavu aplikace podporuje vytvoření scénáře pro vishing a to podle rozhodovacího stromu. Po zadání názvu nového scénáře je uživateli zobrazen text s nápovědou k zadání úvodní věty, kterou bude navazovat kontakt s obětí. Poté se postupuje podle rozhodovacího stromu. Tedy po vytvoření úvodní věty je uživateli zobrazen text s nápovědou k vytvoření odpovědi v případě negativní reakce oběti a poté k vytvoření pozitivní odpovědi. Tímto způsobem se postupuje až do chvíle, kdy je dosaženo cíleného konce a útočník je buď úspěšný a získá informace nebo oběť neuvěří a hovor ukončí.

5.2.3 Využití scénáře

Pro využití již napsaného scénáře stačí zadat jméno, pod kterým byl uložen do databáze. Uživatel si tato jména nemusí pamatovat, neboť v okně, ve kterém se nachází čtení scénářů, je zobrazena databáze v textové podobě obsahující názvy všech již vytvořených scénářů. Po zadání názvu scénáře je zobrazeno textové pole s úvodní větou a útok může začít. V tomto okně jsou přítomné tlačítka pro negativní a pozitivní odpovědi oběti. Podle reakce oběti na úvodní větu stačí kliknout na tlačítko odpovídající reakci oběti a do textového pole je načtena další věta, kterou by měl uživatel pokračovat. Zároveň je zde tlačítko pro návrat pro případ chyby způsobené uživatelem nebo změny odpovědi oběti.

5.2.4 Právní kontrola

V navazující diplomové práci bude vytvořena funkce pro kontrolu rozsahu testování a zajištění, že bude testování probíhat v souladu s právem.

Tato funkce bude fungovat na principu upozornění uživatele na možné porušení práv nebo nemožnosti využití nějakého typu scénáře pro útok. Pro tuto funkci bude potřebné zadat informace při vytváření nového úkolu, aby mohlo dojít ke kontrole.

Při vytváření úkolu uživatel zadá do předem připraveného formuláře údaje ze smlouvy, která byla vytvořena se zadavatelem. Pomocí těchto informací budou filtrovány scénáře pro útok, které je možné využít a uživatel bude upozorněn, které praktiky lze využít a které nikoliv.

5.3 Možné vylepšení v navazující diplomové práci

V diplomové práci budou provedena vylepšení aplikace, aby odpovídala zadání práce. Mezi tyto vylepšení patří právní kontrola, zadávání úkolů skupinám nebo jednotlivci, generování zpráv o testování a další funkce sloužící pro vylepšení aplikace. Zároveň bude upravena grafická stránka aplikace, aby byla pro uživatele více přívětivá a dalo se v ní lépe orientovat.

Závěr

V teoretické části semestrální práce bylo vysvětleno, co je a čím se vyznačuje sociální inženýrství a popsány jeho nejvyužívanější techniky společně s uvedenými scénáři a možnostmi obrany proti těmto technikám. Byl vysvětlen princip autentizace a uvedeny možnosti, kterými je možné autentizaci provést. Důraz byl kladen na autentizaci znalostí, na kterou se sociální inženýři nejčastěji zaměřují.

Bylo popsáno, čím se vyznačuje Red Teaming a jeho rozdíly oproti penetračnímu testování. Byly popsány subjekty, které figurují při testování zabezpečení a aktivity, kterých je třeba dosáhnout. Byl popsán Cyber Kill Chain, který je při testování využíván, a jeho části se zaměřením na jeho prvotní část - Průzkum. Bylo popsáno zabezpečení objektu s liniemi, se kterými je možné se setkat při testování fyzické bezpečnosti a vysvětleno, proč je lepší využít metody sociálního inženýrství pro vnik do objektu.

V poslední kapitole teoretické části byly popsány zákony, které je možné při praktikování sociálního inženýrství porušit a uvedeny příklady jak je možné tyto zákony porušit.

V praktické části semestrální práce, která se věnuje vývoji aplikace, byly popsány využívané frameworky, pomocí kterých je vyvíjena aplikace a základní funkce, kterými v současné době aplikace disponuje. Zároveň bylo uvedeno řešení právní kontroly, kterým bude aplikace ve finální verzi disponovat a uvedeny návrhy pro přidání funkcí a vylepšení, které bude v navazující diplomové práci provedeno.

Literatura

[1] *POLÁŠEK, Adam. Sociální inženýrství jako metoda vytěžování osob.* Zlín, 2018. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Dora Lapková.

[2] *What is Social Engineering?* [online]. WEEBROOT [cit. 2022-10-31]. Dostupné z: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

[3] ŠIMEK, Richard. *Sociotechnika (sociální inženýrství)* [online]. Brno, 2003 [cit. 2022-10-31]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.

[4] *What Is Social Engineering?* [online]. proofpoint [cit. 2022-10-31]. Dostupné z: https://www.proofpoint.com/us/threat-reference/social-engineering

[5] BURDA, Karel. *Elektronická kontrola vstupu.* VUT Brno.

[6] ČERMÁK, Miroslav. *Autentizace: řekni mi své heslo* [online]. 2009, 29.08.2011 [cit. 2022-10-31]. Dostupné z: https://www.cleverandsmart.cz/autentizace-neco-vi/

[7] GOODCHILD, Joan. *Social engineering techniques: 4 ways criminal outsiders get inside* [online]. 2010 [cit. 2022-10-31]. Dostupné z: https://www.csoonline.com/article/2125205/social-engineering-techniques–4-ways-criminal-outsiders-get-inside.html

[8] HEJDA, Daniel. *TECHNIKY SOCIÁLNÍHO INŽENÝRSTVÍ, NA ČEM JSOU ZALOŽENY A JAK JSOU VYUŽÍVÁNY PŘI INICIALIZAČNÍM VEKTORU.*

[9] *PRETEXTING LIKE A BOSS* [online]. TrustedSec: 2015 [cit. 2022-10-31]. Dostupné z: https://www.trustedsec.com/blog/pretexting-like-boss/

[10] *Caller ID Spoofing* [online]. 2022 [cit. 2022-10-31]. Dostupné z: https://www.fcc.gov/spoofing

[11] *What Is Pharming and How to Protect Yourself* [online]. [cit. 2022-10-31]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/pharming

[12] MIKULOVÁ, Petra a Barbora FUKAROVÁ. *Příběhy sociálního inženýrství [online].* [cit. 2022-10-31]. Dostupné z: https://security.muni.cz/socialni_inzenyrstvi

[13] *Social Engineering and Malicious Code* [online]. [cit. 2022-10-31]. Dostupné z: https://studyrocket.co.uk/revision/gcse-computer-science-aqa/written-assessment/social-engineering-and-malicious-code

[14] *Scareware* [online]. [cit. 2022-10-31]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/scareware

[15] *All about ransomware attacks* [online]. [cit. 2022-10-31]. Dostupné z: https://www.malwarebytes.com/ransomware

[16] https://images.techhive.com/images/article/2017/05/wannacry_ransom_screenshot-100722810-large.jpg

[17] WINER, Stuart. *'Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad* [online]. 2019 [cit. 2022-10-31]. Dostupné z: https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/

[18] ANTAL, Lukáš. *Red Teaming – Červená proti modré, aneb evoluce penetračních testů* [online]. 2019 [cit. 2022-11-20]. Dostupné z: https://hackinglab.cz/cs/blog/red-teaming-cervena-proti-modre-aneb-evoluce-penetracnich-testu/

[19] *WHAT IS THE CYBER KILL CHAIN? PROCESS MODEL* [online]. 2022 [cit. 2022-11-20]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/

[20] ¨*Intelligence Gathering* [online]. 2014 [cit. 2022-11-20]. Dostupné z: http://www.pentest-standard.org/index.php/Intelligence_GatheringIndividual

[21] Zákon č. 89/2012 Sb. (Zákon občanský zákoník)

[22] *Jednotlivé druhy kyberkriminality* [online]. [cit. 2022-11-19]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[23] Zákon č. 40/2009 Sb. (Zákon trestní zákoník)

[24] *What is Python? Executive Summary* [online]. [cit. 2022-12-11]. Dostupné z: https://www.python.org/doc/essays/blurb/

[25] *What is PyCharm? Features, Advantages Disadvantages* [online]. 2022 [cit. 2022-12-11]. Dostupné z: https://hackr.io/blog/what-is-pycharm

[26] *What Is SQLite?* [online]. 2022 [cit. 2022-12-11]. Dostupné z: https://www.sqlite.org/index.html