Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Monitorování datové sítě pomocí nástrojů Kali Linux

Bakalářská práce

Autor: Zuzana Vojíková
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Ing. Pavel Blažek, Ph.D.

Hradec Králové duben 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 23.4.2024 Zuzana Vojíková

Poděkování:

Děkuji vedoucímu bakalářské práce panu Ing. Pavlu Blažkovi, Ph.D. za metodické vedení práce a za cenné rady, trpělivost a podporu při tvorbě této práce.

Anotace

Tato práce obsahuje nejprve základní seznámení s oblastí kybernetické bezpečnosti, zahrnující analýzu bezpečnostních hrozeb, druhy útoků (např. Man in the middle nebo SQL injection), popis různých skupin útočníků (např. black hat nebo green hat) a klíčová východiska týkající se zabezpečení sítě. V rámci praktické části je podrobně popsán proces odposlechu datového provozu, s využitím nástrojů dostupných v operačním systému Kali Linux a malého počítače Raspberry Pi. Následuje demonstrace útoku na bezdrátovou síť na jednoduchém scénáři. Ten zahrnuje získání přístupu, přes MITM útok, až po narušení protokolu HTTPS. Etické hackování slouží jako edukační nástroj, který pomáhá uživatelům lépe pochopit hrozby kybernetického prostředí a efektivněji chránit své sítě. Výsledkem je ucelený přehled o aktuálních bezpečnostních výzvách a možnostech jejich prevence a detekce.

Annotation

Title: Data network monitoring using Kali Linux tools

This thesis first provides a basic introduction to the field of cybersecurity, including an analysis of security threats, types of attacks (e.g., man in the middle or SQL injection), a description of different groups of attackers (e.g., black hat or green hat), and key assumptions regarding network security. In the practical part, the process of eavesdropping on data traffic is described in detail, using the tools available in the Kali Linux operating system and a small Raspberry Pi computer. This is followed by a demonstration of an attack on a wireless network using a simple scenario. This involves gaining access, through a MITM attack, to a breach of the HTTPS protocol. Ethical hacking serves as an educational tool to help users better understand cyber threats and protect their networks more effectively. The result is a comprehensive overview of current security challenges and how to prevent and detect them.

Obsah

Seznam obrázků

1 Úvod

Kybernetická bezpečnost se stává stále důležitějším a diskutovanějším tématem v souvislosti s neustálým rozvojem informačních technologií a rozšiřováním digitálního prostoru. S nárůstem počtu zařízení připojených k internetu, díky oblasti Internetu věcí, a rostoucí závislostí společnosti na digitálních službách se lidstvo stává stále zranitelnější vůči kybernetickým hrozbám a útokům. Tato bakalářská práce prozkoumává problematiku kybernetické bezpečnosti s využitím sledování datového provozu a přispívá k lepšímu porozumění současných bezpečnostních hrozeb.

Práce se zaměřuje na problematiku monitorování datové sítě pomocí nástrojů, které jsou součástí distribuce Kali Linux. Během následujících kapitol se práce bude zabývat různými aspekty kybernetické bezpečnosti, jako jsou různé druhy útoků a hrozeb, typy útočníků, fyzické hrozby, útoky na aktivní prvky sítě a metody zabezpečení a monitorování síťových prvků. Dojde k analýze technologií a postupů používaných pro detekci, prevenci a reakci na kybernetické hrozby. Důkladné pochopení kybernetických hrozeb a adekvátní reakce na ně jsou zásadní pro ochranu citlivých dat, zachování integrity a spolehlivosti digitální infrastruktury v dnešním technologickém světě jak pro jednotlivce, tak pro organizace.

2 Cíl práce

Cílem této bakalářské práce je prozkoumat a demonstrovat techniky a postupy používané při etickém hackování, se zaměřením na hackování bezdrátových sítí a monitorování datové sítě pomocí nástrojů Kali Linux. Práce se zaměří na praktickou ukázku útoku, včetně získání přístupu do sítě, provádění ARP spoofingu a hackování zabezpečených spojení, jako je HTTPS.

Práce také představí nástroje a postupy používané při etickém hackování. Hlavním cílem je zvýšit povědomí o kybernetické bezpečnosti a poskytnout praktické znalosti, které mohou být využity k ochraně před kybernetickými útoky.

3 Metodika zpracování

Bakalářská práce bude obsahovat dvě hlavní části: teoretickou a praktickou.

Teoretická část:

Teoretická část bakalářské práce se zaměří na klíčové aspekty kybernetické bezpečnosti a bezpečnostní hrozby. Na základě literární rešerše budou definovány základní pojmy a analyzovány různé druhy útoků. Každý typ útoku bude popsán a budou ilustrovány příklady jeho dopadů.

Další část se bude věnovat typům útočníků, včetně analýzy jejich motivací a technik. Fyzická bezpečnost bude také zahrnuta, s důrazem na ochranu síťové infrastruktury.

Následně se prozkoumají útoky na aktivní prvky sítě a možnosti jejich zabezpečení. Monitoring datového provozu bude diskutován z pohledu útočníka a obránce.

Závěr teoretické části se zaměří na penetrační testování, představí různé přístupy, jako jsou black box, gray box, white box, fuzzing testy a etické hackování, a popíše jejich význam.

Tato část poskytne ucelený pohled na kybernetickou bezpečnost a bude základem pro praktickou část bakalářské práce.

Praktická část:

Praktická část práce bude zaměřena na hackování bezdrátové sítě a bude sestávat z několika kroků, které demonstrují různé techniky používané při etickém hackování.

Prvním krokem bude získání přístupu do bezdrátové sítě. Tento krok zahrnuje identifikaci a analýzu dostupných bezdrátových sítí, výběr cílové sítě, a následné prolomení bezpečnostních opatření pro získání přístupu.

Druhým krokem bude provedení útoku ARP spoofing. Tento krok zahrnuje manipulaci s ARP tabulkou v síti, což útočníkovi umožňuje vydávat se za jiné zařízení v síti. Bude ukázáno, jak tento útok provést, a jeho potenciální dopady na síťovou komunikaci.

Třetím krokem bude hacknutí HTTPS. Tento krok ukáže, jak lze zneužít bezpečnostní slabiny v šifrovaných spojeních, za účelem získání citlivých informací. Budou předvedeny techniky, které umožňují sledovat a zachytávat šifrovaný provoz.

Praktická část poskytne detailní náhled do procesů etického hackování a umožní lépe porozumět rizikům spojeným s kybernetickou bezpečností. Všechny kroky budou prováděny v kontrolovaném prostředí, s důrazem na bezpečnost a dodržování etických zásad.

4 Kybernetická bezpečnost

Kybernetická bezpečnost (angl.: cybersecurity) nemá jednu jedinou určenou definici, jak to bývá například u jiných pojmů. Tento pojem se dá totiž těžko vyjádřit jednou krátkou stručnou větou. Pro lepší pochopení tohoto pojmu je důležité, aby člověk prostudoval informace v daném kontextu. Přesto se v odborné literatuře objevuje velké množství různých definic, které se vztahují k tomuto pojmu a jsou vytvářeny s ohledem na konkrétní účel či potřeby.

1. "Kybernetická bezpečnost se z velké části skládá z obranných metod, které slouží k odhalení a zmaření potenciálních útočníků [1].“
2. "Kybernetická bezpečnost zahrnuje ochranu počítačových sítí a informací v nich obsažených před průnikem a před škodlivým poškozením nebo narušením [1], [2].“
3. "Kybernetická bezpečnost zahrnuje snížení rizika škodlivého útoku na software, počítače a sítě. Patří sem nástroje používané k odhalování průniků, zastavování virů, blokování škodlivého přístupu, vynucování autentizace, umožnění šifrované komunikace a mnoho dalších [3].“
4. "Kybernetická bezpečnost je soubor nástrojů, politik, bezpečnostních koncepcí, bezpečnostních záruk, směrnic, přístupů k řízení rizik, opatření, školení, osvědčených postupů a zajištění technologií, které lze použít k ochraně kybernetického prostředí a majetku organizace a uživatelů [3], [4]."
5. "Prevence poškození, ochrana a obnova počítačů, elektronických zařízení a jejich funkcí systémů elektronických komunikací, služeb elektronických komunikací, drátové komunikace a elektronické komunikace, včetně informací v nich obsažených, s cílem zajistit jejich dostupnost, integritu, autentizaci, důvěrnost a nepopiratelnost [5]."
6. "Umění zajistit existenci a kontinuitu informační společnosti národa, zaručit a chránit v kyberprostoru jeho informace, aktiva a kritickou infrastrukturu [6]."
7. "Činnost nebo proces, schopnost či stav, kdy jsou informační a komunikační systémy a informace v nich obsažené chráněny před poškozením, neoprávněným použitím nebo modifikací nebo zneužitím a/nebo jsou proti nim chráněny [7]."

Na kybernetickou bezpečnost se dá dívat z mnoha úhlů pohledů. Zapojuje se do ní mnoho oborů, které si lidé ani neuvědomují, že ke kybernetické bezpečnosti pomáhají. Taktéž se může pojem kybernetická bezpečnost rozdělit na jednotlivá slova a tyto slova rozebrat. Označení "**kybernetická**" se vyvinulo z termínu "kybernetika", který označoval "obor teorie řízení a komunikace, ať už u strojů, nebo u zvířat" [8]. Také je to předpona pro kyberprostor, což je globální doména v rámci informačního prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních systémů včetně internetu, telekomunikačních sítí, počítačových systémů a vestavěných procesorů a kontrolérů [5].

„**Bezpečnost**“ je opravdu široký pojem, který může znamenat a vyjadřovat mnohé. Záleží, v jakém kontextu je „bezpečnost“ použita.

U tohoto pojmu nás v tomto případě zajímá, kdo zabezpečuje, v jakých otázkách (hrozbách), pro koho (referenční objekt), proč a s jakými výsledky a za jakých podmínek (striktura) [9].

Věda o kybernetické bezpečnosti otevírá mnoho možností pro pokrok, protože se v podstatě týká soupeření. Lidé musí bránit stroje před útoky jiných lidí pomocí strojů. Proto je kromě tradičních oborů informatiky, elektrotechniky a matematiky důležité zahrnout i pohledy z jiných oblastí.

Kybernetická bezpečnost se v poslední době stala předmětem živých diskusí, zejména v souvislosti s rozvojem Internetu věcí (IoT), který přináší rapidní nárůst počtu zařízení připojených k internetu a jsou schopny sbírat a přenášet data automaticky bez nutnosti lidské interakce. Zahrnuje jakýkoli fyzický objekt, kterému lze přidělit IP adresu a který může přenášet data (např.: domácí spotřebiče, kamery, hodinky atd). Tato situace sice nabízí uživatelům mnoho výhod, ale zároveň přináší i množství hrozeb a rizik.

5 Bezpečnostní hrozby

Podle zdroje [10] hrozby představují záměrné akce směřující k získání výhody z porušení bezpečnosti systému a jeho negativnímu ovlivnění.

Bezpečnostní hrozby se neustále vyvíjejí a mohou zahrnovat různé formy malwaru (viz 5.1.1), phishingových útoků (viz 5.1.8) a útoků využívající zranitelností v softwaru

Ochrana před těmito hrozbami vyžaduje neustálou pozornost, aktualizaci bezpečnostních opatření a informovanost zaměstnanců o kybernetickém nebezpečí. O

ochraně před nimi zajišťuje právě oblast kybernetické bezpečnosti, která je popsána v kapitole 4.

Oproti tomu zranitelnosti, jakožto chyby v systému nebo jeho návrhu, umožňují útočníkovi spouštět škodlivý kód, neoprávněně přistupovat k datům a/nebo realizovat různé útoky typu jako například denial-of-service (viz. kapitola 5.1.2).

Nadměrné využívání online obchodu, bankovnictví, reklamy a dalších služeb vede k nárůstu kybernetických aktivit zločinců. Tento růst je přímým důsledkem častého využívání webových aplikací v různých aspektech života. Tyto aplikace často obsahují chyby ve struktuře, které počítačoví zločinci využívají k nelegálnímu přístupu k systémům.

5.1 Útoky a hrozby

Příspěvky [11] [12] charakterizují pojmy útok a hrozba následovně.

Kybernetická **hrozba** představuje stav nebo jakékoli okolnosti a události, které mohou mít potenciálně negativní dopad na fungování systému. Může to také označovat schopnost úspěšného zneužití existujících zranitelností systému zdrojem ohrožení (resp. útočníkem). Za hrozby lze považovat například riziko ztráty nebo úniku dat, kompromitace, případně zneužití, systémových prostředků, což může vést až k finanční újmě a ztrátě důvěryhodnosti.

Oproti tomu, **útok** označuje jakoukoli škodlivou aktivitu nebo činnost, jejíž cílem je poškodit nebo narušit fungování systému, například v podobě krádeže, narušení, znehodnocení či zničení zdrojů systému a dat. Útočníci při něm využívají velkou škálu různých technik a nástrojů, které jim pomáhají nejen se samotným provedením útoku, ale i s jeho přípravou (mapování sítě a identifikace zranitelností).

Charakteristika vybraných hrozeb a útoků ilustruje rozmanitost strategií a technik, které mohou být použity k napadení sítě nebo systému. Následující podkapitoly se pak detailně zaměřují na specifické typy útoků, poskytující podrobnější analýzu jejich mechanismů a dopadů.

5.1.1 Malware

Malware je podle [13], [14] zkratka pro "malicious software" (škodlivý software), je obecný termín, který označuje škodlivý kód, který má za cíl infikovat počítače, mobilní zařízení nebo sítě. Malware může být ve formě virů, trojských koní, spyware, ransomware a dalších škodlivých programů.

Malware se šíří tím, že napadá a kopíruje sám sebe do dalších souborů nebo systémů. **Trojský kůň** je program, který se maskuje jako legitimní software, ale ve skutečnosti obsahuje skryté škodlivé funkce. **Spyware** je software navržený k sledování uživatele, sběru informací o jeho aktivitách a přenosu těchto dat bez jeho vědomí. **Ransomware** je malware, který blokuje nebo šifruje data na infikovaném zařízení a požaduje výkupné za jejich obnovení.

Malware může být šířen prostřednictvím e-mailových příloh, nebezpečných odkazů, infikovaných webových stránek, sdílených sítí a dalších kanálů. Jeho cílem je získat neoprávněný přístup k datům, odcizit citlivé informace, vydírat, poškodit systém nebo provádět jiné škodlivé aktivity.

Ochrana proti malware zahrnuje používání antivirového softwaru, aktualizace operačního systému a aplikací, opatrnost při otevírání neznámých e-mailů a stahování souborů, a pravidelné zálohování dat. Také je důležité být obezřetný při procházení internetu a vyhnout se podezřelým stránkám a odkazům.

5.1.2 Denial of service (DoS)

Zdroje [10], [15] popisují útok tak, že je založen na odepření nebo omezení přístupu k určitému zařízení, síťovému prostředku nebo službě. Tento druh útoku využívá situací, kdy jsou narušeny normální operace sítě, což může způsobit selhání či výpadek spojení. Útočníci vytvářejí situace, které přetěžují síťové prvky nebo spotřebovávají veškerou dostupnou kapacitu, čímž brání uživatelům v používání těchto zařízení. Jeden z nejprimitivnějších příkladů DoS útoku je nekonečné opakování příkazu „ping“ na cílový server (tzv. Ping of Death). Tímto způsobem útočník neustále bombarduje server žádostmi o odpověď, čímž zahltí jeho síťovou kapacitu a způsobí, že bude nedostupný pro uživatele. Důvodem, proč jsou tyto útoky tak úspěšné, je skutečnost, že mnoho odvětví využívá podobné technologie, což útočníci zneužívají k útokům na síťovou infrastrukturu. Tímto způsobem se útočníci snaží vyčerpat prostředky zařízení, zejména v prostředí IoT (viz kapitola 4), kde jsou paměťové a výpočetní kapacity často omezené.

Ochrana proti DoS útokům je klíčová pro zajištění dostupnosti sítí a služeb. Monitorování provozu, detekce anomálií, implementace bezpečnostních mechanismů, jako jsou firewally a další, jsou důležité prvky obrany proti těmto útokům. Navíc je důležité pravidelně aktualizovat a zabezpečovat zařízení IoT, aby se minimalizovala jejich zranitelnost vůči takovým útokům, a i jejich zneužití k těmto útokům.

5.1.3 Distributed Denial of Service (DDoS)

Podle [15], [16] jsou DDoS útoky rozšířenou formou DoS (viz předchozí kapitola) útoků, které se zaměřují na přetížení webových serverů nebo sítí. DDoS, ale oproti DOS útokům využívá větší počet stanic a dokáže generovat daleko větší provoz. Útočníci ho realizují prostřednictvím velkého množství infikovaných počítačů (tzv. botnet viz kapitola následující), které jsou ovládány pomocí malwaru (viz 5.1.1), aniž by to jejich majitelé věděli. Tato síť infikovaných počítačů je pak využita k odesílání obrovského množství provozu na cílovou adresu.

DDoS útoky jsou zvláště nebezpečné, protože využívají distribuovanou sílu útočníků a jsou obtížněji zastavitelné pomocí tradičních metod obrany. Cílem útoků je opět vyřadit služby nebo sítě, čímž znemožní přístup ostatním uživatelům. Tímto způsobem jsou organizace vystaveny výpadkům, finančním ztrátám a narušení reputace.

DDoS útoky představují závažnou hrozbu pro online podnikání, zákazníky, poskytovatele služeb a další. Obrana proti nim vyžaduje především schopnost detekovat a filtrovat nelegitimní provoz, implementovat technologie jako jsou speciální firewally nebo služby pro distribuované zpracování provozu a mít připravené plány pro obnovu služeb po útoku.

5.1.4 Botnet

Dle [17], [18] je botnet zkratka pro „robot network“ je síť počítačů, která je infikována škodlivým softwarem, který je ovládán jedinou útočící stranou nazývanou "bot-herder". Každý počítač v této síti, který je pod kontrolou bot-herdera, se nazývá bot. Z centrálního místa může útočící strana přikázat každému počítači v botnetu, aby současně provedl koordinovaný útok. Díky rozsahu botnetu, který může obsahovat miliony botů, je útočník schopen provádět rozsáhlé akce, které by byly samy o sobě s malwary (viz 5.1.1) nemožné. Protože botnety zůstávají pod kontrolou vzdáleného útočníka, infikované počítače mohou přijímat aktualizace a měnit své chování za běhu. Z tohoto důvodu jsou bot-herdeři často schopni nabídnout přístup k segmentům svého botnetu za účelem dosažení finančního zisku.

Běžné akce botnetu zahrnují: útoky DDoS (viz 5.1.3), cílená narušení, kdy se řídicí uzly pokoušejí získat neoprávněný přístup k citlivým informacím, infiltrovat systémy nebo poškozovat data. Tyto činnosti mohou mít vážné důsledky pro bezpečnost a stabilitu internetu a digitálních systémů.

5.1.5 Cross site scripting (XSS)

Je způsoben zneužitím zranitelnosti na webových stránkách. Útočník se snaží spustit kód psaný v JavaScriptu v prohlížeči klienta s cílem získat citlivá data od uživatele. XSS útoky jsou běžnou hrozbou, která postihuje moderní webové stránky. Útočník využívá chyby v zabezpečení stránky, aby vkládal škodlivý kód do webových formulářů, komentářů nebo odkazů. Když uživatel navštíví takovou zranitelnou stránku, spustí se škodlivý kód v jeho prohlížeči, což umožňuje útočníkovi získat přístup k citlivým datům, jako jsou přihlašovací údaje, osobní informace nebo dokonce provést neoprávněné akce v rámci webového prostředí [10].

Ochrana proti XSS útokům zahrnuje správnou validaci a ošetření uživatelského vstupu, filtrování vstupních dat a striktní používání bezpečných metod pro vkládání obsahu na webové stránky. Bezpečnostní audity a pravidelné aktualizace softwaru jsou také důležité pro minimalizaci rizika XSS útoků. Je nezbytné, aby tvůrci webových stránek a aplikací byli obeznámeni s touto zranitelností a věnovali dostatečnou pozornost zabezpečení svých systémů, aby ochránili uživatele před ztrátou dat a dalšími negativními důsledky XSS útoků [15], [19].

5.1.6 Man in the Middle (MITM)

Ze zdrojů [20], [21] jsme se dozvěděli, že MITM útok je jedním z nejdiskutovanějších a nejvážnějších hrozeb v oblasti počítačové bezpečnosti. Tento typ útoku představuje závažné riziko pro uživatele i bezpečnostní odborníky, neboť umožňuje útočníkovi proniknout do komunikace mezi dvěma koncovými body (viz kapitola 6.3) a manipulovat s ní. Útočníci, kteří se zabývají MITM útoky se zaměřují na aktuální data, která proudí mezi těmito body, což může mít vážné důsledky pro integritu a důvěrnost těchto dat odposloucháváním či modifikací. V extrémních případech může útočník dokonce zachytit, upravit nebo zcela zablokovat komunikaci, což vede k ohrožení dostupnosti služeb.

Pro bezpečnostní experty je MITM útok jedním z největších výzev v oblasti počítačové bezpečnosti. Útok se zaměřuje na reálná data, která putují mezi koncovými body, a zneužívá slabiny v zabezpečení komunikace. V rámci útoku dochází k narušení důvěrnosti a integrity dat, což má negativní dopad na bezpečnost informačních systémů. Abychom lépe porozuměli tomuto fenoménu, je nezbytné provést rozsáhlou analýzu a kategorizaci MITM útoků. Tento proces zahrnuje důkladné studium literatury a zohlednění referenčního modelu OSI (Open Systems Interconnection).

Útočník, který provádí MITM útok, získává kontrolu nad komunikačním kanálem mezi koncovými body (viz kapitola 6.3). To mu umožňuje sledovat, získávat, a dokonce manipulovat s citlivými informacemi, které jsou přenášeny. Aby se organizace chránily před tímto typem útoku, je důležité používat zabezpečené protokoly, ověřovat certifikáty a využívat VPN pro zabezpečení komunikace. Bezpečnostní opatření by měla být součástí každodenních postupů a směrnic v oblasti počítačové bezpečnosti, a to jak pro jednotlivce, tak i pro organizace. Pouze tímto způsobem můžeme minimalizovat riziko útoků MITM a zajistit bezpečnost a integritu našich informací.

Existuje několik typů útoků MITM, z nichž každý se zaměřuje na jiný aspekt komunikace a využívá odlišné metody. Jedním z těchto typů je **útok na síťové spojení**, který se zaměřuje na komunikační linky mezi koncovými body v síti. Útočník se snaží vložit do komunikace mezi koncovými body a převzít kontrolu nad nimi, aby mohl sledovat a manipulovat s přenášenými daty. Příkladem tohoto typu útoku je **ARP spoofing**, kdy útočník posílá falešné ARP pakety do sítě, aby přesměroval komunikaci na svůj vlastní stroj a následně mohl provádět různé formy útoků.

Dalším typem je **útok na webovou komunikaci**, při kterém útočníci napadají komunikaci mezi uživatelem a webovými servery, aby získali citlivé informace, jako jsou přihlašovací údaje, nebo prováděli phishingové útoky (viz kapitola 5.1.8). Jeden z příkladů tohoto typu útoku je **SSL hijacking**, při kterém útočník dešifruje a získává data přenášená pomocí zranitelných šifrovacích protokolů, jako je SSL/TLS, a tím ohrožuje soukromí a integritu komunikace.

Dalším typem je **útok na kryptografické** spojení, kde útočníci napadají kryptografické spojení mezi koncovými body s cílem dešifrovat a upravovat přenášená data.

5.1.7 SQL injection (SQLi)

Zdroje [15], [22] uvádí, že útok SQLi se snaží zneužít nesprávně ošetřené uživatelské vstupy do formulářů ve webové aplikaci tak, že útočník do vstupního řetězce vkládá vlastní SQL kód, za účelem přístupu k informacím, které jsou obsaženy v SQL databázi webové aplikace. V případě úspěchu útočník získá přístup k dané databázi, což mu umožní manipulovat s jejím obsahem různými způsoby, včetně použití CRUD operací (CREATE, READ, UPDATE, DELETE). To představuje velké riziko, protože tato situace může způsobit nenapravitelné škody, zničit reputaci organizace, ztrátu dat nebo jejich zneužití osobami, které nemají oprávnění, což může ohrozit funkčnost a důvěrnost

systému. Důsledkem této kompromitace může být únik citlivých informací, jako jsou přihlašovací údaje a osobní informace, a jejich zneužití například pro krádež identity. Je důležité chránit aplikace před útoky SQL injection pomocí správného ošetření vstupních dat a parametrizovaných dotazů (dotazy vytvořeny anebo s využitím parametrů místo pevně zapsaných hodnot). Ošetřování vstupních dat zahrnuje validaci (kontrolu, zda zadaná data splňují určitá kritéria nebo formát), escapování speciálních znaků (neutralizace nebo zneškodnění znaků, které by mohly být interpretovány jako části programového kódu nebo dotazu na databázi) a používání připravených výroků nebo uložených procedur (soubory předem definovaných operací nebo dotazů uložené přímo v databázovém systému). Dále je důležité implementovat přístupová práva k databázi tak, aby uživatelé měli přístup pouze k potřebným datům a operacím. Pravidelné aktualizace softwaru a provádění bezpečnostních auditů jsou také klíčové pro minimalizaci rizika útoků SQL injection. Vědomí o této zranitelnosti a implementace odpovídajících bezpečnostních opatření jsou nezbytné pro ochranu systémů před útoky SQL injection a zachování integrity a důvěrnosti dat.

5.1.8 Phishing

Jedná se o nelegální aktivitu, která využívá sociálního inženýrství a technologií k získávání citlivých informací od uživatelů internetu. Útočníci využívají různé komunikační kanály, jako jsou e-maily, rychlé zprávy, vyskakovací okna nebo webové stránky, aby podvodně získali citlivá data od svých obětí. Cílem phishingu je získat přístupové údaje, finanční informace nebo jiná citlivá data, která mohou být následně zneužita. Je důležité být obezřetný vůči podezřelým komunikačním zprávám a chránit své citlivé informace před phishingovými útoky [15], [23].

5.1.9 Sociální inženýrství

Na základě [15], [24], [25] je sociální inženýrství (angl.: Social Engineering) typ útoku zaměřený na lidský faktor. Útočníci využívají psychologické manipulace a klamání lidí s cílem získat přístup k citlivým informacím nebo získat neoprávněný přístup do systémů.

Existuje mnoho forem sociálního inženýrství, včetně falešných telefonátů, e-mailů, nebo osobního kontaktu. Útočníci se často vydávají za důvěryhodné osoby nebo autority, jako jsou zaměstnanci společnosti, IT technici, nebo dokonce přátelé a rodinní příslušníci. Používají různé taktiky, jako je naléhavá prosba o pomoc, vydírání,

vytváření paniky, nebo vytváření falešných scénářů, aby přiměli oběť ke sdílení citlivých informací nebo provedení nežádoucích akcí.

Příklady sociálního inženýrství zahrnují phishingové e-maily, ve kterých se žádá o zadání přihlašovacích údajů na podvodných webových stránkách, telefonáty od falešných zaměstnanců banky, kteří žádají o potvrzení platebních informací, nebo osobní setkání, během nichž se útočník snaží získat přístupové kódy nebo fyzické přístupy.

Ochrana před sociálním inženýrstvím vyžaduje obezřetnost a povědomí o možných rizicích. Důležité je provádět školení zaměstnanců, aby byli obezřetní při sdílení citlivých informací, ověřovali totožnost osob, které žádají o informace, a nepodléhali manipulaci. Důvěryhodná bezpečnostní opatření, jako jsou silná hesla, dvoufaktorová autentizace a pravidelné aktualizace softwaru, jsou také důležitou součástí ochrany před sociálním inženýrstvím.

5.2 Útočníci

Když se řekne hacker, všichni si představí zloducha za počítačem, který se chce jen obohatit nebo jen ničit pro radost. Existují však i hodní hackeři, kteří pomáhají firmám chránit svá data.

Bezpečnostní hrozba je důvodem, proč organizace využívají expertní hackery, kteří pronikají do počítačových systémů, sítí, aplikací nebo jiných počítačových zdrojů jménem jejich vlastníků a s jejich oprávněním k odhalení potenciálních bezpečnostních slabin, které by mohly zneužít hackeři. V podstatě to, co určuje typ externích hackerů, kteří pronikají do počítačových systémů, je jejich motivace a porušování zákona. Za většinu hlavních hrozeb kybernetického prostoru je odpovědných několik aktéru včetně profesionálů a sofistikovaných jednotlivců ze scény kybernetické kriminality státem sponzorované skupiny, amatérští hackeři jako jsou teroristické pobočky, hacktivisté a script kiddies.

5.2.1 Black hat

Black hat hackeři jsou označováni také jako cyber-kriminalisté. Jsou to zločinci, kteří se se zlými úmysly vloupají do počítačových sítí. Zaměřují se na nelegální činnosti v oblasti počítačové bezpečnosti s cílem získat neoprávněný přístup k cizím počítačovým systémům, sítím nebo datům za účelem dosažení osobního prospěchu nebo poškození jiných osob či organizací. Jejich činnosti mohou zahrnovat uvolňování

malwaru (viz 5.1.1), jako jsou viry, trojské koně, ransomware nebo spyware, které mohou napadnout počítače a sítě, způsobit poškození dat, ukrást citlivé informace nebo dokonce zablokovat přístup k systému a požadovat výkupné. Dále se mohou snažit proniknout do systémů za účelem krádeže osobních údajů, jako jsou hesla, čísla kreditních karet a další citlivé informace, které mohou následně využít k podvodům nebo vydírání. Tyto činnosti představují závažnou hrozbu pro jednotlivce, firmy i celé ekonomiky a jsou často stíhány a postihovány právními orgány [26], [27].

5.2.2 White Hat

Podle [26], [27] jsou white hat hackeři odborníci a výzkumníci zranitelností, kteří se specializují na vyhledávání nedostatků v softwaru a systémech s cílem pomoci postiženým organizacím. Tito experti mohou působit jako součást interního bezpečnostního týmu nebo pracovat jako externí konzultanti třetí strany. Jejich hlavním úkolem je odhalovat a upozorňovat na bezpečnostní zranitelnosti, aby vlastníci systémů mohli tyto nedostatky opravit a posílit bezpečnost svých systémů.

Označují se jako etičtí hackeři, neboť dodržují právní předpisy a etické normy. I když mohou využívat podobné technické nástroje jako hackeři s nekalými úmysly, jejich motivací je posílení bezpečnosti a ochrany digitální infrastruktury. White Hat hackeři hrají klíčovou roli v prevenci kybernetických hrozeb tím, že identifikují a řeší slabiny v bezpečnostních systémech, což umožňuje organizacím minimalizovat rizika útoků a ochránit citlivá data a informace před zneužitím. Jejich práce je neocenitelná pro udržení bezpečnosti a integrity digitálního prostředí.

5.2.3 Gray hat

Dle [26], [27] jsou gray hat hackeři odborníci na počítačovou bezpečnost, kteří systematicky vyhledávají zranitelnosti v systémech bez svolení nebo vědomí jejich vlastníků. Pokud objeví problémy, informují majitele a občas požadují poplatek za jejich opravu. Jejich cílem je zvýšit celkovou bezpečnost systému, avšak jejich činnost často porušuje zákon, protože provádějí testy a penetrační testy (viz kap. 9) bez předchozího povolení. Když hacker najde zranitelnosti nebo systémové chyby, oznámí je majiteli a požádá o poplatek za jejich opravu. Pokud vlastník nespolupracuje, hacker může nově nalezenou hrozbu zveřejnit. Tento typ hackování je nezákonný, protože hacker nezískal před sledováním systému povolení vlastníka. Často hledá zranitelná

místa v systému bez svolení nebo vědomí vlastníka a požaduje poplatek za vyřešení problémů, přičemž čelí potenciálnímu stíhání od podniků.

Pokud gray hat objeví zranitelnost nebo chybu v softwaru, je důležité rychle reagovat. Neopravená zranitelnost může být zneužita jinými osobami. Spolupráce mezi gray hatem a majitelem systému je proto klíčová. Gray hat může dostat odměnu za svou práci a uznání svých schopností. Organizace také mohou mít prospěch ze spolupráce s gray hatem, protože rychlejší identifikace a oprava zranitelností přispívá ke zlepšení celkové bezpečnosti.

Nejlepší gray hati se také snaží vytvořit exploit, který využívá chyby v softwaru a umožňuje jim získat neoprávněný přístup. Spolupráce s majitelem systému je pro ně důležitá, protože chtějí zranitelnosti opravit pro soukromé využití nebo posílit svou pověst. Avšak někdy může vzniknout mezera mezi implementací nového opravného řešení a jeho skutečnou aplikací, což představuje další výzvu.

Dalším problémem je, že gray hat může mít motivaci hromadit zranitelnosti, aby mohl nalézt více chyb a přispět ke zlepšení celkové bezpečnosti. Ne vždy je ochotný oznámit je společnosti a hodlá je použít jako "vstupní bod" pro nalezení dalších chyb.

5.2.4 Ostatní skupiny hackerů

Green hat hackeři jsou typicky nováčci v oblasti hackování. Mají základní znalosti o počítačové bezpečnosti a snaží se získat více informací a zkušeností. Často se učí tím, že zkouší různé techniky hackování na neškodných cílech, jako jsou vlastní testovací prostředí nebo webové stránky s povolením [28].

Blue hat hackeři jsou jedinci, kteří nejsou součástí organizovaného hackovacího společenství, ale přesto se zapojují do hackovacích aktivit z různých důvodů. Mohou to být například amatérští hackeři, kteří se zapojují do hackování jako koníčku, nebo etičtí hackeři, kteří se zaměřují na testování bezpečnosti s dovolením a za účelem zlepšení [28].

Red hat hackeři jsou známí svými nelegálními a agresivními útoky na cíle, které jim mohou poskytnout finanční zisk, moc nebo prostě uspokojení jejich zájmů. Tito hackeři často používají své dovednosti k vydírání, krádeži identit, sabotáži nebo špionáži [28].

Script kiddies jsou skupinou jedinců, kteří mají jen minimální technické dovednosti, ale používají automatické nástroje a skripty vytvořené jinými hackery k provedení útoků. Jsou často považováni za nebezpečné, protože mohou způsobit

značné škody, aniž by sami rozuměli technickým podrobnostem útoku. Mnoho script kiddies se snaží o vzhled "cool" hackera, ale ve skutečnosti jim často chybí hlubší porozumění a respekt k etickým a právním aspektům hackování [29].

Hacktivisté jsou skupina hackerů, kteří používají své dovednosti k prosazování sociálních, politických nebo environmentálních cílů. Jejich činnost se často zaměřuje na zveřejňování citlivých informací, jako jsou dokumenty vládních agentur nebo korporací. Hacktivisté mohou být motivováni snahou zvýšit odpovědnost vlád a korporací, bojem za lidská práva nebo ochranu životního prostředí. Jejich činnost často vzbuzuje kontroverze, přičemž někteří je chválí za jejich odvahu a odhodlání bránit veřejný zájem, zatímco jiní je odsuzují za narušování zákonnosti a způsobování škodlivých dopadů na oběti jejich útoků [30].

5.3 Fyzické hrozby

Ze zdrojů [31], [32], [33] jsme se dozvěděli, že v dnešní době se fyzické hrozby neodmyslitelně pojí s rostoucím významem kybernetické bezpečnosti. S nárůstem propojení zařízení s internetem, včetně rozšíření internetu věcí (IoT), se fyzické systémy stávají součástí digitální infrastruktury, což znamená, že jsou integrovány do sítě elektronických zařízení, softwaru a datových komunikací. Tím vznikají nová rizika a potenciální nebezpečí se zvyšuje.

Kybernetické hrozby se stávají stále sofistikovanějšími a útoky na zařízení se stávají běžnějšími. Zločinci se snaží ukrást citlivá data nebo dokonce způsobit fyzické škody.

Tradiční opatření fyzického zabezpečení, jako je kontrola přístupu nebo dohled, jsou stále důležitější, ale již nestačí samy o sobě. Propojení kybernetické a fyzické bezpečnosti je nezbytné pro účinnou ochranu.

Kybernetická bezpečnost je již dávno nejen technologickým problémem, ale zahrnuje i lidi a procesy. Zabezpečení fyzických prostor, jako jsou vstupní body a pracovní prostory, je klíčové, aby se zabránilo fyzickým útokům, které mohou vést k poškození majetku nebo krádeži dat. Hloubková ochrana, která zahrnuje kombinaci fyzických a kybernetických opatření, je nezbytná pro účinnou ochranu.

Fyzické hrozby mohou zahrnovat širokou škálu situací. Jako například manipulace se zařízením, poškození nebo krádež zařízení, stejně jako manipulace s prostředím, které senzory monitorují. Hrozbu představuje i nežádoucí přítomnost neoprávněných osob v prostorách budov, případně přímo v částech budovy, kde jsou umístěny

prostředky kritické infrastruktury. Vyjma těchto příkladů, u kterých podniky mohou implementovat opatření snižující pravděpodobnost jejich výskytu, existují i hrozby, kde se musí zaměřit spíše na minimalizaci jejich dopadů. Patří sem tedy i přírodní katastrofy a vlivy, jejichž výskyt je zcela mimo kontrolu podniků, a navíc jsou velmi těžko předvídatelné.

Zavedení bezpečnostních opatření, jako jsou bezpečnostní vstupy, biometrické systémy a penetrační testy, spolu s kontrolou přístupu, je klíčové pro snížení rizika fyzických hrozeb a ochranu. Tyto opatření umožňují chránit své prostředí před neoprávněným vstupem a identifikovat potenciální slabiny, které by mohly být zneužity útočníky. Zabezpečení vstupů je důležité pro ochranu prostředí, zatímco penetrační testy pomáhají identifikovat a odstranit možné zranitelnosti. Kontrola přístupu dále posiluje ochranu proti fyzickým hrozbám tím, že omezuje přístup pouze na oprávněné osoby.

Je klíčové si uvědomit, že fyzická a kybernetická bezpečnost jsou vzájemně propojeny a ovlivňují se navzájem. Integrace obou aspektů do celkové strategie bezpečnosti umožňuje lépe chránit svá aktiva a data. Útočníci mohou využívat nedostatky ve fyzické bezpečnosti k proniknutí do kybernetických systémů. Proto je důležité, aby uživatelé chápaly tuto synergii a přijaly komplexní přístup k ochraně svých aktiv v obou oblastech.

6 Útoky na aktivní prvky sítě

Útoky na aktivní prvky sítě představují vážnou hrozbu pro stabilitu a bezpečnost celého síťového prostředí. Tyto aktivní prvky zahrnují routery, switche a další zařízení, která aktivně směrují a řídí datový provoz v síti. Útočníci mohou využít různé metody, jako jsou útoky typu Denial of Service (viz 5.1.2) nebo Distributed Denial of Service (viz 5.1.3), aby narušili nebo zcela vypnuli tyto prvky, a tak způsobili výpadky v síti a narušení služeb.

6.1 Aktivní prvky

Aktivní prvky sítě [34] jsou zařízení, která se jakkoliv aktivně podílejí na komunikaci v síti a vzájemně propojují všechny komponenty počítačové sítě uvnitř budovy či areálu. Zajišťují logiku posílání dat z jednoho místa do druhého co největší rychlostí a co nejefektivnějším způsobem. Aktivní chování může například být regenerace, zesílení, oprava nebo modifikace přenášeného signálu. Aktivní prvky sítě například

ovlivňují logickou topologii, rychlost a propustnost. Nejznámější aktivní prvky, se kterými se nejběžněji setkáváme jsou přepínač (switch) a směrovač (router). Přepínače pracují na druhé vrstvě ISO/OSI modelu. Řídí přeposílání informací z jednoho zařízení na jiná v počítačové síti. Směrovače pracují na třetí vrstvě ISO/OSI modelu a musí znát skutečnou topologii sítě. Oproti přepínačům využívají globální pohled na jednotlivé sítě. Patří sem ale také firewally, opakovače (repeater), rozbočovač (hub), most (bridge) [35], [36].

6.2 Pasivní prvky sítě

Pasivní prvky sítě jsou komponenty, které slouží k přenosu dat v síti, ale neúčastní se aktivně na síťové komunikaci. Tyto prvky pouze přenášejí data bez jakékoli další modifikace či zpracování. Mezi běžné pasivní prvky patří kabely, konektory a zásuvky. Jsou základními stavebními prvky sítě a zajišťují fyzické propojení mezi aktivními prvky a koncovými body sítě. Pasivní prvky fungují spíše mechanicky a zajišťují spolehlivý přenos dat bez aktivní účasti na síťovém provozu [35].

6.3 Koncový bod (endpoint)

Zařízení, které komunikuje prostřednictvím sítě, ke které je připojeno. Příklady takových zařízení mohou být: stolní počítače, notebooky, chytré telefony, tablety, servery, zařízení IoT. Právě koncové body jsou zranitelné vstupy pro kyberzločince – spouštění nebezpečných kódů, zašifrování aktiv. S tím, jak se pracovní síly organizací stávají mobilnějšími a uživatelé se připojují k interním zdrojům z koncových zařízení mimo provozovnu po celém světě, jsou koncové body stále náchylnější ke kybernetickým útokům [37], [38].

7 Zabezpečení prvků v síti

Právě na koncové body (viz předchozí kapitola) se velmi často zaměřují útoky hackerů. Zabezpečení zařízení (jak je popsáno na [38], [39]) je tedy chrání před útoky a neoprávněnou činností. Řešení zabezpečení koncových zařízení se vyvinula z tradičního antiviru a poskytují širokou škálu obranných prostředků k zastavení známého i neznámého malwaru (viz 5.1.1) a dalších. Jelikož je napadení velmi časté, organizace je často schopna izolovat napadené koncová zařízení a zabránit tak šíření útoků na více endpointů. S rostoucím počtem vzdálených a mobilních pracovníků roste počet vystavených koncových bodů, čímž se zvyšuje zóna bezpečnosti z uzavřeného

firemního prostředí na koncové body rozptýlené po celém světě. Organizace musí zajistit, aby všechny zařízení, která ukládají firemní data nebo k nim přistupují, včetně zařízení vlastněných zaměstnanci, byly chráněny proti kybernetickým útokům.

Stále častěji se ochrana koncových bodů stává součástí řešení rozšířené detekce a reakce (XDR – Extended detection and response), která zahrnují zdroje dat a zajišťují prevenci, detekci a reakci na hrozby v rámci celého podniku. Nejsilnější a nejkomplexnější bezpečnostní řešení pro koncová zařízení (často zařazovaná do kategorie XDR řešení) dokáží centrálně shromažďovat a propojovat všechna tato data a zároveň provádět místní analýzy jednotlivých koncových zařízení [38], [39].

Doposud se organizace spoléhaly zejména na antivirové programy jako prostředek k zajištění bezpečnosti koncových zařízení. Avšak v dnešní době již tradiční antivirové programy nedokážou efektivně chránit proti sofistikovaným hrozbám. Pokročilé bezpečnostní řešení pro koncové body by ideálně mělo být schopno chránit před známými i neznámými viry a zneužitím zranitelností, využívat automatizaci k odlehčení práce bezpečnostního týmu a poskytovat ochranu a podporu uživatelům bez negativního dopadu na výkon systému [38], [39].

Moderní bezpečnostní řešení pro koncové body se zaměřují méně na identifikaci konkrétních virů a více na detekci podezřelého chování. Tyto řešení kombinují různé schopnosti, jako je ochrana proti virům, ochrana před využitím zranitelností, detekce a reakce na incidenty v koncových zařízeních (EDR – Endpoint detection and response) a analytika a kontrola zařízení. Takováto řešení ve formě softwarových produktů se instalují na koncová zařízení a zabezpečují je proti kybernetickým útokům. Strategie zabezpečení koncových bodů v podnikovém prostředí spojují platformy pro ochranu koncových bodů (EPP) a EDR řešení s cloudovými a síťovými nástroji, například analýzou síťového provozu (NTA), aby poskytly přehled o stále větším počtu zařízení připojených k síti, která nejsou spravována (což znamená, že nemají nebo nemohou mít nainstalovaný software pro ochranu koncových bodů), jako je například mnoho zařízení Internetu věcí [37].

8 Monitoring datového provozu

V souladu se zdrojem [40] je sledování datového provozu nezbytnou součástí bezpečnostní strategie, jak z pohledu útočníka, tak i obránce. Zajišťuje sledování a analýzu dat v síti. Umožňuje identifikovat neobvyklé aktivity a anomálie v síti. Tato aktivita může být prováděna jak útočníky, kteří se snaží proniknout do systému nebo

způsobit škodu, tak i obránci, kteří monitorují a chrání síť před neoprávněným přístupem a útoky.

Nové sítě s mnoha uzly, jako je například Internet věcí, potřebují pravidelný dohled, aby zůstaly efektivní a spolehliví. Správci sítí se zabývají různými aspekty, jako je zajištění bezpečnosti, zlepšení kvality služeb nebo optimalizace využití zdrojů. K dosažení těchto cílů využívají různé techniky.

Jedním z klíčových trendů v oblasti sledování datového provozu je využití umělé inteligence a strojového učení pro detekci hrozeb. Tyto technologie umožňují automatizovanou analýzu velkého objemu dat, což zvyšuje schopnost identifikovat anomálie a potenciální bezpečnostní hrozby v reálném čase. Díky tomu mohou být obránci schopni rychleji reagovat na hrozby a minimalizovat potenciální škody. Dalšími inovativními přístupy jsou analýza vzorů chování uživatelů a zařízení, což pomáhá odhalit neobvyklé aktivity a upozornit na možné útoky. Tato kombinace technologií posiluje schopnost obránců chránit sítě a zajistit jejich stabilitu a bezpečnost. Útočníci také využívají umělou inteligenci a strojové učení ke zlepšení svých útoků. Například mohou používat tyto technologie k automatizaci shromažďování dat, hledání zranitelností nebo provádění sociálního inženýrství. Tím se zvyšuje schopnost útočníků provádět sofistikované a adaptivní útoky. Tyto metody jim umožňují obcházet tradiční bezpečnostní mechanismy a rychleji identifikovat slabá místa v síti.

8.1 Pohled útočníka

Dle [40] útočníci využívají sledování datového provozu k různým cílům. Jedním z hlavních úkolů je špehování komunikace, kdy sledují přenos dat mezi jednotlivými uzly sítě. Tímto způsobem mohou odhalit citlivé informace nebo získat přístup k důležitým datům. Dalším důvodem pro sledování provozu je vyhledávání slabých míst v síťové infrastruktuře. Útočníci sledují komunikaci, aby identifikovali potenciální zranitelnosti a slabiny, které by mohly být zneužity k útokům. Monitorováním provozu mohou zjistit, kde se nacházejí slabá místa v systémech nebo aplikacích, která mohou být následně využita k infiltraci nebo sabotáži.

Dále útočníci provádějí analýzu obranných mechanismů, jako jsou systémy detekce (IDS) a prevence (IPS) neoprávněného přístupu. **IDS** (Intrusion Detection System) je systém, který monitoruje síťový provoz a detekuje neobvyklé nebo podezřelé aktivity, které by mohly naznačovat načasované útoky nebo neoprávněný přístup. Na druhou

stranu, **IPS** (Intrusion Prevention System) je systém, který nejen detekuje nebezpečné aktivity, ale také aktivně zasahuje a blokuje podezřelé provozní vzory, aby zabránil útokům v reálném čase. Útočníci provádějí analýzu reakcí těchto systémů na síťový provoz, aby lépe porozuměli tomu, jak jsou sítě chráněny. Tím mohou identifikovat slabiny v obranných mechanismech a přizpůsobit své útoky tak, aby se jim úspěšně vyhnuli. Analýza obranných mechanismů jim umožňuje lépe plánovat a provádět útoky, které mají vyšší šanci na úspěch.

8.2 Pohled obránce

Pro správce sítě je zásadní využití nástrojů, které umožňují filtrování, třídění a blokování komunikace, aby byla zajištěna bezpečnost a integrita sítě. Jedním z klíčových prvků je detekce anomálií, kterou zajišťuje IDS (Intrusion Detection System). Tento systém monitoruje provoz v síti a identifikuje jakékoli podezřelé vzory nebo chování, které by mohly naznačovat možný útok. Dalším důležitým aspektem je prevence útoků, kterou zajišťuje IPS (Intrusion Prevention System). IPS aktivně reaguje na identifikované hrozby a brání síťové infrastruktuře před neoprávněným přístupem nebo škodlivým provozem, což výrazně zvyšuje bezpečnost sítě. Analytická data z monitorování datového provozu poskytují obráncům cenné informace pro analýzu bezpečnostních incidentů a optimalizaci obranných strategií. Díky těmto informacím mohou obránci lépe porozumět hrozbám a útokům, čímž posilují celkovou bezpečnost sítě a chrání důvěrnost a integritu dat [40].

K monitorování síťového provozu uvedenými systémy je nutné mít k dispozici datový tok, pokud možno ode všech komunikujících zařízení a aktivních prvků. Dohlídající systémy k tomu používají sondy, které jsou zapojené do různých segmentů tak, aby byl přehled kompletní. Jejich provoz je realizovaný na portech aktivních prvků, v režimu promiskuitního modu, kdy se veškerý datový provoz daného aktivního prvku kopíruje na takto nastavený port. Sondy jsou pak schopné jej zpracovat a odeslat do nadřízeného systému.

9 Penetrační testy zařízení služeb

Penetrační testy jsou nedílnou součástí dnešní digitální doby. Cokoliv, co má přístup k internetu nebo má alespoň bluetooth, může být napadeno. Proto je důležité technologie před uvedením na trh testovat. Bohužel čím chytřejší a sofistikovanější jsou testeři, tím záludnější jsou hackeři. Tento boj je neustálý. Penetrační testování

(angl.: penetration testing, zkráceně pentest) je testování a útočení na produkt z pohledu útočníka. Tester se snaží využít jakoukoliv zranitelnost systému, využít ji a proniknout do něj, popřípadě ho poškodit. Pokud tester najde takovouto chybu, nahlásí ji a chyba se opraví [41].

Existuje několik typů penetračního testování: Black box, Grey box a White box.

9.1 Black box

Black box testování představuje přístup k testování softwaru nebo systému, při kterém tester nemá předchozí znalost vnitřní struktury nebo implementace testovaného objektu. Podobně jako útočník nemá přístup k interním detailům cílového systému. Tento přístup simuluje situaci, kdy útočník zkoumá cílový systém, aniž by měl přístup k jeho interním mechanismům nebo zdrojovým kódům. Útočník může využívat veřejně dostupné informace, jako jsou dokumentace systému, webové stránky, sociální média nebo jiné veřejně přístupné zdroje, aby získal potřebné informace pro útok. Takovýto black box přístup umožňuje testerovi nebo útočníkovi zkoumat systém zvenčí, podobně jako by se snažil najít slabá místa či chyby bez interních znalostí nebo přístupu [41].

9.2 Gray box

Při Gray box testování má útočník oproti black box testování o něco větší povědomí o testovaném systému. Tento přístup je něco mezi black box (viz předchozí kapitola) a white box (viz kapitola následující) testováním, kde útočník nebo tester má omezené znalosti o vnitřní struktuře a implementaci systému. Na rozdíl od black box testování může útočník mít některé omezené informace o architektuře, rozhraních nebo komponentách systému, ale nemá přístup k samotnému zdrojovému kódu nebo detailním technickým specifikacím. To mu umožňuje provádět pokročilejší útoky než při čistém black box testování, protože má povědomí o některých aspektech systému, ale stále mu chybí kompletní přehled o jeho fungování. Gray box testování tedy poskytuje útočníkovi nějaký stupeň znalostí, které může využít k lepšímu zaměření útoku a hledání zranitelností [41].

9.3 White box

White box testing, známý také jako clear box testing nebo structural testing, je metoda testování softwaru, která umožňuje testování na základě znalosti vnitřního fungování

systému. V případě white box testingu má hacker neomezený přístup ke všem informacím o systému, včetně dokumentace, architektury a zdrojového kódu. Tato úroveň transparentnosti umožňuje testerům provádět detailní analýzu systému a identifikovat potenciální slabiny, které by jinak mohly zůstat skryty. Díky tomu je white box testing považován za nejúčinnější a nejpreciznější formu testování, jelikož umožňuje důkladné pokrytí všech částí softwarového systému a odhalení i velmi subtilních chyb a nedostatků. I když ostatní varianty testování, jako jsou black box testing nebo gray box (viz předchozí kapitoly) testing, jsou rovněž důležité, white box testing představuje ideální volbu pro dosažení maximální úrovně zabezpečení a kvality softwarového produktu [41].

9.4 Fuzzing testy

Dle [42] mohou být Fuzzing testy součástí penetračního testování s kombinací například už zmíněného Grey boxu. Při Fuzzing testingu jsou generovány různé vstupy do systému, aby se opět vyzkoušela bezpečnost a správnost systému proti náhodným i systematickým útokům a zároveň se zkontrolovala robustnost celého systému. Fuzzing testing se od penetračního testingu ovšem liší. Fuzzing testy nezahrnují tak široké spektrum metod a technik jako penetrační testy. Nejsou tedy totožné.

Testy, jako jsou penetrační testy a Fuzzing, jsou prováděny za účelem zjištění bezpečnostních chyb a navržení jejich oprav. Tyto testy provádějí buď zaměstnanci dané firmy, která vyvíjí software, nebo externí pracovníci najatí společností potřebující otestovat svůj software.

9.5 Etické hackování

V knize [43] se etické hackování podobně jako penetrační testing snaží najít v systému chybu a najít slabiny v zabezpečení, aby mohl být systém opraven a vylepšen. Díky němu můžeme udržovat digitální soukromí uživatelů, a dokonce můžeme předvídat potencionální kybernetické útoky a odvrátit jejich výskyt. Etické hackování provádějí lidé, kteří mají od firmy povoleno takovéto hackování provádět. Ať už to jsou lidé z firmy nebo externí pracovníci.

Etické hackování a penetrační testy mají společné to, že v obou případech se musejí dodržovat určitá pravidla, zásady a postupy a všechny jsou schváleny majitelem nebo vlastníkem softwaru. Po provedení testování se všechny zjištěné chyby a nedostatky musí nahlásit, a to co nejdříve. Hlavním rozdílem obou testování je jejich cíl, kdy

penetrační testování celkově ověřuje systémy a sítě v organizacích a etické hackování podává důvěrnou zprávu přímo vlastníkům systému. Dalším rozdílem je způsob a průběh provádění testingu. Penetrační testování má obvykle už svoje zavedené postupy, plán a metodiku, zatímco etické hackování je velmi volné, kdy testeři používají svou kreativitu a schopnosti.

Etický hacking může udržovat digitální soukromí uživatelů. Zároveň může organizace předvídat potenciální kybernetické útoky a odvrácení jejich výskytu.

10 Kali Linux na platformě Raspberry Pi

Kombinace Kali Linuxu a platformy Raspberry Pi představuje šikovný nástroj pro hacking a penetrační testování. Raspberry Pi je kompaktní a přenosné zařízení, které lze snadno skrýt nebo diskrétně umístit do cílové sítě. Kali Linux pak poskytuje širokou škálu nástrojů určených pro bezpečnostní testování a penetrační testování, což umožňuje uživatelům provádět různé typy útoků a testovat zranitelnosti sítí a systémů. Tato kombinace poskytuje uživatelům flexibilitu a mocné prostředky pro zkoumání a zlepšování bezpečnosti jejich síťových prostředí.

10.1 Raspberry Pi

Technické specifikace k desce Raspberry Pi převzaty z oficiálních stránek [44].

Raspberry Pi, jak je možno vidět na obrázku 1, je malý, výkonný, a hlavně levný počítač. Jeho cenová dostupnost je velkou výhodou, a i proto je tak populární. U ceny musíme zmínit ještě jeho výkon. Raspberry využívá pouhých 15 wattů a šetří tak energii, planetu i peníze. Dá se využít v domácnosti i v průmyslu. Může zastoupit místo inteligentního hubu, domácího počítače či chytrého reproduktoru. Raspberry Pi disponuje všemi nezbytnými funkcemi, které se u běžného počítače očekává. Disponuje bezdrátovým přístupem k internetu, HDMI porty pro připojení monitoru a USB porty pro připojení periférií. Poskytuje tedy dostatečný výpočetní výkon a paměť RAM pro uspokojení každodenních potřeb. Raspberry Pi se využívá celosvětově pro výuku. Například programování nebo celkově práci s počítačem. Je určený pro všechny věkové kategorie a ve všech prostředí. Raspberry Pi nabízí také mnoho doplňkových modulů. Jako například kamery, výpočetní moduly nebo přídavné desky.

Raspberry Pi 3 Model B+, který používám v praktické části je vylepšenou verzí populárního jednodeskového počítače Raspberry Pi. Tento model nabízí vylepšený výkon a funkce vhodné pro různé projekty, včetně hackingu a kybernetické

bezpečnosti. Je vybaven čtyřjádrovým procesorem ARM Cortex-A53 s frekvencí 1,4 GHz, což poskytuje dostatečný výkon pro běh náročnějších aplikací. Kromě toho má Raspberry Pi 3 Model B+ vestavěný bezdrátový modul Wi-Fi a Bluetooth, což umožňuje snadnější připojení k síti a dalším zařízením. Tento model je kompaktní, energeticky úsporný a cenově dostupný, což ho činí ideální volbou pro různé experimenty a projekty v oblasti počítačového hackování.

Raspberry Pi nabízí výpočetní řešení vhodné pro různorodou škálu aplikací, od mikropočítačů až po ARM založené počítače. Jeho nízká energetická náročnost poskytuje mimořádně efektivní platformu. Raspberry Pi je aktuální a pořád se vyvíjí. Vychází uživatelům vstříc a nabízí od designerských partnerů zabudování raspberry do produktu co si přejí.

Obrázek 1 - Vývojová platforma Raspberry Pi 3 B+
Zdroj: [43]

Otevřený software (open source) sehrává zásadní roli v systému Raspberry Pi. Operační systém pro Raspberry Pi je obvykle open source, což umožňuje jeho úpravu a sdílení. Toto platí i pro mnoho aplikací a nástrojů vytvořených pro Raspberry Pi, což podporuje spolupráci a inovace v komunitě. Raspberry Pi a open source společně umožňují tvorbu inovativních projektů a řešení s nízkými náklady.

Raspberry Pi nabízí platformu, kterou lze využít všude, od průmyslových scénářů po náročná vestavěná prostředí, a poskytují přesvědčivé řešení i pro vesmírné aplikace. Model Astro Pi a GASPACS.

Hardware Raspberry Pi je běžně dostupný mikrokontroler a počítače jsou spolehlivé a výkonné.

10.2 Kali Linux

Kali Linux je linuxová distribuce, založená na Debian GNU/Linux, která vyniká svou schopností poskytnout bezpečnostním profesionálům a IT administrátorům komplexní prostředí pro provádění pokročilých bezpečnostních operací. Jeho bohatá sada nástrojů a funkcí zahrnuje možnosti, jako penetrační testování, forenzní analýzu a bezpečnostní audit, což umožňuje efektivně identifikovat a řešit různé bezpečnostní hrozby a slabiny v síťových systémech. Díky své flexibilitě a širokému spektru funkcí se Kali Linux stal klíčovým nástrojem v boji proti kybernetickým hrozbám a posilování zabezpečení informačních systémů. Na druhou stranu je často využíván i útočníky [45].

11 Hackování bezdrátové sítě

Hackování bezdrátové sítě představuje vážnou hrozbu pro bezpečnost informačních systémů a soukromí uživatelů. Jedním z hlavních cílů útočníků je získání neoprávněného přístupu do sítě, což může mít škodlivé důsledky včetně úniku citlivých dat, sledování komunikace a možnosti provádění dalších útoků.

Prolomení hesla k bezdrátové síti je často prvním krokem útočníka k dosažení neoprávněného přístupu. Útoky hrubou silou, slovníkovými útoky nebo využití bezpečnostních nedostatků v šifrování Wi-Fi jsou běžnými metodami používanými k získání hesla. Po úspěšném prolomení hesla má útočník možnost volného přístupu do sítě a provádění dalších útoků. Například využitím techniky ARP spoofing, který se v následujících kapitolách prakticky vyzkouší. Tento typ útoku umožňuje útočníkovi manipulovat s ARP (Address Resolution Protocol) tabulkami v síťovém zařízení a vytvořit falešné mapování mezi IP adresami a MAC adresami zařízení v síti. Tím se umožní útočníkovi převzít kontrolu nad komunikací mezi dvěma zařízeními a provádět útok Man-in-the-Middle (viz 5.1.6), což mu dává možnost sledovat, upravovat nebo přerušovat komunikaci a může vést k úniku citlivých informací nebo dalším nežádoucím důsledkům.

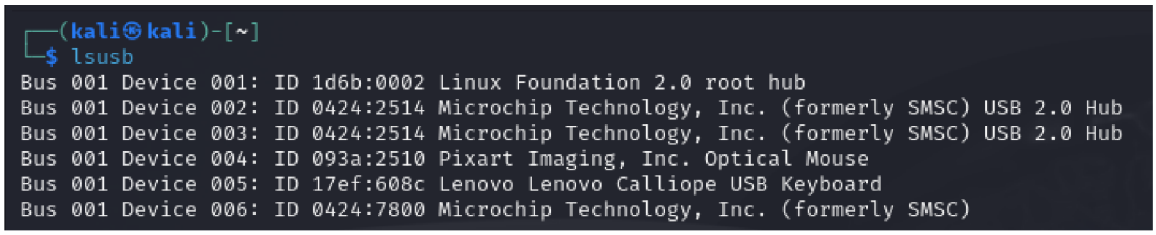
11.1 1. krok – Získání přístupu do sítě

Tato část práce se zaměřuje na proces odchytávání čtyřcestných handshakes a testování průniku do bezdrátové sítě. Odchytávání těchto handshakes (spojení) je klíčové pro penetraci bezdrátových sítí. Veškeré dále demonstrované postupy byly provedeny v laboratorním prostředí a pouze v lokální síti bez přístupu k internetu, vyjma poslední části, kde byl sledován https provoz. Zároveň se v průběhu praktické

části mohou lišit rozsahy IP adres a konkrétní použité IP adresy, jelikož jednotlivé kroky byly zpracovány s různými zařízeními a na různých místech.

Pro uvedení do kontextu práce se musí vysvětlit, co znamená pojem handshake. Handshake je proces navazování spojení mezi dvěma zařízeními v síti. Existují různé typy, včetně trojcestného a čtyřcestného. Čtyřcestný handshake je speciální typ handshake, který se často používá při navazování bezpečného spojení pomocí protokolu TCP/IP s využitím protokolu TLS/SSL (Transport Layer Security/Secure Sockets Layer), například při vytváření spojení pomocí protokolu TLS/SSL (HTTPS). TLS a jeho předchůdce SSL jsou protokoly zajišťující bezpečnou komunikaci mezi dvěma aplikacemi přes nezabezpečenou síť, jako je internet. Tyto protokoly poskytují šifrování a autentizaci datové komunikace, což znamená, že údaje přenášené mezi klientem a serverem jsou chráněny proti odposlechu a manipulaci třetími stranami. Trojcestný handshake se v praktické části práce nevyskytuje [46].

Pro úspěšné získání přístupu do sítě je nezbytné mít k dispozici síťovou kartu. Její přítomnost lze ověřit pomocí příkazu "lsusb", který zobrazuje seznam dostupných zařízení a jejich stav (viz obrázek 2). Je důležité, aby síťová karta byla viditelná a funkční pro úspěšné provedení operace odchytávání navázaných spojení.

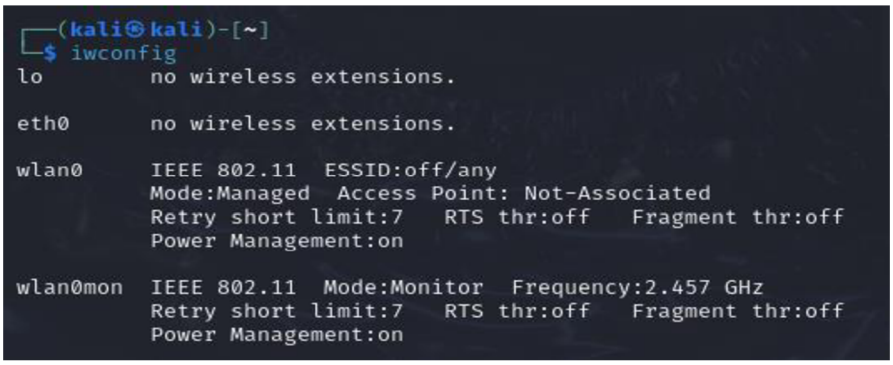


Obrázek 2 - Kontrola síťové karty
Zdroj: vlastní

Zjištění a ověření dostupnosti síťové karty je klíčovým krokem před započetím procesu zachytávání a testování průniku do bezdrátové sítě. Použití vhodného hardwaru je zásadní pro úspěšnou realizaci bezpečnostních analýz a zajištění bezpečnosti bezdrátových sítí.

Jedním z prvních kroků, které lze podniknout, je provedení příkazu "iwconfig" (viz obrázek 3) k ověření přítomnosti přístupového bodu (access point) a režimu monitoru síťové karty. Přístupový bod je základním prvkem bezdrátové sítě, který umožňuje připojení k bezdrátové síti. Monitorovací režim je speciální režim, který umožňuje sledování a zachytávání síťových paketů. Existují dva hlavní režimy pro síťovou kartu: režim správy (manage mode), který umožňuje běžné připojení k internetu, a režim monitoru (monitor mode), který umožňuje aktivní poslouchání a analýzu paketů v

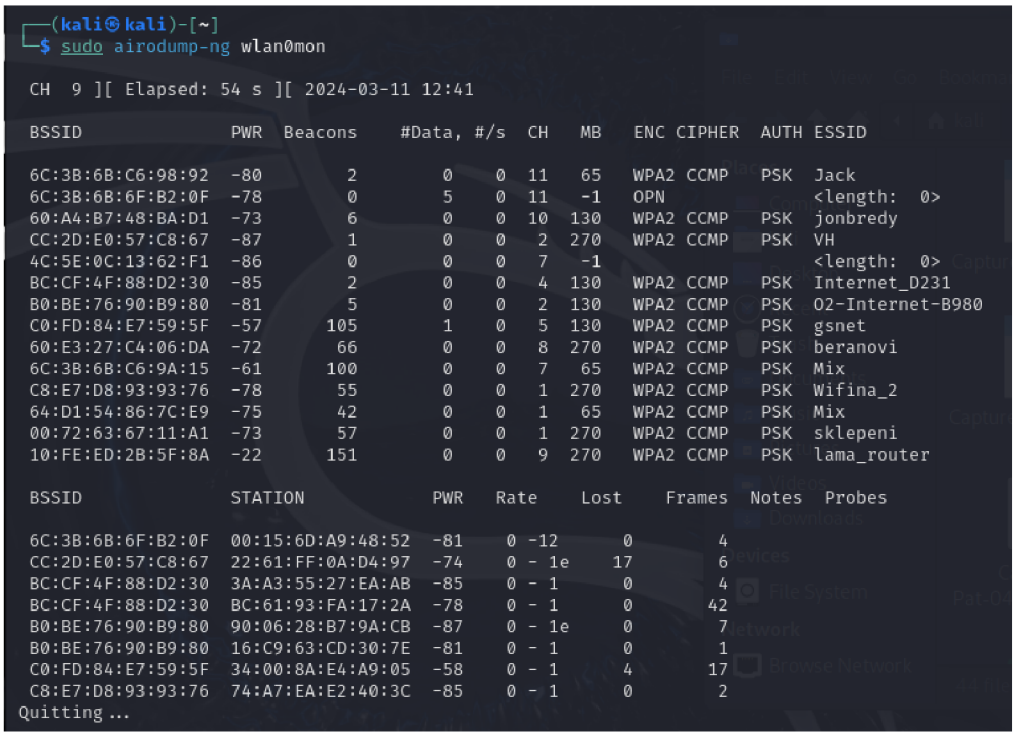
bezdrátové síti. Přepnutím karty do režimu monitoru se získá schopnost sledovat komunikaci v bezdrátové síti a provádět další analýzy nezbytné pro účely bezpečnostního testování.



Obrázek 3 - Režim síťové karty

Zdroj: vlastní

V současné fázi výzkumu je nutné přerušit proces zachytávání síťových paketů. K tomuto účelu se využije specializovaný nástroj nazvaný "airodump-ng". Po zadání příkazu "airodump-ng wlan0mon" se spustí výpis znázorňující právě probíhající komunikaci, zachycenou na rozhraní wlan0mon a bezdrátové sítě, spolu s přístupovými body.



Obrázek 4 – Výpis procesu zachytávání síťových packetů

Zdroj: vlastní

Během procesu zobrazování seznamu dostupných sítí prostřednictvím nástroje "airodump-ng" byly identifikovány různé sítě v okolí (viz obrázek 4). Tento krok slouží k výběru cílové sítě, která bude dále analyzována. Pro tento konkrétní případ byl

zvolen bezdrátový přístupový bod s názvem "lama_router". Tento router se stal hlavním cílem pro další fáze bezpečnostní analýzy a testování.

Po identifikaci cílové sítě, je vhodné přerušit běh nástroje "airodump-ng" a to stisknutím klávesové zkratky Ctrl+C. Tímto krokem se ukončí proces zachytávání informací o síťových paketech. Ukončením běhu nástroje se zajistí, že se nebude nadále zatěžovat síť zbytečným provozem a může se přejít k dalším činnostem či analýzám v bezpečnostním auditu.

Nyní bude pozornost věnována vybrané síti a provede se specifické nastavení opět pomocí nástroje "airodump-ng". Pro tento účel se zadá příkaz "airodump-ng -c2 -w Capture -d". V tomto příkazu se specifikuje, že se bude zachytávat na kanálu (channel) 9, protože se na něm nachází cílová síť. Parametr "-w Capture" určuje výstupní soubor, do kterého budou zaznamenány zachycené pakety. K tomuto souboru se přistoupí pod názvem "Capture". Dále, s ohledem na cílovou síť, se provede přiřazení přístupového bodu. Výsledný příkaz tedy bude "airodump-ng -c2 -w Capture -d 10:FE:ED:2B:5F:8A wlan0mon". Tímto nastavením se zajistí, že nástroj "airodump-ng" bude zaměřen pouze na cílovou síť, aniž by přeskakoval do jiných sítí nebo prováděl jiné nežádoucí operace.

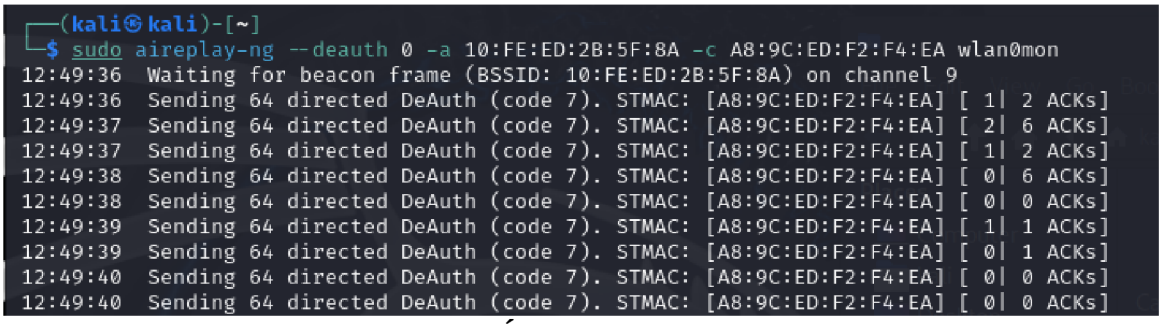
Obrázek 5 – Zaměření cílové sítě

Zdroj: vlastní

V předchozím výpisu příkazu (viz obr. 5) lze pozorovat, že v cílové síti je připojený klient. V rámci této simulace je jím mobilní telefon, který je aktivně připojen k dané bezdrátové síti.

Další nezbytný krok je zrušení ověření v síti. K tomu můžeme provést útok deautentizace, který nám umožní získat čtyřcestný handshake. Útok deautentizace je technika, která umožňuje vyřadit zařízení připojená k síti z jejího přístupového bodu. Tímto způsobem můžeme vyvolat připojení nových zařízení a získat navázané spojení, což je klíčový prvek pro některé bezpečnostní útoky a analýzy.

V terminálu se otevře nové okno a provede se příkaz "aireplay-ng --deauth 0 -a 10:FE:ED:2B:5F:8A -c A8:9C:ED:F2:F4:EA wlan0mon" (viz obrázek 6). Parametr "--deauth 0" znamená, že se provede nekonečný počet deautentizačních útoků. Argument "-a 10:FE:ED:2B:5F:8A " identifikuje cílový přístupový bod. Argument "-c A8:9C:ED:F2:F4:EA" identifikuje klienta, kterým je v tomto případě mobilní telefon. Nakonec "wlan0mon" označuje monitorovací rozhraní. Tímto příkaze se spustí útok deautentizace, který následně vyřadí klienta (mobilní telefon) připojeného k cílové síti a umožní získat spojení.



Obrázek 6 - Útok deautentizace a výpis
Zdroj: vlastní

Trvání útoku deautentizace může být ovlivněno několika faktory, jako je vzdálenost mezi útočníkem a přístupovým bodem, počet připojených klientů k síti a další okolnosti. Pokud je přístupový bod umístěn blízko a má omezený počet připojených klientů, útok může probíhat rychleji. Naopak, v případě vzdálenějšího umístění přístupového bodu a většího počtu klientů se může trvání útoku prodloužit.

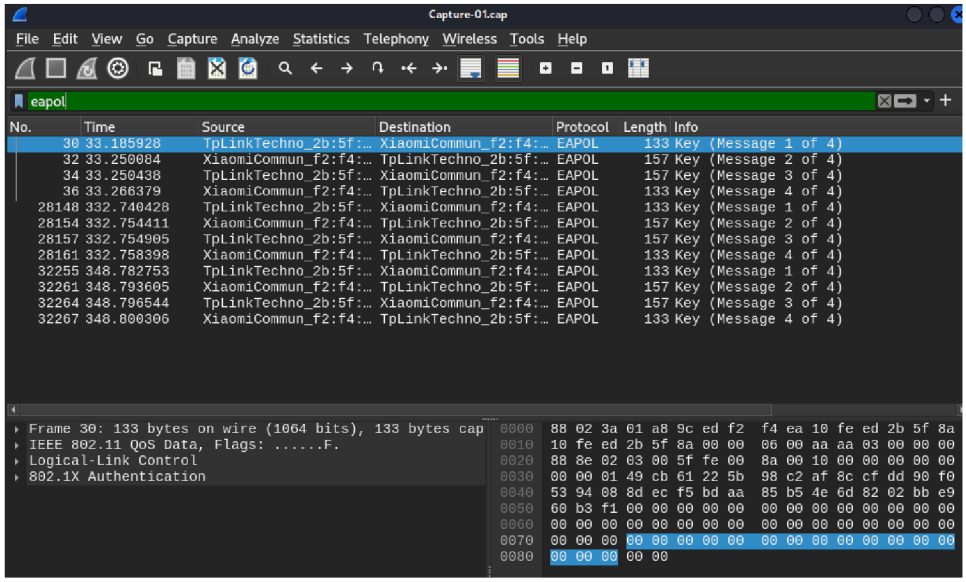
Pro urychlení procesu v této simulaci se provede ruční připojení a odpojení mobilního telefonu od sítě. Tímto způsobem se umožní rychlejší generování provozu a získání čtyřcestného handshake.

Ukončí se probíhající procesy. Přeruší se útok deautentizace, který byl spuštěn pomocí příkazu "aireplay-ng --deauth 0 -a 10:FE:ED:2B:5F:8A -c A8:9C:ED:F2:F4:EA wlan0mon", a zastaví se také předchozí proces zachytávání paketů s použitím příkazu "airodump-ng -c2 -w Capture -d 10:FE:ED:2B:5F:8A wlan0mon" na předchozí kartě.

Nyní se provede příkaz "ls" pro zobrazení seznamu souborů v aktuálním adresáři. Mezi několika zachycenými soubory bude jeden soubor s příponou ".cap", což je klíčový soubor. Tento ".cap" soubor obsahuje zachycený síťový provoz a poskytuje nezbytné informace pro provedení těchto útoků. Tento soubor je zásadní, protože díky němu lze následně provádět různé typy útoků, jako jsou slovníkové útoky, offline útoky hrubou silou a další. Bez tohoto souboru by bylo provádění útoků obtížné, proto je jeho získání klíčovým krokem.

V tuto chvíli se může otevřít získaný ".cap" soubor pomocí programu Wireshark a provést jeho analýza. Je nutné si dávat pozor, kde se soubor nachází a být v určené složce nebo napsat celou cestu souboru. I když by prolomení hesla mohlo fungovat i bez této analýzy, je užitečné si prohlédnout síťový provoz zachycený v souboru. Analyzování tohoto provozu může poskytnout další informace o síti, komunikaci mezi zařízeními a případných slabých bodech, které by mohly být využity k dalším útokům. Tento krok umožní lépe porozumět struktuře sítě a získat důležité poznatky pro zlepšení zabezpečení. Pomocí příkazu "sudo wireshark Capture-01.cap" se tedy spustí program Wireshark.

V rámci analýzy bezdrátové sítě pomocí programu Wireshark je možné provést důkladné zkoumání použitého protokolu, kterým je EAPOL (Extensible Authentication Protocol over LAN) (viz obrázek 7), jak je patrné z přehledu protokolů v horní části uživatelského rozhraní. Dále lze detailně prozkoumat čtyřcestný handshake. Z úrovně paketů je to nejvyšší úroveň detailů, kterou lze získat při analýze sítě.



Obrázek 7 - Protokol EAPOL
Zdroj: vlastní

Nyní bude použit příkaz „ls“ a znovu se zobrazí dokumenty. V dokumentech je zobrazen dokument s názvem „rockyou.txt“. To je textový soubor s nejčastějšími hesly. Popřípadě mohou být použity i jiné slovníky například common.txt, passwords.txt nebo top-passwords.txt. Je možné nechat zjistit, kolik slov má tento textový soubor pomocí příkazu "wc rockyou.txt". Vzhledem k počtu slov ve slovníku bude průběh rychlý.

Bude napsán příkaz "aircrack-ng Capture-01.cap -w rockyou.txt". Tento nástroj se použije k prolomení hesla. Po spuštění program vyzkouší všechna slova ve slovníku a heslo buď prolomí, nebo ne.

V ukázkové simulaci (viz obrázek 8) došlo k úspěšnému prolomení hesla. Heslo zní "12345678".

Obrázek 8 - Nalezení hesla
Zdroj: vlastní

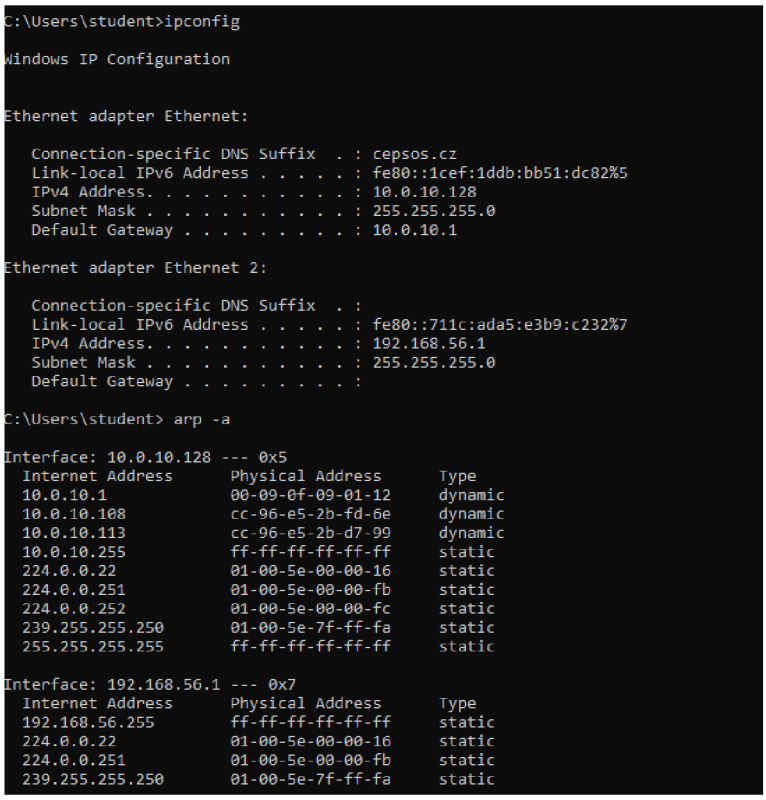
11.22. krok – ARP Spoofing

V druhém kroku v úvodní fázi ARP spoofingu (viz 5.1.6) je nezbytné získat klíčové informace o zařízeních zapojených do sítě. Tato analýza zahrnuje identifikaci IP adresy a MAC adresy konkrétního zařízení, které komunikuje v dané síti. Současně je nezbytné získat tyto identifikační údaje i pro zařízení, které bude využíváno k provedení ARP spoofingu, a rovněž pro centrální síťový prvek – router.

Pro získání těchto informací jsou použity nástroje a příkazy, které umožňují detailní průzkum sítě. Tyto příkazy poskytují nejen aktuální IP adresu, ale také MAC adresu, což je klíčový identifikátor zařízení na síti.

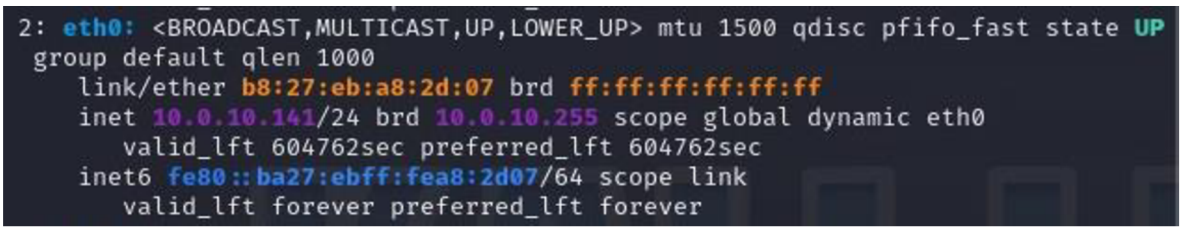
Provedené kroky zahrnují nejen identifikaci koncových zařízení, ale také sledování komunikačních toků v síti. Tímto způsobem se získává důležitý kontext pro další fázi ARP spoofingu. Získané informace slouží jako výchozí bod pro manipulaci s ARP tabulkami a vytvoření falešných ARP záznamů pro realizaci útoku. Celý proces lze považovat za kritický krok před samotným provedením ARP spoofingu, neboť přesná znalost topologie sítě je klíčová pro úspěch tohoto útočného scénáře.

Určení IP adres a MAC adres pro zařízení v síti lze provést několika způsoby. V případě pro PC s Windows 11 je možné získat IP adresu pomocí příkazu v powershellu, konkrétně použitím "ipconfig" (viz obrázek 9) a vyhledáním ve výsledné tabulce IPv4 Address v prvním odstavci Ethernet adapter Ethernet. Z tabulky, co nám tento příkaz vypsal je možné také vyčíst IP adresu routeru, a to ve stejném odstavci na řádku Default Gateway. Následně můžeme zjistit MAC adresu prostřednictvím příkazu "arp -a" a identifikovat ji v prvním řádku pod sloupcem Physical Address.



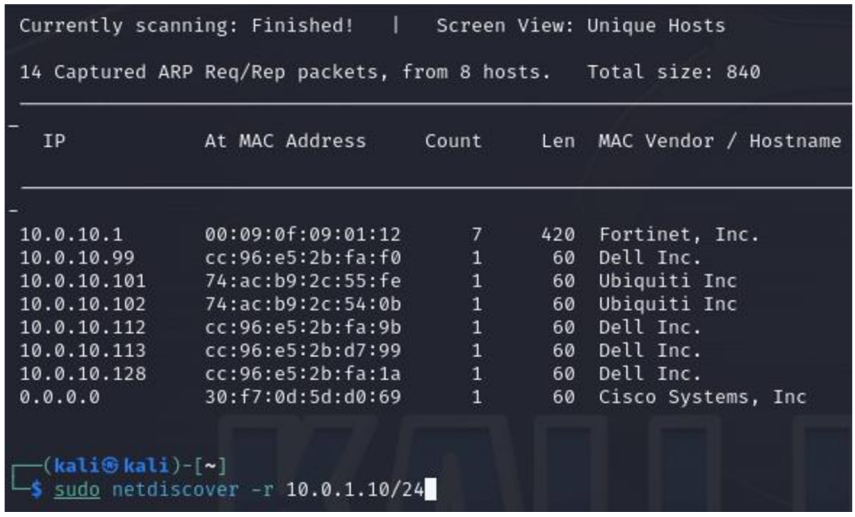
Obrázek 9 - Výstup příkazu ipconfig
Zdroj: vlastní

Pro Raspberry Pi s Kali Linuxem lze IP adresu zjistit v terminálu pomocí příkazu "ip add" (viz obrázek 10), kde se IP adresa nachází ve výsledné tabulce v odstavci eth0 za inet (Internet Protocol). MAC adresa se poté nachází v tabulce nad touto informací za link/ether.



Obrázek 10 - Výstup příkazu ip add
Zdroj: vlastní

Další z efektivních metod k dosažení identifikace IP a MAC adres zařízení v síti na platformě Raspberry Pi s operačním systémem Kali Linux je využití příkazu „sudo netdiscover -r <IP sítě s prefixem>“ (viz obrázek 11). Tento příkaz umožňuje skenování sítě a identifikaci aktivních zařízení včetně jejich přidělených IP a MAC adres. Získané výsledky poskytují cenný přehled o topologii sítě, přičemž první řádek výstupu obsahuje MAC adresu pro výchozí bránu (router). Tato informace je klíčová pro pochopení struktury sítě a stanovení centrálního síťového uzlu. V rámci výstupu je též možné identifikovat cílové zařízení, například s operačním systémem Windows 11. Předposlední řádek výsledků obsahuje IP a MAC adresu tohoto koncového zařízení. Tyto údaje představují důležitý vstupní bod pro následné fáze analýzy a potenciálního provedení ARP spoofingu. Celkově lze tuto metodu považovat za klíčový krok v identifikaci aktivních prvků v síti a přípravě na bezpečnostní analýzu.



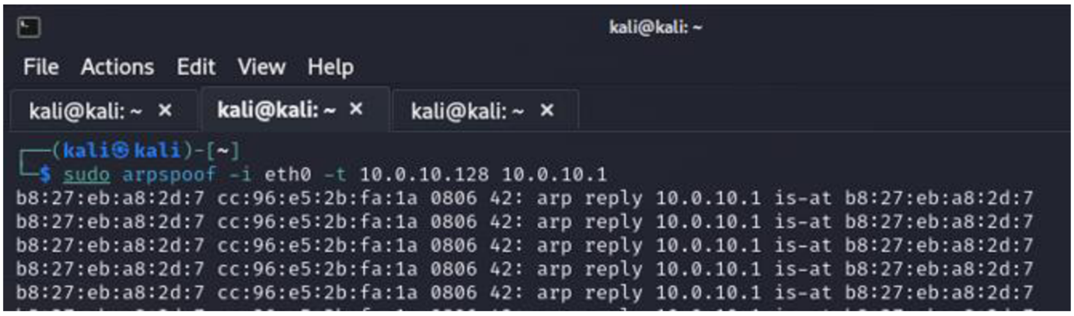
Obrázek 11 - Identifikace IP a MAC
Zdroj: vlastní

Pro spuštění Wiresharku v Kali Linux je nezbytné použít příkaz „sudo wireshark“. Tímto způsobem se může úspěšně provádět analýza síťového provozu a identifikovat potenciální bezpečnostní hrozby. Když se Wireshark otevře, úvodní obrazovka programu nabízí výběr síťových rozhraní. Po spuštění se aplikoval filtr "app" k

zobrazení pouze relevantních paketů spojených s aplikací. Tím se lépe porozumí provozu této aplikace a mohou se detailněji analyzovat přenášená data.

Poté se bude potřeba vrátit zpět do terminálu. Pokud je za cíl falšovat MAC adresu routeru, použije se v Kali příkaz "sudo arpspoof -i eth0 -t <IP win11> <IP routeru>" (viz obrázek 12). Tímto způsobem se provede tzv. "spoofing" MAC adresy routeru a odesílá se přesměrovaný provoz na cílové zařízení s Windows 11.

Když se vše nastavilo na aktivní, ovlivnila se ARP tabulka na zařízení s operačním systémem Windows 11.



Obrázek 12 – Spoofing MAC adresy routeru

Zdroj: vlastní

Pro ověření provedených změn se znovu zadalo do Powershellu na zařízení s Windows 11 příkaz „arp -a“. Tím se získal seznam ARP záznamů, které byly aktualizovány na základě úprav.

Na zařízení s Windows 11 byla provedena změna ARP záznamů tak, aby zařízení s Raspberry Pi a Kali Linuxem bylo identifikováno jako router. Tím bylo dosaženo toho, že provoz směřovaný na adresu routeru bude ve skutečnosti směrován na zařízení s Kali Linuxem.

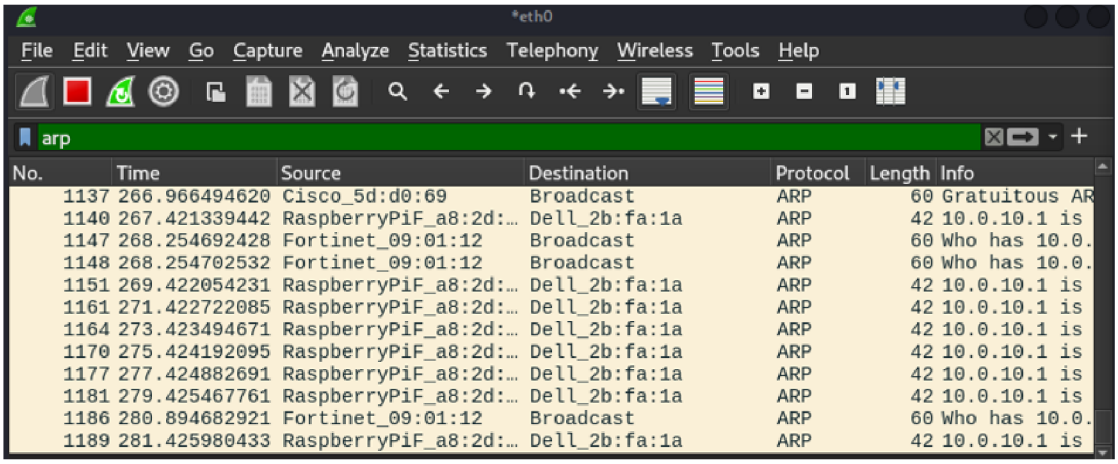
Pokud jde o MAC adresu, její záznamy byly změněny manipulací s ARP tabulkou tak, aby zařízení s Windows 11 vnímalo MAC adresu zařízení s Raspberry Pi jako adresu routeru. Tato manipulace může mít vliv na směrování síťového provozu a může vést k potenciálním bezpečnostním rizikům.

Nyní bylo routeru sděleno, že zařízení s Raspberry Pi a Kali Linuxem je ve skutečnosti zařízení s Windows 11. Tím bylo zajištěno, že směrování síťového provozu odpovídalo novým ARP záznamům a MAC adresa na routeru byla aktualizována tak, aby odpovídala MAC adrese zařízení s Windows 11.

Poté se otevřel terminál a zadal se znovu příkaz "sudo arpspoof -i eth0 -t <IP routeru> <IP win11>", který obrací IP adresy. Tím bylo umožněno zařízení Raspberry Pi s Kali Linuxem vydávat se za router a přesměrovávat síťový provoz z cílového zařízení na Raspberry Pi. Tím bylo dosaženo manipulace směrování provozu v síti.

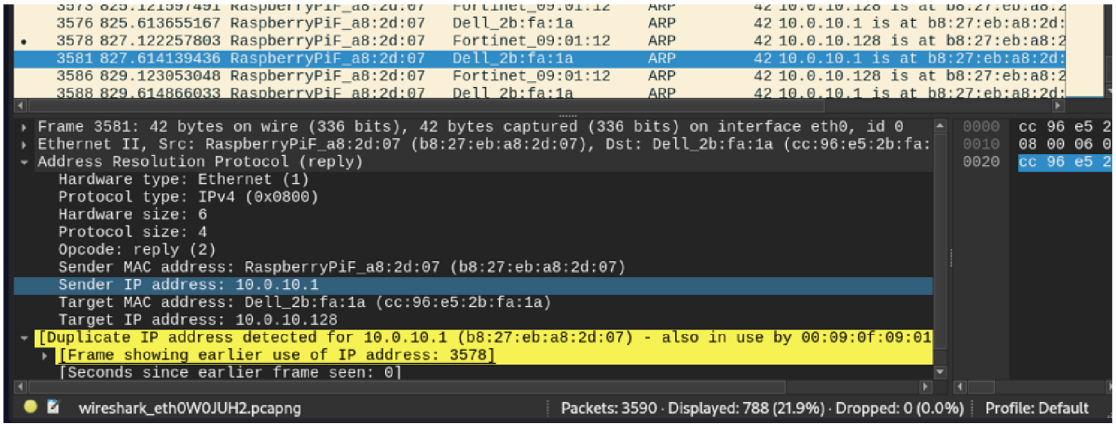
Tímto je útok typu "Man-in-the-Middle" dokončen.

Nyní je možné přejít do aplikace Wireshark a zastavit proces zachytávání. Poté můžou být prozkoumána zachycená data (viz obrázek 13). Při prohlížení tabulky paketů bude vybrán náhodný paket. Většina z nich logicky pochází z Raspberry Pi.



Obrázek 13 - Přehled packetů
Zdroj: vlastní

Dole pod tabulkou paketů můžeme nalézt detailnější informace o vybraném packetu (viz obrázek 14). Z jaké IP adresy byl odeslán a komu. Žlutě zvýrazněná informace například říká, že tento packet byl duplikován.



Obrázek 14 - Detailní informace
Zdroj: vlastní

11.33. krok hacknutí HTTPS

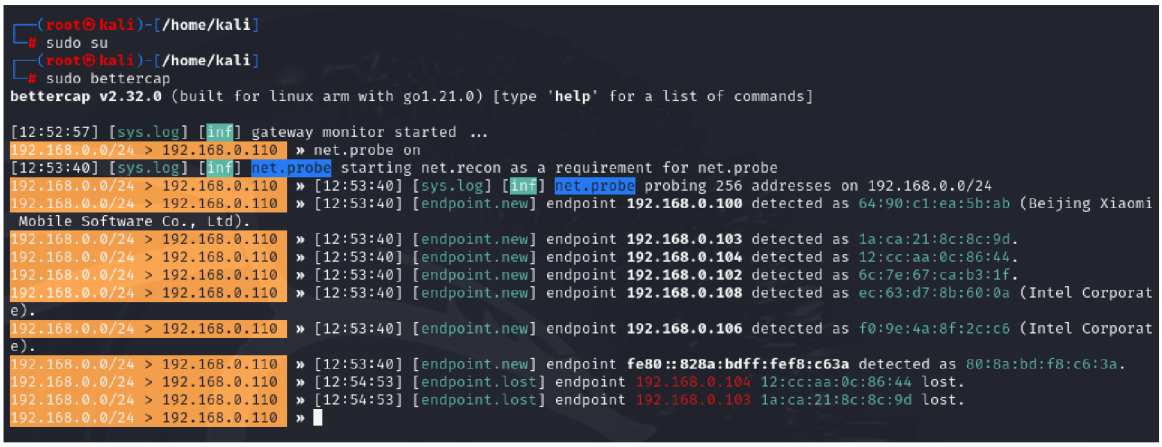
V tomto kroku praktické části se bude zkoumat nástroj **bettercap**, který je součástí nástrojů etického hackování a používá se k provádění útoků typu Man-in-the-Middle (viz 5.1.6), včetně útoku na SSL spojení, známého jako SSL hijacking. Představí se, jaká jsou rizika používání veřejných otevřených sítí. Bettercap může hacknout jakýkoliv počítač či jiné zařízení v síti, protože může vidět provoz nebo webové stránky, na které se uživatelé snaží přistupovat. Hacker, který tento nástroj používá se tedy umístí mezi

cíl a samotný router, takže bude moci odposlouchávat veškerou komunikaci, která probíhá mezi cílem a routerem. Bettercap je všestranný nástroj, který umožňuje hackování Wi-Fi, Bluetooth, nízkoenergetických bezdrátových zařízení, a dokonce i ethernetových připojení. Jeho flexibilita a rozmanitost ho činí neocenitelným pomocníkem pro zkoumání bezpečnosti sítě a identifikaci možných bezpečnostních nedostatků.

Nyní je cílem zařízení (notebook) se systémem Windows 10. Útočník používá zařízení Raspberry Pi s operační systém Kali Linux.

Nejprve se otevře okno terminálu v Kali a ověří se přihlášení jako superuživatel (příkaz „sudo su“). Následně bude zadán příkaz "sudo bettercap" (viz obrázek 15). Pokud není nainstalován, musí se nainstalovat (pomocí příkazu „apt install bettercap“). Tímto příkazem se do počítače načte Bettercap.

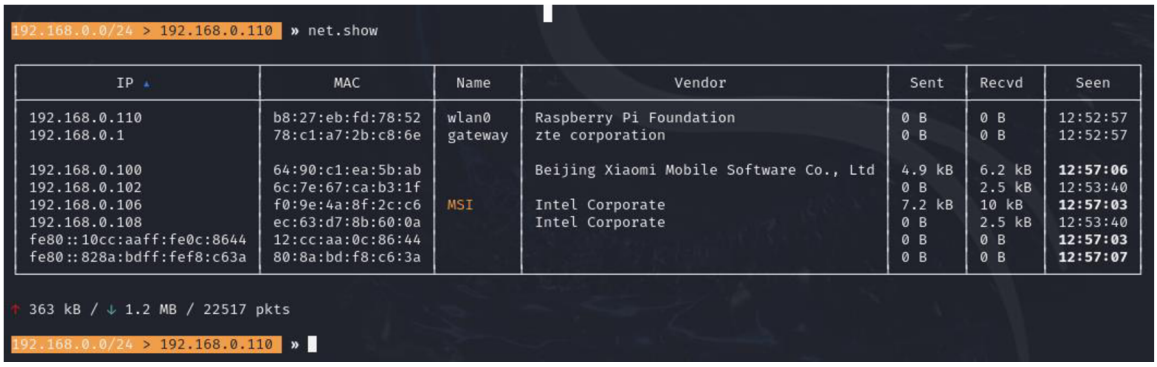
Pro zobrazení všech uživatelů, kteří jsou aktuálně připojení k síti, ke které je připojené i zařízení, ze kterého se bude útočit, respektive aby bylo možné vidět všechny zařízení v síti, bude potřeba zadat příkaz „net.probe on“ (viz obrázek 15).



Obrázek 15 - Načtení Bettercap
Zdroj: vlastní

Takže nyní budou vyhledány všechny počítače, které jsou v současné době k dispozici v naší síti a některá zařízení budou identifikována. Cílem je počítač s operačním systémem Windows 10 s IP adresou 192.168.0.108. Jelikož je praktická část realizována v laboratorním prostředí, ověření IP adresy cílového počítače lze provést zadáním příkazu „ipconfig“ na daném notebooku.

Všechna zařízení se mohou zobrazit graficky v tabulce po zadání příkazu „net.show“ (viz obrázek 16). V tabulce je obsažen i záznam o zařízení, které je cílem útoku a jehož IP adresa byla identifikována v předchozích krocích.

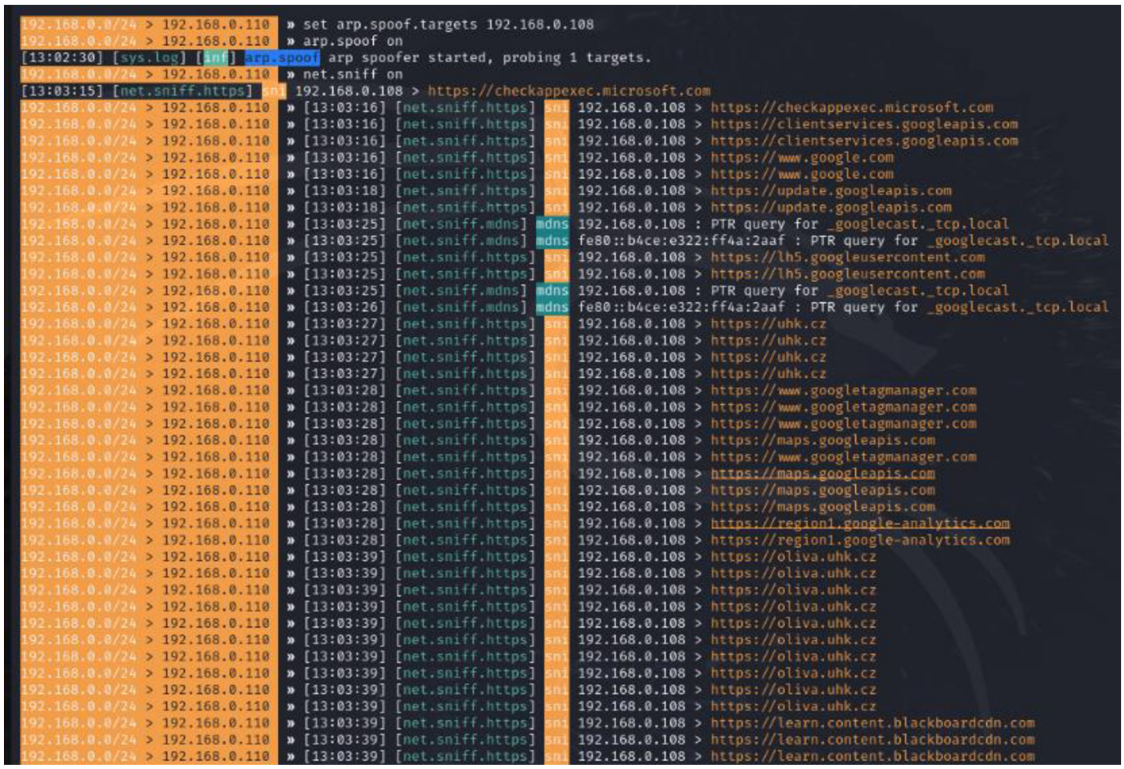


Obrázek 16 - Zobrazení zařízení v tabulce
Zdroj: vlastní

Po identifikaci cíle bude zahájen pokus o ARP útok. Je známo, že v rámci tohoto útoku bude umístění zasazeno mezi počítač s Windows 10 a routerem. Veškerá komunikace, která probíhá mezi těmito zařízeními bude možné v síti sledovat. Pro tento krok je potřebný příkaz „set arp.spoof.targets 192.168.0.108“. Tento příkaz tedy povoluje spoofing pro zařízení s touto IP adresou.

Na vybraném cíli bude povolen spoofing, což se provede zadáním příkazu „arp.spoof on“ (viz obrázek 17). Tím byl spuštěn spoofing cílového počítače. To, že byl spoofing odstartován lze ověřit níže pod příkazem.

Bude se sledovat veškerá aktivita na cílovém zařízení. Aktivita se opět vypíše pod příkazem po povolení sledování což je „net.sniff on“ (viz obrázek 17).



Obrázek 17 - ARP útok
Zdroj: vlastní

Pokud nyní uživatel na odposlouchávaném zařízení například otevře webový prohlížeč, v terminálu se vše zaznamená.

Nejnebezpečnějším aspektem této činnosti je, když je uživatel nebo cíl připojen k libovolné webové stránce HTTP, kde je komunikace prováděna v čistém textovém formátu. Komunikace může být zachycena a dokonce dešifrována, což umožní útočníkovi vidět uživatelské jméno a heslo.

12 Shrnutí výsledků

V praktické části bylo přistoupeno k provedení aktivního prověření zabezpečení sítě, které by mělo být, vedle pasivního monitoringu, pravidelnou prověrkou spravovaného systému a také prověrkou monitorovacího systému, který by měl být schopen na aktivně vedené fáze útoku reagovat. Provedený penetrační test byl proveden ve třech krocích na bezdrátovou část sítě.

První krok se zaměřil na získání přístupu do cílové sítě. Použitím nástrojů pro analýzu Wi-Fi signálu a zjištění zranitelností se podařilo identifikovat cílovou síť a následně získat přístup pomocí prolomení hesla. Tento proces ukázal, jak mohou útočníci zneužít slabiny v zabezpečení bezdrátových sítí, zejména pokud jsou používána slabá hesla nebo zastaralé šifrovací protokoly.

Druhý krok zahrnoval útok ARP Spoofing, kde se útočník snaží přesměrovat síťový provoz mezi cílovým zařízením a směrovačem. Tento typ útoku umožňuje útočníkovi sledovat a zachycovat komunikaci mezi těmito dvěma body. Praktická část ukázala, jakým způsobem lze provést tento útok a jaké informace mohou být touto metodou odhaleny.

Třetí krok se zaměřuje na hacknutí komunikace zabezpečené protokolem HTTPS. Ukázalo se, že i tato šifrovaná komunikace může být zranitelná, zejména při využití technik jako SSL hijacking. Tento krok demonstroval, jak útočníci mohou získat citlivé informace, jako jsou uživatelská jména a hesla, a jak důležité je používat nejnovější bezpečnostní opatření k ochraně dat.

Celkově výsledky praktické části zdůrazňují důležitost silného zabezpečení bezdrátových sítí a obezřetnosti při práci s citlivými informacemi v prostředí, které může být vystaveno potenciálním útokům. Tato analýza poskytuje užitečné poznatky pro zlepšení zabezpečení a ochranu proti útokům na bezdrátové sítě.

13 Závěry a doporučení

Závěry a doporučení v této práci vycházejí z podrobného zkoumání bezpečnostních aspektů datového provozu v sítích a z praktických ukázek různých typů útoků a obran. Byly zjištěny klíčové postupy a metody používané jak útočníky, tak obránci, což vedlo k řadě závěrů a doporučení.

Výsledky dosažené v praktické části naznačují, že kybernetické útoky na bezdrátové sítě představují vážnou hrozbu, zejména v prostředí s omezenými bezpečnostními opatřeními. Zjištěné slabiny v bezpečnostních protokolech a časté nedostatky v zabezpečení síťových prvků poukazují na potřebu zvýšené ostražitosti a proaktivních opatření. Tato zjištění jsou v souladu s literaturou, která zdůrazňuje, že zranitelnosti v síťových systémech často pramení z nedostatečného zabezpečení nebo zastaralých bezpečnostních mechanismů.

Praktická část demonstrovala různé techniky útoků, jako je ARP spoofing a snadnost provedení MITM útoku. Poskytla konkrétní návody, jak lze tyto útoky provádět. Tyto ukázky jsou užitečné nejen pro studenty, kteří chtějí pochopit základní principy kybernetických útoků a obranných strategií, ale také pro odborníky na zabezpečení sítí, kteří chtějí rozšířit své znalosti o pokročilé bezpečnostní nástroje a techniky.

Doporučení plynoucí z této práce zahrnují posílení zabezpečení bezdrátových sítí prostřednictvím implementace silnějších šifrovacích protokolů, pravidelných penetračních testů a zavádění nástrojů pro monitorování sítě. Zvláštní pozornost by měla být věnována zabezpečení koncových zařízení, protože právě ta často tvoří slabé články v bezpečnostním řetězci. Organizace by měly investovat do řešení rozšířené detekce a reakce (XDR) a zaměřit se na prevenci, detekci a rychlou reakci na potenciální hrozby.

Cíle, které se na začátku stanovily, byly splněny. Praktické ukázky a teoretické výzkumy prokázaly, že je možné vytvořit systematický návod a zdroj informací o monitorování datového provozu a aktivnímu testování bezpečnosti sítí.

Nejen díky této praktické ukázce je práce určena pro studenty, kteří hledají systematický návod a zdroj informací o monitorování datového provozu a bezpečnosti sítí. Zároveň je cenným zdrojem pro všechny uživatele, kteří chtějí prohloubit své znalosti v této oblasti, porozumět a získat ucelený přehled o ochraně sítí před kybernetickými hrozbami a naučit se, jak se účinně chránit před potenciálními kybernetickými útoky.

Budoucí studie by se mohly zaměřit na další techniky útoků a obrany, zkoumání nových technologií, jako je umělá inteligence a strojové učení v oblasti kybernetické bezpečnosti, a také na problematiku bezpečnosti v prostředí Internetu věcí. Otevřenou otázkou zůstává, jak efektivně integrovat různé bezpečnostní nástroje do komplexní obranné strategie a jak zajistit bezpečnost v době rostoucí propojenosti a digitalizace. Tato témata poskytují bohatý prostor pro další výzkum a diskusi v oblasti kybernetické bezpečnosti.

14 Seznam použité literatury

[1] R. A. Kemmerer, „Cybersecurity", in *25th International Conference on Software Engineering, 2003. Proceedings.*, Portland, OR, USA: IEEE, 2003, s. 705–715. doi: 10.1109/ICSE.2003.1201257.

[2] J. A. Lewis, „Cybersecurity and Critical Infrastructure Protection". Center for Strategic and International Studies, leden 2006. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection

[3] E. G. Amoroso, *Cyber security*. Summit, NJ: Silicon Press, 2007.

[4] ITU, „Overview of cybersecurity, X.1205". International Telecommunication Union, duben 2008. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] CNSS, „Committee on National Security Systems (CNSS) Glossary, No. 4009". Committee on National Security Systems, květen 2015. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[6] C. Canongia a R. Mandarino, „Cybersecurity: The New Challenge of the Information Society", in *Crisis Management: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2014, s. 21. doi: 10.4018/978-1-4666-4707-7.

[7] NICCS, „Cybersecurity", *A Glossary of Common Cybersecurity Words and Phrases*. NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, březen 2023. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary

[8] N. Wiener, *Cybernetics: or, Control and communication in the animal and the machine*, Second edition, 2019 reissue. Cambridge, Massachusetts: The MIT Press, 2019.

[9] B. Buzan, O. Wæver, a J. de Wilde, *Security: a new framework for analysis*. Boulder, Colo: Lynne Rienner Pub, 1998.

[10] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, a S. Mahmood, „Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study", *Arab J Sci Eng*, roč. 45, č. 4, s. 3171–3189, dub. 2020, doi: 10.1007/s13369-019-04319-2.

[11] M. Abomhara, Department of Information and Communication Technology, University of Agder, Norway, G. M. Kien, a Department of Information and Communication Technology, University of Agder, Norway, „Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", *JCSM*, roč. 4, č. 1, s. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[12] NICCS, „Cyber Threat", *A Glossary of Common Cybersecurity Words and Phrases*. NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, duben 2024. Viděno: 12. duben 2024. [Online]. Dostupné z: https://csrc.nist.gov/glossary/term/cyber_threat

[13] Red Hat, „What is malware?", redhat.com. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://www.redhat.com/en/topics/security/what-is-malware

[14] K.-K. R. Choo, „The cyber threat landscape: Challenges and future research directions", *Computers & Security*, roč. 30, č. 8, s. 719–731, lis. 2011, doi: 10.1016/j.cose.2011.08.004.

[15] H. S. Brar a G. Kumar, „Cybercrimes: A Proposed Taxonomy and Challenges", *Journal of Computer Networks and Communications*, roč. 2018, s. 1–11, 2018, doi: 10.1155/2018/1798659.

[16] VPSBG, „DDoS", VPSBG. Viděno: 5. březen 2024. [Online]. Dostupné z: https://www.vpsbg.eu/blog/what-is-a-ddos-

attack?gad_source=1&gclid=CjwKCAiAopuvBhBCEiwAm8jaMTcE89xZivItZsaHp5zM-wl7Tt6x-9ZNyP8HzIF2toaXeJFvLCXd4BoCCzEQAvD_BwE
[17] NIST, „Botnet", *COMPUTER SECURITY RESOURCE CENTER*. březen 2024. Viděno: 5. březen 2024. [Online]. Dostupné z: https://csrc.nist.gov/glossary/term/botnet
[18] SANS, „Botnet", *Glossary of Cyber Security Terms*. březen 2024. Viděno: 5. březen 2024. [Online]. Dostupné z: https://www.sans.org/security-resources/glossary-of-terms/
[19] KirstenS, „Cross Site Scripting (XSS)", OWASP.org. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://owasp.org/www-community/attacks/xss/
[20] B. Bhushan, G. Sahoo, a A. K. Rai, „Man-in-the-middle attack in wireless and computer networking — A review", in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, Dehradun: IEEE, zář. 2017, s. 1–6. doi: 10.1109/ICACCAF.2017.8344724.
[21] M. Conti, N. Dragoni, a V. Lesyk, „A Survey of Man In The Middle Attacks", *IEEE Commun. Surv. Tutorials*, roč. 18, č. 3, s. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.
[22] P. Sharma, R. Johari, a S. S. Sarma, „Integrated approach to prevent SQL injection attack and reflected cross site scripting attack", *Int J Syst Assur Eng Manag*, roč. 3, č. 4, s. 343–351, pro. 2012, doi: 10.1007/s13198-012-0125-6.
[23] R. C. Dodge, C. Carver, a A. J. Ferguson, „Phishing for user security awareness", *Computers & Security*, roč. 26, č. 1, s. 73–80, úno. 2007, doi: 10.1016/j.cose.2006.10.009.
[24] Kaspersky, „What is Social Engineering?", kaspersky.com. Viděno: 10. červenec 2023. [Online]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering
[25] „Social Engineering". Viděno: 10. červenec 2023. [Online]. Dostupné z: https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html
[26] D. Cohen, A. Elalouf, a R. Zeev, „Collaboration or separation maximizing the partnership between a “Gray hat” hacker and an organization in a two-stage cybersecurity game", *International Journal of Information Management Data Insights*, roč. 2, č. 1, s. 100073, dub. 2022, doi: 10.1016/j.jjimei.2022.100073.
[27] Kaspersky, „Black hat, White hat, and Gray hat hackers – Definition and Explanation", kaspersky.com. Viděno: 11. červenec 2023. [Online]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types
[28] M. Lemmy, „The Difference Between the 6 Types of “HAT” Hackers and How They Work", Lemmy Morgan. Viděno: 15. duben 2024. [Online]. Dostupné z: https://www.lemmymorgan.com/difference-between-the-6-types-of-hat-hackers/
[29] Kaspersky, „Script kiddie", *Kaspersky IT Encyklopedia*. Viděno: 15. duben 2024. [Online]. Dostupné z: https://encyclopedia.kaspersky.com/glossary/script-kiddie/
[30] Kaspersky, „Hacktivism", *Kaspersky IT Encyklopedia*. Viděno: 15. duben 2024. [Online]. Dostupné z: https://encyclopedia.kaspersky.com/glossary/hacktivism/
[31] K. O’Brien, „Cyber & Physical Security: Why You Need Both", Cmpass IT Compliance. Viděno: 16. duben 2024. [Online]. Dostupné z: https://www.compassitc.com/blog/cyber-physical-security-why-you-need-both
[32] BoonEdam, „MAKING PHYSICAL SECURITY PART OF CYBERSECURITY BEST PRACTICES." Viděno: 16. duben 2024. [Online]. Dostupné z: https://www.boonedam.com/en-us/pillar-page/making-physical-security-part-of-cybersecurity-best-practices

[33] DevoTeam, „Safeguarding Your Assets: The Critical Role of Physical Security in Cybersecurity", DevoTeam. Viděno: 16. duben 2024. [Online]. Dostupné z: https://www.devoteam.com/expert-view/cybersecurity-the-importance-of-physical-security/
[34] DC Computers, „Aktivní síťové prvky", DC Computers. Viděno: 11. červenec 2023. [Online]. Dostupné z: https://dccomp.cz/produkty-a-sluzby/aktivni-sitove-prvky/
[35] P. Bouška, „TCP/IP a ethernet - cesta v síti, aktivní síťové prvky", samuraj-cz.com. Viděno: 11. červenec 2023. [Online]. Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-a-ethernet-cesta-v-siti-aktivni-sitove-prvky/
[36] J. English, „An introduction to 8 types of network devices", TechTarget. Viděno: 11. červenec 2023. [Online]. Dostupné z: https://www.techtarget.com/searchnetworking/tip/An-introduction-to-8-types-of-network-devices
[37] Paloalto, „What is an Endpoint?", paloaltonetworks.com. Viděno: 11. červenec 2023. [Online]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint
[38] Fortinet, „Endpoint Security", fortinet.com. Viděno: 11. červenec 2023. [Online]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security
[39] Paloalto, „Endpoint Security", paloaltonetworks.com. [Online]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-security
[40] M. Abbasi, A. Shahraki, a A. Taherkordi, „Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey", *Computer Communications*, roč. 170, s. 19–41, bře. 2021, doi: 10.1016/j.comcom.2021.01.021.
[41] „Penetrační testování". cesnet. Viděno: 19. červenec 2023. [Online]. Dostupné z: https://hsoc.cesnet.cz/_media/cs/dokumenty/tech/penetracni_testovani-summary.pdf
[42] J. Stárek, „Fuzz testování webových aplikačních rozhraní", Masarykova univerzita, Brno, 2019. Viděno: 19. červenec 2023. [Online]. Dostupné z: https://is.muni.cz/th/krkvh/text.pdf
[43] D. Meredith, *Certified Ethical Hacker (CEH) V11 312-50 Exam Guide: Keep up to Date with Ethical Hacking Trends and Hone Your Skills with Hands-On Activities*. Birmingham: Packt Publishing, Limited, 2022.
[44] R. P. Ltd, „Raspberry Pi", Raspberry Pi. Viděno: 28. říjen 2023. [Online]. Dostupné z: https://www.raspberrypi.com/
[45] R. Hertzog, J. O'Gorman, a M. Aharoni, *Kali Linux revealed: mastering the penetration testing distribution*. Cornelius: Offsec Press, 2017.
[46] A. Alabdulatif, X. Ma, a L. Nolle, „Analysing and attacking the 4-way handshake of IEEE 802.11i standard", in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, London, United Kingdom: IEEE, pro. 2013, s. 382–387. doi: 10.1109/ICITST.2013.6750227.

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Zuzana Vojíková**
Studium:	I2000438
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Monitorování datové sítě pomocí nástrojů Kali Linux**
Název bakalářské práce AJ:	Data network monitoring using Kali Linux tools

Cíl, metody, literatura, předpoklady:

V práci zohlednit osnovu:

Cybersecurity – všeobecný přehled

Bezpečnostní hrozby

Útoky na aktivní prvky sitě

Zabezpečení prvků v síti

Monitoring datového provozu

Penetrační testy zařízení a služeb

KALI na platformě Raspberry Pi

Monitoring: Odchytávání provozu na portu v promiskuitním modu

Penetrační testy: útok na webové rozhraní

William Stallings; Effective Cybersecurity; Pearson Education; 2018; ISBN: 0134772806
Charles J. Brooks, Christopher Grow, Philip A. Craig Jr., Donald Short; Cybersecurity Essentials; WILEY; 2018; ISBN: 978-1-119-36239-5
John Vacca; Computer and Information Security Handbook; Sciencediret; 2017; ISBN: 978-0-12-803843-7
Hwaiyu Geng; Internet of Things and Data Analytics Handbook; Whiley; 2017; ISBN: 978-1-119-17364-9
Diogenes Yuri; Cybersecurity: Attack and Defense Strategies; Packt; 2019; ISBN: 9781788475297

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Pavel Blažek, Ph.D.
Datum zadání závěrečné práce:	15.10.2021