Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Simulace síťových útoků za využití Kali Linux

Diplomová práce

Autor: Bc. Aleš Lajvr
Studijní obor: Aplikovaná informatika (ai2-k)

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2024

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 26.3.2024 Aleš Lajvr

Poděkování:

Děkuji vedoucímu diplomové práce doc. Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, ochotu a vstřícnost. Dále děkuji své rodině za podporu po celou dobu studia.

Anotace

Význam kybernetické bezpečnosti stále roste. Souvisí to s růstem výpočetního výkonu, miniaturizací elektroniky i se vstupem umělé inteligence do všech oborů lidské činnosti. Účinnou ochranou před kybernetickou kriminalitou by mělo být zavedení systému řízení bezpečnosti informací.

Tato práce se zabývá kybernetickou bezpečností na úrovni zabezpečení síťových prvků v drátových a bezdrátových sítích. Jejím cílem je poukázat na vybrané zranitelnosti a možnosti jejich zneužití pomocí nástrojů Kali Linux, a především informovat čtenáře, jak zneužití předejít.

V experimentální části bylo laboratorně ověřeno, jak snadné je provedení síťových útoků. Po nakonfigurování zabezpečení síťových prvků byla úspěšnost zabezpečení prakticky ověřena pomocí opětovného spuštění útoků. V závěru práce jsou uvedena doporučení vycházející z provedených experimentů.

Annotation

Title: Simulation of network attacks using Kali Linux

The importance of cyber security continues to grow. This is related to the growth of computing power, the miniaturization of electronics and the entry of artificial intelligence into all fields of human activity. An effective protection against cybercrime should be the implementation of an information security management system.

This thesis deals with cyber security at the level of securing network elements in wired and wireless networks. Its goal is to highlight selected vulnerabilities and the possibilities of exploiting them using Kali Linux tools, and most importantly, to inform the reader on how to prevent exploits.

In the experimental part, it was verified in the laboratory how easy it is to perform network attacks. After configuring the security of the network elements, the success of the security was practically verified by re-executing the attacks. The paper concludes with recommendations based on the experiments performed.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Počátky etického hackingu sahají do konce 70. let minulého století. V současné době je tomuto tématu věnována velká pozornost v souvislosti s prudkým růstem využití výpočetní techniky a Internetu. Tento růst je zapříčiněn zejména probíhajícím procesem elektronizace a digitalizace agend státní správy a samosprávy, zdravotnictví atd. Možnosti, které moderní technologie nabízí, se snaží využít i soukromé firmy. Jejich motivací je především využití Internetu pro elektronické obchodování a reklamu, přičemž výsledkem by mělo být zlepšení kvality zákaznických služeb. Při využívání potenciálu nových technologií je však zároveň nutné dbát i na zajištění jejich bezpečnosti.

V kapitole 2 je představen aktuální stav kybernetické bezpečnosti. Nejprve jsou zde uvedeny vybrané výzkumné práce související s tématem kybernetické bezpečnosti a vysvětleny základní pojmy. V další části je prezentována situace na poli národní i evropské legislativy, včetně porovnání se situací v USA. Dále je zde uveden přehled hackerských taktik a technik. Závěr kapitoly je věnován představení kurzů a certifikací použitelných v boji proti kybernetické kriminalitě. K opatření zdrojů v části zabývající se porovnáním evropských a amerických úřadů a pojmů z oblasti kybernetické bezpečnosti byla použita umělá inteligence. Konkrétně nástroj Bing Chat společnosti Microsoft, přejmenovaný v prosinci 2023 na Microsoft Copilot. Tento nástroj je založený na technologii Chat GPT4 společnosti OpenAI.

Kapitola 3 se zabývá teoretickou analýzou nástrojů, které je možné využít k simulaci síťových útoků s cílem ověření skutečného stavu zabezpečení drátových i bezdrátových sítí. Jsou zde představeny nástroje Nmap, Wireshark, Aircrack-ng, Wifite, Ettercap, Yersinia, Scapy a Macof.

Kapitola 4 se věnuje aktuálním vědeckým pracím na téma síťových útoků vůči drátovým i bezdrátovým sítím. V podkapitolách je nejprve uvedena vybraná zranitelnost. Poté následuje popis způsobu, jakým lze danou zranitelnost zneužít, a v závěru podkapitol jsou doporučeny možnosti obrany před zneužitím.

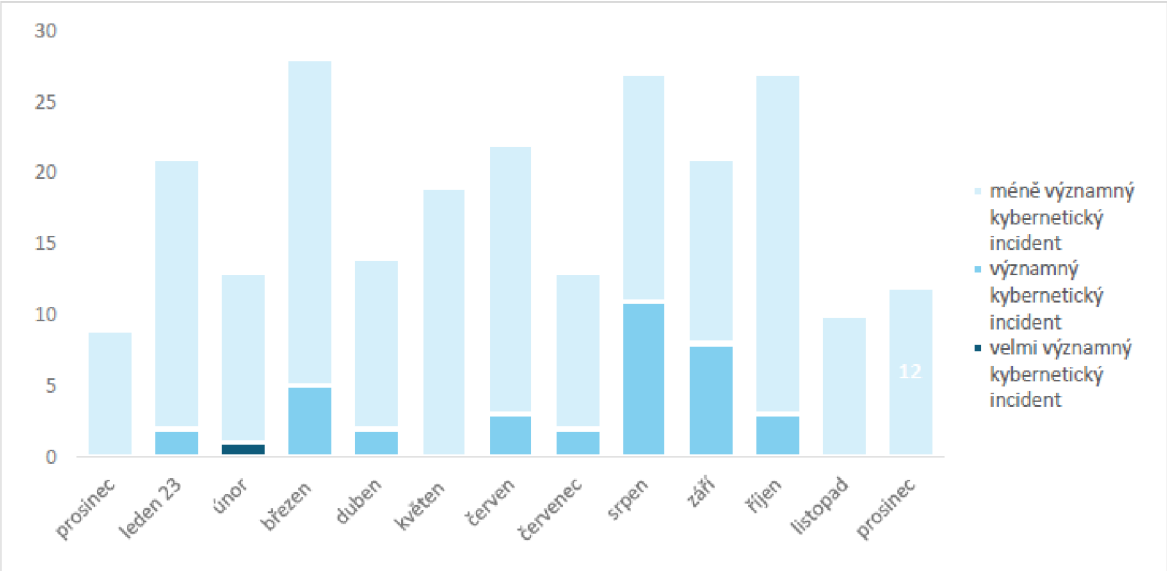
Kapitola 5 se zabývá experimentálním ověřením bezpečnostních rizik v laboratorním prostředí. S pomocí nástrojů představených v kapitole 3 byla provedena simulace útoků představených v kapitole 4. Cílem bylo otestovat vliv útoků, poté provést doporučená zabezpečení a prakticky ověřit jejich účinnost.

2 Teoretická část

S rostoucí závislostí na výpočetní technice a Internetu se podle [1] zvyšuje i množství bezpečnostních událostí a bezpečnostních incidentů. S tím podle autora souvisí i růst výše případných škod. Autor dále uvádí, že tato rizika si nemohou dovolit ignorovat zejména velké společnosti, například průmyslové podniky, banky a státní správa. Na větší cíle si podle autora mohou dovolit útočit zkušení hackeři. Existuje však mnoho hackerů, kteří podle autora dávají přednost menším a středním firmám, protože předpokládají, že bude snadnější je napadnout a poškodit. Podle Verizon 2018 DBIR [2] se 58 % kybernetických útoků zaměřuje na malé podniky.

O zvyšujícím se počtu bezpečnostních incidentů, zejména v souvislosti s technikou phishing a škodlivým kódem, informují i tuzemské zdroje. Zpráva o činnosti CSIRT.CZ (NÁRODNÍHO CSIRT ČR) za rok 2021 [3] například uvádí: *„V roce 2021 bylo řešeno dohromady 1 726 incidentů, tzn. meziroční nárůst dosáhl 36,2 %. V porovnání se statistikou incidentů před pandemií je to však nárůst až o 80 %.“* zpráva dále uvádí: *„V roce 2021 došlo stejně jako v předchozím roce zejména k zásadnímu nárůstu phishingu. Mimo to došlo ke zvýšení počtu incidentů v kategorii malware. Ve všech zbylých kategoriích, tedy u spam, other, probe (kategorie zahrnující brute force útoky), DOS, botnet, pharming došlo naopak k poklesu incidentů.“*

O dominujícím počtu incidentů v kategorii dostupnosti v průběhu roku 2023 informuje také měsíčník Kybernetické incidenty pohledem NÚKIB [4], který uvádí: *„Ačkoli v prosinci došlo k mírnému nárůstu evidovaných incidentů oproti předešlému měsíci, i nadále byla výsledná hodnota poměrně nízko pod ročním průměrem, který se pohyboval okolo 19 incidentů měsíčně. Stejně jako v listopadu NÚKIB registroval během prosince pouze méně významné kybernetické incidenty, které v roce 2023 tvořily více než čtyři pětiny všech evidovaných incidentů.“* Měsíčník dále uvádí: *„Podobně jako v průběhu celého roku, také v prosinci v rámci klasifikace incidentů dominovala kategorie Dostupnosti. Incidenty z této kategorie v roce 2023 tvořily téměř dvě třetiny všech evidovaných incidentů. Mimo to NÚKIB řešil také incidenty z kategorií Informační bezpečnost a Průnik.“* Na Obr. 1 je graf četností bezpečnostních incidentů řešených NÚKIB v roce 2023. Incidenty jsou rozdělené do kategorií podle významnosti.



Obr. 1 Kybernetické incidenty řešené NÚKIB v roce 2023.
Zdroj: [4]

Další oblastí, kde v současné době probíhá prudký rozvoj, je Internet věcí (IoT). K rozvoji IoT dochází například v průmyslu, což mimo jiné souvisí s Národní iniciativou Průmysl 4.0 Ministerstva průmyslu a obchodu [5]. Dá se předpokládat, že velké firmy si s otázkami kybernetické bezpečnosti poradí, protože jsou si dostatečně vědomy rizik souvisejících s nasazením těchto technologií.

Velkým problémem je však rozšiřování Internetu věcí v domácnostech. Ve snaze rychle dodat na trh výrobek, po kterém je poptávka, totiž výrobci často zanedbávají oblast kybernetické bezpečnosti. Na testy kybernetické bezpečnosti produktů IoT pro domácnosti se zaměřila například studie [6]. V rámci této studie autoři provedli systematické penetrační testování dvaceti dvou zařízení zařazených do pěti kategorií: chytré dveřní zámky, chytré kamery, chytré adaptéry do auta/garáže, chytré spotřebiče a různá chytrá domácí zařízení. V rámci studie bylo celkem objeveno sedmnáct zranitelností, které byly zveřejněny jako nové CVE (Common Vulnerabilities and Exposures). Některé z těchto zranitelností získaly v Národní databázi zranitelností USA (NVD) hodnocení kritické závažnosti (9,8/10). Tato zařízení se podle autorů již prodávají a používají po celém světě, objevené zranitelnosti by tedy mohly vést k vážným následkům. Podle autorů by útočník například mohl získat fyzický přístup do domu. Kromě výše uvedených zranitelností bylo autory dále objeveno 52 slabých míst, která by v budoucnu potenciálně mohla vést ke vzniku dalších zranitelností.

Také práce [7] se zabývá bezpečnostními riziky domácích IoT zařízení. Autoři se zde zaměřili na možné zneužití výkonných a zároveň snadno dostupných nástrojů určených k monitorování a provádění útoků na WiFi sítě (např. aircrack-ng). Smyslem

práce je představit způsoby provedení některých běžných útoků a poskytnout proti nim obranu. Ta podle autorů spočívá v implementaci měniče MAC adres do IoT software. Uvedené řešení má zabránit útokům typu DoS (Denial Of Service) nebo DDoS (Distribuované DoS), prováděným na základě MAC adresy oběti. Jiný přístup k problematice ochrany před ARP spoofingem byl zvolen v práci [8]. K ochraně IoT zařízení autoři použili bránu v podobě PC s operačním systémem Ubuntu. Brána podle autorů detekuje škodlivé ARP pakety pomocí nástroje Wireshark a zachytává je pomocí nástroje arptables.

Další oblastí, kde dochází k prudkému rozvoji, je cloud computing. Některé firmy už k outsourcingové formě IT služeb přešly. V současné době se tímto směrem postupně vydávají i orgány státní správy. Práce [9] se zabývá otázkami detekce zranitelností a možnostmi penetračního testování v prostředí cloud computing. Podle autorů usnadňují služby cloud computing nejen přístup k aktivům z Internetu, ale také šíření škodlivého kódu z jednoho napadeného subsystému na ostatní, proto je nezbytné řádné zabezpečení. Hodnocení zranitelností v prostředí cloud computing je podle autorů složitější, takže jsou nutné nové metodiky. Autoři testovali platformu Vulcan, která umožňuje centrální řízení rizik v prostředí cloud computing. Autoři uvádějí, že stejně jako tradiční služby je možné i služby cloud computing podrobit penetračnímu testování. Nejprve je podle autorů nutné provést klonování služby pomocí PTaaS (PenTest as a Service), aby nedošlo k poškození produkčního systému. Autoři dále uvádějí, že jedním z možných řešení PTaaS je Potassium, které klonuje systém včetně jeho dynamického stavu, takže výsledek testování je platný i pro reálný systém. Udržení bezpečnosti v prostředí cloud computing může být podle autorů problematické. Autoři dále uvádějí, že k vyšší bezpečnosti lze přispět použitím specifických platforem a nástrojů.

Předchozí část shrnuje aktuální rizika související s vývojem v oblasti IT a Internetu. Kromě těchto rizik je podle [1] nezbytné připomenout i možné důsledky kybernetických útoků. Kybernetické útoky mohou podle autora například ohrozit podnikání. Autor uvádí, že je důležité nepodléhat falešnému pocitu bezpečí a podniknout prevenci i v případech, kde by se mohlo na první pohled zdát, že útočník nemůže způsobit žádné škody. Oprava systému po poškození kybernetickým útokem může být podle autora velmi drahá.

Na zvýšený výskyt kybernetické kriminality v posledních letech upozorňuje i Policie České republiky [10]: *„Kybernetická kriminalita, dříve také označovaná jako informační kriminalita, je definována v Policii ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.“* V článku se dále uvádí: *„Policie ČR od r. 2011 sleduje počet trestných činů spáchaných v kyberprostoru (zejm. v síti Internet). V uvedeném období je zaznamenán trend setrvalého nárůstu evidovaných případů kybernetické kriminality (od 1 502 trestných činů v roce 2011, do 8 417 trestných činů v roce 2019).“*

2.1 Základní pojmy

Podle NIST (National Institute of Standards and Technology) [11] je **kybernetická bezpečnost** definována jako prevence poškození, ochrana a obnova počítačů, elektronických komunikačních systémů, elektronických komunikačních služeb, drátové komunikace a elektronické komunikace, včetně informací v nich obsažených, aby se zajistila jejich dostupnost, integrita, autentizace, důvěrnost a nezpochybnitelnost. Podle ENISA (European Union Agency for Cybersecurity) [12] pokrývá kybernetická bezpečnost nejen všechny aspekty prevence, tj. prognostiku, toleranci, detekci a zmírňování, ale také odstraňování, analýzu a vyšetřování kybernetických incidentů. Podle autorky by kybernetická bezpečnost měla zahrnovat následující atributy: dostupnost, spolehlivost, bezpečnost, důvěrnost, integritu, udržovatelnost (u hmotných systémů a sítí), robustnost, schopnost přežít, odolnost, odpovědnost, autenticitu a nepopiratelnost.

Z výše uvedeného je patrné, že v definici kybernetické bezpečnosti se obě agentury téměř shodují. Přesto mezi nimi existují určité rozdíly. NIST je federální agentura spadající pod Ministerstvo obchodu Spojených států amerických. Posláním NIST je podle [13] vyvíjet a podporovat měření, standardy a technologie pro zvýšení produktivity, usnadnění obchodu a zlepšení kvality života. Autor dále uvádí, že NIST je zodpovědný za stanovení standardů a pokynů souvisejících s počítačovými a informačními technologiemi pro federální agentury. Podle autora tyto standardy a pokyny dobrovolně používá mnoho organizací soukromého sektoru. NIST se tedy více zaměřuje na technickou stránku a definuje konkrétní aspekty, které by měly být chráněny (např. dostupnost, integrita atd.). ENISA je agentura Evropské unie, která podporuje

spolupráci a harmonizaci mezi členskými státy v oblasti kybernetické bezpečnosti. Podle [12] poskytuje ENISA širší rámec pro řízení kybernetického rizika a zdůrazňuje potřebu ochrany v kyberprostoru na různých úrovních. Autorka uvádí metodu hierarchického členění kategorizace potřeb v kybernetickém prostoru, viz Obr. 2.

Obr. 2 Vrstvy ochrany kybernetické bezpečnosti dle ENISA.
Zdroj: Vlastní zpracování podle [12]

Obě agentury vydaly soubory předpisů, které by měly přispět ke zvýšení kybernetické bezpečnosti. V případě NIST se jedná o Cybersecurity Framework (CSF) [14], který nabízí sadu doporučených postupů pro řízení kybernetických rizik pro organizace všech velikostí a odvětví. Aktuální CSF je verze 1.1 a byl vydán 16. 4. 2018. V současnosti je připravován CSF verze 2, podle [13] by měl být vydán na začátku roku 2024. V případě ENISA se jedná o Směrnici NIS2 [15] vydanou 14. 12. 2022, dvojka ve zkráceném názvu označuje verzi 2. NIS2 má sloužit k implementaci evropských politik a právních předpisů týkajících se kybernetické bezpečnosti, více viz kapitola 2.2.3.

Kyberprostor je podle NIST [11] definován jako globální doména v rámci informačního prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních systémů včetně internetu, telekomunikačních sítí, počítačových systémů a vestavěných procesorů a řadičů. Autoři dále uvádějí, že se jedná o komplexní prostředí vyplývající z interakce lidí, softwaru a služeb na internetu, prostřednictvím k němu připojených technologických zařízení a sítí, které však ve fyzické podobě neexistuje.

Za **kybernetický útok** je podle NIST [11] považován jakýkoli druh škodlivé činnosti, která se pokouší shromažďovat, narušovat, popírat, degradovat nebo zničit prostředky informačního systému nebo samotné informace. Autoři dále uvádějí, že kybernetický útok je relace nějaké konkrétní hrozby, která má dopad na důvěrnost, integritu nebo dostupnost výpočetního zdroje.

Informační systém je podle NIST [11] diskrétní sada informačních zdrojů uspořádaná pro shromažďování, zpracování, údržbu, používání, sdílení, šíření nebo likvidaci informací.

Podle [16] se každý informační systém skládá z **informačních aktiv**. Za informační aktivum se podle NIST [11] považuje cokoliv, co má hodnotu pro osobu nebo organizaci. Autoři dále dělí aktiva na hmotná (např. hardware, výpočetní platforma, síťové zařízení nebo jiná technologická součást) a nehmotná (např. lidé, data, informace, software, schopnost, ochranná známka, autorské právo, patent, duševní vlastnictví, obrázek nebo dobrá pověst). Podle ENISA [17] je aktivem vše, co má hodnotu pro organizaci, její obchodní operace a jejich kontinuitu, včetně informačních zdrojů, které podporují poslání organizace. Vůči informačním aktivům mohou být podle [16] vedeny kybernetické útoky, proto je nutné všechna informační aktiva identifikovat za účelem budování jejich ochrany. Autor dále uvádí, že identifikaci informačních aktiv lze provést pomocí objektově hierarchické dekompozice informačního systému. Informační systémy jsou podle autora zpravidla tvořeny následujícími informačními aktivy, včetně konkrétních příkladů (výčet není úplný):

- **Data**: obchodní data, údaje o zakázkách, data zákazníků, osobní údaje zaměstnanců, know-how, data o produktech či technologiích, přihlašovací údaje apod.
- **Koncová zařízení**: desktopy, notebooky, tablety, smartphony.
- **Servery**: webové, aplikační, databázové, souborové, tiskové.
- **Průmyslové systémy**: SCADA, HW i SW roboti.
- **Pasivní a aktivní síťové prvky**: switche, routery, kabely.
- **Zabezpečovací systémy**: CCTV, PZTS, EPS, ACS.
- **IoT**: bílá elektronika, televize, hodinky, termostatické hlavice, auta.
- **Prostory**: společné prostory, serverovny, technické místnosti, okolí.
- **Zálohy**: zálohovací servery, NAS, SAN, cloud.
- **Dokumentace**: v elektronické podobě, v papírové podobě.
- **Osoby**: uživatelé, správci, vývojáři, dodavatelé.

Po provedení identifikace aktiv je podle [16] dalším důležitým krokem rozdělení podle jejich významu pro organizaci na aktiva primární a sekundární, přičemž sekundární aktiva mohou být alternativně označena jako podpůrná. Vyhláška o kybernetické bezpečnosti [18] definuje primární aktivum jako informaci nebo službu, kterou zpracovává nebo poskytuje informační a komunikační systém. Mezi podpůrná aktiva podle vyhlášky patří technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. Technickým aktivem se podle vyhlášky rozumí takové technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém.

Hrozba je podle NIST [11] definována jako jakákoli okolnost nebo událost s potenciálem nepříznivě ovlivnit organizační operace, aktiva nebo jednotlivce prostřednictvím informačního systému. Autoři dále uvádějí, že může dojít k neoprávněnému přístupu, zničení, zveřejnění nebo modifikaci informací, případně odepření služby. Podle ENISA [17] je hrozba jakákoli okolnost nebo událost s potenciálem nepříznivě ovlivnit aktivum neoprávněným přístupem, zničením, zveřejněním, úpravou dat, případně odmítnutím služby. Podle vyhlášky o kybernetické bezpečnosti [18] je hrozba definována jako potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu. Podle [16] je pro dosažení úspěšné ochrany nutné hrozby identifikovat. Autor uvádí, že na informační systém mohou působit hrozby obecné neboli generické a hrozby specifické. Obecným hrozbám je podle autora vystavena většina informačních systémů. Autor dále uvádí, že jejich výčet je uveden v různých standardech a metodikách. Informační systém však podle autora mohou ohrožovat i hrozby specifické, týkající se pouze konkrétního systému. Autor dále uvádí, že hrozby se nejčastěji dělí podle úmyslu na hrozby náhodné (způsobené událostí), nebo úmyslné (naplánované), případně podle umístění zdroje na hrozby vnitřní (zdroj se nachází uvnitř organizace), nebo vnější (zdroj se nachází mimo organizaci). Příklady kategorizace hrozeb viz Tabulka 1.

Tabulka 1 Základní typy hrozeb.

Hrozby	Náhodné	Úmyslné
Vnější	přírodního původu	Hacking
Vnitřní	technické selhání (lidská chyba)	Sabotáž

Zdroj: [16]

Hrozby lze podle [16] dále dělit na základě dopadu na systém na hrozby aktivní (dochází ke změně stavu systému v důsledku narušení integrity a dostupnosti), nebo pasivní (nedochází ke změně stavu systému, ale dochází k narušení důvěrnosti neboli k úniku informací). Autor dále uvádí, že pro stanovení míry hrozby je nutné zohlednit následující faktory:

- **Četnost výskytu**: statistiky, průzkumy, evidence bezpečnostních incidentů.
- **Příležitost**: pravděpodobnost hrozby je přímo úměrná příležitosti realizace.
- **Motiv**: finanční prospěch, konkurenční převaha, dokázání schopností útočníka, odplata.
- **Schopnosti**: neúmyslné selhání zaměstnance nebo schopnosti útočníka.
- **Peníze**: náklady na realizaci kybernetického útoku.
- **Vybavení**: nároky na HW a SW vybavení útočníka.
- **Čas**: pravděpodobnost hrozby je nepřímo úměrná době potřebné k přípravě a realizaci hrozby.
- **Atraktivita aktiva**: pravděpodobnost hrozby je přímo úměrná vnímání hodnoty aktiva z pohledu útočníka.
- **Počet osob**: pravděpodobnost hrozby je přímo úměrná počtu osob, které aktivum využívají nebo se podílejí na jeho provozu, rozvoji, správě či zajištění bezpečnosti informačního a komunikačního systému.
- **Stáří aktiva**: posuzuje se i u lidí, např. nezkušený zaměstnanec → zkušený zaměstnanec → zaměstnanec trpící syndromem vyhoření.

Zranitelnost je podle NIST [11] definována jako slabina v informačním systému, postupech zabezpečení systému, vnitřních kontrolách nebo implementaci, která by mohla být zneužita nebo spuštěna zdrojem hrozby. ENISA [17] definuje zranitelnost jako slabinu, kterou by útočník mohl využít k ohrožení důvěrnosti, dostupnosti nebo integrity zdroje. Podle vyhlášky [18] je hrozba definována jako slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami. Podle [16] se jedná o vlastnost aktiva, která se může nacházet nejen v software, ale také v hardware, procesu nebo lidech, kteří jsou součástí informačního systému. Autor uvádí následující seznam nejčastěji se vyskytujících chyb primárních a technických aktiv:

- **Software error** je implementační chyba v kódu (může se jednat o chybu syntaktickou, sémantickou nebo logickou).
- **Bug** se používá pro označení HW i SW chyb.
- **Flaw** je označení chyby, která vznikla už při návrhu aplikace.
- **Defekt** nebo **fault** označuje důsledek chyby v návrhu nebo implementaci, může se projevit hned nebo při splnění určitých podmínek.
- **Hole**, **zranitelnost** nebo **slabina** označuje chybu, která může být zneužita k narušení důvěrnosti, integrity nebo dostupnosti systému či dat.

V práci [19] byla provedena studie dopadu lidských zranitelností na kybernetickou bezpečnost. Celkově bylo dosaženo 61 % úrovně informovanosti respondentů v oblasti kybernetické bezpečnosti, což autor označil jako znepokojivě nízkou úroveň. Autor také provedl rozdělení zranitelností do následujících kategorií včetně vyhodnocení úrovní nedostatečného povědomí o kybernetické bezpečnosti v jednotlivých kategoriích:

- Sociální inženýrství: 37 %
- Sociální média: 35 %
- Phishing: 30 %
- Používání hesel: 30 %
- Používání e-mailů: 22 %
- Antivirová ochrana: 33 %
- Ochrana dat: 29 %

Speciálním případem zranitelnosti primárních a technických aktiv je podle vyhlášky [16] **zranitelnost nultého dne**. Toto označení se používá pro zranitelnost, která ještě není všeobecně známá, a tudíž pro ni neexistuje záplata. Časový interval mezi objevením zranitelnosti a vydáním záplaty se podle vyhlášky označuje jako **okno zranitelnosti**. Útok, který takovou zranitelnost zneužívá, se podle vyhlášky označuje jako **útok nultého dne**. Ve vyhlášce je dále uvedeno, že k rozlišení závažnosti jednotlivých zranitelností se používá **hodnocení zranitelností**. V rámci tohoto procesu se podle vyhlášky vyhodnocuje, zda zranitelnost může být zneužitá pro narušení důvěrnosti, integrity nebo dostupnosti. Podle vyhlášky se při tom posuzuje několik faktorů. Procesem hodnocení zranitelností se zabývá více organizací, nejznámější z nich jsou uvedeny níže.

Pro identifikaci a definici zranitelností a zároveň jako veřejný katalog slouží program **Common Vulnerabilities and Exposures** (CVE) [20] společnosti MITRE, která je sponzorovaná vládou USA. Každé zranitelnosti je v okamžiku jejího nahlášení přiděleno tzv. CVE ID ve formátu CVE-YYYY-NNNN, kde CVE je prefix, YYYY je rok přidělení ID a NNNN je pořadové číslo zranitelnosti. Detailní popis a závažnost zranitelnosti jsou uvedeny v tzv. Národní databázi zranitelností (**National Vulnerability Database**, zkr. NVD) [21]. Závažnost zranitelnosti je vypočítána podle metodiky **Common Vulnerability Scoring System** (CVSS) spravované organizací First [22]. Skóre závažnosti se nachází v intervalu <0, 10>, přičemž 0 je žádná, 0,1–3,9 nízká, 4,0–6,9 střední, 7,0–8,9 vysoká a 9,0–10,0 kritická zranitelnost.

Kybernetické útoky lze podle [16] rozdělit na základě rozsahu působení na útoky **cílené** a **plošné**. Plošné útoky jsou podle autora nejjednodušší, nejrychlejší a nejlevnější způsob průniku do systému. Autor dále uvádí, že útočníka v tomto případě zajímá pouze tzv. low hanging fruit neboli ovoce, které roste nízko a lze jej snadno utrhnout. Pokud útočník hned napoprvé neuspěje, tak si podle autora okamžitě hledá další cíl, protože ví, že brzy narazí na nedostatečně zabezpečený systém. Chování útočníka je podle autora racionální. Autor dále uvádí, že zavedením alespoň základní sady bezpečnostních opatření je možné většinu útočníků provádějících plošné útoky odradit. Cílené útoky se podle autora naopak zaměřují na konkrétní oběť. Ochrana před cílenými útoky je podle autora mnohem složitější, protože útočník soustředí veškerou svou pozornost na tuto jedinou oběť. Při cíleném útoku je podle autora důležité uspět napoprvé, aby útočník nevzbudil podezření, proto cílenému útoku předchází pečlivé plánování.

Stav, kdy dojde k realizaci určité hrozby a následnému zneužití určité zranitelnosti, se podle [16] nazývá **bezpečnostní událost**. Pokud tato událost může vést i k narušení dostupnosti informačního systému, případně důvěrnosti nebo integrity dat, jedná se podle autora o **bezpečnostní incident**. Podle NIST [11] je bezpečnostní událost změna v kybernetické bezpečnosti, která může mít dopad na organizační operace. Bezpečnostní incident autoři popisují jako událost, která skutečně nebo potenciálně ohrožuje důvěrnost, integritu nebo dostupnost informačního systému nebo informací, které systém zpracovává, ukládá nebo přenáší, nebo která představuje porušení nebo bezprostřední hrozbu porušení bezpečnostních zásad, bezpečnostních postupů nebo zásad přijatelného užívání.

Bezpečnostní incident má zpravidla i nějaký **dopad** na fungování napadené organizace a kvalitu služeb, které poskytuje. Podle NIST [11] je dopad definován jako rozsah škody, kterou lze očekávat v důsledku neoprávněného zveřejnění informací, neoprávněné změny informací, neoprávněného zničení informací, ztráty informací nebo nedostupnosti informačního systému. ENISA [17] dopad definuje velmi stručně jako výsledek nežádoucího incidentu.

Existence určité hrozby představuje podle [16] **kybernetické riziko**. Každé riziko by podle autora mělo být analyzováno a mělo by být rozhodnuto o způsobu jeho zvládání, typicky pomocí **bezpečnostních opatření**, která se dále dělí na opatření organizační a opatření technické povahy.

Informační aktiva, na která se dá útočit, jsou podle [16] označována termínem **povrch útoku**. Podle NIST [11] je povrch útoku definován jako sada bodů na hranici systému, systémového prvku nebo prostředí, do kterého se útočník může pokusit vstoupit, způsobit na ně vliv nebo z nich extrahovat data. Pojmem **vektor útoku** se podle [16] označuje způsob, jakým je útok veden. Podle autora se jedná o způsob, jakým dochází ke zneužití zranitelnosti a kompromitaci cílového systému.

Hacking si podle [1] vysloužil negativní pověst tím, že bývá zejména v médiích často spojován s kybernetickými útoky. Kromě hackerů, kteří se zabývají kybernetickou kriminalitou, však podle autora existují i etičtí hackeři. Jak autor dále uvádí, tento termín se poprvé objevil koncem 70. let 20. století, kdy vláda USA najala expertní skupiny zvané *„červené týmy“* za účelem prověření zabezpečení vládního počítačového systému.

Hacker je podle [1] člověk, který je schopný vstoupit do systému, aniž by měl přidělená potřebná přístupová oprávnění. Podle NIST [11] se jedná o neoprávněného uživatele, který se pokouší získat nebo získá přístup k informačnímu systému. Použití termínu hacker pro označení kybernetického zločince je podle [1] sice nevhodné, je však v tomto smyslu běžně používáno. Podle autora je hacker osoba s vysokou úrovní počítačové gramotnosti a jde především o kybernetického experta, ať už využívá své znalosti legálně nebo nelegálně. Podle autora lze hackery kategorizovat na základě jejich úmyslů následovně:

- **White hat hacker** využívá své znalosti k legální činnosti. Je to etický hacker. Jeho primární funkcí je ověření slabých míst a zranitelností informačních a komunikačních systémů za účelem ochrany a obrany před kybernetickými útoky.

- **Black hat hacker** využívá své znalosti k nelegální činnosti. Do této kategorie patří nejznámější typ hackerů páchajících trestnou činnost.
- **Gray hat hacker** je kategorie hackerů, u kterých nelze jednoznačně určit, jestli jsou etičtí nebo neetičtí.

Toto rozdělení je však podle [1] poněkud sporné, protože v některých případech nelze kategorii jednoznačně určit, jak je uvedeno výše. Firmy a organizace mohou podle autora využívat služeb jednoho etického hackera nebo celého týmu. Podle [23] může být tým hackerů ještě dále rozdělen na:

- **Red team**, někdy nazývaný též Tiger team. Hlavním cílem tohoto týmu je útok na informační a komunikační systémy zadavatele. Snahou týmu je najít zranitelnosti a pokusit se je využít pro získání přístupu k aktivům.
- **Blue team** se stará o ochranu a obranu proti Red teamu a zároveň i proti skutečným kybernetickým hrozbám a útokům.
- **Purple team** je ve skutečnosti spíše metodologie, než skutečný tým. Jedná se o virtuální tým složený ze členů červeného a modrého týmu. Cílem tohoto týmu je zajištění kooperace, průběžného přenosu zpětné vazby a znalostí tak, aby se maximalizovaly schopnosti obrany proti kybernetickým útokům.

Etičtí hackeři jsou podle [1] také často označováni jako **penetration testers**, nebo zkráceně **pen testers**, což ještě lépe vystihuje podstatu odhalení a odstranění zranitelností. Podle NIST [11] je **penetrační testování** definováno jako testování zabezpečení, ve kterém hodnotitelé napodobují reálné útoky ve snaze identifikovat způsoby, jak obejít bezpečnostní funkce aplikace, systému nebo sítě. Autoři dále uvádějí, že penetrační testování často zahrnuje provádění skutečných útoků na skutečné systémy a data pomocí stejných nástrojů a technik, které používají skuteční útočníci. Většina penetračních testů podle autorů zahrnuje hledání kombinací zranitelností v jednom nebo více systémech, které lze použít k získání většího rozsahu přístupu, než jakého by bylo možné dosáhnout prostřednictvím jediné zranitelnosti. Nevýhodou procesu penetračního testování může podle [1] být možnost podcenění nebo zneužití nalezených zranitelností pracovníky pověřenými testováním, proto je doporučeno zapojit do procesu také externí pracovníky.

Cyber Kill Chain (CKC) definuje podle [24] pořadí úloh, kterými musí útočník během útoku projít. Podle [25] byl koncept Kill Chain původně vyvinut v roce 2007 Americkým ministerstvem obrany pro vojenské účely. V roce 2010 autor tento koncept převzal a upravil pro využití v oboru kybernetické bezpečnosti. Model se podle [25, 26] skládá z následujících fází:

1. **Reconnaissance** (Průzkum): Průzkum, identifikace a stanovení cílů. Více informací o Reconnaissance viz kapitola 2.3.
2. **Weaponization** (Ozbrojení): V této fázi je vytvořen payload, typicky pomocí automatizovaného nástroje (weaponizer). Jako payload často slouží datové soubory aplikací, zejména Adobe Portable Document Format (PDF) nebo dokumenty Microsoft Office. Cílem útočníka je vytvořit payload tak, aby bylo riziko jeho detekce a odhalení bezpečnostními analytiky nebo řešeními co nejnižší.
3. **Delivery** (Doručení): Přenesení payload do cílového prostředí. Podle pozorování týmu Lockheed Martin Computer Incident Response Team (LM-CIRT) [25] patřily v letech 2004–2010 mezi nejpoužívanější tyto tři způsoby doručení: přílohy e-mailů, webové stránky a přenosná paměťová média USB. Podle [26] bývá k doručení payloadu často zneužit vztah důvěry mezi třetí stranou a cílovou organizací.
4. **Exploitation** (Zneužití): Po doručení payloadu na zařízení oběti je spuštěn exploit. Během této fáze se útočník nejčastěji zaměřuje na zranitelnost aplikace nebo operačního systému. Alternativně útočník může zneužít zranitelnost uživatele.
5. **Installation** (Instalace): Instalace trojského koně nebo zadních vrátek s cílem zajištění trvalého přístupu k zařízení oběti.
6. **Command and control (C2)** (Velení a řízení): V této fázi útočník naváže komunikaci s napadeným hostitelem přes některý z C2 serverů.
7. **Actions on objectives** (Akce na cíle): Teprve po úspěšném průchodu prvních šesti fází může útočník podniknout kroky k dosažení svých cílů. Mezi nejobvyklejší cíle patří Exfiltrace, narušení integrity nebo dostupnosti dat.

U nejpokročilejších kybernetických útoků podle [1] trvá dlouhou dobu, než způsobí nějakou škodu nebo jsou objeveny. Z toho podle autora vyplývá, že útočníci postupují podle dobře strukturovaných a připravených plánů. Klíčem k zajištění úspěšné ochrany je podle [24] pokrytí všech fází Cyber Kill Chain. Zároveň však podle autorů

platí, že jediné úspěšné protiopatření může narušit celý řetězec útočníka. Autoři dále uvádějí, že prostřednictvím včasného provedení protiopatření je možné získat převahu nad útočníkem. Model Cyber Kill Chain slouží podle [25] jako vodítko při analýze útoku. Součástí této analýzy je podle autorů pochopení důvodů útoku, jednotlivých kroků a motivace útočníka. Autoři dále uvádějí, že díky modelu mohou být racionálně vyhodnocena možná rizika a následně přijata adekvátní bezpečnostní opatření sloužící ke zmírnění rizik, včetně inteligentního stanovení jejich priority.

OODA loop je podle [24] označením strategie, kterou vyvinul plukovník letectva Spojených států John Boyd. Podle autorů byla tato strategie, stejně jako v případě Cyber Kill Chain, původně vyvinuta pro vojenské účely, později se však začala využívat také v dalších oborech včetně kybernetické bezpečnosti. Autoři uvádějí, že se jedná o uzavřenou smyčku sestávající z kroků Observe → Orient → Decide → Act (pozorování → orientace → rozhodnutí → akce). Princip podle autorů spočívá v tom, že smyčka musí být dokončena dříve, než se totéž podaří protivníkovi. Podle autorů smyčka OODA podporuje agilitu a rychlost reakce na kroky protivníka. Na základě odhalení záměrů útočníka a vyhodnocení jednotlivých kroků CKC je podle autorů umožněno vytvoření taktické výhody, čímž je zajištěna převaha obrany nad útočníkem.

2.2 Bezpečnostní opatření

Tato kapitola je zpracována podle **Zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)** [27] a podle **Vyhlášky ze dne 21. května 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)** [18], která je prováděcím předpisem k zákonu. Zákon byl vydán v reakci na zhoršující se situaci v kyberprostoru ještě před přijetím Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii [28], vycházel tedy z řady norem ISO/IEC 27000, což je mezinárodně platný standard, který definuje požadavky na systém řízení bezpečnosti informací. Zákon rozděluje podle § 5 **Bezpečnostní opatření** na **Organizační opatření** a **Technická opatření**. Ve vyhlášce jsou uvedeny konkrétní metodické postupy k zajištění bezpečnostních opatření. Následuje přehled vybraných bezpečnostních opatření relevantních k této práci. Paragrafy v následujících podkapitolách odkazují na výše uvedenou vyhlášku.

2.2.1 Organizační opatření

§ 3 **Systém řízení bezpečnosti informací** (SŘBI) určuje následující povinnosti. Je nutné stanovit rozsah SŘBI, tj. organizační části a aktiva, kterých se SŘBI týká. Povinná osoba dále musí stanovit cíle SŘBI, zavést přiměřená bezpečnostní opatření, řídit rizika, vytvořit a schválit bezpečnostní politiku v oblasti SŘBI, zajistit provedení auditu kybernetické bezpečnosti, zajistit pravidelné vyhodnocování účinnosti SŘBI, průběžně identifikovat a následně řídit významné změny, aktualizovat SŘBI včetně dokumentace (např. na základě zjištění auditů kybernetické bezpečnosti) a řídit provoz a zdroje SŘBI.

§ 4 **Řízení aktiv** zavádí povinnost stanovení metodiky pro identifikaci aktiv. Povinná osoba identifikuje a eviduje primární a podpůrná aktiva a vazby mezi nimi, určí a eviduje garanty aktiv, stanovuje a zavádí pravidla ochrany pro jednotlivé úrovně aktiv, stanovuje přípustné způsoby používání aktiv a určuje způsob likvidace dat, provozních údajů, informací atd.

§ 5 **Řízení rizik** určuje v návaznosti na § 4 následující povinnosti. Povinná osoba stanovuje metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik. Dále s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti, provádí hodnocení rizik, přičemž zohlední relevantní hrozby a zranitelnosti a posoudí možné dopady na aktiva, zpracovává zprávu o hodnocení rizik, zpracovává prohlášení o aplikovatelnosti, zpracovává a zavádí plán zvládání rizik a zavádí bezpečnostní opatření.

§ 6 **Organizační bezpečnost** stanovuje následující povinnosti: zajistit stanovení bezpečnostní politiky a cílů SŘBI, zajistit integraci SŘBI do procesů povinné osoby, zajistit dostupnost zdrojů potřebných pro SŘBI, informovat zaměstnance o významu SŘBI, zajistit podporu k dosažení zamýšlených výstupů SŘBI, vést zaměstnance k rozvíjení efektivity SŘBI, prosazovat neustálé zlepšování SŘBI, podporovat osoby zastávající bezpečnostní role, zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role, a zajistit jim příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a zajistit jejich mlčenlivost. Dále je nutné zajistit testování plánů kontinuity činností, obnovy a procesu spojených se zvládáním kybernetických bezpečnostních incidentů. V rámci SŘBI je rovněž nutné určit složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související se SŘBI. Dále je nutné zajistit také zastupitelnost jednotlivých rolí. Konkrétně se se jedná o role:

- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti
- Garant aktiva
- Auditor kybernetické bezpečnosti

§ 7 **Bezpečnostní role** definuje v návaznosti na § 6 odpovědnosti v rámci SŘBI, požadavky na vzdělání a odbornou způsobilost osob zastávajících jednotlivé role. **Manažer kybernetické bezpečnosti** je bezpečnostní role odpovědná za systém řízení bezpečnosti informací. Jeho povinností je pravidelné informování vrcholového vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti a stavu SŘBI. **Architekt kybernetické bezpečnosti** je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému. **Garant aktiva** je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnosti aktiva. **Auditor kybernetické bezpečnosti** je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti. Auditor kybernetické bezpečnosti zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné, a nesmí být pověřen výkonem jiných bezpečnostních rolí.

§ 8 **Řízení dodavatelů** definuje další důležité požadavky v boji proti kybernetickým hrozbám. Mnoho významných bezpečnostních incidentů, které způsobily škody globálním podnikům, bylo podle [1] způsobeno zranitelností nalezenou v dodavatelském řetězci. Proto je nutné při navázání spolupráce s dodavatelem stanovit pravidla, která zohledňují požadavky SŘBI. V rámci výběrového řízení a před uzavřením smlouvy je nutné provést hodnocení rizik souvisejících s plněním předmětu výběrového řízení. V rámci uzavíraných smluvních vztahů je nutné stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření. Poté je nutné provádět pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění a pamatovat zejména na otázky ochrany sítí, systémů a dat, zásady pro likvidaci dat, dodržování pravidel a kontroly zaměstnanců. Součástí implementace procesu řízení dodavatelů by měla být i pravidelná aktualizace hodnocení rizik a co největší integrace s koordinací incidentů a monitorováním hrozeb.

§ 9 **Bezpečnost lidských zdrojů** je rovněž nedílnou součástí SŘBI. Každý řetěz je silný jen tak, jak silný je jeho nejslabší článek. Proto je nutné stanovit plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí. V souladu s tímto plánem je nutné poučit uživatele,

administrátory, osoby zastávající bezpečnostní role a dodavatele o jejich povinnostech a o bezpečnostní politice. Dále je potřeba zajistit vstupní a pravidelná školení výše uvedených osob. Pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí je nutné zajistit pravidelná odborná školení. V rámci školení zaměstnanců je podle [1] důležité zmínit především nutnost používat silná hesla. Podle autora by dále zaměstnanci měli vědět, jak identifikovat podezřelý e-mail nebo hovor. Podle autora je také vhodné seznámit zaměstnance s bezpečnostní politikou, dbát na kontrolu jejího dodržování a určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel. V neposlední řadě je podle autora vhodné rozvíjet týmovou atmosféru a vyzvat všechny členy týmu, aby si vzájemně pomáhali a přispěli tím ke zlepšení organizační bezpečnosti.

§ 12 **Řízení přístupu** k informačnímu a komunikačnímu systému je prováděno na základě provozních a bezpečnostních potřeb s využitím skupin a rolí. Každý uživatel a administrátor obdrží přístupová práva a oprávnění a jedinečný identifikátor. Řízeny jsou rovněž technické účty. Povinná osoba přijímá opatření, aby nedošlo ke zneužití těchto údajů neoprávněnou osobou. V rámci řízení přístupu je podle [1] nutné důsledně definovat a také dodržovat omezení přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce. Podle autora by ke všem funkcím nástrojů, systémů a sítí měli mít přístup výhradně administrátoři. Ostatní uživatelé by podle autora měli mít přístup pouze k funkcím, datům a oblastem souvisejícím s jejich prací. Autor dále uvádí, že v rámci řízení přístupu by mělo být pamatováno i na bezpečnostní opatření pro bezpečné používání mobilních zařízení a jiných technických zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve své správě. Povinná osoba dále omezí a kontroluje používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly, přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu a provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí. Přidělování a odebírání přístupových práv je nutné dokumentovat. Technická opatření řízení přístupu dále upravuje § 19 a § 20.

§ 14 **Zvládání kybernetických bezpečnostních událostí a incidentů** nařizuje zavedení procesu detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů. Tento proces je realizován přidělením odpovědnosti a stanovením postupů pro detekci a vyhodnocování

kybernetických bezpečnostních událostí a incidentů a koordinaci a zvládání kybernetických bezpečnostních incidentů. Dále je nutné definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu. Povinná osoba zajistí detekci kybernetických bezpečnostních událostí pomocí zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů, viz § 22. K útokům může podle [1] dojít kdykoli a kdekoli, proto je nezbytné implementovat také detekci kybernetických bezpečnostních událostí, viz § 23. Nástroj pro detekci kybernetických bezpečnostních událostí (Security Information and Event Management, zkráceně SIEM) podle autora zajistí ověření a kontrolu přenášených dat v rámci komunikační sítě, mezi komunikačními sítěmi a na perimetru komunikační sítě. Autor dále uvádí, že nástroj zajistí blokování nežádoucí komunikace. Díky tomu je podle autora možné včas zachytit podezřelou aktivitu uživatele nebo datové anomálie, které mohou naznačovat probíhající útok, a předejít tak škodám nebo je aspoň minimalizovat. Povinná osoba musí dále zajistit sběr a vyhodnocování kybernetických bezpečnostních událostí, viz § 24.

§ 15 **Řízení kontinuity činností** definuje povinnost stanovení práv a povinností administrátorů a osob zastávajících bezpečnostní role. Dále stanovuje povinnost vyhodnotit a dokumentovat možné dopady kybernetických bezpečnostních incidentů a posoudit možná rizika související s ohrožením kontinuity činností. Součástí SŘBI je předpoklad, že všechny implementované funkce obrany a ochrany nikdy nemohou být 100% účinné. Proto je nutné mít v záloze dobře navržený a komplexní plán reakce, který umožní rychlou a efektivní reakci v případě výskytu bezpečnostního incidentu. Plán by měl mimo jiné definovat vhodnou cestu eskalace. Administrátoři a osoby zastávající bezpečnostní role by měli být okamžitě informováni. Povinná osoba na základě výstupu hodnocení rizik a analýzy dopadů stanoví cíle řízení kontinuity činností formou určení minimální úrovně poskytovaných služeb, doby obnovení chodu a bodu obnovení dat ve smyslu časového období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání. Plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému a souvisejících služeb musí být pravidelně aktualizovány a testovány. Podrobnosti o zajištění úrovně dostupnosti informací jsou uvedeny v § 27.

§ 16 **Audit kybernetické bezpečnosti** je základním kamenem SŘBI. Bez znalosti aktuálního stavu je podle [1] nemožné vybudovat adekvátní obranu a ochranu. Pravidelná hodnocení kybernetické bezpečnosti jsou podle autora klíčovou součástí

každého dobrého bezpečnostního programu. Silné stránky podle autora potvrzují úspěšnost ochrany a obrany, slabé stránky naopak upozorňují na to, co je potřeba zlepšit. Jak autor dále uvádí, důkladná analýza by měla rovněž přispět ke stanovení priorit. Po dokončení auditu kybernetické bezpečnosti lze přistoupit k plánování a provádění dalších kroků SŘBI. V rámci auditu kybernetické bezpečnosti je nutné provést kontrolu dodržování bezpečnostní politiky včetně zdokumentování, provést přezkoumání technické shody a posoudit soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určit případná nápravná opatření pro zajištění souladu. Audit je nutné provádět při významných změnách a nadále v pravidelných intervalech. Alternativně je možné v odůvodněných případech provádět audit průběžně po systematických celcích.

2.2.2 Technická opatření

§ 17 **Fyzická bezpečnost** je podle [1] stejně důležitá jako bezpečnost digitálních aktiv. Pozornost je podle autora nutné věnovat mimo jiné následkům krádeží zařízení. Pokud firma používá mobilní zařízení, například notebooky, tablety nebo jiná zařízení včetně BYOD, tak je podle autora nutné chránit data na těchto zařízeních vzdáleně. V ideálním případě dochází podle autora pouze ke sledování těchto zařízení, případně k vynucení politik. Autor dále uvádí, že v případě odcizení zařízení musí existovat možnost uzavření spojení, případně vymazání dat uložených na zařízení. V mobilních zařízeních by podle autora měly být aktivovány kryptografické prostředky.

V případě fyzického vniknutí do budovy nebo datového centra může podle [1] útočník získat nejen přístup k informačnímu a komunikačnímu systému, ale také k obchodnímu tajemství, schématům infrastruktury, případně dalším užitečným informacím. Proto je podle autora nutné stanovit fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému a dále používat osvědčené metody prevence, jako například přístupové systémy (ACS), poplachové zabezpečovací a tísňové systémy (PZTS), kamerové systémy (CCTV) a zásady sledování návštěv. Kromě toho je podle autora vhodné seznámit zaměstnance s ochranou svého prostředí nejen v kanceláři, ale zejména mimo kancelář.

§ 18 **Bezpečnost komunikačních sítí** definuje povinnosti, které je nutné dodržet při návrhu a provozování komunikačních sítí. Povinná osoba musí zajistit segmentaci komunikační sítě a řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě. Dále musí být zajištěna důvěrnost a integrita dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií, a to pomocí kryptografie. Dále je třeba zajistit aktivní blokování nežádoucí komunikace. Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty je nutné využít nástroj, který zajistí ochranu integrity komunikační sítě.

Kromě výše uvedených technických opatření existují i další, která ve vyhlášce o kybernetické bezpečnosti explicitně uvedená nejsou. Přesto je vhodné na tato opatření pamatovat, protože mohou výrazně přispět ke zvýšení kybernetické bezpečnosti v organizaci. Mezi nejvýznamnější z nich patří následující.

Podle [1, 29] je nezbytné **udržovat software aktuální**. Starší verze aplikací mohou být podle autorů zranitelné vůči zero-day útokům a exploitům, které mohou krást informace, pronikat do sítí a způsobit vážné škody. Proto je podle autorů vhodné zaměřit se především na programy, které se neaktualizují automaticky. Autoři však zároveň upozorňují na nutnost kontrol automaticky aktualizovaných programů, protože automatické aktualizace mohou selhat. Podle autorů by kontroly měly být prováděny pravidelně, alespoň jednou za dva týdny. Autoři dále uvádějí, že je vhodné zvážit implementaci procesů správy zranitelností, které hledají chybějící záplaty a zranitelná místa.

Externí analýza hrozeb je podle [1, 29] rovněž důležitou součástí efektivního programu kybernetické bezpečnosti. Tato analýza podle autorů spočívá ve sběru dat, informací, bezpečnostních hrozeb a aktérů hrozeb. Autoři uvádějí, že díky monitorování Darkwebu a dalším metodám lze lépe porozumět tomu, jaké útoky jsou plánovány, které zločinecké sítě je organizují a jaký je plán útoku. Na základě těchto informací je podle autorů možné zmírnit škodlivé události v kyberprostoru. Dále je podle autorů možné identifikovat přihlašovací údaje nebo informace, které se už dostaly na černý trh. Autoři dále uvádějí, že na základě těchto znalostí lze vyvinout přesnou obrannou strategii.

2.2.3 Nový zákon o kybernetické bezpečnosti

V současné době je připravován nový zákon o kybernetické bezpečnosti (dále jen nový ZoKB) včetně prováděcích předpisů (vyhlášek). Tato podkapitola je zpracována podle návrhu zákona zveřejněného na webových stránkách NÚKIB [30]. Nový

ZoKB musí aplikovat do české legislativy směrnici Evropského parlamentu a Rady (EU) 2022/2555 (dále jen směrnice NIS2) [15]. Tato směrnice nařizuje všem členským státům EU přijmout a zveřejnit opatření nezbytná pro dosažení souladu s touto směrnicí nejpozději do 17. října 2024. Směrnice NIS2 byla vytvořena z důvodu rychlé digitální transformace a stoupajícího počtu a rozsahu kybernetických hrozeb a útoků. Oproti stávající směrnici (EU) 2016/1148 [28] (dále jen směrnice NIS) je směrnice NIS2 přísnější. Rozšiřuje se především rozsah povinných osob (tj. subjektů, společností a státních organizací), které budou nově spadat do regulace. Tím bude zajištěno komplexní pokrytí odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu. Podle odhadů NÚKIB bude v ČR spadat pod nový ZoKB minimálně 6 000 povinných osob ve srovnání s cca 400 povinnými osobami spadajícími pod stávající zákon 181/2014 Sb., o kybernetické bezpečnosti [27] (dále jen stávající ZoKB). Rozšířena budou regulovaná odvětví (např. o odvětví odpadového hospodářství), stávající regulovaná odvětví budou rozšířena o nové regulované služby (např. odvětví digitální infrastruktury bude rozšířeno o služby cloud computing). Novinkou je také povinné vzdělávání vrcholového vedení organizace a větší odpovědnost managementu za zajišťování kybernetické bezpečnosti v organizaci.

NÚKIB dne 25. ledna 2023 zveřejnil první návrh nového ZoKB (označený jako v1.0). Tento návrh mohl být do 12. března včetně připomínkován veřejností. Po zpracování připomínek veřejnosti zákon dále musí projít legislativním procesem, který byl zahájen 19. června 2023 meziresortním připomínkovým řízením. Dá se tedy předpokládat, že se návrhy předpisů mezitím změnily. Nebylo však možné slevit z minimálních požadavků definovaných ve směrnici NIS2. Nový ZoKB musí vstoupit v účinnost nejpozději 17. října 2024. Při návrhu nového ZoKB NÚKIB reflektoval zkušenosti a poznatky související s aplikací stávajícího ZoKB. Cílem autorů bylo mimo jiné zjednodušit některé instituty. To se týká zejména § 3 stávajícího ZoKB, který stanovuje regulované orgány a osoby. Organizace s více systémy se teoreticky mohla vyskytnout až ve třinácti různých kategoriích, což znesnadňovalo pochopení zákona, proto návrh nového ZoKB zavádí jediný typ povinné osoby, nazvaný *„poskytovatel regulované služby“*.

Dále jsou nově zavedeny dva režimy, které se liší rozsahem povinností. Bezpečnostní opatření stanovená pro režim vyšších povinností vycházejí z obsahu stávající vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti [18]. Zde dochází pouze k minimálním změnám, jedná se spíše o upřesnění. Cílem zavedení režimu nižších povinností je ulehčit menším společnostem od přísných pravidel. Posouzení, zda je organizace

poskytovatelem regulované služby a do jakého režimu povinností spadá, lze určit na základě přesně definovaných kritérií. Jedná se o kritéria pro identifikaci regulované služby (spočívající v tom, že organizace provede tzv. samoidentifikaci, a pokud splňuje kritéria, sama provede registraci u NÚKIB) a kritéria pro určení regulované služby (která spočívají v tom, že NÚKIB v rámci správního řízení s organizací posoudí, zda došlo k naplnění kritérií). Jedna organizace (vymezená identifikačním číslem osoby, tzv. IČO) může spadat pouze do jednoho z těchto dvou režimů. Pokud organizaci lze teoreticky zařadit do režimu nižších i vyšších povinností zároveň, nebo poskytuje-li organizace více služeb, z nichž některé spadají do režimu nižších povinností a některé do režimu vyšších povinností, pak je organizace vždy zařazena do režimu vyšších povinností.

Zásadním krokem v rámci právní úpravy je stanovení rozsahu řízení kybernetické bezpečnosti. Pro komplexní ochranu regulované služby je nutné řešit kybernetickou bezpečnost na úrovni celé organizace, nebo alespoň v té části organizace, která poskytuje regulované služby. Návrh nového ZoKB obsahuje zpřesnění podmínek stanovení rozsahu řízení kybernetické bezpečnosti a definuje následující presumpci. Pokud poskytovatel nestanoví rozsah řízení kybernetické bezpečnosti, tak se rozsahem rozumí celá organizace.

Pro režim vyšších povinností zůstává zachována povinnost hlásit NÚKIB všechny kybernetické bezpečnostní incidenty bez výjimky, a to bezodkladně po jejich detekci. Důvodem stanovení této povinnosti je skutečnost, že incident, který se z pohledu organizace může jevit jako bezvýznamný, může být důležitý v národním kontextu. Novinkou v režimu vyšších povinností je povinnost poskytovatele neprodleně informovat NÚKIB, zda nahlášený incident klasifikuje jako významný. Organizace spadající pod režim nižších povinností musí povinně hlásit jen ty incidenty, které vyhodnotí jako významné. Dále platí, že v obou režimech povinností se hlásí pouze ty incidenty, které mají původ v kybernetickém prostoru.

Pro hlášení incidentů má sloužit jednotná platforma nazvaná Portál NÚKIB. Hlavním důvodem pro vytvoření této platformy je snížení administrativní zátěže na straně regulovaných organizací i na straně NÚKIB. Přes portál bude možné provádět všechny standardizované úkony, například registraci relevantních organizací, hlášení kontaktních údajů pověřených zástupců organizací, hlášení kybernetických incidentů, provedení protiopatření nebo nápravného opatření, případně hlášení dodavatelů. Mezi základní principy navrhovaného řešení patří maximální automatizace

a samoobslužnost platformy. Návrh zákona počítá i s případnou nedostupností portálu, proto jsou u jednotlivých úkonů specificky vymezeny možné situace a náhradní způsoby komunikace. Provádění vybraných úkonů bude podmíněno autentizací relevantních osob. K autentizaci budou sloužit prostředky elektronické identifikace a kvalifikované systémy elektronické identifikace (například bankovní identita s ověřením prostřednictvím Národního bodu pro identifikaci a autentizaci). Do budoucna se předpokládá navázání užší spolupráce a komunikace přes portál zejména s inspektory (viz níže), případně s orgány posuzování shody v rámci certifikací v oblasti kybernetické bezpečnosti. Platforma by také měla umožňovat dobrovolné hlášení incidentů, hrozeb a zranitelností ze strany neregulovaných subjektů.

Způsob kontroly poskytovatelů regulované služby v režimu vyšších povinností se zásadně neliší od dosavadní praxe. Kontroly tedy bude provádět i nadále NÚKIB prostřednictvím svých zaměstnanců. Kontroly poskytovatelů regulované služby v režimu nižších povinností budou provádět tzv. inspektoři. Kontrolovaná organizace má povinnost si zajistit kontrolu inspektorem v pravidelných intervalech a nese i náklady na provedení této kontroly. Osoba vykonávající funkci inspektora bude muset splňovat podmínky vymezené navrhovaným zákonem a navazující vyhláškou o inspektorech, kromě toho si musí zajistit u NÚKIB autorizaci k výkonu kontrolní činnosti. Nad činností inspektorů vykonává dohled NÚKIB, přičemž v odůvodněných případech má pravomoc provést kontrolu u poskytovatele regulované služby v režimu nižších povinností, případně pověřit k provedení kontroly inspektora. V případě zjištění nedostatků je NÚKIB oprávněn uložit kontrolované organizaci nápravná opatření k odstranění zjištěných nedostatků. Tento princip je obdobou § 24 stávajícího ZoKB. Ve vymezených případech může NÚKIB přistoupit k vydání výstrahy, která může informovat veřejnost mimo jiné o porušování určitých povinností daných zákonem o kybernetické bezpečnosti.

Mezi navrhované sankční prostředky patří zejména pokuty. Výše pokut vychází převážně z požadavků směrnice NIS2, nebo alespoň řádově odpovídá výši pokut stanovených touto směrnicí. Pro sankce platí následující principy, měly by být účinné, přiměřené a odrazující a také by měly zohledňovat okolnosti každého případu, zároveň však nesmí být likvidační. V návrhu nového ZoKB jsou stanoveny pouze horní limity pokut. Kromě pokut počítá návrh zákona s tzv. jinými správními tresty. Může se jednat například o pozastavení platnosti certifikace nebo pozastavení výkonu funkce. Tyto tresty lze uplatnit pouze u poskytovatelů regulovaných služeb v režimu vyšších

povinností. K pozastavení platnosti certifikace může dojít například v případě, kdy NÚKIB uložil poskytovateli regulované služby povinnost odstranit nedostatky zjištěné při kontrole, a poskytovatel tuto povinnost nesplnil. Pozastavení výkonu řídící funkce fyzické osobě je nejzazší sankční prostředek. O této sankci však může rozhodnout jedině soud na základě návrhu podaného NÚKIB. Důvodem návrhu by mohlo být opakované nebo závažné porušení povinností při výkonu řídící funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí NÚKIB.

Nový ZoKB je více zaměřen na vzájemnou spolupráci NÚKIB a dalších organizací. Nejedná se však jen o spolupráci na národní úrovni, nezbytná je rovněž spolupráce na mezinárodní úrovni, a to v rámci EU i mimo EU. Spolupráce je vyžadována například při výkonu kontrol subjektů, které poskytují služby na území České republiky nebo zde mají infrastrukturu k poskytování těchto služeb, ale díky umístění své hlavní provozovny spadají do působnosti kompetentních orgánů jiného členského státu. V případě národní úrovně se jedná zejména o spolupráci s provozovatelem Národního CERT, Úřadem pro ochranu osobních údajů, Českou národní bankou, Generálním ředitelstvím Hasičského záchranného sboru a dalšími orgány. V některých případech jsou podmínky spolupráce nastaveny specificky, aby měl NÚKIB přístup k informacím nezbytným pro posouzení naplnění kritérií regulovaných služeb. Jedná se například o spolupráci s Generálním finančním ředitelstvím nebo Ministerstvem spravedlnosti ČR. Do budoucna lze předpokládat nastavení mechanismů užší spolupráce i s dalšími orgány. V případě mezinárodní spolupráce musí NÚKIB plnit informační povinnosti vůči orgánům a agenturám EU, a to v pravidelných intervalech. Jedná se zejména o spolupráci s Evropskou komisí a Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA). NÚKIB je také kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti.

Návrh zákona také upravuje stav kybernetického nebezpečí tak, aby byl více prakticky využitelný. Inspirace vychází z opatření obvyklých pro stavy nebezpečí v rámci krizového řízení obecně. Jedná se o opatření, která mohou zvrátit situaci významně ohrožující Českou republiku. Ve stavu kybernetického nebezpečí lze například nařídit povinným osobám pohotovostní režim (v rámci možností), nechat zpřístupnit neveřejnou telekomunikační síť pro použití NÚKIB nebo zakázat používání technických aktiv ohrožených incidentem.

Neméně důležitý je i proces prověřování rizikovosti dodavatelů. Bezpečnost produktů ICT nelze efektivně posoudit pouze technickými prostředky, proto musí být vyhodnocena důvěryhodnost dodavatelů. Navrhovaná úprava zákona by měla odhalovat rizikové dodavatele mimo jiné za pomoci proporciálního mechanismu prověřování. Prověřování dodavatelů bude provádět NÚKIB ve spolupráci s ministerstvy, zpravodajskými službami a dalšími orgány státu.

V návrhu zákona se počítá i s náklady potřebnými na zajištění kybernetické bezpečnosti v požadovaném rozsahu a kvalitě. Díky navýšení počtu subjektů, které budou nově spadat pod regulaci, budou náklady několikanásobně vyšší než dosud. Organizace proto musí počítat s navýšením rozpočtu nutného k zajištění souladu se zákonem. Náklady nelze přesně vyčíslit z pozice centrální autority, protože se u jednotlivých organizací mohou diametrálně lišit v závislosti na aktuálním stavu kybernetické bezpečnosti, požadovaném cílovém stavu atd. Náklady lze podle NÚKIB rozdělit do tří kategorií:

- Náklady na bezpečnostní opatření veřejné správy
- Náklady na bezpečnostní opatření soukromých společností
- Náklady na zajištění činnosti NÚKIB

Náklady na bezpečnostní opatření veřejné správy a náklady na zajištění činnosti NÚKIB jsou hrazeny z veřejných rozpočtů. Podle NÚKIB se náklady na zavedení a následné provádění bezpečnostních opatření hrazených z veřejných rozpočtů mohou orientačně pohybovat mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Přitom službu jako celek může zajišťovat i více jednotlivých informačních systémů.

2.3 Taktiky a techniky

Podkapitola je zpracována podle MITRE ATTACK Enterprise Matrix [31]. Kybernetický útok je velmi komplexní proces. V rámci tohoto procesu je možné, v závislosti na aktuálním vývoji situace, uplatnit více než deset různých taktik.

Taktika představuje rozhodování útočníka mezi jednotlivými fázemi útoku. Podstatou taktiky je zvolit v momentální situaci optimální řešení, jehož prostřednictvím útočník získá výhodnější pozici. **Taktika představuje důvod,** tedy **proč provést konkrétní akci**. Je to reprezentace momentálního dílčího cíle útočníka.

Technika je souhrnným označením pro nástroje, zařízení a postupy, které lze využít při útoku. **Technika představuje způsob,** tedy **jakou akci zvolit** pro dosažení taktického cíle. Podle [1] se hackeři vždy nejprve snaží využít a optimalizovat stávající techniky, protože vynalézat znovu kolo by bylo neefektivní. Tento přístup jim umožňuje provádět sofistikovanější a složitější útoky.

Hackeři při útoku obvykle využívají následují taktiky. U vybraných taktik relevantních k obsahu této práce je uveden i stručný přehled útočných technik:

- **Reconnaissance** (Průzkum): Útočník se nejprve snaží shromáždit co nejvíce informací o cíli. Tyto informace může následně použít k plánování budoucích operací nebo ke zvýšení efektivity útoku. Průzkum může zahrnovat následující techniky:
    - Aktivní skenování infrastruktury oběti.
    - Shromažďování informací o hostitelích (typicky serverech) v síti oběti, např. informace o hardware a software.
    - Shromažďování informací o identitě oběti, např. o přihlašovacích údajích, e-mailových adresách nebo jménech zaměstnanců.
    - Shromažďování informací o síti oběti, např. o doméně, DNS, vztazích důvěry, topologii sítě, IP adresách nebo použitém zabezpečení.
    - Shromažďování informací o organizaci, např. o fyzickém umístění, obchodních vztazích, pracovní době nebo rolích zaměstnanců.
    - Shromažďování informací pomocí spear phishingu.
    - Shromažďování informací z renomovaných uzavřených zdrojů, případně z Darkwebu.
    - Shromažďování informací z otevřených technických databází, např. DNS, WHOIS, digitálních certifikátů, CDN sítí.
    - Vyhledávání informací na otevřených webových stránkách, např. sociálních sítích, vyhledávačích, úložištích kódu.
    - Vyhledávání informací na webových stránkách oběti.
- **Resource Development** (Vývoj zdrojů): Dalším krokem před započetím útoku může být příprava zdrojů, které mohou útok umožnit nebo usnadnit. Jedná se o následující techniky:
    - Nákup nebo pronájem infrastruktury, např. domény, DNS serveru, VPN serveru, fyzického serveru, botnetu, webové služby nebo bezserverové architektury (kontejnerizace).

- Zajištění kompromitujících účtů, např. na sociálních sítích, dále e-mailových účtů nebo cloud computing účtů.
- Zajištění kompromitující infrastruktury s obdobnými možnostmi jako v případě nákupu či pronájmu infrastruktury.
- Vývoj škodlivého kódu, např. malware a exploitů včetně vytvoření digitálních certifikátů pro účely podepsání zpráv nebo kódu.
- Vytvoření účtů, např. na sociálních sítích, dále e-mailových účtů nebo cloud computing účtů.
- Nákup nebo krádež škodlivého kódu.
- Nasazení škodlivého kódu na výše uvedenou infrastrukturu.

- **Initial Access** (Prvotní přístup): Útočník se snaží dostat do sítě oběti. Toto je první fáze vlastního útoku. Útočník přitom může použít následující techniky:
  - Kompromitace při běžné práci uživatele. Uživatel může navštívit zranitelnou nebo kompromitovanou webovou stránku.
  - Zneužití veřejné aplikace. Často se jedná o webovou stránku, ale může jít i o databáze (např. SQL), standardní služby (např. SMB nebo SSH), protokoly pro správu (např. SNMP a Smart Install) či jakékoli jiné aplikace s otevřenými sokety přístupnými z internetu, např. služby související s provozem webových serverů.
  - Využití vzdálené služby. Jedná se například o VPN, Citrix, vzdálenou správu systému Windows, VNC a další přístupové mechanismy umožňující připojení k interním prostředkům podnikové sítě z externích umístění.
  - Útočník může jako vektor k získání přístupu použít počítačové příslušenství, síťový hardware nebo jiná výpočetní zařízení.
  - Mezi techniky prvotního přístupu patří rovněž phishing, zvláště pak spear phishing.
  - Další možností zajištění přístupu do sítě je replikace malware prostřednictvím vyměnitelných médií.
  - Přístup je možné získat také prostřednictvím dodavatelských řetězců. Například pomocí manipulace se závislostmi a vývojovými nástroji, které používá dodavatel. Mezi další možnosti patří kompromitace software, ať už ve fázi vývoje, při předání software odběrateli nebo ve formě

aktualizace. Další možností je manipulace s hardwarovými komponentami nebo úprava firmware.
    - Přístup prostřednictvím vztahu důvěry třetí strany. Takové spojení může být nechráněné nebo méně zabezpečené než standardní mechanismy získávání přístupu.
    - Zneužití přihlašovacích údajů stávajících účtů, např. výchozích účtů operačních systémů, lokálních účtů, doménových účtů nebo cloud computing účtů.
- **Execution** (Spuštění): Útočník se pokouší spustit škodlivý kód. Používá při tom například následující techniky:
    - Zneužití příkazového a skriptovacího interpretu k provádění příkazů, skriptů nebo binárních souborů se škodlivým kódem. Jedná se například o PowerShell, AppleScript, příkazový řádek Windows (CMD), Unix/Linux Shell (sh, bash, zsh atd.), Visual Basic, Python, JavaScript, příkazový řádek (CLI) síťového zařízení.
    - Zneužití příkazů pro správu kontejnerů.
    - Nasazení vlastního kontejneru připraveného útočníkem.
    - Zneužití chyb v zabezpečení klientských aplikací.
    - Zneužití mechanismů meziprocesové komunikace (IPC) pro lokální provedení kódu nebo příkazů. Jedná se například o zneužití Component Object Model (COM), Dynamic Data Exchange (DDE) nebo služeb XPC.
    - Zneužití nativního rozhraní API operačního systému. API poskytuje prostředky pro volání nízkoúrovňových služeb operačního systému v rámci jádra.
    - Zneužití naplánovaných úkolů nebo úloh, včetně možnosti plánování ve vzdáleném systému. Zneužít lze například nástroje At, Cron, Plánovač úloh ve Windows, časovače Systemd nebo plánování úloh v nástrojích pro orchestraci kontejnerů.
    - Zneužití bezserverových výpočetních, integračních a automatizačních služeb ke spuštění libovolného kódu v prostředích cloud computing.
    - Spuštění škodlivého kódu prostřednictvím načtení modulů sdílených knihoven DLL.
    - Zneužití nástrojů pro řízení nasazení software v podnikových sítích, např. SCCM, HBSS, Altiris atd.

    - Zneužití systémových služeb k jednorázovému, případně trvalému spuštění škodlivého kódu. Jedná se například o zneužití macOS Launchctl nebo správce služeb ve Windows.
    - Útočník také může spoléhat na spuštění škodlivého kódu uživatelem. Typickým příkladem je použití technik phishingu, přičemž uživateli může být doručen škodlivý odkaz, soubor nebo obrázek.
    - Zneužití služby WMI operačního systému Windows. Služba WMI umožňuje místní i vzdálený přístup. Vzdálený přístup zajišťuje model DCOM a služba WinRM.
- **Persistence** (Perzistence): V této fázi útočník hledá možnosti zachování přístupu k napadeným systémům. Přístup útočníka může být přerušen během restartování, při změnách oprávnění atd. Mezi techniky zajišťující perzistenci patří například nahrazení nebo úpravy legitimního kódu, včetně modifikací spouštěcího kódu.
- **Privilege Escalation** (Eskalace oprávnění): Eskalace oprávnění se skládá z technik, které útočník používá k získání přístupového oprávnění vyšší úrovně. Při vstupu do systému nebo sítě útočník často disponuje pouze neprivilegovaným přístupem. K plnění svých cílů však obvykle vyžaduje zvýšená oprávnění. K provedení eskalace oprávnění lze využít slabiny systémů, chyby v konfiguracích a zranitelná místa. Tyto techniky se často překrývají s technikami perzistence.
- **Defense Evasion** (Vyhýbání se obraně): Smyslem této taktiky je skrývání činností útočníka ve snaze zabránit odhalení útoku. Útočník může použít techniku odinstalování nebo vypnutí bezpečnostního softwaru. Dále může skrýt škodlivý kód (data a skripty) za pomoci kryptografických prostředků nebo zneužít názvy důvěryhodných systémových procesů.
- **Credential Access** (Přístup k přihlašovacím údajům): Útočník se snaží krást přihlašovací údaje uživatelů, tj. názvy účtů a hesla. K získání přihlašovacích údajů mohou být použity například následující techniky: keylogger nebo prostý výpis přihlašovacích údajů. Použití legitimních přihlašovacích údajů při pohybu v napadeném systému nebo síti může ztížit odhalení útočníka. Větší množství přihlašovacích údajů může přispět k urychlení nebo usnadnění útoku.

- **Discovery** (Objevování): V této fázi získává útočník znalosti o prostředí oběti. Techniky získání znalostí o systému a vnitřní síti útočníkovi pomáhají pozorovat prostředí a orientovat se v něm. Na základě těchto informací se pak může rozhodovat o dalším postupu. Mezi užitečné informace patří například zjištění, co se nachází v okolí vstupního bodu, a co lze ovládat. K dosažení tohoto postkompromitujícího cíle shromažďování informací se často používají nativní nástroje operačního systému.
- **Lateral Movement** (Laterální pohyb): Útočník používá techniky k zajištění vstupu do vzdálených systémů a sítí a jejich ovládání. Po získání přístupu je potřeba najít primární cíl útoku, a poté k němu získat přístup. V této fázi je často nutné projít přes více systémů a účtů. K pohybu v prostředí oběti mohou útočníkovi posloužit jeho vlastní nástroje pro vzdálený přístup nebo může využít nativní síťové nástroje a nástroje operačního systému. Použití nativních nástrojů může přispět ke zvýšení obtížnosti odhalení útočníka.
- **Collection** (Shromažďování): V rámci této fáze útočník shromažďuje data, která jsou relevantní při sledování cíle útoku. Po shromáždění dat často následuje Exfiltrace (krádež dat). Jako zdroje dat jsou obvykle využívány různé typy diskových jednotek, webové prohlížeče, zvuk, video a e-maily. Mezi techniky využívané v této fázi patří také pořizování snímků obrazovky a ukládání vstupu z klávesnice.
- **Command and Control (C2)** (Velení a řízení): V této fázi se útočník snaží ovládnout kompromitované systémy. Existuje mnoho způsobů, jak toho docílit. Útočník se obvykle pokouší napodobit normální provoz, aby se vyhnul odhalení. Dosažená úroveň utajení závisí na síťové struktuře a účinnosti obrany oběti.
- **Exfiltration** (Exfiltrace): Exfiltrace si klade za cíl krádež dat. Po úspěšném shromáždění dat je útočník často nejprve zkomprimuje a zašifruje. Přenos dat obvykle probíhá přes C2 kanál nebo přes alternativní kanál. Útočník může omezit šířku pásma z důvodu snížení podezření.
- **Impact** (Dopad): V této fázi se útočník snaží maximalizovat rozsah škod. Použité techniky mohou přispět k narušení dostupnosti nebo ohrožení integrity dat. To může mít dopad i na obchodní a provozní procesy. Obchodní procesy mohou být změněny tak, aby prospěly cílům útočníka, přestože na první pohled vypadají, že jsou v pořádku.

2.4 Kurzy a certifikace

Pro požadavky na vzdělání etického hackera neexistují podle [1] žádná oficiální kritéria. Jako základ lze podle autora doporučit bakalářský nebo magisterský titul v oboru informační bezpečnosti, informatiky, případně matematiky. Výhodou může podle autora být bezpečnostní prověrka, vojenský výcvik, zejména v oblasti zpravodajství, nebo certifikace o absolvování některého z kurzů v oboru kybernetické bezpečnosti. Pro zvládnutí ochrany a obrany před kybernetickými útoky je podle autora zásadní pochopit principy útoků. Jak autor dále uvádí, užitečné mohou být i znalosti z oboru forenzní analýzy kybernetických bezpečnostních incidentů. Princip školení etických hackerů spočívá podle autora v tom, že by měli být schopní, myslet stejně jako neetičtí hackeři, díky tomu mohou být při ochraně a obraně systému vždy o krok napřed.

Jednou z nejznámějších organizací, které nabízejí vzdělávání v oblasti kybernetické bezpečnosti po celém světě, je podle [1] americká společnost EC-Council [32]. Tato společnost byla založena v reakci na teroristické útoky z 11. září 2001. Nejoblíbenějším a nejuznávanějším kurzem této společnosti je podle [1] kurz Certified Ethical Hacker (CEH, aktuálně verze 12). Kurz lze absolvovat přímo v pobočkách EC-Council nebo v akreditovaných školících střediscích. Kurz je rozdělen do dvaceti modulů a obvykle trvá pět dní. Absolvovat jej lze online formou nebo osobně.

Součástí každého z modulů je podle [1, 32] rozsáhlé praktické laboratorní cvičení. Studenti mají k dispozici více než 3 500 předinstalovaných hackerských nástrojů a různých operačních systémů. Díky tomu získají praktické zkušenosti s nejběžnějšími bezpečnostními nástroji, nejnovějšími zranitelnostmi a operačními systémy. Studenti jsou v rámci kurzu seznámeni s taktikami, technikami a nástroji, které jsou běžně používány hackery nebo při penetračním testování. Získají také ucelený přehled technik, jakými jsou například skenování sítí či systémů v celopodnikovém rozsahu, tvorba malwaru a trojských koňů nebo pokročilé síťové útoky eliminující omezení VLAN. K vyučovaným praktikám patří i testování zabezpečení webových serverů a aplikací, techniky SQL Injection nebo útoky na mobilní platformy. Kurz je zakončen certifikační zkouškou, při které studenti prokazují zvládnutí vyučovaných technik. Zkouška je zahrnutá v ceně kurzu, skládá se ze 125 otázek s možností výběru více odpovědí a trvá čtyři hodiny. Pro získání certifikátu 312-50-ANSI CEH je nutná alespoň 70% úspěšnost.

Kromě CEH stojí podle [1] za pozornost rovněž program SANS GIAC [33], který nabízí certifikace například v následujících oborech:

- **GPEN**: Penetration Tester
- **GXPN**: Exploit Researcher and Advanced Penetration Tester
- **GCLD**: Cloud Security Essentials
- **GCPN**: Cloud Penetration Tester
- a dalších…

Další firmou, která podle [1] nabízí kurzy pro etické hackery, je Mile2 [34]. Jedná se například o tyto certifikace:

- **CVA**: Vulnerability Assessor
- **CPEH**: Professional Ethical Hacker
- **CPTE**: Penetration Testing Engineer
- **CPTC**: Penetration Testing Consultant

Podle [1] mohou být užitečné také certifikace zaměřené na proces forenzní analýzy, kde se studenti naučí používat vhodné nástroje a techniky k získávání důkazů a počítačových dat. Jedná se například o kurz Hacking Forensic Investigator (CHFI) společnosti EC-Council [32]. Mezi další významné forenzní certifikáty patří GIAC Certified Forensic Analyst (GCFA) [33].

Většina certifikací souvisejících s kybernetickou bezpečností podle [1] pokrývá obecné znalosti fyzické bezpečnosti. Jedná se například o následující certifikáty: Certified Information Systems Security Professional (CISSP) společnosti $(ISC)^2$ [35], Certified Information Security Manager (CISM) společnosti ISACA [36] nebo Security+ společnosti CompTIA [37]. Pro odborníky zabývající se zejména fyzickou bezpečností je k dispozici například certifikace Physical Security Professional (PSP) společnosti ASIS International [38].

3 Analýza nástrojů

Distribuce Kali Linux, původně nazývaná BackTrack Linux, byla vyvinuta pro profesionální penetrační testování a provádění bezpečnostního auditu [39]. Vychází z distribuce Debian a je dostupná jako open source. Funguje na široké škále hardwarových platforem, což výrazně rozšiřuje její použitelnost. Kali Linux obsahuje více než šest set předinstalovaných nástrojů určených pro různé úkoly spojené s kybernetickou bezpečností, konkrétně pro penetrační testování, výzkum zabezpečení, forenzní analýzu, reverzní inženýrství, řízení zranitelností atd. Nabízí podobné nástroje a techniky, které by použil hacker při kybernetickém útoku. Díky tomu je možné včas najít případné zranitelnosti a postarat se o nápravu.

Největší výhodou Kali Linux v porovnání s komerčními bezpečnostními řešeními je podle [40] jednoznačně cena. Komerční nástroje mohou být podle autora velmi drahé, zatímco Kali Linux je zdarma. Autor dále uvádí, že Kali Linux obsahuje open source verze mnoha komerčních bezpečnostních produktů. V případě zájmu je podle autora možné provést upgrade na plně funkční placené verze, a ty pak používat přímo v prostředí Kali Linux.

Kali Linux lze instalovat na běžné fyzické i virtuální počítače, případně na jednodeskové minipočítače Raspberry Pi nebo BeagleBone Black. Pro potřeby testování v terénu existuje platforma Kali NetHunter, což je varianta Kali Linux upravená pro zařízení s operačním systémem Android. Podle [39] je k dispozici 64bitová i 32bitová verze, doporučená je však 64bitová verze. Pro plnohodnotné využití s grafickým desktopovým prostředím Xfce4 je v sekci systémové požadavky doporučeno minimálně 2 GB RAM a 20 GB volného místa na disku. Pro běh některých velmi náročných aplikací (například Burp Suite) však nemusí stačit ani 8 GB RAM. Následuje stručný popis a možnosti využití vybraných nástrojů dostupných v distribuci Kali Linux.

3.1 Nmap

Podkapitola je zpracována podle dokumentace nástroje Nmap [41]. Nmap, celým názvem Network Mapper, je bezplatný open source nástroj určený pro průzkum sítě a provádění bezpečnostního auditu. Podle [1] byl Nmap představen v roce 1997, čímž se řadí mezi nestarší bezpečnostní nástroje. Navzdory svému stáří je však stále pravidelně aktualizován a dostává i nová vylepšení. Podle [41, 42] tento nástroj aktivně odesílá do sítě sondy v podobě surových paketů a zobrazuje informace o hostitelích na základě jejich reakcí. Na základě kategorizace hackerských taktik podle [31] lze

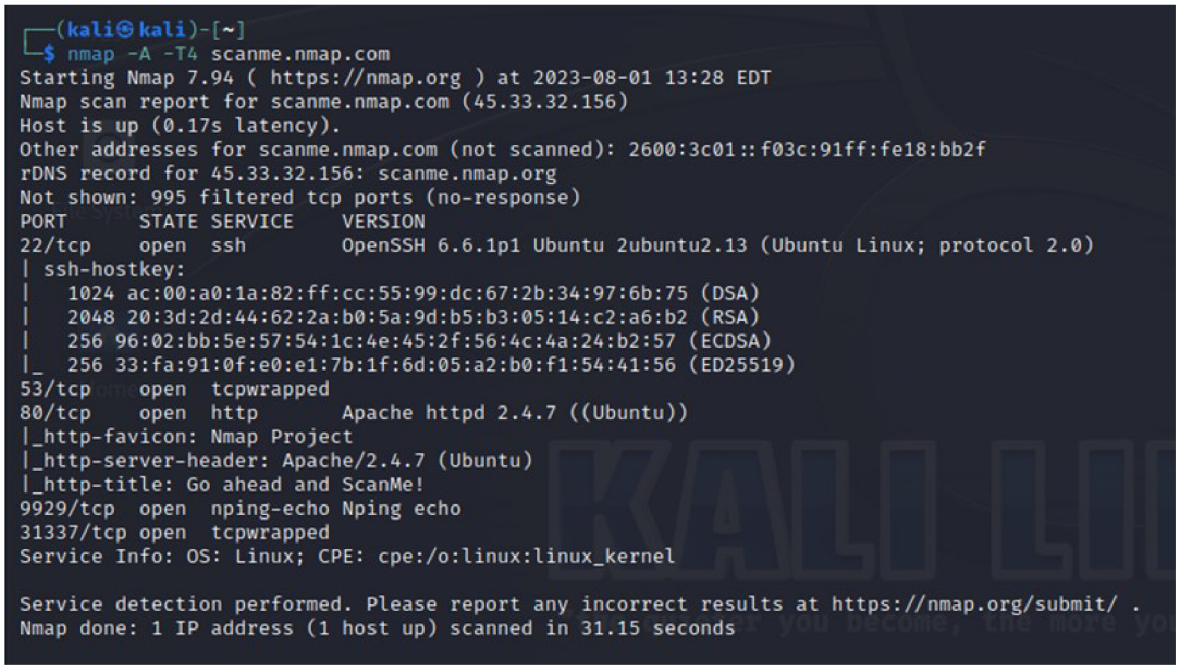
nástroj zařadit do kategorií průzkum a objevování (Reconnaissance a Discovery). Tuto skutečnost potvrzují i práce [43, 44], kde autoři nástroj zařadili do kategorie *„Information Gathering“*. Informace získané pomocí Nmap jsou následně využitelné pro komplexní bezpečnostní šetření. Nmap umožňuje určit:

- Kteří hostitelé v síti jsou dostupní.
- Jaké služby hostitelé poskytují (název a verze aplikace).
- Operační systémy hostitelů (název a verze OS).
- Typy použitých paketových filtrů / firewallů.
- Podporované IP protokoly, reverzní DNS názvy, typ zařízení, MAC adresy atd.

Díky těmto vlastnostem je Nmap využitelný pro provádění bezpečnostních auditů. Správci sítí jej však často využívají také pro inventarizaci, plánování upgradů nebo sledování dostupnosti hostitelů a služeb. Výstupem programu je seznam skenovaných hostitelů zahrnující informace využitelné při plánování útoku. Typ a rozsah informací o hostitelích je ovlivněn parametry zadanými při spuštění skenování.

Mezi klíčové informace, které lze pomocí Nmap získat, patří především tabulka 1 000 nejčastěji používaných portů, viz příklad na Obr. 3. Tato tabulka obsahuje číslo portu, použitý protokol, stav portu, název a verzi služby. Stav portu je klasifikován podle reakce na sondy prováděné programem Nmap a může nabývat hodnot: open, closed, filtered, unfiltered, open|filtered a closed|filtered. Podle stavu portu je možné určit, zda aplikace na cílovém počítači očekává na tomto portu spojení (naslouchá), případně zda je spojení blokováno filtrem, firewallem nebo jinou překážkou v síti. Nmap je nástroj určený pro práci v terminálu, ale existuje i rozšíření Zenmap umožňující práci v grafickém prostředí. Nmap je dostupný pro operační systémy macOS, Linux, OpenBSD, Solaris a Windows.

Parametry skenování jsou programu Nmap předávány ve formě argumentů příkazového řádku. Nejdůležitějším parametrem je specifikace cíle. Jako cíl lze uvést názvy hostitelů, IP adresy (konkrétních zařízení, celých sítí pomocí CIDR notation, případně jako rozsah od–do). Seznam cílů je možné programu předat také ve formě souboru. Pro lepší přehlednost jsou parametry programu Nmap sdruženy do skupin podle toho, kterou část skenování ovlivňují.



Obr. 3 Informace o hostiteli poskytnuté nástrojem Nmap.
Zdroj: Vlastní zpracování

První skupina parametrů se týká způsobu objevování hostitelů. Ve výchozím stavu Nmap nejprve ověřuje přítomnost hostitelů pomocí ICMP ping a skenuje pouze porty dostupných hostitelů. Zprávy ICMP ping jsou z bezpečnostních důvodů často blokovány administrátory. Proto Nmap nabízí parametr *-Pn* (No ping) pro vynucení skenování všech hostitelů. Tento způsob je však časově velmi náročný, a proto Nmap nabízí také širokou škálu alternativních způsobů zjištění dostupnosti hostitelů. Dále Nmap umožňuje použít explicitně zadané DNS servery místo systémových pomocí parametru *--dns-servers*.

Další skupina parametrů se týká technik skenování. Místo výchozího parametru *-sT* (TCP connect scan) je doporučeno použít parametr *-sS* (TCP SYN scan), protože je rychlejší a Nmap při něm komunikuje přímo s TCP stack místo systémového volání Connect. Pro skenování UDP portů slouží parametr *-sU* (UDP scan). Skenování UDP portů je výrazně pomalejší, než skenování TCP portů, přesto je doporučeno jej provést, protože výskyt UDP služeb, které je možné zneužít, je poměrně častý. Oba tyto parametry vyžadují spuštění Nmap pod uživatelským účtem s administrátorskými právy.

Do další skupiny jsou zařazené parametry pro specifikaci portů a pořadí jejich skenování. Stejně jako v případě IP adres je možné i zde použít zadání pomocí rozsahů. Ve výchozím stavu je pořadí skenovaných portů náhodné, parametrem *-r* je možné vynutit sekvenční skenování portů.

Další skupiny parametrů se týkají podrobného nastavení detekce služeb a jejich verzí, spouštění uživatelských skriptů, detekce operačních systémů, časování a výkonu aplikace, obcházení firewallu / IDS, možností falšování identity a formátování výstupních informací. Mezi nejužitečnější parametry z těchto skupin patří následující. Parametr *-sV* povoluje detekci služeb a jejich verzí. Parametr *-O* povoluje detekci operačních systémů. Parametr *-T* umožňuje volbu šablony časování z množiny hodnot: paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4) a insane (5). Výstupní informace lze uložit do souboru pomocí parametrů *-oN* pro normální formát, *-oX* pro XML formát atd. Pro zvýšení úrovně informovanosti je možné použít parametr *-v*, případně *-vv*.

Poslední skupinou jsou ostatní parametry. Parametr *-6* povoluje skenování IPV6 sítí. Parametr *-A* souhrnně povoluje detekci operačního systému, detekci verze služby, prohledávání uživatelských skriptů a provedení trasování hostitele. Parametr *-V* zobrazí verzi programu Nmap a parametr *-h* vypíše stručnou nápovědu.

3.2 Wireshark

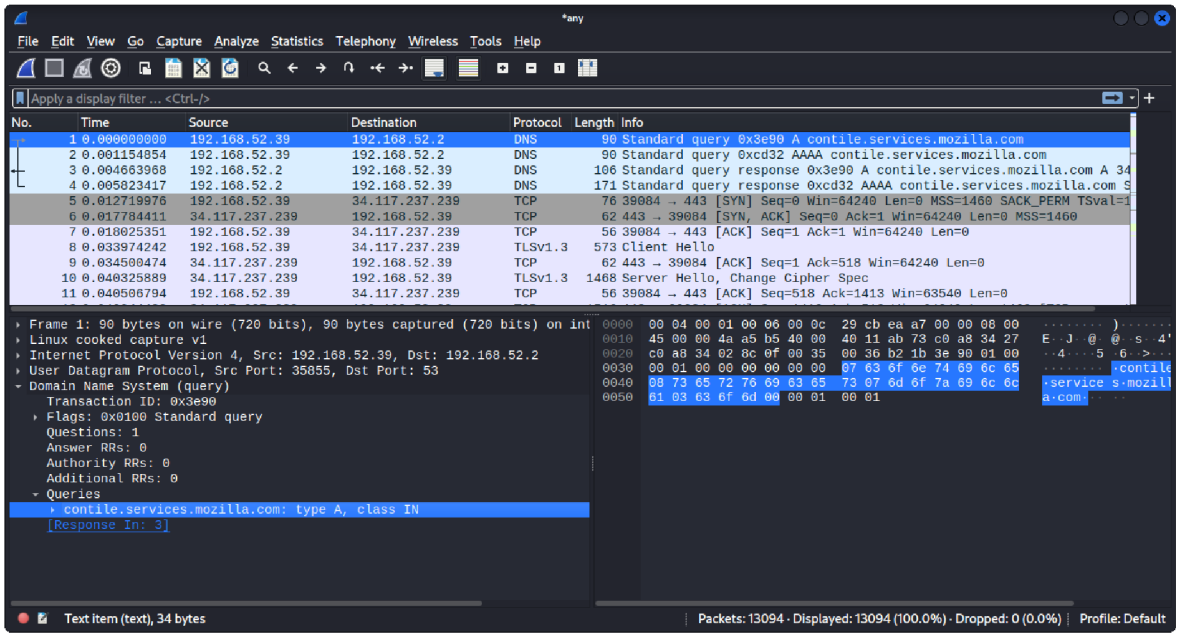
Podkapitola je zpracována podle dokumentace nástroje Wireshark [45]. Wireshark je bezplatný open source nástroj umožňující analýzu síťového provozu v reálném čase. Tento nástroj umožňuje detekci bezpečnostních problémů v jakékoli síti i řešení běžných síťových problémů, proto je podle [1] uznávaný mezi odborníky. Wireshark přepíná vybraná síťová rozhraní (může jich být i více) do promiskuitního režimu a následně zachytává síťovou komunikaci. Výsledky zobrazuje ve formátu čitelném pro člověka, což usnadňuje identifikaci potenciálních problémů, například nízké latence, hrozeb a zranitelností. Podle [45] Wireshark slouží pouze k pasivnímu zachytávání síťového provozu. Autoři dále uvádějí, že Wireshark neodesílá do sítě žádné pakety s výjimkou překladu doménových jmen, ten je však možné zakázat. Z hlediska kategorizace hackerských taktik se podle [31] jedná o nástroj sloužící k objevování (Discovery). Tuto informaci potvrzuje i práce [44], kde je nástroj zařazen do kategorie *„Information Gathering“*. Mezi výhody tohoto nástroje patří:

- Možnost uložení skenu pro pozdější offline kontrolu.
- Výkonné grafické rozhraní.
- Bohaté možnosti analýzy VoIP.
- Dekomprimace a kontrola souborů GZIP.

- Možnost čtení dalších formátů souborů se zachyceným síťovým provozem. Konkrétně se jedná o soubory vytvořené nástroji: Sniffer Pro, tcpdump (libcap), Microsoft Network Monitor, Cisco Secure IDS iplog a další.
- Podpora síťových portů a zařízení: Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI.
- Možnosti dešifrování protokolů: IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, WPA a WPA2 a dalších.
- Export výsledků ve formátech: XML, PostScript, CSV, případně v prostém textu.

Hlavní součástí balíčku nástrojů Wireshark je aplikace Wireshark s grafickým uživatelským rozhraním. Kromě toho balíček obsahuje řadu dalších nástrojů umožňujících práci v terminálu. To je užitečné v situaci, kdy není k dispozici interaktivní uživatelské rozhraní, případně není nutné jej použít. Lze například zachytávat síťový provoz na zařízení, které nemá dostatek zdrojů pro běh grafického rozhraní, a následně provést analýzu provozu na výkonnějším stroji. Balíček nástrojů Wireshark je dostupný pro operační systémy Linux, Windows, macOS, FreeBSD, NetBSD, OpenBSD.

Hlavní okno aplikace Wireshark se skládá z menu, hlavního panelu nástrojů, panelu nástrojů filtru, podokna seznamu paketů, podokna podrobností paketu, podokna bajtů paketu a stavového řádku, viz Obr. 4.



Obr. 4 Okno aplikace Wireshark.
Zdroj: Vlastní zpracování

Z menu, případně z hlavního panelu nástrojů, je možné spustit, zastavit nebo restartovat zachytávání síťového provozu, otvírat, ukládat nebo spojovat soubory se zachyceným síťovým provozem, listovat a vyhledávat v seznamu paketů. Z menu je dále možné provádět různé analýzy pomocí filtrování zachyceného provozu, generovat statistiky síťového provozu, provádět pokročilou analýzu a zobrazovat statistiky telefonního provozu, provádět analýzu aktivity bezdrátového připojení (Bluetooth a IEEE 802.11). V sekci Tools lze generovat pravidla pro firewally nebo vyhledat v zachyceném provozu přihlašovací údaje. Součástí menu je rovněž nápověda.

Při běžném provozu v síti je během velmi krátkého času obvykle zachyceno velké množství paketů. S tím souvisí snížená přehlednost seznamu paketů a rychle rostoucí velikost souboru se zachyceným provozem. Proto Wireshark nabízí funkce filtrování. Filtrování je možné provést už při zachytávání paketů, případně je možné zachytit veškerý provoz a filtrování provést až dodatečně. Pro účely dodatečného filtrování slouží panel nástrojů filtru. S jeho pomocí lze zobrazit pakety zejména na základě specifického protokolu, přítomnosti pole, hodnoty pole nebo porovnání mezi poli. Porovnání se provádí pomocí porovnávacích operátorů, viz Tabulka 2. Kromě toho umožňuje Wireshark použít více různých podmínek, regulárních výrazů nebo funkcí (upper, lower, len, count, string, max, min, abs).

V podokně seznamu paketů jsou zobrazeny zachycené pakety z načteného souboru. Každý řádek odpovídá jednomu paketu. Výběrem řádku v tomto podokně se zobrazí detailní informace o paketu v podoknech podrobností paketu a bajtů paketu. Nejdůležitější informace zobrazené v seznamu paketů jsou umístěné do sloupců, přičemž vyšší protokol má přednost před nižším. Jedná se o sloupce *No.* → číslo paketu v rámci souboru, *Time* → časové razítko, *Source* → zdrojová adresa, *Destination* → cílová adresa, *Protocol* → zkratka označující protokol, *Length* → délka paketu a *Info* → doplňující informace o obsahu paketu.

Podokno podrobností paketu zobrazuje jednotlivé protokoly a pole protokolů paketu vybraného v podokně seznamu paketů. Souhrnné informace každého z protokolů jsou uvedeny na jednom řádku ve formě sbalené stromové struktury, kterou je možné rozbalit pro podrobnější pohled na jednotlivá pole protokolu. Po kliknutí pravým tlačítkem myši na některou z položek je k dispozici kontextové menu, kde lze mimo jiné nastavit filtrování na základě pole a jeho obsahu. Některá pole protokolu zobrazují informace, které se v zachycených datech nevyskytují. Tyto informace jsou uzavřené v hranatých závorkách a jedná se například o doby odezvy, analýzu TCP,

informace o geolokaci IP a ověření kontrolního součtu. Pokud Wireshark detekuje vztah k jinému paketu v souboru se zachycenými daty, vygeneruje odkaz na tento paket. Odkazy jsou podtržené a zobrazené modrou barvou.

Tabulka 2 Porovnávací operátory (Wireshark).

Operátor (anglicky)	Alter. zápis	Alter. zápis (jazyk C)	Popis významu operátoru	Příklad
eq	any_eq	==	Rovná se (kterýkoli, pokud je více než jeden)	ip.src == 10.0.0.5
ne	all_ne	!=	Nerovná se (všechny, pokud je více než jeden)	ip.src != 10.0.0.5
	all_eq	===	Rovná se (všechny, pokud je více než jeden)	ip.src === 10.0.0.5
	any_ne	!==	Nerovná se (kterýkoli, pokud je více než jeden)	ip.src !== 10.0.0.5
gt		>	Větší než	frame.len > 10
lt		<	Menší než	frame.len < 128
ge		>=	Větší nebo rovno	frame.len ge 0x100
le		<=	Menší nebo rovno	frame.len <= 0x20
contains			Protokol, pole nebo řez obsahuje hodnotu	sip.to contains "a1762"
matches		~	Protokol nebo textové pole odpovídá regulárnímu výrazu kompatibilnímu s Perl	http.host matches "acme\\.(org|com|net)"

Zdroj: [45]

Podokno bajtů paketu zobrazuje hexadecimální výpis dat paketů, včetně ASCII znaků odpovídajících jednotlivým bajtům. Netisknutelné znaky jsou nahrazené tečkou. Někdy může být k dispozici více stránek, v tom případě jsou zobrazené ve formě karet a jednotlivé stránky se vybírají pomocí záložek umístěných ve spodní části podokna. Ve výchozím režimu jsou zvýrazňována pole, nad kterými se pohybuje ukazatel myši. Pole jsou zvýrazněna také při jejich výběru v podokně podrobností paketu.

Stavový řádek zobrazuje informační zprávy. Levá strana stavového řádku zobrazuje informace související s kontextem, prostřední část zobrazuje informace o počtu zachycených a zobrazených paketů včetně vyjádření v procentech a pravá strana zobrazuje vybraný konfigurační profil.

Zachytávání síťového provozu je možné spustit několika způsoby. Na úvodní obrazovce lze vybrat jedno nebo více rozhraní a poté spustit zachytávání přes kontextové menu vyvolané pravým tlačítkem myši, kliknutím na ikonu v hlavním panelu nástrojů nebo přes menu. Alternativně je možné spustit zachytávání z příkazového řádku.

3.3 Aircrack-ng

Podkapitola je zpracována podle dokumentace balíčku aircrack-ng [46]. Aircrack-ng je kompletní sada bezplatných open source nástrojů pro testování zabezpečení WiFi sítí podle standardů IEEE 802.11. Kromě testování zabezpečení umožňuje také zachytávání síťových rámců. Všechny nástroje patřící do tohoto balíčku jsou určené pro použití v příkazovém řádku, a lze je tedy využít ve skriptech. Této vlastnosti také hojně využívají nástroje s grafickým uživatelským rozhraním. Podle [46] nástroje v tomto balíčku umožňují pasivní odposlech (zachytávání síťových rámců), ale také aktivní útoky s pomocí vkládání rámců do probíhající síťové komunikace. Aircrack-ng lze tedy z hlediska taktik zařadit podle [31] nejen do kategorie průzkum (Reconnaissance), ale také získání přístupu k přihlašovacím údajům (Credential Access). Aircrack-ng je určený primárně pro operační systém Linux, ale je dostupný i pro Windows, macOS, FreeBSD a další. Mezi hlavní vlastnosti této sady nástrojů podle [1] patří:

- Kvalitní dokumentace (wiki a manuálové stránky).
- Aktivní komunita (fóra a IRC kanály).
- Spouštění PTW, WEP a fragmentačních útoků.
- Podpora režimu migrace WPA.
- Vysoká rychlost prolamování hesel.
- Podpora více bezdrátových rozhraní.
- Integrace s nástroji třetích stran.

Nástroj **airmon-ng** slouží k povolení režimu monitorování na bezdrátových rozhraních. Režim monitorování umožňuje zachycení všech rámců a zároveň umožňuje i vkládání rámců do probíhající komunikace. Tento speciální režim musí být podporovaný síťovou kartou. Seznam karet kompatibilních s balíčkem nástrojů aircrack-ng je uvedený v dokumentaci. Mezi další funkce tohoto nástroje patří možnost přepnout rozhraní zpět do spravovaného režimu a dále možnosti zobrazení, případně ukončení procesů, které by mohly narušit funkčnost nástrojů balíčku Aircrack-ng (parametr *check kill*, konflikt mohou způsobit například NetworkManager,

wpa_supplicant nebo dhclient). Konfliktní procesy je nutné ukončit před uvedením karty do režimu monitorování. Spuštění airmon-ng bez parametrů vypíše aktuální stavy všech dostupných bezdrátových rozhraní. Pokud je rozhraní ve spravovaném režimu, zobrazuje se jeho název například jako *wlan0*. Po přepnutí tohoto rozhraní do režimu monitorování (parametr *start wlan0*) se vytvoří monitorovací rozhraní s názvem *wlan0mon, se kterým* pak pracují další nástroje balíčku aircrack-ng.

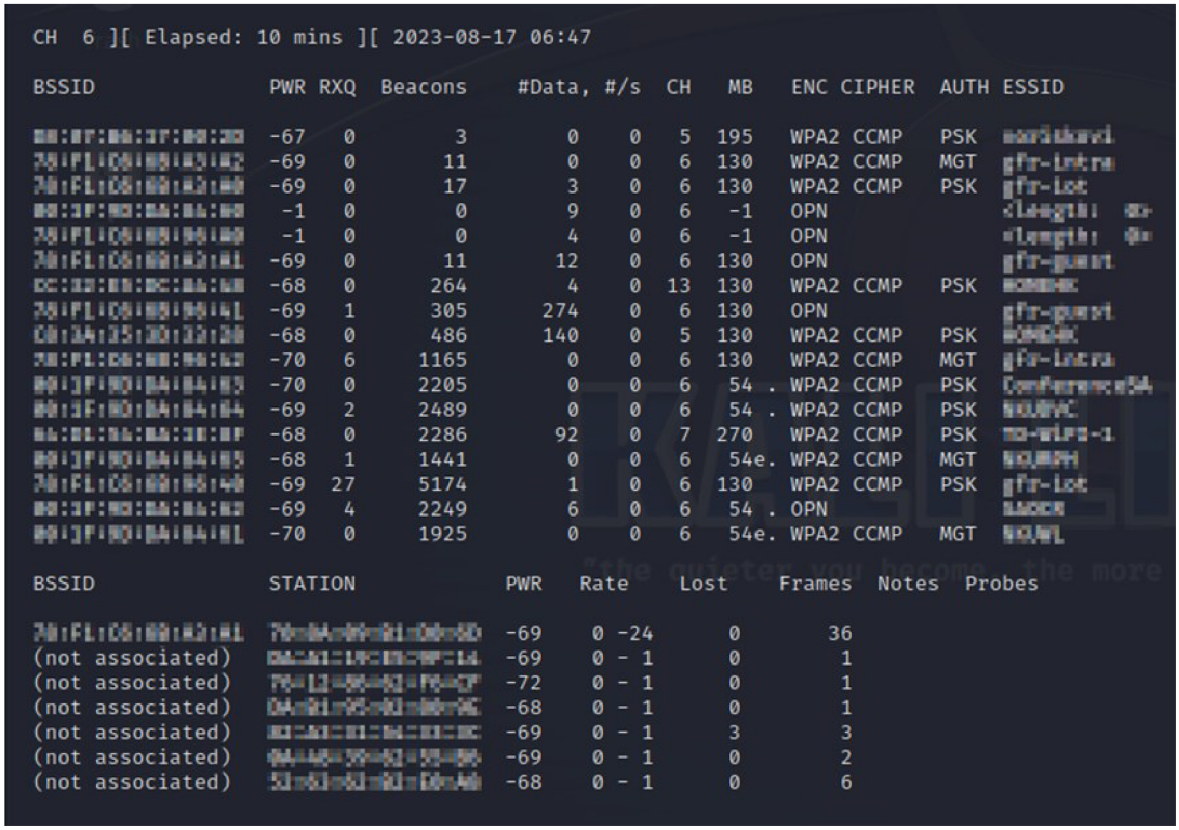
Pomocí nástroje **airodump-ng** lze zachytávat surové rámce standardu 802.11. To může být užitečné například k zachycení inicializačních vektorů WEP nebo WPA handshake. Zachycený provoz lze následně využít jako vstup nástroje aircrack-ng. Pro urychlení procesu může nástroj aircrack-ng běžet současně s airodump-ng. Pokud jsou k dispozici nová zachycená data, tak si je aircrack-ng průběžně načítá. Airodump-ng umožňuje zaznamenávat také GPS souřadnice nalezených přístupových bodů, pokud je k počítači připojený GPS přijímač. Mezi nejužitečnější parametry tohoto nástroje patří především pokročilé možnosti filtrování zachytávaného provozu. Konkrétně filtrování na základě čísla kanálu (parametr *--channel*), použitého šifrovacího protokolu (parametr *--encrypt*), BSSID (parametr *--bssid*) nebo ESSID (parametr *--essid*, případně *--essid-regex* pro použití regulárních výrazů) atd. Důležité je především filtrování podle kanálu, protože při skenování celého pásma nelze zachytit všechny rámce cílové sítě. Výhodou použití filtru je také snížení velikosti souborů se zachyceným provozem.

Po spuštění airodump-ng s parametrem wlan0mon se po chvíli zobrazí informace o síťovém provozu v okolí, viz Obr. 5. Na prvním řádku je zobrazen aktuálně prohledávaný kanál, čas uplynulý od spuštění, aktuální datum a čas, případně WPA/WPA2 handshake včetně BSSID, pokud byl detekován. Pod prvním řádkem následuje seznam detekovaných přístupových bodů (AP) a pod ním seznam detekovaných klientů. Význam zkratek viz Tabulka 3. Na základě výsledků detekce je možné určit, jaký provoz má být zachytáván, a poté spustit airodump-ng s parametrem --write a prefixem určujícím názvy ukládaných souborů.

Nástroj **aireplay-ng** je určený k provedení devíti různých typů útoků pomocí vkládání rámců. Pro útoky na WPA sítě jsou vhodné pouze dva z těchto útoků, Deauthentication a WPA Migration Mode. Přičemž WPA Migration Mode je zaměřený na konkrétní chybu přístupových bodů Cisco Aironet v migračním režimu. Útok Deauthentication (parametr *-0*) zneužívá obecný princip zaměřený na deautentizaci klientů, proto bude dále popsán podrobněji. K provedení slovníkového útoku na zabezpečení WPA je nutné zachytit čtyřcestný handshake. Ten je proveden vždy po dokončení

autentizace a asociace klienta k AP. Je tedy nutné vyčkat na připojení klienta, případně urychlit útok vynucením deautentizace vybraných nebo všech stávajících připojených klientů. Pro provedení deautentizace jednoho klienta je možné spustit program s parametry:
aireplay-ng -0 1 -a XX:XX:XX:XX:XX:XX -c YY:YY:YY:YY:YY:YY wlan0mon, kde:

- *-0* znamená útok Deauthentication
- *1* je požadovaný počet deautentizací
- *-a XX:XX:XX:XX:XX:XX* je MAC adresa přístupového bodu
- *-c YY:YY:YY:YY:YY:YY* je MAC adresa klienta
- *wlan0mon* je název rozhraní



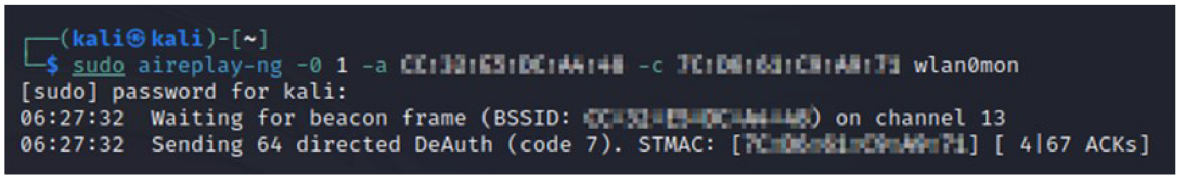
Obr. 5 Informace o AP a klientech (airodump-ng).
Zdroj: Vlastní zpracování

Tabulka 3 Informace zobrazované nástrojem airodump-ng.

Pole	Význam pole
BSSID	MAC adresa AP. V seznamu klientů se zobrazuje MAC adresa AP, ke kterému je klient připojen. Pokud klient není připojen k žádnému AP, zobrazí se „not associated".
PWR	Síla signálu. Některé ovladače o síle signálu neinformují.
RXQ	Kvalita signálu. Zobrazuje se pouze s filtrem nastaveným na konkrétní kanál.
Beacons	Počet přijatých beacon rámců. Pokud není dostupná síla signálu, lze ji odhadnout na základě této hodnoty.
#Data	Počet zachycených datových paketů.
#/s	Počet datových paketů za sekundu.
CH	Číslo kanálu (převzaté z beacon rámců).
MB	Maximální rychlost podporovaná AP: 11 → 802.11b, 54 → 802.11g, Cokoli vyššího → 802.11n nebo 802.11ac. „." za hodnotou → podpora krátké preambule, „e" → povolené QoS.
ENC	Šifrování: OPN → nešifrováno, WEP→ šifrování WEP, WPA → šifrování WPA nebo vyšší, WEP? → šifrování WEP nebo vyšší (nedostatek dat k přesnějšímu určení).
CIPHER	Detekovaná šifra. CCMP, WRAP, TKIP, WEP, WEP40 nebo WEP104.
AUTH	Použitý ověřovací protokol: MGT → WPA/WPA2 pomocí samostatného ověřovacího serveru, SKA → sdílený klíč pro WEP, PSK → sdílený klíč pro WPA/WPA2, OPN → otevřený.
ESSID	Název bezdrátové sítě. Může být skrytý.
STATION	MAC adresa klienta.
Rate	První číslo označuje rychlost příjmu dat (směr od AP ke klientovi), druhé číslo označuje rychlost vysílání dat (směr od klienta k AP).
Lost	Počet ztracených datových rámců odeslaných klientem za posledních 10 sekund.
Frames	Počet datových rámců odeslaných klientem.
Notes	Doplňující informace o klientovi. Například zachycení EAPOL nebo PMKID.
Probes	Názvy sítí, se kterými se nepřipojený klient pokouší spojit.

Zdroj: [46]

Po spuštění aireplay-ng odešle celkem 128 rámců pro každého ze zadaných klientů, z toho 64 rámců přístupovému bodu a 64 rámců klientovi. Výstupem programu je vyhodnocení úspěšnosti, kde první hodnota v hranatých závorkách znamená počet potvrzení obdržených od klienta a druhá hodnota vyjadřuje počet potvrzení obdržených od přístupového bodu, viz Obr. 6. Pokud je některá z hodnot nulová, tak klient nebo AP požadavek na deautentizaci neobdržel. To může být způsobené příliš velkou vzdáleností mezi útočníkem a klientem nebo mezi útočníkem a AP. Rovněž hodnoty blízké nule je vhodné řešit úpravou pozice útočníka nebo použitím jiné antény.



Obr. 6 Informace o provedené deautentizaci (aireplay-ng).
Zdroj: Vlastní zpracování

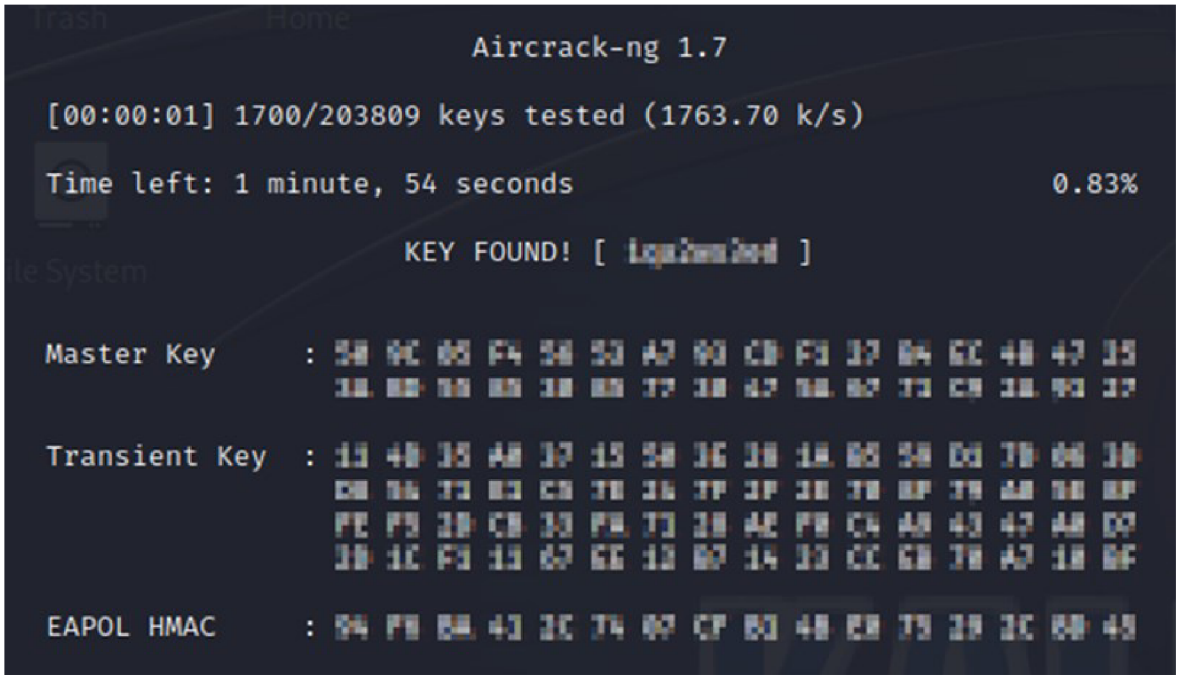
Pomocí nástroje **aircrack-ng** lze určit klíče sítí zabezpečených protokoly WEP, WPA, případně WPA2-PSK. V případě WEP je možné volit mezi novější metodou PTW (Pyshkin, Tews, Weinmann), starší metodou FMS/KoreK (Fluhrer, Mantin, Shamir) nebo slovníkovým útokem. V současné době se zabezpečení WEP již prakticky nevyskytuje, proto tyto útoky nebudou popsány. Zabezpečení WPA a vyšší je aktuálně možné prolomit pouze pomocí slovníkového útoku. V tomto případě je nutným předpokladem zachycení čtyřcestného handshake. Ten se skládá ze čtyřech rámců. Nástroji aircrack-ng však k úspěšnému prolomení zabezpečení stačí pouhé dva z nich (v případě použití protokolu EAPOL se jedná o rámce 2 a 3, jinak 3 a 4). Program využívá instrukce SSE2, AVX, AVX2 a AVX512, což výrazně urychluje zpracování klíčů.

Z poskytnutého slovníku generuje aircrack-ng duplikáty čtyřcestného handshake a porovnává je se zachyceným. Při nalezení shody je identifikován klíč. Tento proces je výpočetně velmi náročný a jeho úspěšnost závisí především na použitém slovníku. Slovník je možné připravit předem, na míru konkrétnímu útoku, pomocí nástroje John The Ripper. Aircrack-ng nabízí mnoho parametrů. Pro určení klíče WPA lze program spustit s těmito parametry:
aircrack-ng -a2 -b XX:XX:XX:XX:XX:XX -w slovnik.txt dump.cap, kde:

- *-a2* odpovídá režimu útoku silou na zabezpečení WPA/WPA2-PSK
- *-b XX:XX:XX:XX:XX:XX* je BSSID
- *-w slovnik.txt* název souboru se slovníkem
- *dump.cap* je název souboru s provozem zachyceným pomocí airodump-ng

Výstup programu aircrack-ng v případě úspěšného nalezení klíče viz Obr. 7. Mezi další pomocné nástroje v balíčku aircrack-ng patří například:

- airbase-ng: Slouží pro vytvoření falešného přístupového bodu.
- airdecap-ng: Slouží k dešifrování souborů se zachyceným provozem.
- airolib-ng: Umožňuje ukládání a správu essid, seznamů hesel a výpočtu jejich Pairwise Master Keys (PMK) pro urychlení vlastního prolamování klíčů pomocí aircrack-ng.



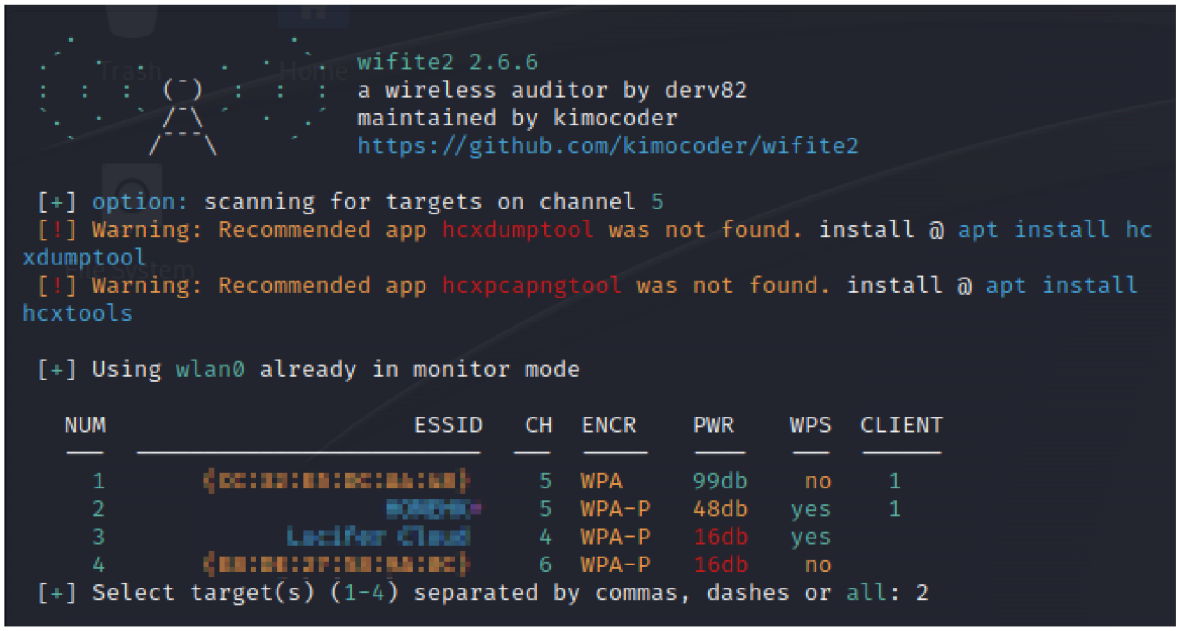
Obr. 7 Informace o úspěšném nalezení klíče (aircrack-ng).
Zdroj: Vlastní zpracování

3.4 Wifite

Podkapitola je zpracována podle dokumentace nástroje Wifite [47]. Wifite je bezplatný open source skript usnadňující provedení auditu bezdrátových sítí. Tento skript je napsaný v jazyce Python a je závislý na dalších nástrojích, mj. z balíčku aircrack-ng. Cílem autora Wifite bylo zjednodušení práce s těmito nástroji. Díky tomu již není nutné pamatovat si parametry a přepínače každého z nich. Na základě těchto informací lze Wifite zařadit podle [31] do stejných kategorií taktik jako aircrack-ng, tedy do kategorie průzkum (Reconnaissance) a získání přístupu k přihlašovacím údajům (Credential Access). Kromě technik uvedených v kapitole Aircrack-ng umožňuje Wifite ještě útoky cílené na Wireless Protection System (WPS). Následuje seznam útoků, které Wifite umožňuje:

- WPS: Offline Pixie-Dust attack.
- WPS: Online Brute-Force PIN attack.
- WPS: Offline NULL PIN attack.
- WPA: WPA Handshake Capture nebo offline crack.
- WPA: PMKID Hash Capture nebo offline crack.
- WEP: Různé známé útoky, včetně fragmentation, chop-chop, aireplay-ng atd.
- WIFI rušička signálu. Blokování jednoho nebo více AP (funkční pouze s WiFi čipsety Atheros).

Wifite je navržen speciálně pro nejnovější verzi Kali Linux. Kromě Kali Linux je podporována linuxová distribuce ParrotSec a platforma Kali NetHunter (určená pro zařízení Android). V případě Kali NetHunter je však vyžadováno vlastní jádro umožňující vkládání rámců. Skript pracuje v interaktivním režimu, viz Obr. 8. Nejprve jsou periodicky vypisovány informace o sítích v dosahu, dokud není stisknuta klávesová kombinace Ctrl+C. Poté skript očekává výběr cíle nebo cílů útoku. Následně je proveden útok na vybrané cíle, viz Obr. 9.

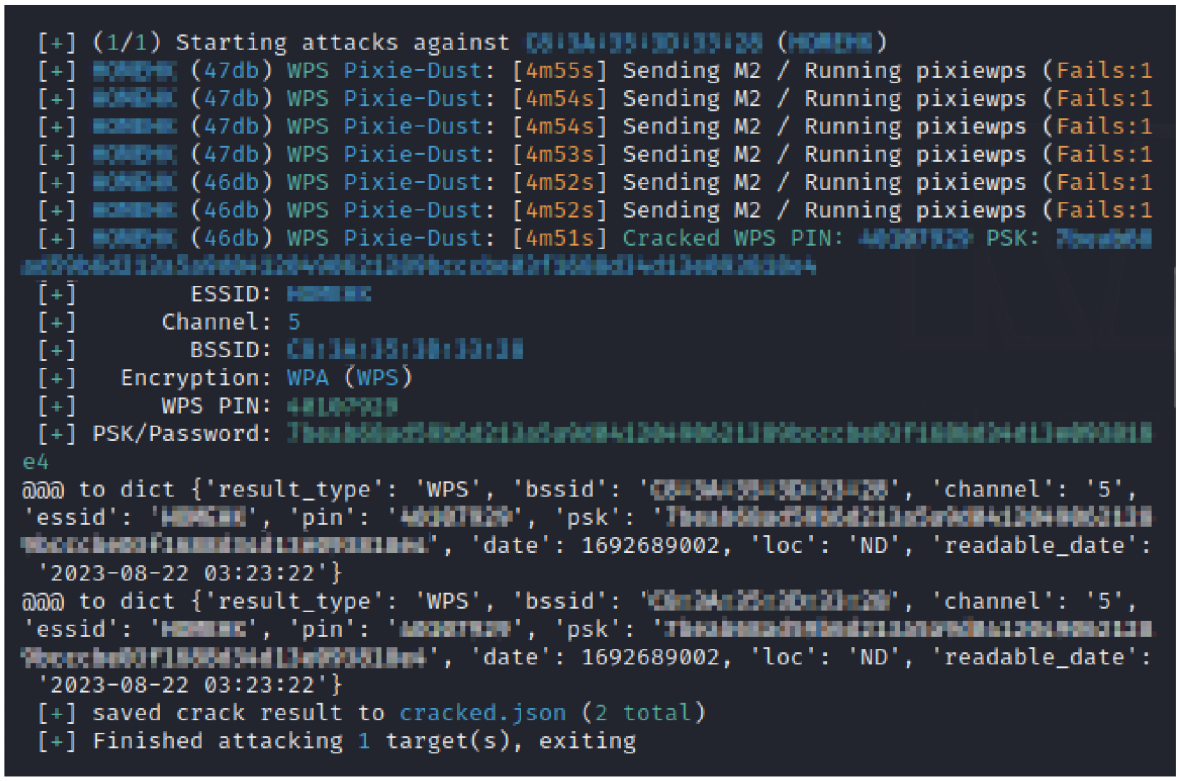


Obr. 8 Výpis potenciálních cílů útoku (Wifite).
Zdroj: Vlastní zpracování

Při spuštění skriptu je možné použít následující parametry. Při skenování nebo útoku umožňuje Wifite automaticky odhalit skrytá AP, ale pouze na konkrétním vybraném kanálu (parametr *-c*). U bezdrátových karet s podporou pásma 5 GHz lze použít parametr *-5*, ale některé nástroje nemusí fungovat správně (například aireplay-ng). Prolomená hesla (klíče) lze spolu s dalšími informacemi (handshake, název AP, BSSID, datum atd.) uložit do aktuálního adresáře pomocí parametru *--cracked*. Dále je možné

skriptu předat slovník (parametr --*dict*). Jak bylo uvedeno výše, tento skript je závislý na dalších nástrojích. Vyžadované jsou balíčky: Python 3.11, Iw, Ip, Aircrack-ng. Mezi volitelné, avšak doporučené nástroje patří následující:

- Tshark: Umožňuje detekci WPS sítě a kontrolu handshake.
- Reaver: Umožňuje útoky vůči WPS (hrubou silou nebo Pixie-Dust attack).
- Bully: Alternativa k Reaver (vynucení pomocí parametru --*bully*).
- John The Ripper: Urychlení prolamování hesel pomocí CPU/GPU (OpenCL).
- coWPAtty: Umožňuje detekci handshake.
- hashcat: Umožňuje prolamování PMKID hash.
- hcxdumptool: Umožňuje zachytávání PMKID hash.
- hcxpcapngtool: Pro konverzi zachycených rámců PMKID na formát hashcat.



Obr. 9 Útok na protokol WPS (Wifite).
Zdroj: Vlastní zpracování

3.5 Ettercap

Podkapitola je zpracována podle dokumentace nástroje Ettercap [48]. Ettercap je bezplatný open source nástroj určený k provedení různých útoků založených na technice Adversary In The Middle (zkráceně AiTM, tato technika byla dříve označována jako Man In The Middle, nebo zkráceně MITM). Tento nástroj je napsaný v jazyce C

a umožňuje odposlech paketů v LAN sítích, včetně možnosti filtrování za běhu. Podporuje aktivní i pasivní skenování a umožňuje analýzu různých síťových protokolů, včetně šifrovaných (např. SSH a HTTPS). Mezi další funkce tohoto nástroje patří analýza sítě a hostitele (např. OS fingerprinting) a manipulace se síťovým provozem. Tyto vlastnosti předurčují Ettercap k provádění bezpečnostního auditu. Podle [31] lze tento nástroj zařadit do kategorií taktik Credential Access (Přístup k přihlašovacím údajům), Collection (Shromažďování) a Impact (Dopad). Mezi funkce nástroje Ettercap patří:

- Podpora SSH1: Možnost zachycení přihlašovacích údajů i přenášených dat v plně duplexním režimu.
- Podpora SSL: Odposlech šifrované SSL komunikace pomocí předložení falešného certifikátu klientovi a dešifrování relace.
- Vkládání znaků do navázaného spojení: Pomocí emulace příkazů určených serveru nebo odpovědí určených klientovi je možné udržet spojení aktivní.
- Filtrování/zahazování paketů: Pomocí filtrovacího skriptu lze vyhledávat řetězec v datové části TCP nebo UDP paketů a následně jej nahradit jiným řetězcem nebo celý paket zahodit.
- Vzdálený odposlech provozu tunelových spojení: Provádění AiTM útoků na tunelová spojení.
- Podpora zásuvných modulů: Pomocí rozhraní API ettercap lze vytvořit svůj vlastní zásuvný modul.
- Odposlech hesel pro protokoly: TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE 3, MSN, YMSG.
- Fingerprinting OS: Pasivní skenování LAN a shromažďování podrobných informací o hostitelích v LAN (operační systém, běžící služby, otevřené porty, IP, mac adresa a dodavatel síťového adaptéru).
- Ukončení spojení: Ze seznamu spojení lze ukončit libovolná spojení.

Ettercap je dostupný pro operační systémy založené na jádře Linux, dále Mac OSX, FreeBSD, OpenBSD a NetBSD. Ettercap je možné spustit ve třech různých režimech. V grafickém režimu založeném na knihovně GTK2 (parametr *-G*), v interaktivním terminálovém režimu založeném na knihovně ncurses (parametr *-C*), případně v příkazovém řádku, což umožňuje využití ve skriptech. Zachytávání síťového provozu je možné spustit v jednom ze dvou režimů.

V režimu UNIFIED je veškerý příchozí i odchozí provoz zachytáván pomocí jediného rozhraní. Ve výchozím režimu je toto rozhraní automaticky přepnuto do promiskuitního režimu, pomocí parametru *-p* je možné přepnutí zakázat. Pakety, které nejsou směrovány na hostitele s nástrojem Ettercap, budou automaticky předávány pomocí směrování na vrstvě 3 modelu TCP/IP. Díky tomu je možné spustit útok AiTM z jiného nástroje a zároveň modifikovat a přeposílat pakety s pomocí Ettercap. Ip_forwarding v jádře operačního systému je nástrojem Ettercap vždy zakázán, aby se zabránilo zdvojení při přeposlání paketu.

V režimu BRIDGED (parametr *-B*) se používají dvě síťová rozhraní. Síťový provoz je předáván z jednoho rozhraní na druhé a zároveň probíhá zachytávání a filtrování obsahu. Tato metoda je zcela nenápadná, protože na rozdíl od útoku AiTM v režimu UNIFIED není generován žádný provoz navíc. V podstatě se jedná o AiTM útok na vrstvě 1 modelu TCP/IP.

Útočný modul nástroje Ettercap je nezávislý na procesu zachytávání a filtrování paketů. Díky tomu je možné spustit i několik útoků současně nebo použít k útoku jiný nástroj. Při výběru cílů útoku je nutné pamatovat na to, že koncept zdroje a cíle vlastně neexistuje, protože spojení je vždy obousměrné. V případě požadavku na filtrování provozu mezi dvěma cíli je tedy spojení filtrováno v obou směrech.

3.6 Yersinia

Podkapitola je zpracována podle dokumentace nástroje Yersinia [49]. Yersinia je bezplatný open source nástroj zaměřený na využití zranitelností v různých síťových protokolech. Tento nástroj je napsán v jazyce C a v současnosti již není aktivně vyvíjen (poslední verze byla vydána 24. 8. 2017), přesto je stále plně funkční a může poskytnout užitečné informace bezpečnostním auditorům nebo správcům sítí. Některé z útoků implementovaných v nástroji Yersinia způsobí odepření síťových služeb, na to je nutné dát pozor při testování v produkčním prostředí. Nástroj však nabízí i další pokročilé útoky na síťovou infrastrukturu. Podle [31] lze tento nástroj zařadit do kategorií taktik Credential Access (Přístup k přihlašovacím údajům), Collection (Shromažďování) a Impact (Dopad). Tuto skutečnost potvrzuje i práce [44], kde autoři nástroj zařadili do kategorií *„Vulnerability Analysis“*, *„Exploitation Tools“* a *„Sniffing & Spoofing“*. Nástroj Yersinia byl úspěšně testován na operačních systémech založených na OpenBSD 3.4, Linux (kernel 2.4.x a 2.6.x), Solaris 5.8 64bitů SPARC a Mac OSX 10.4 Tiger (Intel). Seznam síťových protokolů, na které lze útočit pomocí tohoto nástroje:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)
- MultiProtocol Label Switching (MPLS)

Nástroj je možné spustit ve čtyřech různých režimech. V grafickém režimu založeném na knihovně GTK (parametr *-G*), v interaktivním terminálovém režimu založeném na knihovně ncurses (parametr *-I*), jako službu pro vzdálenou správu (režim daemon, parametr *-D*) nebo v příkazovém řádku, což umožňuje využití ve skriptech. K ovládání nástroje v terminálovém režimu slouží především následující klávesy:

- h: Zobrazení nápovědy.
- g: Volba typu útoku (protokolu, vůči kterému je útok veden). Typ útoku lze volit šipkami ↑ a ↓ a poté potvrdit klávesou Enter.
- x: Spuštění konkrétního typu útoku. Útoky jsou označené číslicemi, volba se provádí stisknutím příslušné číslice na klávesnici.
- e: Editace polí paketu, pokud to daný útok umožňuje. Některé útoky generují do polí paketů náhodné hodnoty.
- l: Zobrazení aktivních útoků.
- K: Ukončení všech běžících útoků.

Pro účely této práce jsou relevantní útoky zaměřené na STP a DHCP, následují seznamy útoků na tyto protokoly:

- Útoky STP:
    - Sending RAW Configuration BPDU
    - Sending RAW TCN BPDU
    - DoS sending RAW Configuration BPDU
    - DoS sending RAW TCN BPDU
    - Claiming Root Role

    - Claiming Other Role
    - Claiming Root Role dual home (MITM)
- Útoky DHCP:
    - Sending RAW DHCP packet
    - DoS sending DISCOVER packet (exhausting ip pool)
    - Setting up rogue DHCP server
    - DoS sending RELEASE packet (releasing assigned ip)

3.7 Scapy

Nástroj Scapy je podle [50] výkonná interaktivní knihovna pro manipulaci s pakety napsaná v Pythonu. Scapy podle autora poskytuje možnosti falšování nebo dekódování paketů pro velké množství protokolů. Autor dále uvádí, že Scapy umožňuje pakety odesílat, zachytávat, párovat žádosti s odpověďmi a má mnoho dalších funkcí. Výhodou Scapy oproti nástrojům jako Nmap nebo Hping je podle autora také to, že odpověď není redukována na pouhou informaci o stavu (otevřeno, uzavřeno nebo filtrováno), ale k dispozici je celý paket.

Podle [50] Scapy umožňuje uživateli popsat paket nebo sadu paketů jako model složený z vrstev. Autor dále uvádí, že jednotlivá pole každé vrstvy obsahují výchozí hodnoty, které mohou být přetíženy, kromě toho Scapy nenutí uživatele k použití předem určených metod nebo šablon. Díky této flexibilitě podle autora není nutné vyvíjet nový nástroj pro každý další scénář. Autor například uvádí, že popis paketu v jazyce C může průměrně obsahovat šedesát řádků kódu. S použitím Scapy se může popis paketů určených k odeslání vejít na jeden řádek, přičemž další řádek bude sloužit k vypsání výsledku. Jak autor dále uvádí, 90 % nástrojů pro sondování sítě lze pomocí Scapy přepsat do dvou řádků.

Následuje stručný popis využití nástroje Scapy zpracovaný podle [51]:

- Manipulace s pakety
    - Pakety jsou reprezentovány jako objekty.
    - Ke skládání paketů se používá operátor „/“.
    - Pro zobrazení seznamu polí slouží funkce „*ls()*“.
    - Scapy vybírá korektní zdrojové IPv4 adresy, MAC adresy atd.
    - Ke všem polím paketu je snadný přístup pomocí atributů objektu.
    - Pole může obsahovat více hodnot, např. posloupnost nebo seznam.

- Interakce se sítí
    - Funkce *„send()“* odešle paket na 3. vrstvě (nečeká na odpověď).
    - Funkce *„sendp()“* odešle rámec na 2. vrstvě (nečeká na odpověď).
    - Funkce *„sr1()“* odešle paket a vrátí požadavek spárovaný s odpovědí.
    - Funkce *„srp()“* odešle seznam paketů a vrátí dvě proměnné, první obsahuje seznam požadavků, ke kterým byly připojeny odpovědi, druhá proměnná obsahuje pakety, které se nepodařilo spárovat s odpovědí.
    - Scapy podporuje zápis a čtení souborů PCAP pomocí funkcí *„wrpcap()“* a *„rdpcap()“*.
    - Funkce *„command()“* umožňuje vytvoření řetězce, pomocí kterého lze vytvořit stejný objekt.
    - Funkce *„sniff()“* slouží k zachycení paketů.
    - Funkce *„lsc()“* vypíše seznam dostupných příkazů.
    - Funkce *„help()“* s názvem příkazu uvedeným jako parametr popíše argumenty a chování příkazu.
- Vizualizace
    - Funkce *„multiplot()“* vykreslí graf.
    - Funkce *„str()“* vypíše paket ve tvaru, v jakém je odeslán do sítě.
    - Funkce *„hexdump()“* vypíše paket v hexadecimálním tvaru.
    - Funkce *„show()“* vypíše obsah polí vrstvu po vrstvě.
    - Funkce *„canvas_dump()“* vykreslí grafickou reprezentaci paketu.
    - Funkce *„make_table()“* vypíše výsledky do tabulky.

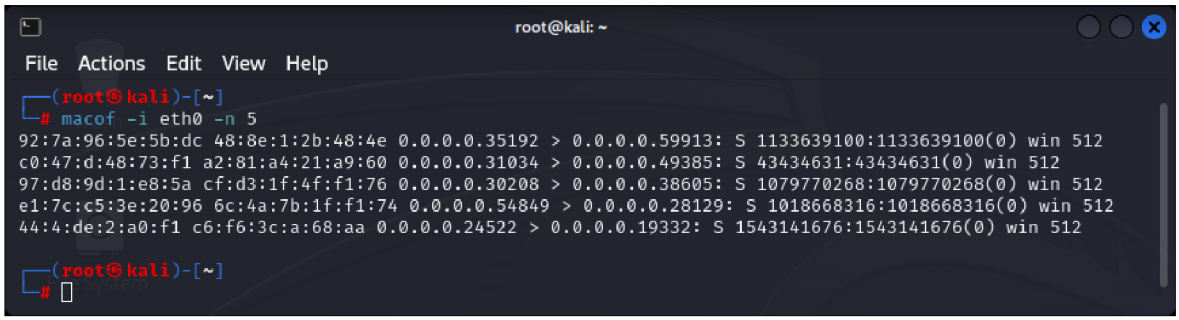
Kromě výše uvedených možností nabízí Scapy podle [51] ještě například následující:

- Import modulu Scapy do python skriptu pomocí příkazu: *„from scapy.all import *“*.
- Možnost implementace nového protokolu.
- Vytvoření objektu *„answering machine“*.
- Možnost průzkumu sítí IPv6.
- Manipulaci s X.509 certifikáty.

3.8 Macof

Macof je nástroj z balíčku Dsniff, který podle [52] slouží k zaplavení přepínané sítě náhodnými MAC adresami. Podle autora se jedná o nástroj napsaný v jazyce C, který je určen pro práci v příkazovém řádku. Příklad použití viz Obr. 10. Program akceptuje následující parametry:

- -i Rozhraní, přes které budou pakety odeslány.
- -s Zdrojová IP adresa.
- -d Cílová IP adresa.
- -e Cílová HW adresa.
- -x Zdrojový TCP port.
- -y Cílový TCP port.
- -n Počet paketů k odeslání.
- Hodnoty nespecifikované pomocí parametrů jsou generovány náhodně.



Obr. 10 Ukázka nástroje macof.
Zdroj: Vlastní zpracování

4 Popis útoků

Cílem této kapitoly je představení aktuálních vědeckých prací na téma útoků vůči síťovým prvkům v drátových i bezdrátových sítích. V každé z podkapitol je nejprve popsána teorie nezbytná k pochopení principu útoku. Následuje popis způsobů zneužití vybrané zranitelnosti včetně podmínek, za kterých lze útok provést, a doporučené síťové topologie. Rovněž jsou zde uvedeny možnosti, jak rozšířit účinky útoku s využitím dalších útoků. V závěru podkapitol jsou uvedeny doporučené postupy konfigurace ochrany před zneužitím uvedených zranitelností.

4.1 Útoky vůči bezdrátovým sítím 802.11

Kapitola je zpracovaná podle [53]. Bezdrátové sítě založené na standardu IEEE 802.11, běžně označované jako Wi-Fi, případně WLAN, umožňují snadný přístup a rychlý přenos dat v oblasti pokryté signálem. Tato výhoda je však zároveň nevýhodou z pohledu zabezpečení datových přenosů. Bezdrátové sítě jsou velmi zranitelné vůči kybernetickým útokům, protože data jsou přenášená vzduchem ve formě rádiových vln. Díky tomu může být podle [54] datový přenos odposloucháván nebo napaden útočníky. Pro zajištění důvěrnosti, integrity a bezpečnosti dat vyvinula organizace Wi-Fi Alliance [55] následující standardy šifrování: Wired Equivalent Privacy (WEP), Wireless Protected Access (WPA), následně byl standard WPA aktualizován na verzi 2 (WPA2) a v roce 2018 byla vydána nejnovější verze standardu WPA verze 3 (WPA3).

WEP je zastaralý šifrovací standard vyvinutý v roce 1999. Pro šifrování používá algoritmus RC4 a pro kontrolu integrity používá algoritmus CRC-32. Poté co kryptoanalytici zjistili, že standard WEP obsahuje mnoho chyb, byl tento standard v roce 2003 nahrazen standardem WPA.

Vývoj standardu WPA však v okamžiku jeho vydání ještě nebyl úplně dokončený. Podle [54] standard WPA využívá pro šifrování algoritmus TKIP, ve kterém byly záhy objeveny nové zranitelnosti. Proto byl v roce 2004 nahrazen standardem WPA2.

Protokol WPA2 používá pro šifrování techniku režimu Counter (CTR) v kombinaci s algoritmem CBC-MAC (CCM), tato kombinace je označována jako CCM Protocol (CCMP). Pro šifrování hesel se používá Advanced Encryption Standard (AES).

Standard WPA3 je podle [56] založený na vylepšeném protokolu handshake (Dragonfly-Handshake), přičemž ověřování probíhá pomocí metody Simultaneous Authentication of Equals (SAE) standardizované normou 802.11. Šifrování podle standardu WPA3 bylo vylepšeno, takže je mnohem obtížnější prolomit heslo, než v případě

starších standardů, přesto však není vůči útokům zcela imunní. Vědci již v protokolu WPA3 našli některé chyby umožňující získat heslo. K praktickému zneužití těchto zranitelností však zatím nedošlo.

Podle [54] nejsou řídící a datové rámce šifrované, takže je velmi snadné číst ze zachycených rámců informace. Díky absenci kontroly integrity je podle autorů také možné vytvořit falešné rámce a použít je k útokům typu injection nebo replay. V současné době je velmi snadné prolomit hesla šifrovaná dle standardů WEP, WPA a WPA2 pomocí slovníkového útoku, například nástrojem Aircrack-ng.

Před zahájením vlastního útoku je nutné nastavit síťovou kartu do promiskuitního režimu, viz kapitola 3.3. Poté je podle [54] možné spustit skenování Wi-Fi pásma, a zjistit tak základní informace o cílové síti, konkrétně počet přístupových bodů (Access Point, zkráceně AP), pracovní kanály, sílu signálu a informace o klientech. Dále je podle autorů vhodné uložit si MAC adresu cílového AP (BSSID), identifikátor sítě ESSID a MAC adresu klienta.

ESSID může být skrytý, ale pokud se k síti připojuje klient, který ESSID zná, tak se podle [54] dá ESSID odposlechnout, protože komunikace není šifrovaná. Skrytí ESSID tedy nemá žádný vliv na zabezpečení sítě. Autoři dále uvádějí, že případné filtrování MAC adres na přístupovém bodu síť před případným útokem také neochrání, protože MAC adresy klientů se rovněž dají odposlechnout, a útočník se díky klonování MAC adresy může vydávat za legitimního klienta.

Po získání informací o cílové síti lze zahájit vlastní útok. Útok může podle [54] být buď pasivní, spočívající v odposlechu a zachytávání dat, nebo aktivní, kdy útočník zachycená data modifikuje a vkládá do probíhající komunikace. Režim šifrování pomocí standardu WEP se vzhledem k jeho stáří už nepoužívá, ale standardy WiFi Protected Setup (WPS) a WPA, zejména verze 2, jsou podle autorů stále aktivně využívány. Autoři dále uvádějí, že metoda prolamování se volí na základě režimu šifrování, který cílová síť používá. Například k prolomení hesla WEP je podle autorů nutné zachytit určité množství dat vyměněných mezi klientem a AP. K prolomení hesla WPA je nutné zachytit pakety čtyřcestného handshake.

Způsoby obrany jsou uvedeny souhrnně na konci kapitoly 4.1.6.

4.1.1 Zachycení čtyřcestného handshake WPA

Podkapitola je zpracována podle [54]. Jedna z aktuálně nejpoužívanějších metod útoku na sítě zabezpečené pomocí WPA/WPA2 spočívá v zachycení paketů čtyřcestného handshake a následném použití slovníkového útoku. Čtyřcestný handshake

probíhá podle autorů na počátku připojení legitimního klienta. Pokud se při útoku žádný nový klient nepřipojí, tak je podle autorů možné útok urychlit vynucením deautentizace stávajících připojených klientů. Autoři dále uvádějí, že při následné autentizaci klientů je možné handshake zachytit. Klíčem k úspěchu průniku šifrování WPA/WPA2 je podle autorů především schopnost útočníka zachytit platné handshake pakety a kvalita použitého slovníku.

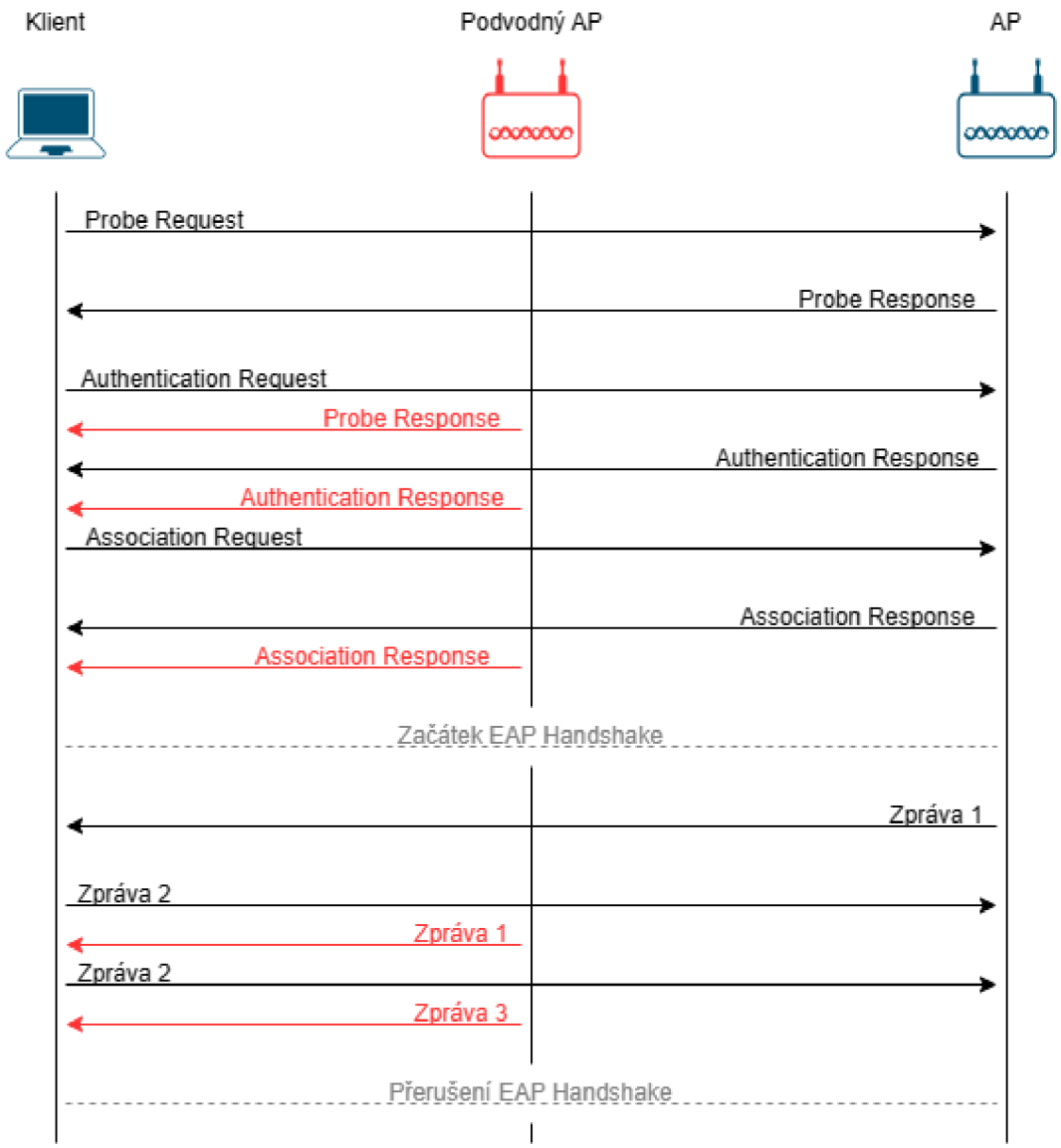
4.1.2 Rogue Access Point

Podkapitola je zpracovaná podle [56]. Dalším ze známých útoků je Rogue Access Point (Rogue AP), označovaný také jako **Evil Twin**. Tento typ útoku spočívá v tom, že útočník vydává své podvodné AP za legitimní a snaží se donutit klienty, aby se k němu připojili, typicky za využití vyšší intenzity signálu. Stávající klienti legitimního AP mohou být také odpojeni, pokud útočník vynutí jejich deautentizaci. Vůči útokům typu Evil Twin jsou zranitelné zejména sítě zabezpečené pomocí WPA2 a starších standardů, lze se proti nim však účinně bránit. Například pomocí detekce duplicitní asociace klienta s různými AP, kdy je ke klientovi na stejném kanálu připojeno legitimní i podvodné AP. Další možností obrany je zabránit komunikaci zařízení s AP bez vzájemného ověření sítě pomocí bezpečnostní politiky.

S podvodným AP může útočník dále provádět útoky typu AiTM nebo způsobit odepření služeb, viz Obr. 11. Klient nejprve odešle sondovací (probe) a ověřovací (authentication) požadavek na legitimní AP. Legitimní AP klientovi na jeho požadavky odpoví, ale zároveň odpoví i podvodné AP. Poté, co klient přijme odpověď na žádost o asociaci, je zahájen čtyřcestný handshake. Klient odpoví zprávou 2 bez ohledu na to, zda přijal zprávu 1 od legitimního nebo podvodného AP. Ve chvíli, kdy klient obdrží další zprávu 1 od druhého AP, dojde k selhání čtyřcestného handshake a navázané spojení je přerušeno.

4.1.3 Key Reinstallation Attacks

Podkapitola je zpracována podle [56]. Další metodou používanou při útocích na Wi-Fi sítě je Key Reinstallation Attacks (KRACK). Pro vzájemné ověřování v systémech zabezpečených pomocí WPA se používá klíč nazvaný Pairwise Master Key (PMK). Pomocí PMK doplněného náhodnými čísly SNonce (vygenerovaným na klientovi) a ANonce (vygenerovaným na AP) je vygenerován klíč relace nazvaný Pairwise Transient Key (PTK).

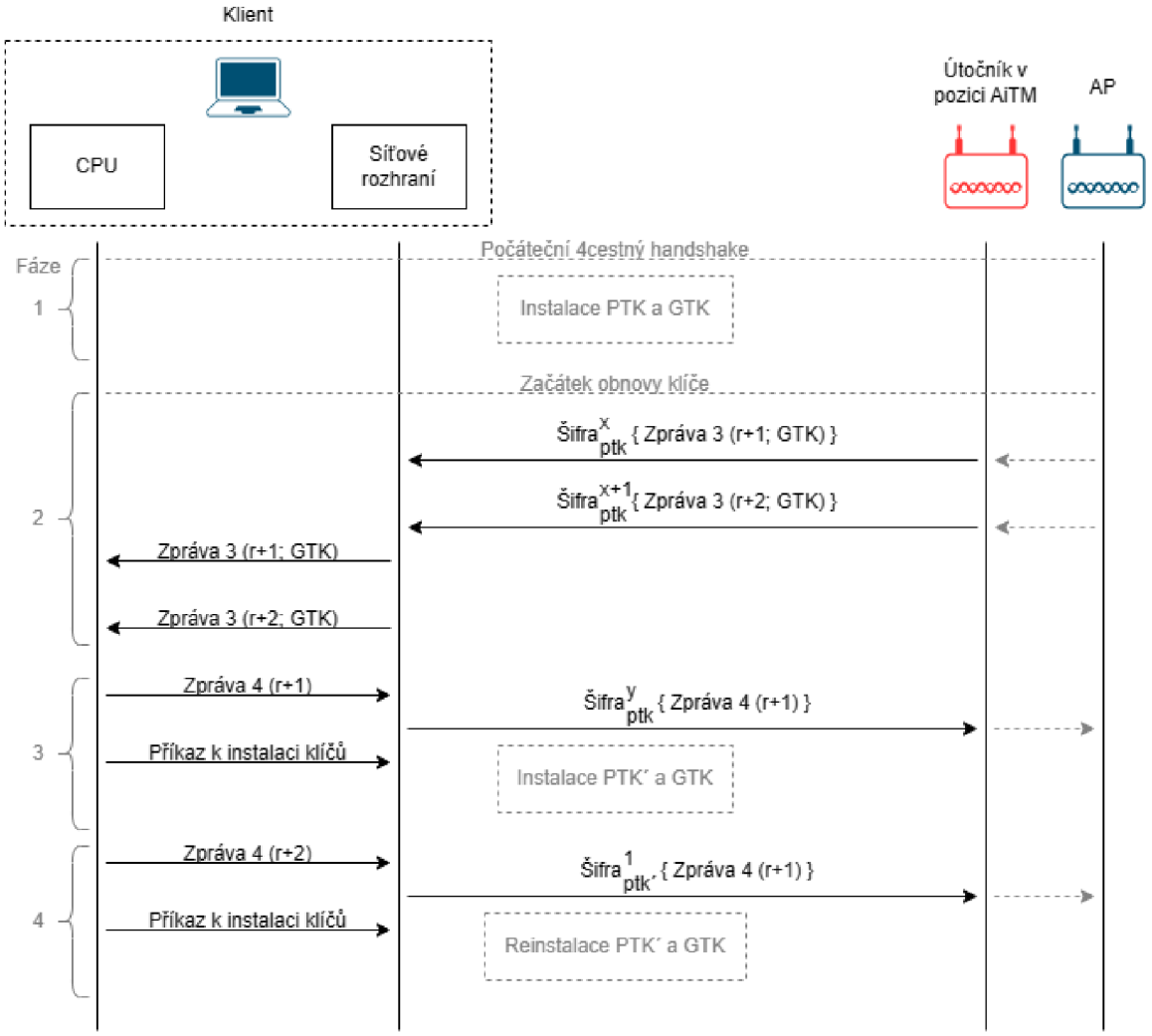


Obr. 11 DoS útok vůči EAP Handshake (Rogue AP).
Zdroj: Vlastní zpracování podle [56]

Vlastní útok spočívá ve vložení zprávy 3 protokolu handshake útočníkem, čímž jsou vynulovány oba čítače Nonce a čítače replay. Důsledkem útoku je to, že se pro následnou komunikaci instaluje předchozí PTK, který byl používán dosud namísto nového. Podmínkou úspěchu je, aby byl útočník v pozici AiTM a povedlo se mu zablokovat doručení zprávy 4 na AP předtím, než sám znovu odešle zprávu 3. Opětovná instalace PTK umožňuje další útoky založené na principu vkládání rámců, dešifrování a falšování zpráv. U některých operačních systémů měla být zranitelnost vůči útokům KRACK vyřešena tím, že při opakovaném přenosu akceptují pouze zašifrovanou verzi zprávy 3. Příkladem mohou být systémy OpenBSD, OS X a macOS.

K útokům KRACK však může dojít i v případech, kdy je zpráva 3 zašifrována. A to díky zranitelnostem v implementacích protokolu handshake v hardwarových komponentách (například v CPU a v síťovém rozhraní), viz Obr. 12. Výměna klíče při

obnově probíhá podobně jako čtyřcestný handshake EAP, ale zprávy jsou v tomto případě již šifrovány aktuálním klíčem. V 1. fázi je stanoven počáteční klíč. Následuje fáze 2, kdy je vyžadována obnova klíče, při které je zahájen handshake s šifrovanými zprávami. Cílem útoku je zašifrovaná zpráva 3. Útočník v pozici AiTM zablokuje přenos zprávy 3 z AP ke klientovi a zprávu 3 si uloží. AP nedostane odpověď od klienta, proto vyšle zprávu 3 znovu. V tomto okamžiku útočník odešle klientovi obě zprávy 3 najednou. Síťové rozhraní obě zprávy dešifruje pomocí aktuálního PTK a odešle je do CPU. Ve 3. fázi CPU obnoví PTK na základě první zprávy. CPU však obdrží i druhou zprávu (původně zašifrovanou starým PTK) a znovu nainstaluje PTK. Důsledkem je reset hodnoty Nonce spojené s PTK na hodnotu 1, což je patrné ve 4. fázi. Oddělení různých bezpečnostních komponent tedy umožňuje vznik dalších zranitelností, přestože byla zavedena opatření v podobě vynuceného šifrování zpráv.



Obr. 12 KRACK útok při vynuceném šifrováním zprávy 3.
Zdroj: Vlastní zpracování podle [56]

4.1.4 DoS útoky vůči WPA3

Podkapitola je zpracovaná podle [56]. Standard WPA3 sice přináší lepší zabezpečení, zároveň však způsobuje velkou výpočetní režii, což může vést ke snížení odolnosti vůči DoS útokům. Protokol Dragonfly-Handshake podporuje kryptografii eliptických křivek (ECC) i kryptografii konečných polí (FFC). K převodu hash hesla na platný bod na eliptické křivce nebo multiplikativní skupině se používá mechanismus pokus-inkrement. Tento proces se skládá z velkého množství operací (řádově většího, než u alternativních metod). Protokol Dragonfly-Handshake obsahuje také mechanismus proti zahlcení, přesto však není zcela odolný vůči DoS útokům. Podle [56] způsobilo podvržení pouhých osmi výměn zpráv protokolu Dragonfly-Handshake za sekundu 100% vytížení CPU AP. Autoři uvádějí, že k útoku bylo využito Raspberry PI B+ se 700 MHz CPU a útok byl veden vůči profesionálnímu AP s 1 200 MHz CPU.

4.1.5 Downgrade útoky

Podkapitola je zpracována podle [56]. Z důvodu zpětné kompatibility obsahuje standard WPA3 tzv. přechodový režim, který umožňuje souběžný provoz WPA3 a WPA2 za použití shodného hesla. Tento režim může být zneužitý k Downgrade útoku, například podvržením zpráv beacon a donucením klientů použít zranitelnější standard WPA2. Proto přechodový režim WPA2 handshake obsahuje prvek RSNE (Robust Security Network Element) se seznamem všech podporovaných standardů zabezpečení. Díky tomu může klient odhalit podvrženou beacon zprávu útočníka.

Tento obranný mechanismus je však přesto zranitelný vůči downgrade útoku. Útočník například může odeslat beacon zprávu obsahující pouze nabídku WPA2 s identifikátorem BSSID legitimního AP (podporujícího WPA3). Klient se připojí k podvodnému AP, přičemž dojde k výměně zpráv 1 a 2 čtyřcestného handshake. Zpráva 2 pak stačí k získání hesla pomocí offline slovníkového útoku. Při tomto typu útoku ani není nutné, aby byl útočník v pozici AiTM.

Další varianta downgrade útoku je zaměřená na množinu eliptických křivek nebo multiplikativních skupin. Framework SAE definuje různé skupiny s možností uživatelské konfigurace. Mechanismus vyjednávání o výběru skupiny může být útočníkem zneužit k vynucení určité skupiny výhodnější pro konkrétní útok. Zde je již nutné, aby byl útočník v pozici AiTM, kde může blokovat některé zprávy a povolit pouze takové, které odpovídají preferované skupině. Různé skupiny mohou vykazovat různé typy zranitelností vůči útokům postranními kanály.

4.1.6 WPS útoky

Podkapitola je zpracovaná podle [54]. WPS je standard, který zjednodušuje proces připojení klienta pomocí kódu PIN nebo stisknutím tlačítka Push Button Configuration (PBC). U některých AP je WPS označeno jako Quick Secure Setup (QSS). WPS se používá pouze při prvním připojení klienta k AP, aby uživatel nemusel zadávat složité heslo, následně již je komunikace zabezpečena pomocí některého ze standardů WPA. Standard WPS však obsahuje bezpečnostní chyby v mechanismu ověřování pomocí kódu PIN. Při tomto způsobu připojení klienta neexistuje kromě ověření PIN žádný jiný požadavek na identifikaci klienta, takže je možné vůči přístupovému bodu použít útok hrubou silou.

Kód PIN se skládá z osmi číslic v rozsahu 0–9. To by teoreticky umožňovalo vytvoření 100 milionů různých kombinací. Ve skutečnosti je osmá číslice kódu PIN kontrolním součtem, takže zbývá pouhých 10 milionů možností. Některá síťová zařízení navíc obsahují další chyby v implementaci standardu WPS, což přispívá k dalšímu urychlení útoku. V současnosti už většina nových bezdrátových síťových zařízení standard WPS kvůli jeho zranitelnostem vůbec nepodporuje. Přesto stále existuje mnoho přístupových bodů, které nebyly aktualizovány a mají z výroby stále povolené připojení pomocí WPS.

Největší slabina bezdrátových sítí spočívá v principu jejich fungování, jak bylo uvedeno výše. Přesto existují možnosti, jak zabezpečení bezdrátových sítí zvýšit. Konkrétně se jedná o následující doporučení:

1. Použít dostatečně silné heslo pro vstup do konfigurace přístupového bodu. Heslo by mělo být komplexní a mělo by obsahovat minimálně dvanáct znaků.
2. Vypnout režim WPS a použít co nejnovější standard šifrování. Tím je v současné době WPA2 + AES, případně vyšší verze WPA3.
3. Použít dlouhé a komplexní heslo pro šifrování provozu WiFi.
4. Filtrovat MAC adresy klientů na přístupovém bodu.
5. Zakázat vysílání ESSID na přístupovém bodu.
6. Deaktivovat možnost automatického připojování klientů.
7. Nepoužívat otevřené sítě s nešifrovaným provozem.
8. Zvýšit povědomí o prevenci mezi uživateli, posílit dohled nad sítí (například formou detekce anomálií nebo detekce narušení), používat otevřené protokoly atd.

4.2 Útok MAC flooding

Podkapitola je zpracována podle [57]. Podle [58] tyto útoky bývají nazývány také *„MAC address table attack“* nebo *„CAM table overflow“*. CAM je označení pro speciální typ počítačové paměti *„Content Addressable Memory“* umožňující velmi rychlé vyhledávání. Tato paměť je součástí přepínačů a obsahuje tabulku s vazbami MAC adresa + fyzický port přepínače + VLAN ID. CAM tabulky jsou obvykle koncipovány pro uložení 100–10 000 záznamů. Při překročení maximálního počtu záznamů dochází k přetečení CAM tabulky. Této zranitelnosti využívají útoky typu CAM table overflow.

Vlastní útok spočívá v tom, že útočník odesílá pakety s různými zdrojovými MAC adresami. Každý záznam je uchován v CAM tabulce přepínače přibližně 300 sekund. Pokud se již MAC adresa v paměti nachází, tak je aktualizováno pouze časové razítko, v opačném případě je MAC adresa uložena. V okamžiku přetečení paměti se přepínač začne chovat jako hub. Přestane filtrovat provoz do jednotlivých portů na základě MAC adres a začne všechny přijaté pakety odesílat na všechny porty kromě příchozího. Útok CAM table overflow je aktivní útok patřící do kategorie útoků odepření služby (Denial of Service, zkráceně DoS). Podle [58] může při neefektivním nastavení zabezpečení a návrhu sítě dojít k úplnému výpadku fungování sítě. Tento útok může útočník dále využít k odposlechu provozu procházejícího přepínačem nebo k provedení AiTM útoku.

Ochrana před útokem spočívá v povolení funkce Port Security a konfiguraci odezvy jednotlivých portů na výskyt nežádoucí komunikace, viz Tabulka 4.

Tabulka 4 Konfigurační příkazy port-security.

Příkaz	Význam
S1(config-if)#switchport mode access	Konfiguruje port přepínače do režimu přístupu.
S1(config-if)#switchport port-security	Identifikuje a omezuje MAC adresy stanic, které mají povolený přístup k portu.
S1(config-if)#switchport port-security maximum 2	Nastavuje maximální počet MAC adres, které mohou být asociovány s daným portem, na hodnotu 2.
S1(config-if)#switchport port-security violation shutdown	Nastavuje port tak, aby byl v případě narušení bezpečnosti vypnut a převeden do chybového stavu.

Zdroj: Vlastní zpracování podle [58]

4.3 Útoky VLAN hopping

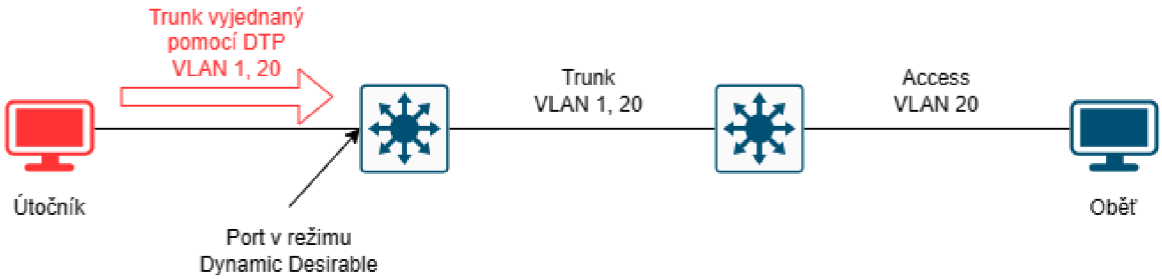
Protokol IEEE 802.1Q podle [57] definuje principy rozdělení jedné fyzické lokální sítě do více logických virtuálních lokálních podsítí (VLAN). Jednotlivé porty přepínače se mohou nacházet v jednom ze dvou režimů. Režim *„trunk port"* umožňuje přenášet provoz jedné nebo více VLAN mezi přepínači. Tento princip se využívá u páteřní části sítě. Druhý režim, nazvaný *„access port"*, umožňuje pouze připojení koncového zařízení do konkrétní VLAN. Díky možnosti zneužití technik VLAN hopping není rozdělení do VLAN podle [59] bezpečné. Autoři dále uvádějí, že je možné provést dva druhy VLAN hopping útoků. Jeden je založený na zneužití proprietárního protokolu Dynamic Trunking Protocol (DTP) firmy Cisco a nazývá se Switch spoofing. Druhý je založený na principu označení jednoho rámce dvěma hlavičkami 802.1Q a nazývá se Double tagging.

4.3.1 Switch spoofing

Podkapitola je zpracována podle [57]. Některé porty přepínače mohou být nastavené v režimu umožňujícím vyjednávání o konfiguraci VLAN pomocí protokolu DTP. Podle [59] jsou takto porty nastavené ve výchozí konfiguraci přepínače a přepínač je díky tomu připraven vytvořit trunk s libovolným síťovým zařízením. Pomocí protokolu DTP pak lze požádat o přepnutí portu do režimu trunk port. Kromě toho je také možné zjistit druh zapouzdření použitého k označení VLAN. Může se jednat o zapouzdření pomocí protokolu 802.1Q nebo Inter-Switch Link (proprietární protokol firmy Cisco označovaný zkratkou ISL).

Přepínače Cisco s podporou DTP protokolu mají celkem čtyři režimy, ve kterých se může port nacházet: *„dynamic auto"* a *„dynamic desirable"* umožňují vyjednání přepnutí do režimu trunk port na základě DTP žádosti, následuje režim *„trunk port"* a dále režim *„access port"*, který jako jediný neumožňuje přepnutí do režimu trunk port. Kromě toho lze na portu deaktivovat DTP vyjednávání pomocí režimu *„nonegotiate"*.

Princip útoku spočívá v odeslání podvržené DTP zprávy útočníkem. Tato zpráva zajistí přepnutí portu z režimu access port do režimu trunk port, a tím útočníkovi zpřístupní veškerý provoz, který by byl za normálních okolností (v režimu access port) filtrován, viz Obr. 13. Podle [59] může útočník získat přístup ke všem VLAN na přepínači. K úspěšnému útoku tedy stačí, aby měl útočník přístup k jednomu přepínači, který má některý z portů nakonfigurovaný v režimu *„dynamic auto"* nebo *„dynamic desirable"*. Výchozí nastavení portů Cisco přepínačů je *„dynamic desirable"*.



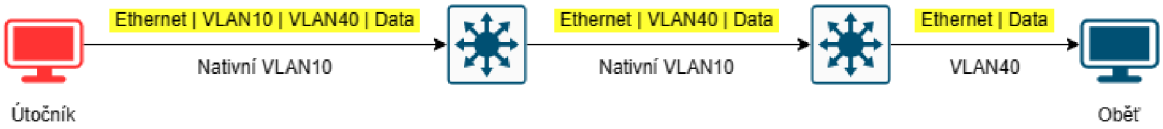
Obr. 13 Útok VLAN hopping – Switch spoofing.
Zdroj: Vlastní zpracování

Způsoby obrany jsou uvedeny souhrnně pro všechny typy útoků zaměřených na VLAN hopping na konci kapitoly 4.3.2.

4.3.2 Double tagging

Podkapitola je zpracována podle [57]. Pro rozlišení jednotlivých VLAN jsou do rámců vloženy další hlavičky 802.1Q. Ty se s výjimkou nativní VLAN vyskytují v rámci celé sítě a obvykle jsou odstraněny až při odeslání rámce koncovému zařízení. Podpora dvojího značení rámců byla zavedena pro využití poskytovateli internetového připojení. Vnější značka slouží k označení koncového uživatele a vnitřní značka slouží k označení poskytovatele.

Princip útoku je následující. Pokud má port přepínače, ke kterému je připojený útočník, přiřazenou nativní VLAN a pokud je vnější značka rámce shodná s nativní VLAN, tak je tato značka odebrána a rámec je odeslán dále, jako by byl určen příjemci v nativní VLAN. Jenže rámec stále obsahuje vnitřní značku. Pokud tento rámec dorazí na další přepínač, tak je vyhodnocena vnitřní značka a na jejím základě je rámec odeslán do cílové VLAN. Tímto způsobem lze obejít síťové mechanismy, které vzájemně logicky izolují jednotlivé VLAN, viz Obr. 14.



Obr. 14 Útok VLAN hopping – Double tagging.
Zdroj: Vlastní zpracování

Nutným předpokladem k provedení tohoto útoku je situace, kdy jsou útočník a oběť připojení k různým přepínačům. Útočník také musí být připojen k portu, který má přiřazenou nativní VLAN, jak bylo uvedeno výše. Konfigurace portu do nativní VLAN je podle [59] obvyklá u portů určených pro administrátory. Další podmínkou úspěšného útoku je podle autorů také to, že útočník musí předem znát MAC adresu a IP adresu oběti.

Obrana před útoky zaměřenými na zneužití VLAN hopping podle [58] spočívá v případě útoku Switch spoofing i útoku Double tagging v zajištění následujících požadavků na konfiguraci přepínače:

- Nepoužívat nativní VLAN 1. Na všech trunk portech změnit nativní VLAN na jiné VLAN ID, než 1.
- Všechny nevyužité porty přepínače by měly být v režimu přístupového portu, měly by být vypnuté a měly by mít přiřazenou tzv. Black hole VLAN. Black hole je VLAN, ve které není nakonfigurované směrování.
- Přístupové porty i trunk porty by se měly konfigurovat výhradně staticky. Mělo by tedy být deaktivováno vyjednávání pomocí DTP.

Konkrétní příkazy, pomocí kterých lze požadované nastavení přepínače zajistit, viz Tabulka 5.

Tabulka 5 Konfigurační příkazy, ochrana před útoky VLAN hopping.

Příkaz	Význam
S1(config-if)#switchport mode access	Konfiguruje port přepínače do režimu přístupu.
S1(config-if)#switchport access vlan 999	Přiřazuje nepoužitému portu VLAN 999 (Black hole).
S1(config-if)#shutdown	Vypíná nepoužitý port.
S1(config-if)#switchport mode trunk	Konfiguruje port přepínače do režimu trunk, to umožňuje přenos provozu více VLAN zároveň.
S1(config-if)#switchport nonegotiate	Deaktivuje DTP vyjednávání.
S1(config-if)#switchport trunk native vlan 10	Přiřazuje trunk portu nativní VLAN 10.

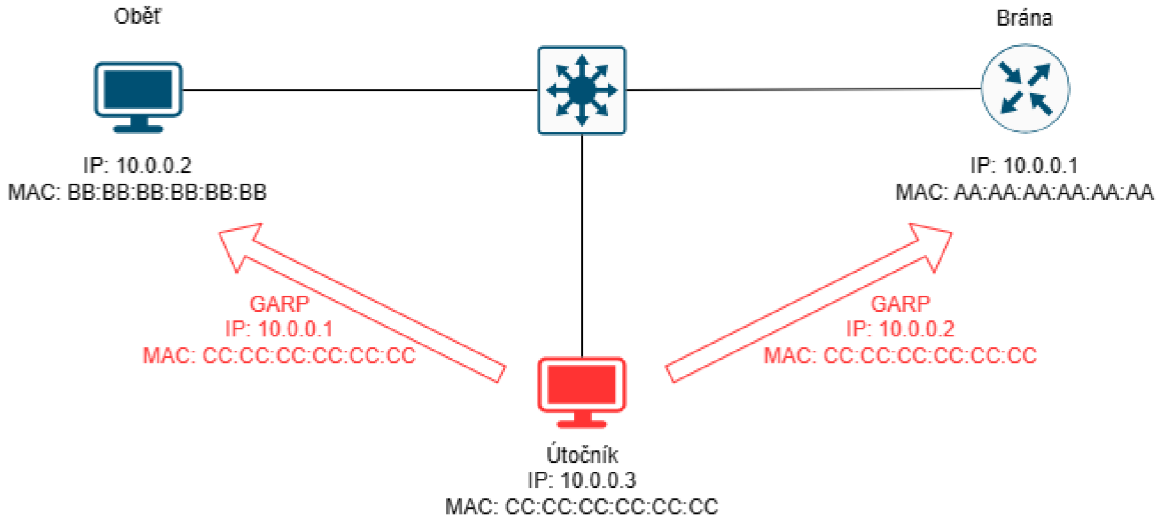
Zdroj: Vlastní zpracování podle [58]

4.4 Útok ARP spoofing

Podkapitola je zpracována podle [57]. Protokol nazvaný Address Resolution Protocol (ARP) za normálních okolností funguje na síťové vrstvě (L2) modelu TCP/IP. Falšování MAC adres se však provádí na vrstvě datového spojení (L1). A to pomocí odpovědi, která nebyla vyvolána požadavkem ARP. Taková nevyžádaná odpověď se nazývá *„Gratuitous ARP“* (GARP). GARP rámec je odeslán jako broadcast, takže odesilatel tímto způsobem oznamuje mapování své MAC adresy na IP adresu všem zařízením v síti. Pomocí podvrženého GARP rámce je možné otrávit MAC tabulky všech zařízení v síti, protože přijaté ARP rámce se nijak neověřují. Podle [58] bývá tento typ útoku označován také *„MAC spoofing“* nebo *„ARP poisoning“*.

Útok může spočívat například v tom, že útočník použije pro vytvoření GARP rámce IP adresu brány a svou MAC adresu, a tím získá přístup k veškerému provozu, který měl být směřován na bránu, viz Obr. 15. Pokud tento provoz přepošle dál na skutečnou bránu, tak jej může pasivně odposlouchávat. V opačném případě je důsledkem útoku odepření služby. Pokud bude útočník zároveň odesílat GARP rámce s IP adresou oběti a svou MAC adresou, tak tímto způsobem může realizovat AiTM útok.

Útokům spočívajícím ve falšování MAC adres se podle [58] dá zabránit několika způsoby. Pokud v síti není DHCP server a spoléhá se na statické adresování, tak je podle autorů nutné specifikovat MAC adresy každého zařízení pro každý z portů přepínače. V opačném případě je situace jednodušší, protože obrana je shodná jako v případě útoku DHCP starvation, viz kapitola 4.6. Dále je podle autorů nutné povolit funkci Dynamic ARP Inspection (DAI), která ověřuje pakety protokolu ARP. Pokud je zachycen paket ARP s neplatnou vazbou MAC adresy na IP adresu, tak je událost zaznamenána a paket zahozen. Tato funkce je závislá na obsahu databáze vazeb DHCP snooping, takže je nutné mít zároveň povolenou i funkci DHCP snooping, viz kapitola 4.6. Příkaz pro povolení DAI viz Tabulka 6.



Obr. 15 Útok ARP spoofing.
Zdroj: Vlastní zpracování

Tabulka 6 Konfigurační příkazy Dynamic ARP Inspection.

Příkaz	Význam
S1(config)#ip arp inspection vlan 10	Aktivuje funkci Dynamic ARP Inspection pouze pro VLAN 10.

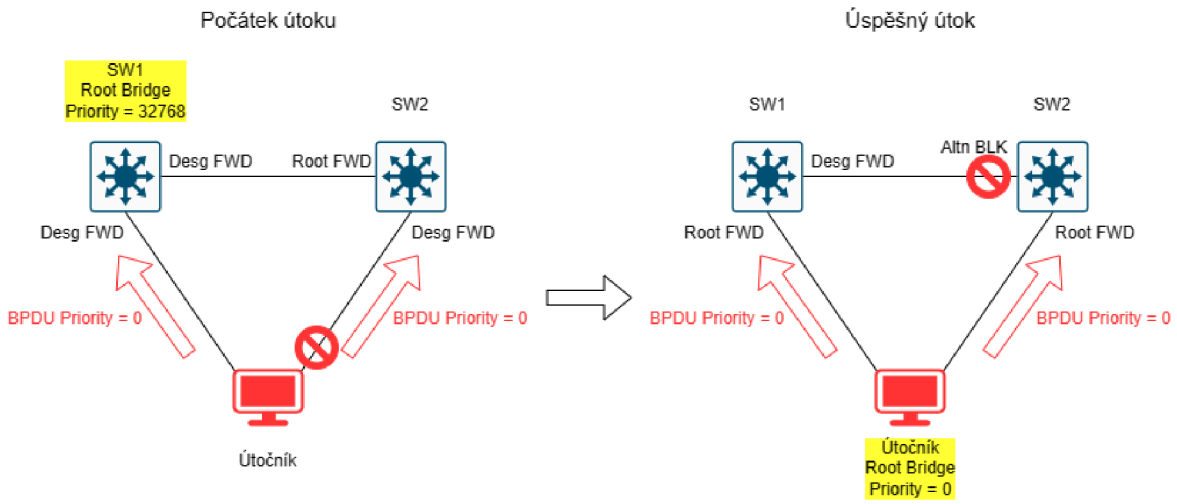
Zdroj: Vlastní zpracování podle [58]

4.5 Útok vůči STP

Podkapitola je zpracována podle [57]. Pro případ selhání trasy v síti může existovat jedna nebo více záložních tras. V takovém případě je však nutné zajistit prevenci před vznikem smyček. Vznik smyčky by totiž mohl být příčinou takzvané *„broadcast storm“*. Tento jev negativně ovlivňuje výkon sítě. Jednou z možností, jak vytvoření nekonečných smyček zabránit, je využít Spanning Tree Protocol (STP). Tento protokol je definovaný normou IEEE 802.1D a je založený na algoritmu *„Spanning Tree Algorithm”* (STA). Protokol STP je možné použít v sítích, které obsahují přepínače, případně mosty kompatibilní s normou 802.1D. Podle [59] STP neposkytuje žádné ověřovací mechanismy a jedná se o protokol důvěryhodný a bezstavový.

V síti podporující protokol STP je jednomu přepínači přiřazena role *„root bridge“*. Ostatní přepínače jsou následně zodpovědné za rozhodnutí o výběru jedné aktivní trasy směrem k *„root bridge“*. Port, přes který tato trasa vede, je označen jako root port. Případné další trasy k *„root bridge“* musí být označeny jako alternativní a příslušné porty přepínačů musí být uvedeny do režimu blokování. Dalším prvkem podílejícím se na fungování STP jsou zprávy *„Bridge Protocol Data Units“* (BPDU). Tyto zprávy jsou vysílané jako multicast. Podle [59] přepínače odesílají ve výchozím nastavení BPDU zprávu každé dvě sekundy. Autoři dále uvádějí, že přepnutí portu ze stavu blokování do stavu předávání trvá padesát sekund. Za distribuci zpráv BPDU na ostatní přepínače v síti je zodpovědný root bridge. Jako root bridge je nastaven přepínač s nejnižším bridge ID (BID). BID se skládá z nastavitelné priority a MAC adresy přepínače.

Princip útoku spočívá v tom, že útočník odešle do sítě VLAN podvržené zprávy BPDU. Na základě těchto zpráv začnou síťová zařízení útočníka považovat za root bridge. Z toho vyplývá, že pro tento druh útoku je nezbytné, aby se v síti nacházely minimálně dva mosty nebo přepínače, zároveň musí mít útočník k oběma z nich přístup, viz Obr. 16. V případě úspěšného útoku připadá v úvahu několik variant. Podle [59] například útočník může odeslat konfigurační zprávu BPDU, narušit tím stabilní topologii bez smyčky a vyvolat broadcast storm. V konečném důsledku pak může dojít k odepření služeb. Alternativně může útočník pasivně odposlouchávat síťový provoz obětí nebo do zachyceného provozu aktivně vkládat síťové rámce. Pokud po úspěšném útoku na STP prochází veškerá komunikace mezi klientem a serverem přes útočníka, tak lze provést AiTM útok.



Obr. 16 Útok STP.
Zdroj: Vlastní zpracování podle [57]

Podle [60] lze útokům zaměřeným na manipulaci STP předcházet pomocí funkcí **Portfast, BPDU guard a Root guard**. Příkazy sloužící k obraně před STP útoky viz Tabulka 7.

Port nakonfigurovaný v režimu **Portfast** je podle [60] okamžitě převeden ze stavu blokování (blocking) do stavu předávání (forwarding), stavy naslouchání (listening) a učení (learning) jsou přeskočeny. U portů nastavených v režimu Portfast je podle autorů zajištěno, že útočník nemůže číst informace o topologii sítě, proto by měly být všechny porty, které se neúčastní výpočtu STP, nastavené v režimu Portfast.

Pokud port přijme rámec BPDU a má aktivovanou funkci **BPDU Guard**, tak podle [60] dojde k okamžité deaktivaci portu do chybového stavu. Autoři dále uvádějí, že tato funkce chrání systém před neplánovaným přidáním dalších přepínačů do topologie a stejně tak případný útočník nebude schopen vynutit volbu root bridge.

Funkce **Root Guard** podle [60] omezuje možnost vyjednat na portech, kde je tato funkce povolena, nastavení root bridge. Díky tomu se podle autorů nemůže z nedůvěryhodného přepínače stát root bridge. Autoři dále uvádějí, že přepínač prozkoumá všechny BPDU rámce přijaté na portech s aktivní funkcí root guard, a pokud nalezne rámec, ve kterém je lepší BID, než má aktuální root bridge, tak se port přepne do stavu naslouchání (listening) a přestane přenášet provoz. Pokud na port přestanou přicházet rámce s lepším BID, tak se port vrátí do stavu předávání (forwarding).

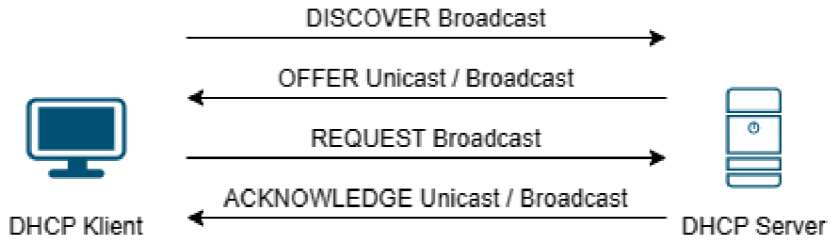
Tabulka 7 Konfigurační příkazy spanning-tree.

Příkaz	Význam
S1(config-if)#spanning-tree portfast	Umožňuje okamžitý přechod portu do stavu předávání (forwarding). Port slouží pro připojení koncových zařízení.
S1(config-if)#spanning-tree bpduguard enable	Nastavuje ochranu portu před nežádoucími BPDU pakety. Pokud port obdrží BPDU od připojeného zařízení, tak se deaktivuje.
S1(config)#spanning-tree portfast bpduguard default	Nastavuje ochranu před nežádoucími BPDU pakety pro všechny porty v režimu portfast. Pokud některý z portů obdrží BPDU od připojeného zařízení, tak se deaktivuje.
S1(config-if)#spanning-tree guard root	Pokud port s aktivní funkcí root guard obdrží BPDU od připojeného zařízení s lepším BID než má aktuální root bridge, tak se přepne do stavu naslouchání (listening).

Zdroj: Vlastní zpracování podle [58]

4.6 Útok DHCP starvation

Podkapitola je zpracována podle [59]. Dynamic Host Configuration Protocol (DHCP) využívá pro svou funkci takzvaný proces DORA sestávající ze zpráv Discover, Offer, Request a Acknowledge, viz Obr. 17. Výměna těchto zpráv probíhá mezi DHCP serverem a klientem.



Obr. 17 Proces komunikace DHCP.
Zdroj: Vlastní zpracování podle [61]

Následuje podrobnější popis procesu přiřazování IP adres pomocí protokolu DHCP, zpracovaný podle [62]:

- Klient nejprve odešle zprávu Discover jako broadcast. Díky této zprávě se DHCP server dozví, že se některý z klientů připojil k síti, a požaduje IP adresu.
- Následně DHCP server poskytne klientovi nabídku (Offer) obsahující IP adresu, obvykle jako unicast zprávu.

- V síti by se měl vyskytovat pouze jeden DHCP server. Pokud se v síti nachází DHCP serverů více, tak může každý z nich odpovědět klientovi. Proto klient musí odeslat požadavek (Request) jako broadcast, čímž potvrdí nabídku serveru, který odpověděl jako první. Díky této zprávě jsou zároveň ostatní servery informovány o tom, že mohou stáhnout svou nabídku a poskytnout IP adresu jiným klientům.
- Poslední zpráva procesu DORA je podle autorů potvrzení (Acknowledge) odeslané vybraným serverem jako unicast. Tato zpráva obsahuje dobu pronájmu a další informace o konfiguraci sítě.

Proces přidělování adres je založený na principu fronty. K identifikaci klientů slouží pouze jejich MAC adresa. Podle [61] poskytuje protokol DHCP kromě IP adres ještě další informace o konfiguraci sítě, například masku podsítě a výchozí bránu. Autoři dále uvádějí, že DHCP protokol využívá služeb protokolu UDP, přičemž server používá port 67 a klient používá port 68. Podle autorů obsahuje DHCP paket zejména následující pole: identifikátor transakce (xid) má délku čtyři oktety, obsahuje náhodné číslo vygenerované klientem a je používáno klientem i serverem k asociaci zpráv do konverzace; hardwarová adresa klienta (chaddr) má délku šestnáct oktetů a v případě legitimního DHCP paketu se jeho obsah shoduje s MAC adresou uvedenou v ethernetovém rámci; možnosti DHCP (DHCP options) je volitelné pole s variabilní délkou obsahující volitelné parametry.

Podle [62] je protokol DHCP zranitelný vůči útokům DHCP starvation a spoofing díky tomu, že zprávy nejsou na DHCP serveru ověřovány. Princip útoku spočívá v tom, že útočník odesílá pakety s jedinečnými identifikátory transakce, tím se pokusí vyčerpat celý rozsah dostupných IP adres. Vyčerpání rozsahu je obvykle docíleno pomocí odesílání zpráv Discover s náhodnými MAC adresami. Po vyčerpání celého rozsahu již server nemůže poskytnout žádné IP adresy legitimním klientům. V této fázi podle [62] může útočník vytvořit falešný DHCP server, který začne odpovídat na požadavky legitimních klientů, a připravit tím prostor k provedení dalších útoků typu spoofing nebo AiTM.

Jako obrana před útoky DHCP starvation slouží podle [62] technika DHCP snooping založená na odposlechu veškeré komunikace v síti. Pokud přepínač detekuje narušení, tak podle autorů zahodí paket, zapíše informaci do logu a deaktivuje port přepínače, na kterém bylo narušení zachyceno. Autoři dále uvádějí, že detekce narušení spočívá v nastavení maximálního počtu DHCP paketů, které může port přijmout během

jedné sekundy. Přepínač s podporou DHCP snooping si podle autorů udržuje databázi vazeb DHCP obsahující MAC adresu, IP adresu, zbývající dobu pronájmu, VLAN a port přepínače. Autoři dále uvádějí, že na přepínačích Cisco je DHCP snooping ve výchozím nastavení zakázán. Pro povolení techniky DHCP snooping a konfiguraci portů slouží příkazy, viz Tabulka 8.

Tabulka 8 Konfigurační příkazy DHCP snooping.

Příkaz	Význam
S1(config)#ip dhcp snooping	Povoluje DHCP snooping.
S1(config)#ip dhcp snooping vlan 10	Povoluje DHCP snooping ve VLAN 10.
S1(config-if)#ip dhcp snooping trust	Důvěryhodný port pro připojení autorizovaného DHCP serveru. Jsou předávány všechny DHCP zprávy.
S1(config-if)#ip dhcp snooping limit rate 5	Port pro připojení klientů akceptující maximálně 5 zpráv DHCP Discover za sekundu.

Zdroj: Vlastní zpracování podle [62]

5 Experimentální část

Cílem experimentální části je praktické ověření možností zneužití vybraných zranitelností síťových prvků v laboratorním prostředí. Bude se jednat o simulaci útoků představených v kapitole 4. Pro vlastní simulaci budou použity vybrané nástroje představené v kapitole 3.

Nejprve budou prověřeny účinky útoků na síťové prvky za použití výchozího nebo minimálního zabezpečení, a to včetně vyhodnocení možných rizik, případně navázání dalších útoků. Poté bude aplikováno doporučené zabezpečení síťových prvků podle kapitoly 4. Následně bude ověřena účinnost provedeného zabezpečení zopakováním útoku se stejnými parametry.

5.1 Scénář

- Útok vůči bezdrátové síti IEEE 802.11, spočívající v zachycení handshake WPA2 a provedení slovníkového útoku. Porovnání časů nutných k prolomení hesla v závislosti na počtu testovaných klíčů WPA.
- Útok MAC flooding s odposlechem síťové komunikace obětí, přičemž útočník je v roli AiTM. Provedení zabezpečení a ověření jeho účinnosti.
- Útok switch spoofing se zachycením podvrženého paketu na PC oběti. Provedení zabezpečení a ověření jeho účinnosti.
- Útok double tagging se zachycením podvrženého paketu na PC oběti. Provedení zabezpečení a ověření jeho účinnosti.
- Útok ARP spoofing s odposlechem síťové komunikace obětí, přičemž útočník je v roli AiTM. Provedení zabezpečení a ověření jeho účinnosti.
- Útok STP s ověřením možnosti převzetí role root bridge útočníkem. Provedení zabezpečení a ověření jeho účinnosti.
- Útok DHCP starvation s ověřením, zda PC oběti získá IP adresu po zahlcení legitimního serveru podvrženými DHCP pakety. Provedení zabezpečení a ověření jeho účinnosti.

5.2 Použitý hardware a software

Při simulacích síťových útoků byl použit hardware a software viz Tabulka 9.

Tabulka 9 Hardware a software použitý při experimentech.

Počet [ks]	Popis
1	PC DELL OptiPlex Tower Plus 7010 CPU: Intel® Core™ i9-13900 @ 2 GHz RAM: 64 GB OS: Kali Linux 2023.4, 64-bit
2	PC DELL OptiPlex Tower Plus 7010 CPU: Intel® Core™ i9-13900 @ 2 GHz RAM: 64 GB OS: Windows 11 Pro 22H2, 64-bit
1	NB DELL Latitude E7440 CPU: Intel® Core™ i5-4300U @ 1,90 GHz 2,50 GHz RAM: 16 GB OS: Microsoft Windows 11 Pro 22H2, 64-bit
2	Přepínač CISCO Catalyst 9300 OS: Cisco IOS XE Software, Version 17.09.03
2	Přepínač CISCO Catalyst 1000 OS: Cisco IOS Software, Version 15.2(7)E7
1	AP Mikrotik RouterBOARD 493GAH WiFi karta: RouterBOARD R52n-M OS: RouterOS v6.43.4
1	USB WiFi karta ALFA AWUS036ACM

Zdroj: Vlastní zpracování

5.3 Přípravné práce

Před započetím prací bylo nutné vypnout firewall na obou PC s operačním systémem Microsoft Windows, protože blokoval příchozí ICMP pakety. Na PC určeném pro Kali Linux bylo nutné v nastavení UEFI deaktivovat funkci Secure Boot, protože kód jádra Kali Linux není opatřen digitálním podpisem.

Po nainstalování distribuce Kali Linux byla většina požadovaných nástrojů připravená k okamžitému použití. Bylo však nutné doinstalovat balíček Yersinia. Nejprve byla provedena aktualizace systémového repozitáře pomocí příkazu **sudo apt update**, a poté byl nainstalován balíček Yersinia pomocí příkazu **sudo apt install yersinia**. Aplikaci Yersinia se nepodařilo spustit v grafickém režimu, takže byl použit interaktivní terminálový režim, podrobnosti viz kapitola 3.6.

Slovník rockyou.txt použitý při útoku vůči bezdrátové síti 802.11 je ve výchozím stavu zabalený. Před použitím bylo nutné jej rozbalit pomocí příkazů **cd /usr/share/wordlists/** a **gunzip rockyou.txt.gz**.

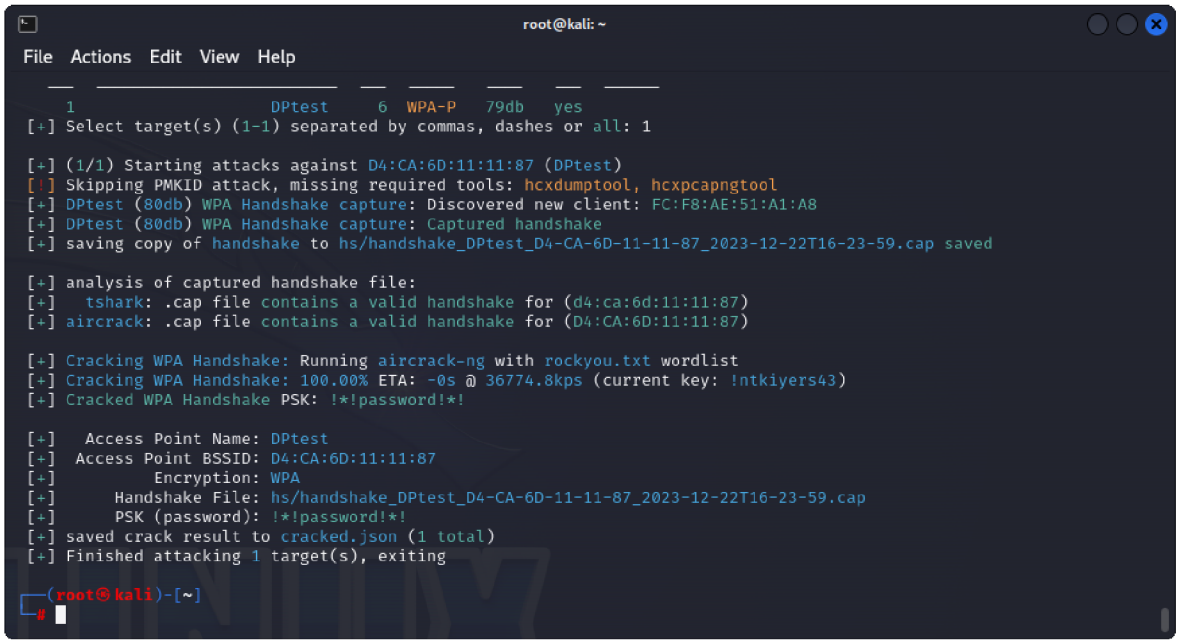
5.4 Útok vůči bezdrátové síti 802.11

Pro simulaci tohoto útoku byl použit AP Mikrotik RouterBOARD, PC s USB WiFi kartou ALFA AWUS036ACM v roli útočníka a NB v roli klienta, vůči kterému byly odeslány deautentizační rámce ve fázi zachytávání čtyřcestného handshake. Simulace útoků byla provedena pomocí nástroje Wifite s použitím dvou slovníků za účelem porovnání časů potřebných k nalezení použitého klíče. Při každém z útoků byl AP zabezpečen šifrovacím standardem WPA2 s použitím předsdílených šifrovacích klíčů. Pro výpočet hash ze slovníkových hesel a porovnání s hash zachyceným z komunikace AP s klientem byl použit nástroj Aircrack-ng. Aircrack-ng provádí výpočty s využitím CPU a je to výchozí nástroj používaný Wifite. Pro urychlení celého procesu byla při obou útocích provedena deautentizace klienta. V okamžiku provedení deautentizace byl na klientském NB pozorován krátký, téměř nepozorovatelný výpadek připojení. Díky zaškrtnuté volbě *„Připojovat automaticky“* v nastavení WiFi sítě ve Windows bylo spojení opětovně navázáno.

Při prvním útoku byl nástroj Wifite spuštěn s následujícími parametry: *„wifite -i wlan0mon -c6 --no-wps“*, přičemž byl použit výchozí slovník nástroje Wifite *„/usr/share/dict/wordlist-probable.txt“*, který obsahuje 203 809 řádků s hesly. Pro zabezpečení WiFi sítě byl použit klíč *„P@ssw0rd“*, který se v uvedeném slovníku nachází na řádku číslo 1 498. Nalezení klíče trvalo cca jednu minutu a čtyři sekundy.

Při druhém útoku byl nástroj Wifite spuštěn s následujícími parametry: *„wifite -i wlan0mon -c6 --no-wps --dict /usr/share/wordlists/rockyou.txt“*. Tentokrát byl použit slovník *„rockyou.txt“* uvedený jako parametr. Slovník *„rockyou.txt“* obsahuje 14 344 392 řádků s hesly. Pro zabezpečení WiFi sítě byl použit klíč *„!*!password!*!“*, který se v uvedeném slovníku nachází na řádku číslo 14 342 737. Nalezení klíče trvalo cca sedm minut a třicet čtyři sekund.

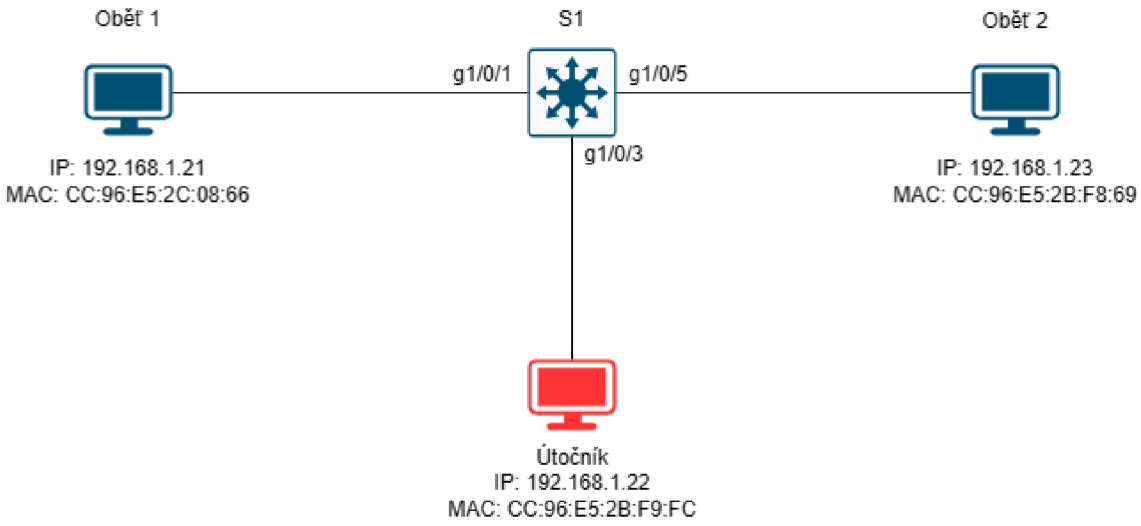
Rozdíl v počtu řádků, které bylo nutné otestovat při výše uvedených útocích tedy činí 14 341 239 řádků a rozdíl časů potřebných k nalezení klíčů činí šest minut a třicet sekund. Ověření jednoho hesla tedy trvalo přibližně 27,2 µs, což přibližně odpovídá hodnotě 36 774,8 kps (keys per second) uvedené ve výpisu nástroje Wifite, viz Obr. 18. Tato hodnota udává počet testovaných klíčů za sekundu.



Obr. 18 Výpis nástroje Wifite s využitím slovníku rockyou.txt.
Zdroj: Vlastní zpracování

5.5 Útok MAC flooding

Pro simulaci tohoto útoku byl použit přepínač CISCO Catalyst 9300, dva PC v roli obětí a jeden PC v roli útočníka. Topologie sítě, použitá čísla portů, IP adresy a MAC adresy jsou uvedeny na Obr. 19. Přepínač CISCO 9300 dle dokumentace disponuje CAM tabulkou o velikosti 32 768 záznamů.



Obr. 19 Topologie sítě při útoku MAC flooding.
Zdroj: Vlastní zpracování

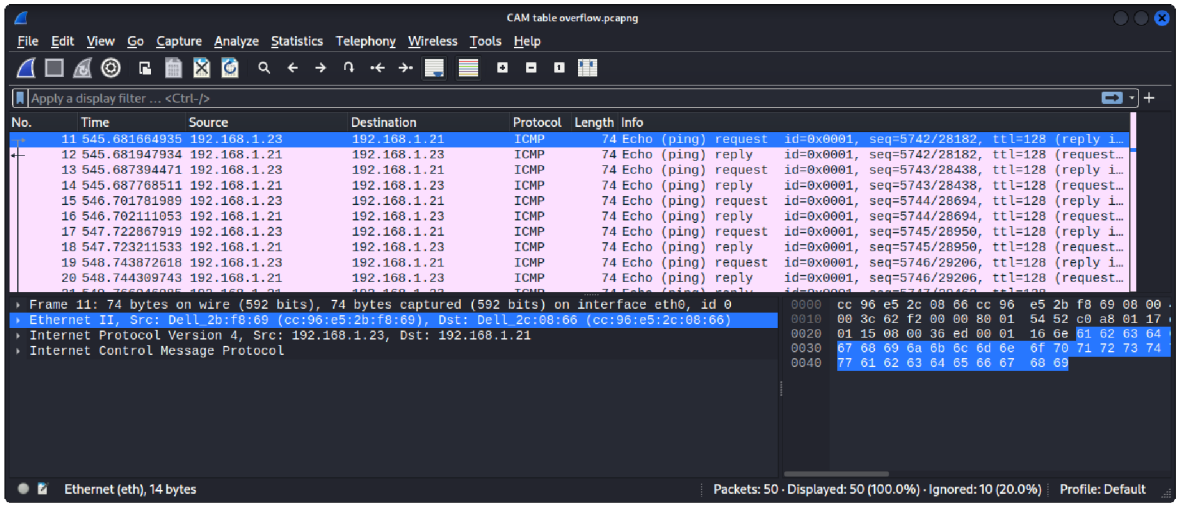
Pomocí nástroje macof z balíčku Dsniff se podařilo zaplnit celou CAM tabulku přepínače fiktivními záznamy, viz Obr. 20. Díky tomu se přepínač začal chovat jako hub. Ovšem pouze vůči zařízením, která byla připojena až po zaplnění CAM tabulky nebo kterým už vypršela platnost záznamů v CAM tabulce. Vůči zařízením, jejichž MAC

adresy byly v okamžiku zahájení útoku uložené v CAM tabulce, se přepínač stále choval jako přepínač. Nebylo tedy možné odposlouchávat jejich komunikaci pomocí nástroje Wireshark spuštěného na PC útočníka.

```
S1#show mac address-table count
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 32767
Static  Address Count  : 1
Total Mac Addresses    : 32768

Total Dynamic Address Count  : 32767
Total Static  Address Count  : 1
Total Mac Address In Use     : 32768
Total Mac Address Space Available: 0
```

Obr. 20 Zaplnění CAM tabulky (MAC flooding).
Zdroj: Vlastní zpracování

Vypršení platnosti záznamů v CAM tabulce lze v laboratorním prostředí simulovat smazáním záznamů svázaných s vybraným portem přepínače pomocí příkazu **clear mac address-table dynamic interface g1/0/1**. Tuto možnost však skutečný útočník obvykle nemá. Při splnění výše uvedených podmínek se podařilo provést útok AiTM, tj. odposlechnout ICMP komunikaci dvou obětí, viz Obr. 21.



Obr. 21 Provoz zachycený útočníkem (MAC flooding).
Zdroj: Vlastní zpracování

DoS útok způsobený přetečením CAM tabulky se nasimulovat nepodařilo. K přerušení komunikace mezi oběťmi nedošlo ani na okamžik. Příčinou neúspěchu bylo pravděpodobně nízké zatížení sítě v kombinaci s vysokým výkonem přepínače. V okamžiku útoku se v síti vyskytovali pouze dva hostitelé a útočník. Všechny porty přepínače byly nastavené na rychlost 1 GB/s v režimu Full Duplex. Pro úspěšné ověření DoS útoku by pravděpodobně bylo nutné použít více hostitelů a generovat více provozu.

Po ověření vlivu útoku MAC flooding na chování přepínače byla provedena konfigurace zabezpečení pomocí funkce Port Security, viz Obr. 22. Při opětovném spuštění útoku došlo k očekávané deaktivaci portu, ke kterému byl připojený útočník, viz Obr. 23. Po vyřešení problému lze port opět aktivovat použitím příkazů **shutdown** a **no shutdown**.

```
S1(config)#interface range g1/0/1 - 23
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 5
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#end
```

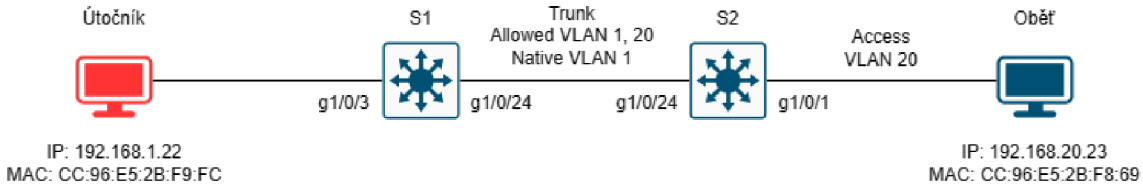
Obr. 22 Konfigurace zabezpečení vůči útoku MAC flooding.
Zdroj: Vlastní zpracování

```
S1#
*Dec 19 14:35:41.895: %PM-4-ERR_DISABLE: psecure-violation error
detected on Gi1/0/3, putting Gi1/0/3 in err-disable
*Dec 19 14:35:41.899: %PORT_SECURITY-2-PSECURE_VIOLATION: Security
violation occurred, caused by MAC address 2a22.723
*Dec 19 14:35:42.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/3, changed state to down
*Dec 19 14:35:43.898: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3,
changed state to down
```

Obr. 23 Deaktivace portu při spuštění útoku MAC flooding.
Zdroj: Vlastní zpracování

5.6 Útoky VLAN hopping

Pro simulaci obou útoků VLAN hopping byly použity dva přepínače CISCO (konkrétní typy jsou uvedené v podkapitolách), jeden PC v roli oběti a jeden PC v roli útočníka. Topologie sítě, použitá čísla portů, IP adresy a MAC adresy jsou uvedeny na Obr. 24.

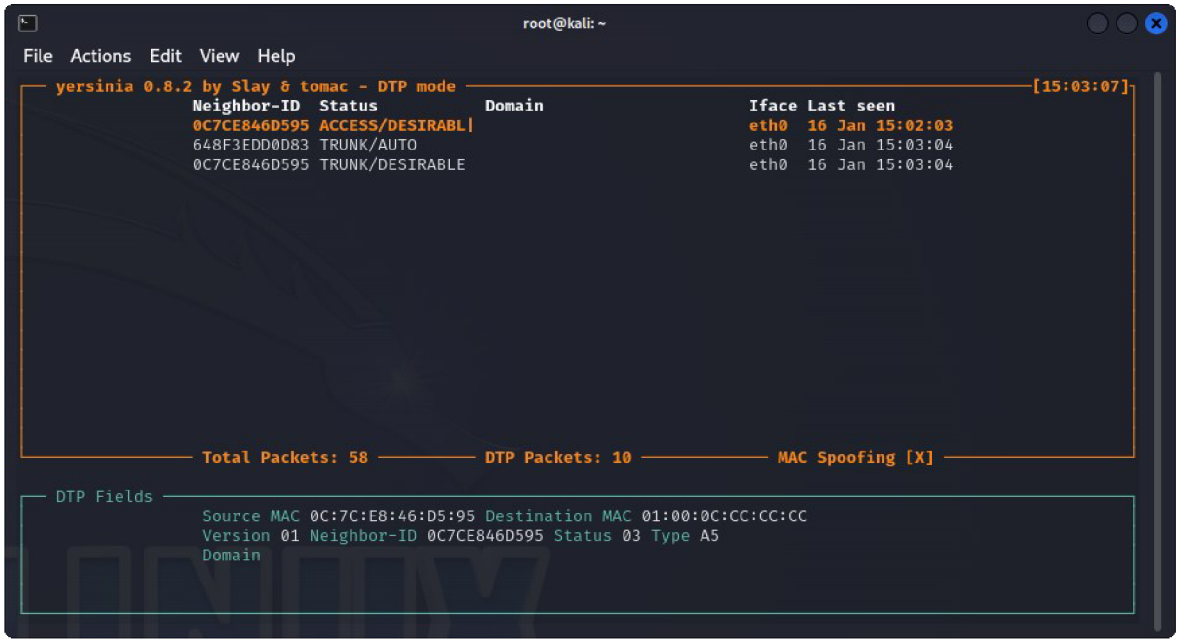


Obr. 24 Topologie sítě při útocích VLAN hopping.
Zdroj: Vlastní zpracování

5.6.1 Útok switch spoofing

Pro útok switch spoofing byly použity přepínače CISCO Catalyst 9300. Port g1/0/3 přepínače S1 byl ponechán bez konfigurace, tj. nebyl vybrán režim portu pomocí příkazu **switchport mode** ani portu nebyla přiřazena žádná VLAN. Port se tedy nacházel ve výchozím režimu *„dynamic desirable“*.

Útok byl proveden pomocí nástroje yersinia, kde byl nejprve vybrán protokol DTP a následně zahájen útok č. 1 *„enabling trunking“*, viz Obr. 25. Po několika desítkách sekund od zahájení útoku došlo k očekávanému přepnutí portu do režimu trunk, viz Obr. 26.



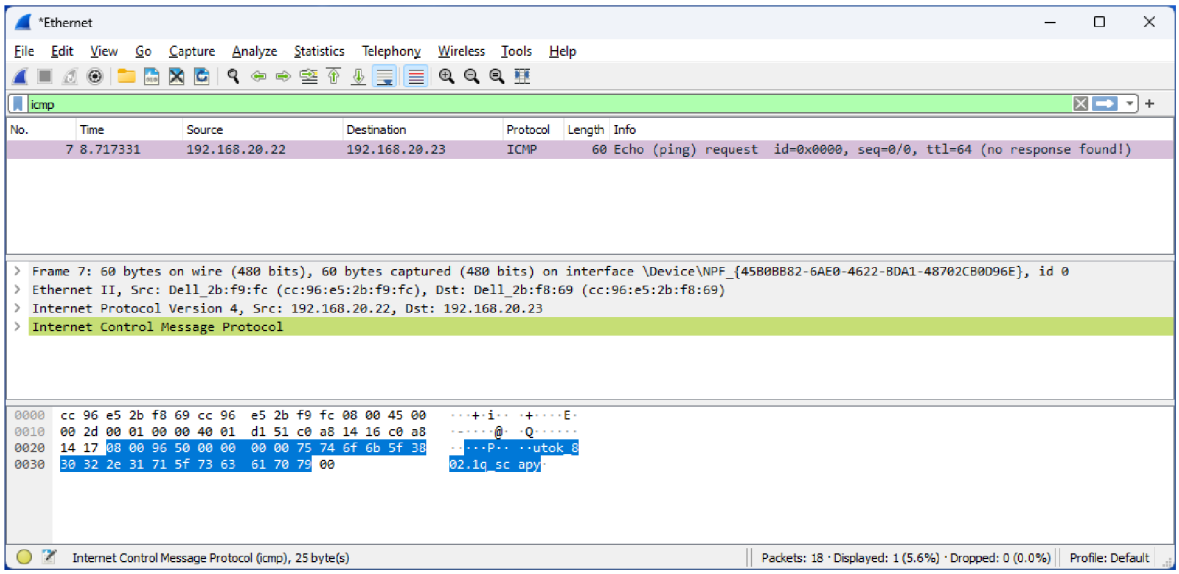
Obr. 25 Vyjednání režimu trunk pomocí DTP (switch spoofing).
Zdroj: Vlastní zpracování

```
S1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/3     auto             802.1q         trunking      1
Gi1/0/24    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/0/3     1-4094
Gi1/0/24    1,20

Port        Vlans allowed and active in management domain
Gi1/0/3     1,20
Gi1/0/24    1,20

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/3     1,20
Gi1/0/24    1,20
```

Obr. 26 Výpis portů přepínače S1 v režimu trunk (switch spoofing).
Zdroj: Vlastní zpracování

Přepnutí portu do režimu trunk bylo následně ještě ověřeno odesláním podvržené ICMP zprávy z PC útočníka na PC oběti pomocí funkce sendp() nástroje Scapy. Do hlavičky ethernetového rámce byl vložen 802.1Q tag s hodnotou VLAN=20, viz Obr. 27. Tato zpráva úspěšně dorazila na PC oběti, kde byla zachycena pomocí nástroje Wireshark, viz Obr. 28.

Obr. 27 Odeslání podvržené ICMP zprávy (switch spoofing).
Zdroj: Vlastní zpracování



Obr. 28 Zachycení podvržené ICMP zprávy na PC oběti (switch spoofing).
Zdroj: Vlastní zpracování

Po ověření útoku byl port g1/0/3 přepínače S1 zabezpečen pomocí příkazů **switchport mode access** a **switchport access vlan 10**. Při opětovném spuštění útoku DTP *„enabling trunking“* s pomocí nástroje Yersinia se již nepodařilo přepnout port do režimu trunk. Tím byl port úspěšně zabezpečen před útokem typu switch spoofing.

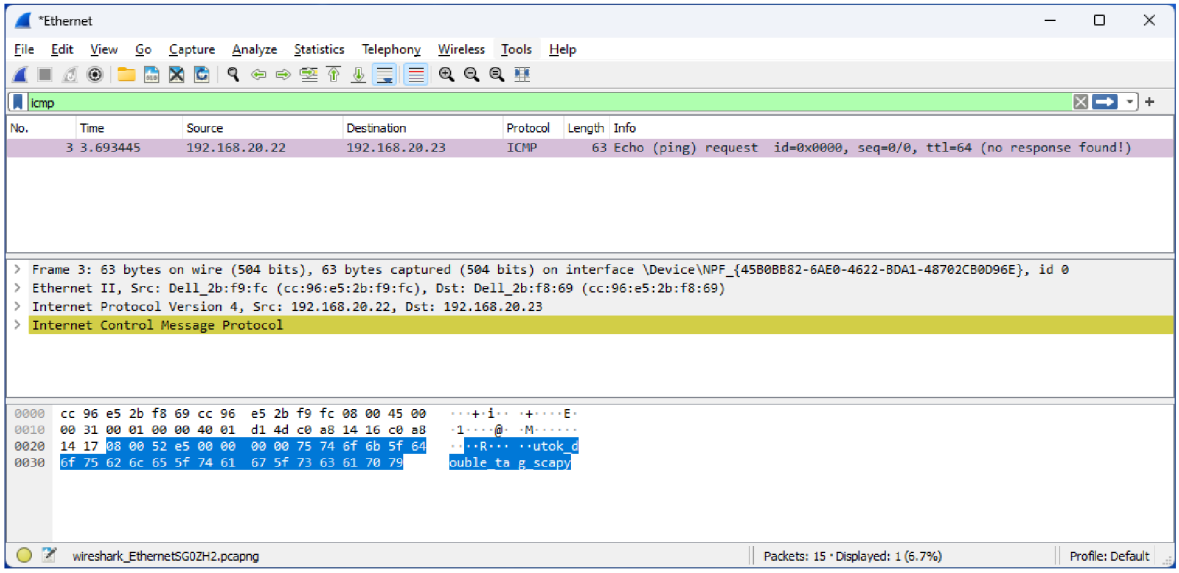
5.6.2 Útok double tagging

Útok double tagging se s použitím přepínačů CISCO Catalyst 9300 nepodařilo nasimulovat, proto byly pro tento typ útoku použity starší přepínače CISCO Catalyst 1000. Port g1/0/3 přepínače S1 byl pro účely tohoto útoku nakonfigurován pomocí příkazů **switchport mode access** a **switchport access vlan 1**. Přičemž VLAN 1 byla nativní VLAN použitá k propojení přepínačů S1 a S2, což je podmínka nutná k provedení tohoto typu útoku.

Poté byla použita funkce sendp() nástroje Scapy k odeslání podvržené ICMP zprávy na PC oběti. Ukázalo se však, že při použití dvou tagů 802.1Q zpráva na PC oběti nedorazila, proto byl do zprávy přidán ještě třetí tag, viz Obr. 29. Následně se již podařilo zprávu ICMP zachytit nástrojem Wireshark na PC oběti, viz Obr. 30. Z toho vyplývá, že přepínač S1 odstranil nikoliv jeden tag, ale dva. Teprve po přidání třetího tagu dorazil tento paket na trunk port přepínače S2, kde zajistil doručení do cílové VLAN.

Poté byl port g1/0/3 přepínače S1 zabezpečen pomocí příkazu **switchport access vlan 10**. Při opětovném odeslání podvržené ICMP pomocí Scapy se tuto zprávu na PC oběti již zachytit nepodařilo. Port přepínače byl zabezpečen před útokem typu double tagging změnou přístupové VLAN portu g1/0/3 tak, aby byla odlišná od nativní VLAN trunk portu.

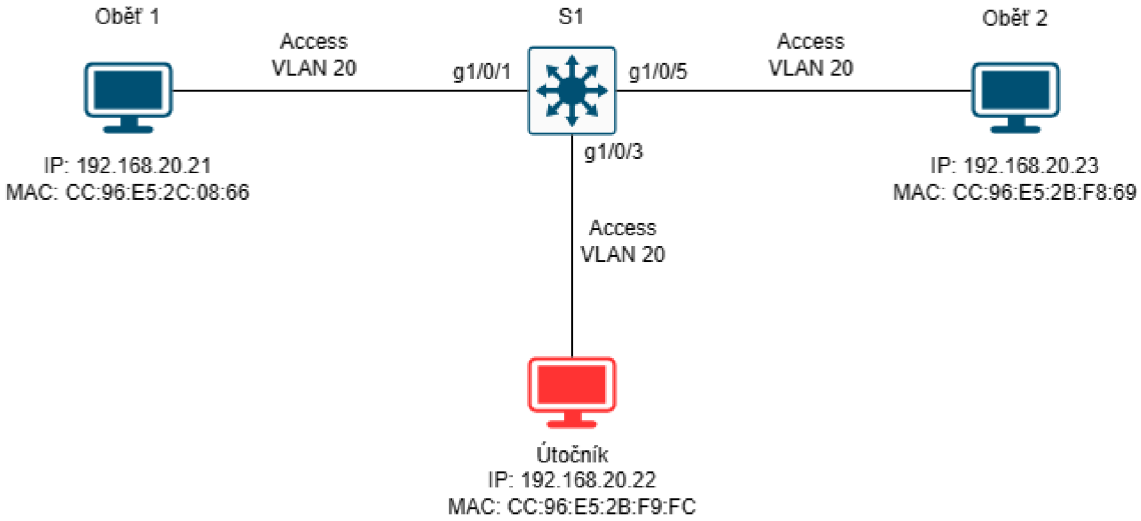
Obr. 29 Odeslání ICMP zprávy s třemi tagy 802.1Q (double tagging).
Zdroj: Vlastní zpracování



Obr. 30 Zachycení podvržené ICMP zprávy na PC oběti (double tagging).
Zdroj: Vlastní zpracování

5.7 Útok ARP spoofing

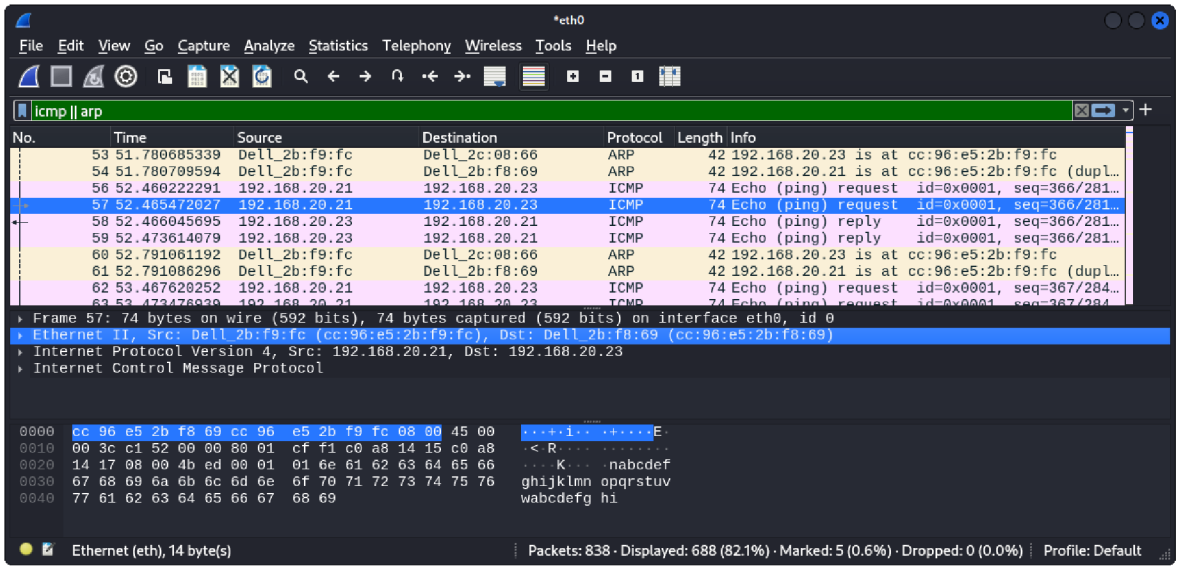
Pro simulaci tohoto útoku byl použit přepínač CISCO Catalyst 9300, dva PC v roli obětí a jeden PC v roli útočníka. Topologie sítě, použitá čísla portů, IP adresy a MAC adresy jsou uvedeny na Obr. 31. Všechny tři porty přepínače byly nastavené v režimu přístup ve VLAN 20 pomocí příkazů **switchport mode access** a **switchport access vlan 20**.



Obr. 31 Topologie sítě při útoku ARP spoofing.
Zdroj: Vlastní zpracování

K útoku byl použit nástroj Ettercap, kde bylo nejprve spuštěno skenování hostitelů. Po dokončení skenování byla přidána Oběť 1 do seznamu cílů *„Target 1“* a Oběť 2 do seznamu cílů *„Target 2“*. Poté byl v sekci *„MITM“* zvolen útok *„ARP poisoning“*. Volitelné parametry byly ponechány ve výchozím nastavení, tedy *„Sniff remote*

connections“ zaškrtnuto a *„Only poison one-way“* odškrtnuto. Následně bylo možné pomocí nástroje Wireshark spuštěného na PC útočníka pozorovat komunikaci mezi Obětí 1 a 2 v podobě ICMP zpráv. Kromě ICMP zpráv lze ve výpisu vidět i nevyžádané ARP pakety generované nástrojem Ettercap, viz Obr. 32.



Obr. 32 Provoz zachycený útočníkem (ARP spoofing).
Zdroj: Vlastní zpracování

Zabezpečení proti útoku ARP spoofing bylo provedeno následovně. Nejprve bylo nutné nakonfigurovat IP adresu a masku podsítě VLAN 20, dále DHCP server a funkci DHCP snooping. Jako poslední byla aktivována funkce IP arp inspection, protože je závislá na funkci DHCP snooping. Výpis konkrétních konfiguračních příkazů viz Obr. 33.

```
S1(config)#interface vlan 20
S1(config-if)#ip address 192.168.20.1 255.255.255.0
S1(config-if)#exit
S1(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.20
S1(config)#ip dhcp pool dhcp20
S1(dhcp-config)#network 192.168.20.0 /24
S1(dhcp-config)#default-router 192.168.20.1
S1(dhcp-config)#dns-server 192.168.20.1
S1(dhcp-config)#domain-name cisco.com
S1(dhcp-config)#exit
S1(config)#ip dhcp snooping
S1(config)#ip dhcp snooping vlan 20
S1(config)#interface range g1/0/1 - 5
S1(config-if-range)#ip dhcp snooping limit rate 5
S1(config-if-range)#exit
S1(config)#ip arp inspection vlan 20
S1(config)#end
```

Obr. 33 Konfigurace DHCP a ARP inspection (ARP spoofing).
Zdroj: Vlastní zpracování

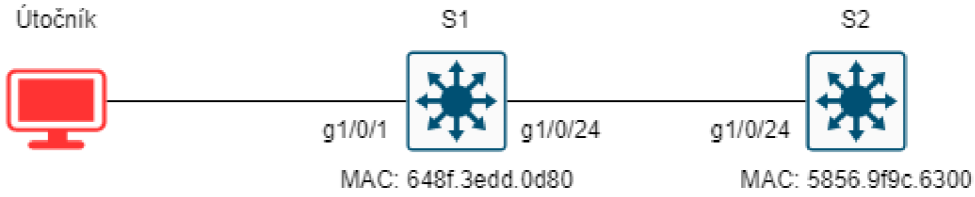
Po provedení zabezpečení byl opět spuštěn útok pomocí nástroje Ettercap. Tento pokus však již nebyl úspěšný, protože ARP pakety odesílané v pravidelných intervalech útočníkem s cílem otrávit ARP cache obou obětí byly zablokovány funkcí ARP inspection, viz Obr. 34.

```
S1#
*Jan 22 18:22:16.749: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on
Gi1/0/3, vlan
20.([cc96.e52b.f9fc/192.168.20.236/cc96.e52c.0866/192.168.20.21/18:22:16 UTC Mon
Jan 22 2024])
*Jan 22 18:22:16.749: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on
Gi1/0/3, vlan
20.([cc96.e52b.f9fc/192.168.20.21/cc96.e52b.f869/192.168.20.236/18:22:16 UTC Mon
Jan 22 2024])
*Jan 22 18:22:17.749: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on
Gi1/0/3, vlan
20.([cc96.e52b.f9fc/192.168.20.236/cc96.e52c.0866/192.168.20.21/18:22:17 UTC Mon
Jan 22 2024])
*Jan 22 18:22:17.749: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on
Gi1/0/3, vlan
```

Obr. 34 Zablokování portu funkcí ARP inspection (ARP spoofing).
Zdroj: Vlastní zpracování

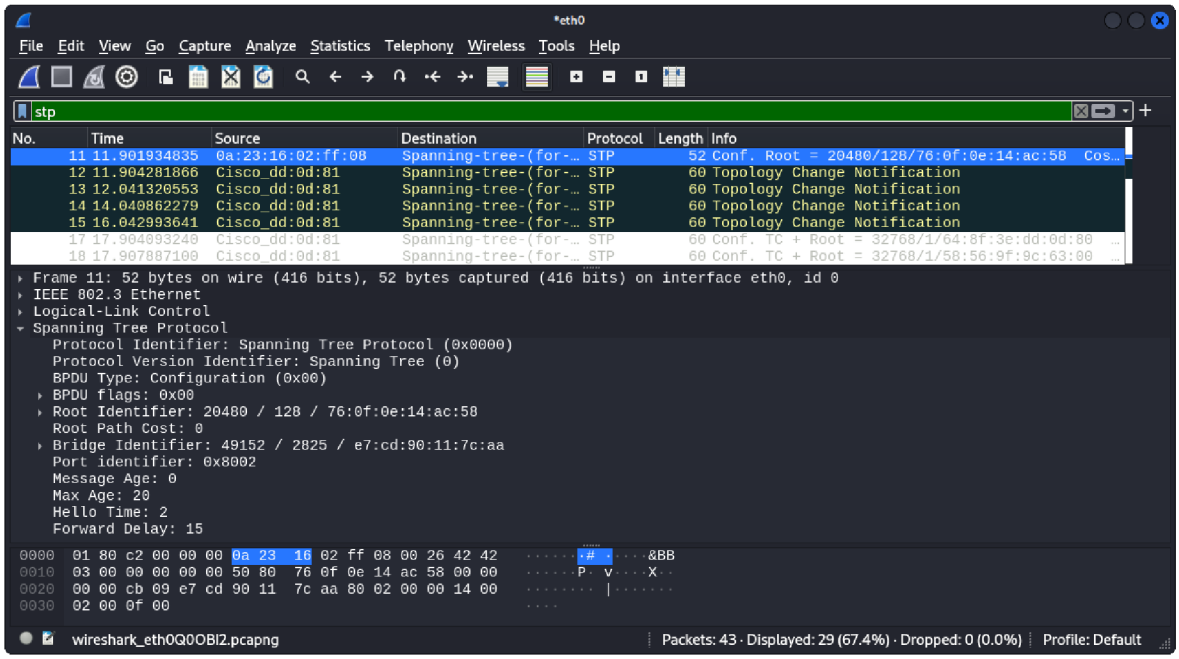
5.8 Útok vůči STP

Pro simulaci tohoto útoku byly použity dva přepínače CISCO Catalyst 9300 a jeden PC v roli útočníka. Při výpočtech STP se používají tzv. základní MAC adresy přepínačů. Topologie sítě, použitá čísla portů a základní MAC adresy přepínačů jsou uvedeny na Obr. 35. Před zahájením útoku zastával roli root bridge přepínač S2. Priorita na obou přepínačích byla ponechána ve výchozím stavu, takže rozhodujícím faktorem v tomto případě byla nižší MAC adresa přepínače S2.



Obr. 35 Topologie sítě při útoku STP.
Zdroj: Vlastní zpracování

K útoku byl použit nástroj Yersinia. Konkrétně se jednalo o útok č. 0 *„sending conf BPDU“* ze sekce STP. Pomocí nástroje Wireshark na PC útočníka bylo ověřeno, že podvržená BPDU zpráva byla odeslána. Po přijetí této zprávy přepínač reagoval odesláním notifikací o změně topologie, viz Obr. 36. Útočník však odeslal pouze jednu útočnou zprávu, takže vzápětí došlo ke změně role root bridge do výchozího stavu.



Obr. 36 Provoz zachycený útočníkem (útok STP).
Zdroj: Vlastní zpracování

Po ověření vlivu útoku byl port g1/0/1 přepínače S1 zabezpečen proti útokům STP aktivováním režimu portfast. Dále byla aktivována funkce BPDU guard pro všechny porty v režimu portfast, viz Obr. 37. Při opětovném spuštění útoku byl port g1/0/1 přepínače S1 po přijetí povržené BPDU zprávy zablokován, viz Obr. 38.

```
S1(config)#interface g1/0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 1
S1(config-if)#spanning-tree portfast
S1(config-if)#exit
S1(config)#spanning-tree portfast bpduguard default
```

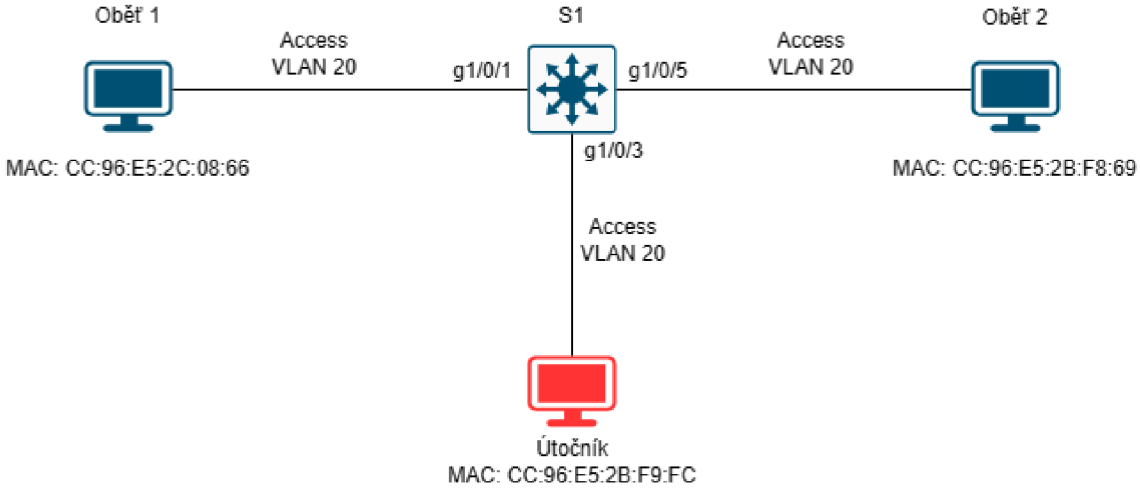
Obr. 37 Zabezpečení pomocí režimu portfast a bpduguard (útok STP).
Zdroj: Vlastní zpracování

```
S1#
*Jan 26 13:13:15.600: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU from bridge
e7cd.9011.7caa on port GigabitEthernet1/0/1 with BPDU Guard enabled. Disabling
port.
*Jan 26 13:13:15.600: %PM-4-ERR_DISABLE: bpduguard error detected on Gi1/0/1,
putting Gi1/0/1 in err-disable state
*Jan 26 13:13:16.602: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/1, changed state to down
*Jan 26 13:13:17.602: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed
state to down
*Jan 26 13:13:24.307: %PLATFORM_MATM-4-QUEUE_OVERLIMIT: MATM dropped mac delete
messages as queue limit has reached.
```

Obr. 38 Zablokování portu po přijetí BPDU zprávy (útok STP).
Zdroj: Vlastní zpracování

5.9 Útok DHCP starvation

Pro simulaci tohoto útoku byl použit přepínač CISCO Catalyst 9300, dva PC v roli obětí a jeden PC v roli útočníka. Topologie sítě, použitá čísla portů a MAC adresy jsou uvedeny na Obr. 39. DHCP server byl nakonfigurován pomocí příkazů uvedených na Obr. 40.



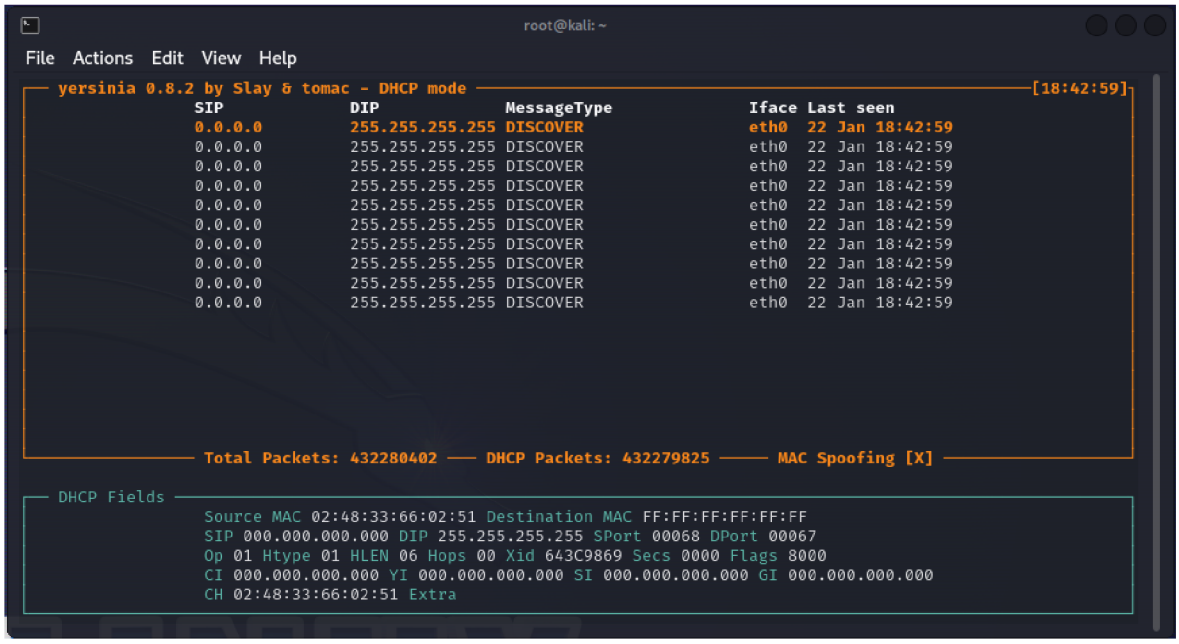
Obr. 39 Topologie sítě při útoku DHCP starvation.
Zdroj: Vlastní zpracování

```
S1(config)#interface vlan 20
S1(config-if)#ip address 192.168.20.1 255.255.255.0
S1(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.20
S1(config)#ip dhcp pool dhcp20
S1(dhcp-config)#network 192.168.20.0 /24
S1(dhcp-config)#default-router 192.168.20.1
S1(dhcp-config)#dns-server 192.168.20.1
S1(dhcp-config)#domain-name cisco.com
S1(dhcp-config)#end
```

Obr. 40 Konfigurace DHCP serveru (DHCP starvation).
Zdroj: Vlastní zpracování

Simulace útoku byla provedena pomocí nástroje Yersinia. Nejprve byl vybrán protokol DHCP a následně zahájen útok č. 1 *„sending DISCOVER packet“*, viz Obr. 41. Pomocí nástroje Wireshark na PC útočníka bylo zjištěno, že při tomto typu útoku generuje Yersinia náhodné zdrojové MAC adresy. Po vyčerpání všech dostupných IP adres, viz Obr. 42, bylo na PC oběti pomocí příkazů **ipconfig /release** a **ipconfig /renew** ověřeno, že legitimní klient již od DHCP serveru neobdrží žádnou nabídku.

Po ověření vlivu útoku byla nakonfigurována funkce DHCP snooping, která slouží k obraně před útoky DHCP starvation, viz Obr. 43. Při opětovném spuštění útoku byl port g1/0/3 přepínače S1 po přijetí nastaveného množství DHCP paketů zablokován, viz Obr. 44. Díky tomu již další pakety generované útočníkem nemohly negativně ovlivnit proces přidělování IP adres DHCP serverem.



Obr. 41 Útok DHCP starvation pomocí nástroje yersinia.
Zdroj: Vlastní zpracování

```
S1#sh ip dhcp pool

Pool dhcp20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 232
 Excluded addresses             : 22
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 0.0.0.0              192.168.20.1     - 192.168.20.254    232   / 22    / 254
S1#
```

Obr. 42 Vyčerpání celého rozsahu IP adres (DHCP starvation).
Zdroj: Vlastní zpracování

```
S1(config)#ip dhcp snooping
S1(config)#ip dhcp snooping vlan 20
S1(config)#interface range g1/0/1 - 5
S1(config-if-range)#ip dhcp snooping limit rate 5
S1(config-if-range)#end
```

Obr. 43 Konfigurace zabezpečení DHCP snooping (DHCP starvation).
Zdroj: Vlastní zpracování

```
S1#
*Jan 22 18:14:51.889: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP
Snooping received 5 DHCP packets on interface Gi1/0/3
*Jan 22 18:14:51.889: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The
interface Gi1/0/3 is receiving more than the threshold set
*Jan 22 18:14:51.890: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on
Gi1/0/3, putting Gi1/0/3 in err-disable state
*Jan 22 18:14:52.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/3, changed state to down
*Jan 22 18:14:53.892: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed
state to down
S1#
```

Obr. 44 Deaktivace portu funkcí DHCP snooping (DHCP starvation).
Zdroj: Vlastní zpracování

6 Shrnutí výsledků

Při slovníkovém útoku vůči bezdrátové síti 802.11 byla pozorována velmi vysoká rychlost celého procesu. Přestože bylo nutné otestovat více než 14 milionů klíčů, útok trval jen necelých sedm minut. Při provádění výpočtů pomocí GPU místo CPU by bylo pravděpodobně dosaženo ještě vyšší rychlosti. Z toho vyplývá, že pro zabezpečení bezdrátových sítí je opravdu nezbytné používat co nejnovější protokol (aktuálně WPA3). Šifrovací klíče by měly být dostatečně komplexní a měly by mít co nejvyšší počet znaků. V korporátním prostředí je vhodné zvolit variantu WPA Enterprise, kde se nepoužívá jeden klíč sdílený všemi klienty, ale každý klient má svůj vlastní klíč. Při vynucené deautentizaci klienta došlo ke krátkému, téměř nepozorovatelnému výpadku spojení. Uživatel zařízení, vůči kterému je útok veden, tedy ani nemusí zpozorovat nějaké bezpečnostní riziko.

Při simulaci útoku MAC flooding bylo možné pozorovat především riziko v podobě možnosti odposlechu komunikace, která vůbec neměla být doručena síťové kartě útočníka. DoS útok se naopak nasimulovat nepodařilo, pravděpodobně z důvodu nízkého vytížení sítě a vysokého výkonu přepínače. Pro úspěšné ověření DoS útoku by zřejmě bylo nutné použít více hostitelů a generovat více provozu. Po ověření vlivu útoku na chování přepínače bylo provedeno zabezpečení pomocí funkce Port Security včetně úspěšného ověření použité ochrany.

Při simulaci útoku switch spoofing z kategorie VLAN hopping bylo prakticky ověřeno riziko spočívající v ponechání výchozí konfigurace portu přepínače. V tomto případě může útočník pomocí protokolu DTP vyjednat přepnutí portu do režimu trunk a díky tomu získá přístup ke všem VLAN v rámci přepínače. Po ověření vlivu útoku na chování přepínače bylo provedeno zabezpečení spočívající v nastavení portu útočníka do režimu access a přidělení konkrétní VLAN. Následně byla použitá ochrana úspěšně otestována.

Útok double tagging z kategorie VLAN hopping se nepodařilo provést s použitím přepínačů CISCO Catalyst 9300, proto byly pro simulaci tohoto útoku použity starší přepínače CISCO Catalyst 1000. Zároveň se ukázalo, že ani s přepínači CISCO Catalyst 1000 nelze provést útok s použitím dvou tagů 802.1Q, jak bylo avizováno v kapitole 4.3.2. Útok byl úspěšný teprve po přidání třetího tagu. Navzdory očekávanému odstranění pouze jednoho tagu na prvním přepínači ve skutečnosti byly odstraněny dva tagy. Teprve třetí tag dorazil na trunk port druhého přepínače, kde zajistil doručení do

cílové VLAN. Poté byl port útočníka zabezpečen pomocí změny přístupové VLAN na jinou než nativní VLAN. Následně byla provedená ochrana úspěšně ověřena.

Při simulaci útoku ARP spoofing vše probíhalo dle očekávání. Nejprve byl proveden útok na nezabezpečený přepínač a ověřena možná rizika útoku v podobě odposlechu komunikace útočníkem. Díky nepřetržitému odesílání nevyžádaných ARP paketů útočník dosáhl pozice AiTM. Poté bylo provedeno zabezpečení pomocí aktivace funkce ARP inspection. Zároveň byl na přepínači nakonfigurován DHCP server a aktivována funkce DHCP snooping, protože funkce ARP inspection je závislá na databázi vazeb DHCP snooping. Následně byla provedená ochrana úspěšně otestována.

Pro ověření skutečného potenciálu simulace útoku vůči STP protokolu by bylo vhodné útok provést dle topologie naznačené v kapitole 4.5. K tomu je však nutné, aby PC útočníka disponoval dvěma síťovými kartami. Druhou kartu se však zajistit nepodařilo, takže bylo provedeno pouze obecné ověření možnosti převzetí role root bridge útočníkem s využitím podvržené zprávy BPDU. Poté bylo provedeno zabezpečení spočívající v nastavení portu útočníka do režimu portfast a aktivaci funkce BPDU guard pro všechny porty v režimu portfast. Následně byl úspěšně ověřen vliv provedené ochrany.

Při simulaci útoku DHCP starvation bylo ověřeno riziko spočívající ve vyčerpání všech dostupných IP adres útočníkem. Tento útok je nebezpečný zejména tím, že útočník může připravit vlastní podvržený DHCP server a ten pak klientům přiděluje IP adresy místo legitimního DHCP serveru. Vyčerpání rozsahu IP adres bylo ověřeno zobrazením statistiky na přepínači s rolí DHCP serveru i na klientovi, kterému se nepodařilo opětovně získat IP adresu. Poté bylo provedeno zabezpečení pomocí aktivace funkce DHCP snooping s následným úspěšným otestováním vlivu provedené ochrany.

7 Závěry a doporučení

Provedení výše popsaných útoků je relativně triviální, přesto představují významné riziko z hlediska systému řízení bezpečnosti informací. Je to dáno především dostupností a snadným použitím nástrojů, pomocí kterých lze útoky provést, ale i růstem výkonu výpočetní techniky. Například k prolamování klíčů WPA je vhodnější použít výkonné PC, ale lze jej provést až dodatečně. K zachycení čtyřcestného handshake v lokalitě cíle útoku naopak stačí mobilní telefon s operačním systémem Android nebo miniaturní počítač Raspberry PI. Raspberry PI lze použít i pro další útoky popsané v této práci.

Kombinací útoků je navíc možné docílit dalšího zvýšení rizika. Například při simulaci útoku switch spoofing se podařilo doručit podvržený ICMP paket na PC oběti, ale odpověď vygenerována nebyla, protože ARP tabulka oběti neobsahovala příslušný záznam. Zajistit vytvoření záznamu v ARP tabulce oběti by mělo být možné pomocí generování nevyžádaných ARP zpráv, viz kapitola 4.4.

Obrana před všemi popsanými útoky je však také relativně triviální, jak bylo ověřeno v kapitole 5. Větší firmy a orgány státní správy a samosprávy navíc používají nástroje pro centrální správu síťových prvků, které údržbu sítě usnadňují. Centrální dohledové místo přináší ucelený přehled o aktuálním stavu sítě. Aktualizace operačních systémů síťových prvků je spouštěna z jednoho místa, nemělo by se tedy stát, že správce zapomene na některý ze síťových prvků. Kromě toho jsou jednotlivé síťové prvky konfigurovány pomocí šablon, takže všechna provedená zabezpečení by se měla projevit v celé síti.

Další výzkum navazující na tuto práci by se mohl týkat například:

- Využití nástroje Scapy pro popsané útoky, jejich kombinace, případně pro další síťové útoky. Za cenu mírného zvýšení nároků na studium a implementaci útoků nabízí Scapy univerzálnost a mnohem širší možnosti využití než ostatní popsané nástroje, které jsou buď jednoúčelové nebo nabízejí jen omezenou množinu použití.
- Vlivu zabezpečení pomocí standardu IEEE 802.1X na popsané zranitelnosti.
- Možnostmi útoků vůči protokolům spadajícím pod IPv6.

8 Seznam použité literatury

[1] DUNTON, Jeremy. Hacking with Kali Linux: A Step By Step Guide To Ethical Hacking, Hacking Tools, Protect Your Family And Business From Cyber Attacks Using The Basics Of Cybersecurity. B.m.: Amplitudo Ltd, 2021. ISBN 978-1-80114-974-7.

[2] VERIZON. Verizon. Data Breach Investigations Report [online]. 2023 [vid. 2023-01-19]. Dostupné z: https://www.verizon.com/business/resources/reports/dbir/

[3] CZ.NIC, Z. S. P. O. Národní CSIRT ČR. ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2021 [online]. 2023. Dostupné z: https://csirt.cz/media/filer_public/b8/97/b897d087-6854-4c69-8e99-3bb90561e6b7/220302_csirt_vyrocni_zprava_2021.pdf

[4] NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost. Kybernetické incidenty pohledem NÚKIB - prosinec 2023 [online]. 2024 [vid. 2024-02-21]. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2067-kyberneticke-incidenty-pohledem-nukib-prosinec-2023/

[5] MINISTERSTVO PRŮMYSLU A OBCHODU. Průmysl 4.0 má v Česku své místo [online]. 2023 [vid. 2023-08-28]. Dostupné z: https://www.mpo.cz/cz/prumysl/zpracovatelsky-prumysl/prumysl-4-0-ma-v-cesku-sve-misto--176055/

[6] HEIDING, Fredrik, Emre SÜREN, Johannes OLEGÅRD a Robert LAGERSTRÖM. Penetration testing of connected households. Computers & Security [online]. 2023, **126**, 103067. ISSN 0167-4048. Dostupné z: doi:https://doi.org/10.1016/j.cose.2022.103067

[7] RAGHUPRASAD, Aswin, Suraj PADMANABHAN, M ARJUN BABU a P.K BINU. Security Analysis and Prevention of Attacks on IoT Devices. In: 2020 International Conference on Communication and Signal Processing (ICCSP) [online]. 2020, s. 0876–0880. Dostupné z: doi:10.1109/ICCSP48568.2020.9182055

[8] GAO, Weihua, Yuhao SUN, Qingying FU, Zhouzhe WU, Xiao MA, Kai ZHENG a Xin HUANG. ARP Poisoning Prevention in Internet of Things. In: 2018 NINTH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY IN MEDICINE AND EDUCATION (ITME 2018) [online]. B.m.: IEEE Comp Soc; China Jiliang Univ; Zhejiang Univ; Zhejiang Provincial Nat Sci Fdn; Fujian Univ Tradit Chinese Med; Univ Texas San Antonio; Swinburne Univ Technol; Iwate Prefectural Univ; Shandong Normal Univ; Xiamen Univ; Fuzhou Univ; Hunan Univ Humanities Sci & Technol; Lanzhou Univ; Henan Univ Technol; Wuhan Univ Technol; E China Normal Univ; Birmingham City Univ; Univ Southern Queensland, 2018, s. 733–736. ISBN 978-1-5386-7743-8. Dostupné z: doi:10.1109/ITME.2018.00166

[9] YURTSEVEN, Ilke a Selami BAGRIYANIK. A Review of Penetration Testing and Vulnerability Assessment in Cloud Environment. In: 2020 Turkish National

Software Engineering Symposium (UYMS) [online]. 2020, s. 1–6. Dostupné z: doi:10.1109/UYMS50627.2020.9247071

[10] POLICIE ČESKÉ REPUBLIKY. Policie České republiky. Kyberkriminalita [online]. 2023 [vid. 2023-02-04]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[11] NIST. Glossary [online]. 2023 [vid. 2023-07-03]. Dostupné z: https://csrc.nist.gov/glossary/term/vulnerability

[12] TIRTEA, Rodica. ENISA overview of cybersecurity and related terminology. 2017.

[13] NIST. Cybersecurity Framework FAQS Framework Basics. NIST [online]. 2015 [vid. 2023-09-28]. Dostupné z: https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics

[14] NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 [online]. NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology. 2018 [vid. 2023-09-28]. Dostupné z: doi:10.6028/NIST.CSWP.04162018

[15] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Text s významem pro EHP) [online]. 14. prosinec 2022 [vid. 2023-03-22]. Dostupné z: http://data.europa.eu/eli/dir/2022/2555/oj/ces

[16] ŠULC, Vladimír. Kybernetická bezpečnost. B.m.: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-737-5.

[17] ENISA. European Union Agency for Cybersecurity: Risk Management Glossary. ENISA [online]. 2023 [vid. 2023-07-03]. Dostupné z: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

[18] Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [online]. 21. květen 2018. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[19] ALSHARIF, Maher, Shailendra MISHRA a Mohammed ALSHEHRI. Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering [online]. 2021, **40**. Dostupné z: doi:10.32604/csse.2022.019938

[20] THE MITRE CORPORATION. Common Vulnerabilities and Exposures [online]. 2023 [vid. 2023-04-01]. Dostupné z: https://cve.mitre.org/

[21] NIST. National Vulnerability Database [online]. 2023 [vid. 2023-04-01]. Dostupné z: https://nvd.nist.gov/

[22] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS, INC. FIRST - Improving Security Together. FIRST — Forum of Incident Response and Security Teams [online]. 2023 [vid. 2023-04-01]. Dostupné z: https://www.first.org/

[23] DIOGENES, Yuri a Dr Erdal OZKAYA. Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. B.m.: Packt Publishing Ltd, 2018. ISBN 978-1-78847-385-9.

[24] ZANNA, Paul, Peter RADCLIFFE a Dinesh KUMAR. Preventing Attacks on Wireless Networks Using SDN Controlled OODA Loops and Cyber Kill Chains. Sensors [online]. 2022, **22**(23). ISSN 1424-8220. Dostupné z: doi:10.3390/s22239481

[25] HUTCHINS, Eric M, Michael J CLOPPERT a Rohan M AMIN. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. 2010.

[26] BAHRAMI, Pooneh Nikkhah, Ali DEHGHANTANHA, Tooska DARGAHI, Reza M. PARIZI, Kim-Kwang Raymond CHOO a Hamid H.S. JAVADI. Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. Journal of Information Processing Systems [online]. 2019, **15**(4), 865–889 [vid. 2023-07-05]. Dostupné z: doi:10.3745/JIPS.03.0126

[27] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). 2014

[28] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii [online]. 6. červenec 2016 [vid. 2023-03-22]. Dostupné z: http://data.europa.eu/eli/dir/2016/1148/oj/ces

[29] THE MITRE CORPORATION. Mitigations - Enterprise [online]. 2023 [vid. 2023-04-09]. Dostupné z: https://attack.mitre.org/mitigations/enterprise/

[30] NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost. Nová směrnice EU o bezpečnosti sítí a informací „NIS2“ a návrh nového zákona o kybernetické bezpečnosti [online]. 2023 [vid. 2023-03-22]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145

[31] THE MITRE CORPORATION. Tactics - Enterprise [online]. 2023 [vid. 2023-01-28]. Dostupné z: https://attack.mitre.org/tactics/enterprise/

[32] EC-COUNCIL. EC-Council [online]. 2023 [vid. 2023-01-18]. Dostupné z: https://www.eccouncil.org/

[33] SANS™ INSTITUTE. SANS. Cyber Security Training, Certifications, Degrees and Resources [online]. 2023 [vid. 2023-01-18]. Dostupné z: https://www.sans.org/

[34] MILE2 CYBERSECURITY CERTIFICATIONS. Mile2 [online]. 2022 [vid. 2023-01-18]. Dostupné z: https://mile2.com/

[35] (ISC)², INC. (ISC)² [online]. 2023 [vid. 2023-01-19]. Dostupné z: https://www.isc2.org/

[36] ISACA. ISACA [online]. 2023 [vid. 2023-01-19]. Dostupné z: https://www.isaca.org/

[37] COMPTIA, INC. CompTIA [online]. 2023 [vid. 2023-01-19]. Dostupné z: https://www.comptia.org

[38] ASIS INTERNATIONAL. ASIS International [online]. 2022 [vid. 2023-01-19]. Dostupné z: http://www.asisonline.org/

[39] OFFSEC SERVICES LIMITED. Kali [online]. 2023 [vid. 2023-01-20]. Dostupné z: https://www.kali.org/

[40] DIETERLE, Daniel W. Basic Security Testing With Kali Linux, Third Edition. 3rd edition. B.m.: CreateSpace Independent Publishing Platform, 2018. ISBN 978-1-72503-198-2.

[41] LYON, Gordon. Nmap Network Scanning [online]. 2023 [vid. 2023-07-30]. Dostupné z: https://nmap.org/book/toc.html

[42] SINCHANA, K, C SINCHANA, H L GURURAJ a B R SUNIL KUMAR. Performance Evaluation and Analysis of various Network Security tools. In: 2019 International Conference on Communication and Electronics Systems (ICCES) [online]. 2019, s. 644–650. Dostupné z: doi:10.1109/ICCES45898.2019.9002531

[43] KUMAR, Rajiv a Katlego TLHAGADIKGORA. Internal Network Penetration Testing Using Free/Open Source Tools: Network and System Administration Approach. In: AK LUHACH, D SINGH, PA HSIUNG, KB HAWARI, P LINGRAS a PK SINGH, ed. ADVANCED INFORMATICS FOR COMPUTING RESEARCH, PT II [online]. B.m.: Comp Soc India, Chandigarh Chapter; So Fed Univ, 2019, s. 257–269. Communications in Computer and Information Science. ISBN 978-981-13-3143-5. Dostupné z: doi:10.1007/978-981-13-3143-5_22

[44] HASSAN, Syed Zain ul, Zainab MUZAFFAR a Saleem Zubair AHMAD. Operating Systems for Ethical Hackers - A Platform Comparison of Kali Linux and Parrot OS. International Journal of Advanced Trends in Computer Science and Engineering [online]. 2021, **10**(3), 2226–2233 [vid. 2023-07-21]. ISSN 22783091. Dostupné z: doi:10.30534/ijatcse/2021/1041032021

[45] SHARPE, Richard, Ed WARNICKE a Ulf LAMPING. Wireshark User's Guide [online]. 2023. Dostupné z: https://www.wireshark.org/download/docs/Wireshark%20User%27s%20Guide.pdf

[46] AIRCRACK-NG. Aircrack-ng - Main documentation [online]. 2023 [vid. 2023-08-14]. Dostupné z: https://www.aircrack-ng.org/documentation.html#

[47] BREMVÅG, Christian. Wifite [online]. Python. 21. srpen 2023 [vid. 2023-08-21]. Dostupné z: https://github.com/kimocoder/wifite2

[48] ORNAGHI, Alberto a Marco VALLERI. ettercap(8) - Linux man page [online]. 2023 [vid. 2023-08-24]. Dostupné z: https://linux.die.net/man/8/ettercap

[49] OMELLA, Alfredo Andres a David Barroso BERRUETA. yersinia(8): FrameWork for layer 2 attacks - Linux man page [online]. 2023 [vid. 2023-08-23]. Dostupné z: https://linux.die.net/man/8/yersinia

[50] BIONDI, Philippe. Scapy 2.5.0 documentation. Introduction [online]. 2024 [vid. 2024-02-09]. Dostupné z: https://scapy.readthedocs.io/en/latest/introduction.html

[51] VALADON, Guillaume. GitHub. Scapy in 0x30 Minutes [online]. 2024 [vid. 2024-02-09]. Dostupné z: https://github.com/guedou/guedou.github.io/blob/master/talks/2022_GreHack/Scapy%20in%200x30%20minutes.ipynb

[52] SONG, Dug. macof(8) - Linux man page [online]. 2024 [vid. 2024-02-06]. Dostupné z: https://linux.die.net/man/8/macof

[53] BARAY, Elyas a Nitish Kumar OJHA. 'WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique'. In: 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) [online]. 2021, s. 23–30. Dostupné z: doi:10.1109/ICCMC51019.2021.9418230

[54] LU, He-Jun a Yang YU. Research on WiFi Penetration Testing with Kali Linux. COMPLEXITY [online]. 2021, **2021**. ISSN 1076-2787. Dostupné z: doi:10.1155/2021/5570001

[55] WI-FI ALLIANCE. Wi-Fi Alliance [online]. 2023 [vid. 2023-09-21]. Dostupné z: https://www.wi-fi.org/

[56] RAMEZANPOUR, Keyvan, Jithin JAGANNATH a Anu JAGANNATH. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. Computer Networks [online]. 2023, **221**, 109515. ISSN 1389-1286. Dostupné z: doi:https://doi.org/10.1016/j.comnet.2022.109515

[57] ELSHAFEE, Ahmed a Walid EL-SHAFAI. Design and analysis of data link impersonation attack for wired LAN application layer services. Journal of Ambient Intelligence and Humanized Computing [online]. 2022 [vid. 2023-07-21]. ISSN 1868-5137, 1868-5145. Dostupné z: doi:10.1007/s12652-022-03800-5

[58] MOREIRA SANTOS, María Genoveva a Pedro Antonio ALCÍVAR MARCILLO. Security in the data link layer of the OSI model on LANs wired Cisco. Journal of Science and Research: Revista Ciencia e Investigación [online]. 2018, **3**(CITT2017), 106–112 [vid. 2023-07-21]. ISSN 2528-8083, 2528-8083. Dostupné z: doi:10.26910/issn.2528-8083vol3issCITT2017.2018pp106-112

[59] INAMDAR, Mohammed Suhel a Ali TEKEOGLU. Security Analysis of Open Source Network Access Control in Virtual Networks. In: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops

(WAINA): 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA) [online]. Krakow: IEEE, 2018, s. 475–480 [vid. 2023-07-21]. ISBN 978-1-5386-5395-1. Dostupné z: doi:10.1109/WAINA.2018.00131

[60] AYE, Zin May. A LAN Campus Infrastructure with Spanning Tree Protocol Attack and Mitigation. University Journal of Research and Innovation. 2019, 123.

[61] ALDAOUD, Manar, Dawood AL-ABRI, Ahmed AL MAASHRI a Firdous KAUSAR. DHCP attacking tools: an analysis. Journal of Computer Virology and Hacking Techniques [online]. 2021, **17**(2), 119–129 [vid. 2023-07-21]. ISSN 2263-8733. Dostupné z: doi:10.1007/s11416-020-00374-8

[62] NUHU, Abdulhafiz A, Faith O ECHOBU a Oyenike M OLANREWAJU. Mitigating DHCP starvation attack using snooping technique. Fudma Journal of Sciences. 2020, **4**(1), 560–566.

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor: **Bc. Aleš Lajvr**

Studium: I2100436

Studijní program: N1802 Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Název diplomové práce: **Simulace síťových útoků za využití Kali Linux**

Název diplomové práce AJ: Simulation of network attacks using Kali Linux

Cíl, metody, literatura, předpoklady:

Cílem práce je provést analýzu a podrobný popis nástrojů pro síťové útoky dostupných v prostředí Kali Linux a navrhnout a sestavit sadu úloh pro ověření zabezpečení sítě. V teoretické části práce autor provede podrobnou analýzu nástrojů využitelných pro síťové útoky v prostředí Kali Linux. Na základě provedené analýzy v praktické části navrhne, otestuje a podrobně popíše minimálně pět komplexních řešených úloh využitelných pro ověření síťového zabezpečení.

DANIEL W. DIETERLE, 2018. *Basic Security Testing With Kali Linux*. 3rd ed. B.m.: Createspace Independent Publishing Platform. ISBN 1725031981.

JEREMY DUNTON, 2021. *Hacking with Kali Linux*. B.m.: Amplitudo LTD. ISBN 1801149747.

KARNEL ERICKSON, 2020. *Kali Linux for Hackers*. B.m.: Francesco Cammardella. ISBN 1990151000.

Zadávající pracoviště: Katedra informačních technologií, Fakulta informatiky a managementu

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

Datum zadání závěrečné práce: 15.10.2021