VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ LOKÁLNÍCH SÍTÍ NA LINKOVÉ VRSTVĚ
LINK LAYER LAN NETWORK SECURITY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Jiří Sedláček
AUTHOR

VEDOUCÍ PRÁCE — Mgr. Karel Slavíček, Ph.D.
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Jiří Sedláček ***ID:*** 203714
Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Zabezpečení lokálních sítí na linkové vrstvě

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je analyzovat možnosti útoku na lokální počítačové sítě na linkové vrstvě (např. podvržený DHCP server, napadení spanning tree protokolu, útok na protokol ARP a další) a rovněž možnosti detekce takových útoků a obrany proti nim. Věcným výstupem je soubor doporučení na konfiguraci aktivních sítových prvků.
Úkolem bakalářské práce je připravit přehled možných útoků na linkové vrstvě a připravit návrh zapojení laboratorní úlohy, která by tyto útoky a možnosti obrany proti nim demonstrovala. Student laboratorní úlohu rovněž realizuje a připraví návod k jejímu řešení.

DOPORUČENÁ LITERATURA:

[1] SCHAFER, Gunter. Security in fixed and wireless networks: and introduction to securing data communications. Hoboken, NJ: Wiley, c2003. ISBN 978-0470863701.

[2] STALLINGS, William, Lawrie BROMWN, Michael D. BAUER a Michael HOWARD. Computer Security: principles and practice. Upper Saddle River, N.J.: Prentice Hall, C2008. ISBN 0-13-600424-5.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Mgr. Karel Slavíček, Ph.D.

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

ABSTRAKT

Bakalářská práce se zabývá zabezpečením lokálních sítí na linkové vrstvě. Cílem práce je popis základních funkcí referenčního modelu ISO/OSI a linkové vrstvy pro pochopení problematiky, vystihnout možnosti útoků na linkové vrstvě (například podvržený DHCP server, ARP spoofing, CAM table overflow, napadení Spanning tree protokolu a další) a možná bezpečnostní opatření na ochranu proti nim. Cílem práce je rovněž návrh na zapojení laboratorní úlohy týkající se této problematiky. Teoretická část vystihuje nejdůležitější protokoly linkové vrstvy, metody vedoucí k jejich zneužití a ochrana těchto protokolů. Praktická část obsahuje stručný popis útoků, použité nástroje k realizaci útoků, topologii sítě, provedení samotných útoků, případnou detekci útoků a obranu proti nim a shrnutí každého z nich, které obsahuje stručný popis proveditelnosti konkrétního útoku. V práci je rovněž shrnuto několik doporučení na konfiguraci zabezpečení a chování v kyberprostoru. K provedení jednotlivých útoků jsou především užity operační systémy Kali linux a Windows 10.

KLÍČOVÁ SLOVA

ARP, CAM, detekce, DHCP, Ettercap, ICMP, IEEE 802, linková vrstva, podvržený, riziko, STP, VTP, Wireshark, Yersinia, zabezpečení

ABSTRACT

The bachelor‘s thesis is about security concerning local area networks of the data link layer. The goal of the thesis is to characterize basic functioning of the ISO/OSI reference model as well as describing how the data link layer works to understand the topic, specify the possibilities of attacking the data link layer (for example rogue DHCP server, ARP spoofing, CAM table overflow, attacking the spanning tree protocol and others) and possible security measures to protect against the attacks. The purpose of the thesis is also a suggestion for assembling an experimental network relating to the topic of the thesis. Theoretical part determines the most important protocols of the data link layer, methods of abusing them and protection of those protocols. The practical part contains a brief description of the attacks, used utilities for accomplishing the attacks, a network topology, execution of the attacks, detection and protection against the attacks as well as briefly summarizing the results. The thesis also sums up some of the possible recommended configuration to repel the attacks and suggesting how to behave in a cyber environment. For the purpose of simulating the attacks, Kali Linux and Windows 10 are the operating systems that were used the most in this thesis.

KEYWORDS

ARP, CAM, detection, DHCP, Ettercap, ICMP, IEEE 802, security risk, security, spoofed, STP, the data link layer, VTP, Wireshark, Yersinia

SEDLÁČEK, Jiří. *Zabezpečení lokálních sítí na linkové vrstvě*. Brno, 2020. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Mgr. Karel Slavíček, Ph.D.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	Jiří Sedláček
VUT ID studenta:	203714
Typ práce:	Bakalářská práce
Akademický rok:	2019/20
Téma závěrečné práce:	Zabezpečení lokálních sítí na linkové vrstvě

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brně dne: …… ……

Podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu práce panu Mgr. Karlu Slavíčkovi, Ph.D. za obrovskou ochotu, pedagogickou a odbornou pomoc a cenné rady při zpracování mé bakalářské práce.

V Brně dne ....

podpis autora

Obsah

1 Úvod

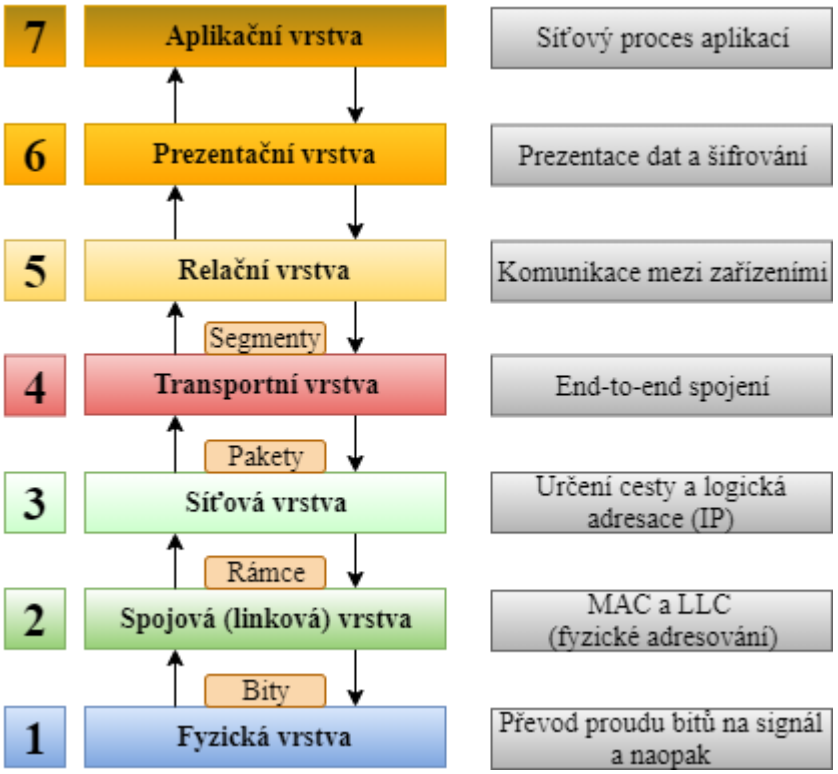
Bezpečnost v telekomunikacích je jedním z nejdůležitějších faktorů v rámci každodenního života. V dnešní moderní době stále narůstá potřeba ochrany různých informací a dat. Nejčastějším narušením bezpečnosti je krádež informací, vymazání, zašifrování, nebo poškození dat. Existuje celá škála útoků, kterými se dá narušit soukromí uživatele, nebo útoky, které mají za následek přerušení spojení se zařízeními v lokální síti nebo přerušení internetového spojení. Jedním z nejdůležitějších opatření je prevence. Předcházením hrozbě dříve, než nastane, se dá eliminovat spousta problémů v případě útoku. Téměř každý člověk má přístup k internetu a rovněž vlastní v drtivé většině případů několik zařízení, pomocí kterých může k internetu přistupovat a je tedy potřeba jisté obezřetnosti. To samé platí ve firemní, nebo domácí síti. Útočníci přicházejí s čím dál tím více sofistikovanými typy útoků a je tedy možné případnou nedbalostí napomoci takovému útočníkovi.

V této bakalářské práci je realizován popis bezpečnostních rizik na úrovni linkové vrstvy ISO/OSI modelu a výčet druhů případné obrany proti nim. Cílem první části práce je vysvětlit fungování protokolů linkové vrstvy, možnosti jejich zneužití a soubor bezpečnostních opatření na jejich ochranu. Druhá část se zabývá provedením samotných útoků a vytvořením návrhu na jejich zapojení a provedení v laboratorním prostředí. Celkově byly vytvořeny dva návrhy zapojení laboratorní úlohy, každý po třech útocích. První návrh (LAB 1) řeší útoky na pomezí linkové a síťové vrstvy a druhý (LAB 2) útoky na úrovni linkové vrstvy.

2 Model ISO/OSI

Před vysvětlením zranitelností linkové vrstvy je potřeba pochopit několik věcí o tom, jak funguje model ISO/OSI – pro ty, kteří mají v této oblasti méně zkušeností. Linková vrstva je jednou částí modelu OSI – sedmivrstvého hierarchického modelu.

ISO vyvinula model OSI, aby mohla určit požadavky vzájemné spolupráce mezi komunikačními zařízeními (včetně počítačů) – jak spolu fungují v rámci jednotlivých vrstev.



Obr. 2.1: Model ISO/OSI.

2.1 Linková vrstva

Linková vrstva přenáší data mezi sousedními síťovými uzly v síti WAN nebo mezi uzly ve stejném segmentu LAN. Linková vrstva poskytuje funkční a procedurální prostředky pro přenos dat mezi entitami v síti a také může poskytovat prostředky pro detekci a korekci chyb, které mohou vzniknout na fyzické vrstvě. Zabývá se také doručováním datových rámců mezi uzly na stejné úrovni sítě (rámce nepřekračují hranice lokální sítě). Funkci mezisíťového směrování a globální adresování plní vyšší vrstvy a tím umožňují protokolům linkové vrstvy zaměřit se na lokální doručování a adresování.

Tímto způsobem linková vrstva řídí tok dat.

2.1.1 Funkce linkové vrstvy

- **Virtual LAN (VLAN)** je jakákoli broadcastová doména, která je rozdělena a izolována v počítačové síti na linkové vrstvě – realizuje se na přepínačích. Sítě VLAN fungují tak, že aplikují tagy na síťové rámce a manipulují s těmito tagy v síťových systémech – vytvářejí design a funkčnost síťového provozu, který je fyzicky v jediné síti, ale funguje tak, jako by byl rozdělen na samostatné sítě. Tímto způsobem mohou sítě VLAN udržovat síťové aplikace oddělené, přestože jsou připojeny ke stejné fyzické síti, a to bez nutnosti nasazení více sad kabelů a síťových zařízení. VLAN umožňuje správcům sítě seskupovat hostitele společně, i když nejsou přímo připojeni ke stejnému přepínači. Protože příslušnost k VLAN lze konfigurovat, může být výrazně zjednodušen návrh a realizace zapojení sítě.
- **Media access control (MAC)** odkazuje k podvrstvě, která určuje, kdo má kdykoliv povolen přístup k médiu (např. CSMA/CD). Jindy se odkazuje na strukturu rámců dodanou na základě MAC adres. Obecně existují dvě formy řízení přístupu k médiím: distribuovaný přístup a centralizovaný přístup. Obě tyto možnosti lze přirovnat ke komunikaci mezi lidmi. V sítí tvořené komunikujícími lidmi, tj. konverzace, kde každý přestane komunikovat a poté se pokusí mluvit znovu, čímž efektivně vytvoří propracovaný systém, který určuje, kdo bude moci mluvit jako první. Podvrstva MAC také určuje, kde končí jeden rámec dat a kde další začíná:
    - ► **Synchronizace rámců** – v telekomunikacích je synchronizace rámců (také framing) proces, kdy se při příjmu proudu orámcovaných dat identifikují příchozí signály zarovnání rámců (tj. rozlišovací bitové sekvence neboli syncwords), což umožňuje datovým bitům v rámci, aby byly extrahovány pro dekódování nebo opakovaný přenos.
    - ► **MAC address** – unikátní identifikátor přidělený NIC. Pro komunikaci v rámci segmentu sítě se používá jako síťová adresa pro většinu síťových technologií IEEE 802, včetně Ethernetu, Wi-Fi a Bluetooth. MAC adresy se skládají z šesti skupin dvou hexadecimálních číslic, oddělených spojovníky, dvojtečkami, nebo bez oddělovače.
- **Logical link control (LLC)** je horní podvrstvou linkové vrstvy modelu OSI. Poskytuje mechanismy multiplexování (při vysílání), které umožňují, aby několik síťových protokolů přenášených pomocí MAC podvrstvy koexistovalo v point-to-multipoint zapojení sítě a aby mohly být síťové protokoly transportovány přes stejné síťové médium. LLC také umožňuje dekódování protokolů a jejich demultiplexování (při příjmu), případně potom také:

- **Flow control (řízení toku dat)** – proces řízení rychlosti přenosu dat mezi dvěma uzly, aby se zabránilo výpočetně silnějšímu odesílateli zahltit výpočetně slabšího příjemce. Řízení toku dat by mělo být odlišeno od řízení přetížení (congestion control), které se používá pro řízení toku dat pouze v případě přetížení. Řízení toku je důležité, protože je možné, aby odesílající počítač přenášel informace rychleji, než je dokáže přenášet přijímací počítač (např. z důvodu provozního zatížení přijímacího počítače nebo jeho menší kapacity zpracování dat).
- **Error detection and correction (detekce a oprava chyb)** – v teorii informací a teorii kódování s aplikacemi v informatice jsou detekce chyb a korekce chyb techniky, které umožňují spolehlivé doručování digitálních dat přes nespolehlivé komunikační kanály. Mnoho komunikačních kanálů podléhá kanálovému šumu, a tak mohou během přenosu ze zdroje do přijímače vznikat chyby. Techniky detekce chyb umožňují takové chyby detekovat, zatímco korekce chyb v mnoha případech umožňuje rekonstrukci původních dat. Dobrý výkon při kontrole chyb vyžaduje, aby bylo schéma vybráno na základě charakteristik komunikačního kanálu.
- **L2 switching (přepínání v rámci linkové vrstvy)** – v typické síti LAN jsou všechna zařízení připojena k jednomu centrálnímu zařízení, přepínači. Přepínač na linkové vrstvě je víceportovým zařízením, které používá fyzické (MAC) adresy ke zpracování a předávání dat na linkové vrstvě. Propojení mezi přepínači může být regulováno např. pomocí STP. V minulosti byl pro potřeby přepínání používán hub (rozbočovač). Huby však měly mnoho nevýhod (např. nemožnost vlastní kontroly provozu, který jimi prochází nebo vytvoření jedné velké kolizní domény) K překonání některých problémů s huby byly vytvořeny tzv. „mosty“ (bridge), které sice jsou schopné vytvořit několik kolizních domén, ale mají omezený počet portů. Nakonec byly vytvořeny přepínače (switche) a dnes se stále široce používají. Přepínače mají více portů než mosty, mohou kontrolovat příchozí provoz a podle toho rozhodovat o přepínání. Každý port přepínače je také samostatnou kolizní doménou, takže by nemělo docházet ke kolizím paketů.

2.1.2 Protokoly na linkové vrstvě

- **STP (Spanning Tree Protocol)** je síťový protokol, který vytváří logickou topologii bez smyček pro sítě Ethernet. Základní funkcí STP je zabránit přemostění smyček a broadcastovému vysílání, které z nich vyplývá. Spanning tree také umožňuje, aby návrh sítě zahrnoval záložní odkazy, které poskytují odolnost proti chybám, pokud aktivní spojení selže. Jak název napovídá, STP

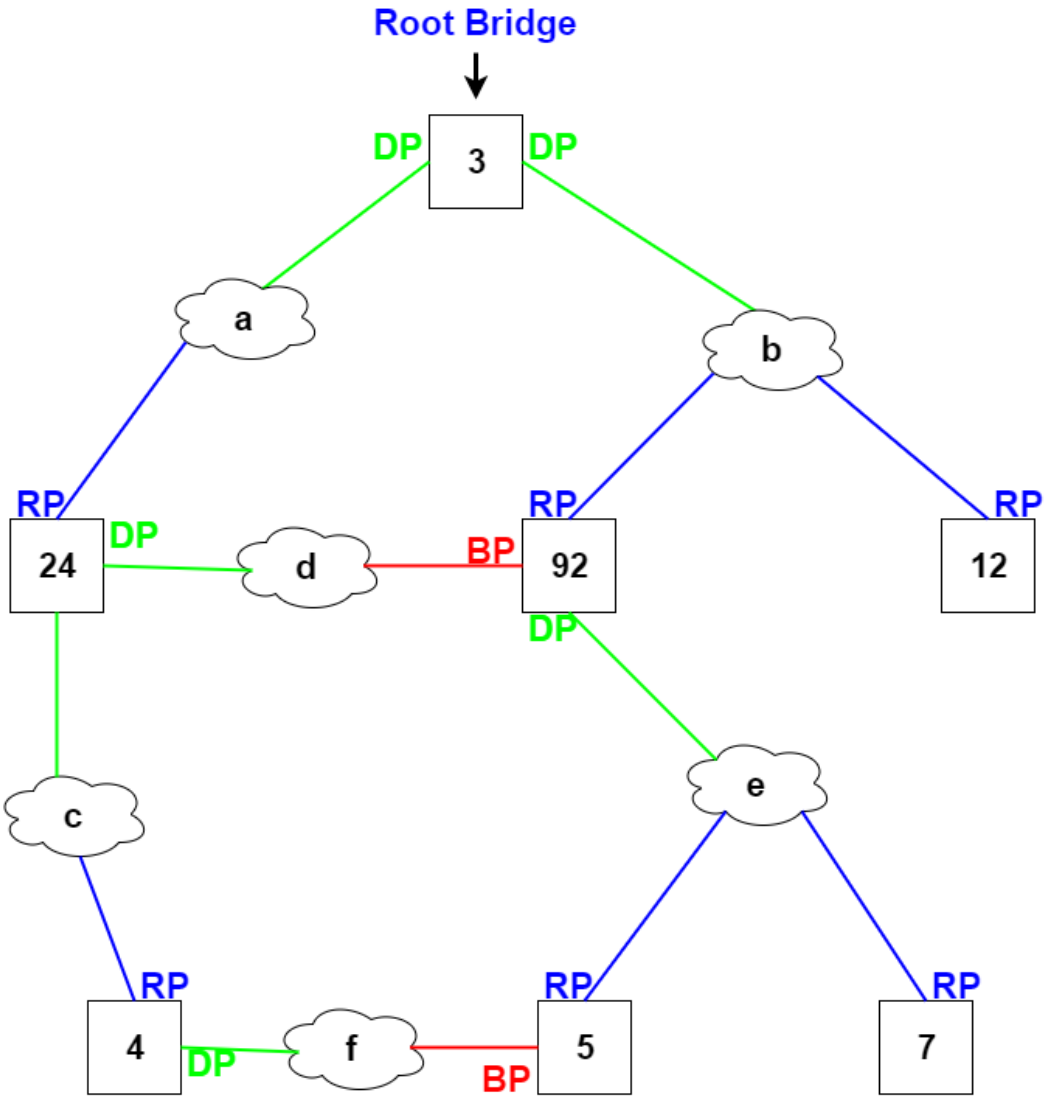
vytváří kostru grafu (spanning tree) v síti propojených mostů linkové vrstvy a zakáže ty odkazy, které nejsou součástí kostry grafu, a ponechává jedinou aktivní cestu mezi dvěma libovolnými síťovými uzly. Potřeba STP vznikla, protože přepínače v lokálních sítích jsou často propojeny pomocí redundantních odkazů, aby se zlepšila odolnost v případě selhání jednoho spojení. Tato konfigurace připojení však vytváří přepínací smyčku vedoucí k „broadcast radiation“ (kumulace broadcastového a multicastového provozu v síti) a nestabilitě tabulky MAC adres. Pokud se pro připojení přepínačů používají redundantní (přebytečná) spojení, je třeba se vyhnout přepínacím smyčkám. Aby se předešlo problémům spojeným s redundantními spoji v přepínané LAN, je do přepínačů implementován STP pro sledování topologie sítě. Každá vazba mezi přepínači, zejména nadbytečné propojení, je katalogizována. STP pak deaktivuje nadbytečná spojení nastavením jednoho preferovaného spojení mezi přepínači v síti LAN. Toto preferované spojení se používá pro všechny rámce Ethernet, pokud ovšem neselže. V takovém případě je povoleno nepreferované redundantní spojení. Když je STP implementován v síti, označí jeden přepínač jako root bridge (kořenový most). Na tomto kořenovém mostu se vypočítají preferovaná a nepreferovaná spojení. Přepínač, zvolený jako kořenový most, neustále komunikuje s ostatními přepínači v síti LAN pomocí BPDUs.

Primární funkcí STP je tedy odstranění potenciálních smyček v síti. Bez STP by v mnoha případech L2 LAN sítě jednoduše přestaly fungovat, protože smyčky vytvořené v síti by zaplavily přepínače nadbytečným provozem. Optimalizovaný provoz a konfigurace STP zajišťuje, že síť LAN zůstává stabilní a že provoz vede po síti nejoptimalizovanější cestou. Všechny porty přepínačů v síti, kde je STP nastaven, jsou kategorizovány:

- **Blocking** – blokovaný port, který by způsobil přepínací smyčku, kdyby byl aktivní. Aby se zabránilo použití smyčkových cest, nejsou přes blocking port odesílána ani přijímána žádná uživatelská data. Data BPDU jsou stále přijímána ve stavu blocking. Blokovaný port může přejít do režimu forwarding, pokud ostatní používané odkazy selžou a algoritmus STP určí, že port může přejít do stavu forwarding.
- **Listening** – přepínač zpracovává BPDU a čeká na možné nové informace, které by způsobily návrat do stavu blocking. Nezaplňuje tabulku MAC a nepředává rámce.
- **Learning** – zatímco port ještě nepředává rámce, učí se zdrojové adresy z přijatých rámců a ty jsou přidávány do tabulky MAC adres.
- **Forwarding** – port v normálním provozu, který přijímá a předává rámce. Port monitoruje příchozí BPDUs, které by naznačovaly, že by se měl vrátit do stavu blocking, aby se zabránilo smyčce.
- **Disabled** – port manuálně zakázaný správcem sítě.

Příklad sítě po implementaci STP je znázorněn v *Obr. 2.2*: Příklad sítě STP

– číslované rámečky představují mosty, tj. přepínače v síti LAN. Číslo představuje bridge ID. Obláčky označené písmeny představují segmenty sítě. Nejmenší bridge ID je 3. Přepínač s bridge ID 3 se proto stane root bridge.

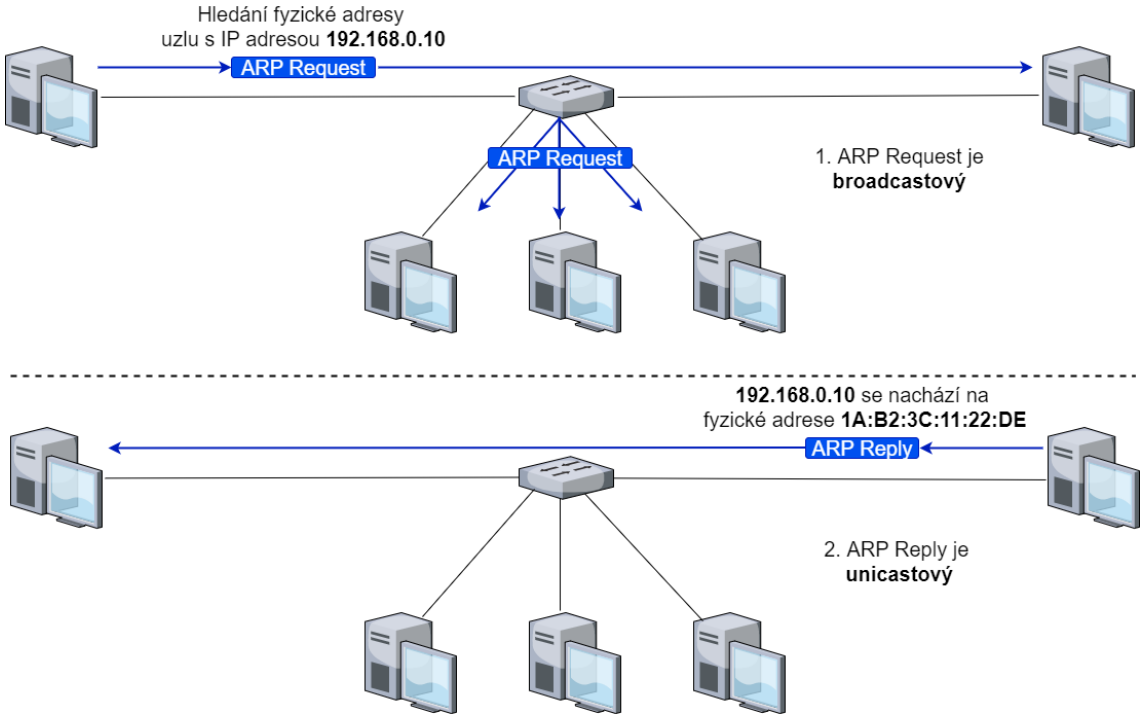


Obr. 2.2: Příklad sítě STP

- **RP (Root Port)** – port s nejnižší cenou cesty k root bridge.
- **DP (Designated Port) –** port s nejnižší cenou cesty v segmentu lokální sítě.
- **BP (Blocked Port) –** zablokovaný port z důvodu zamezení utváření smyček.

- **ARP (Address Resolution Protocol)** je komunikační protokol používaný pro identifikaci adres na linkové vrstvě, jako je MAC adresa spojená s danou adresou ze sady TCP/IP, obvykle IPv4 adresou. Toto mapování je kritickou

funkcí v sadě internetových protokolů. ARP byl implementován s mnoha kombinacemi technologií síťových a datových spojů, jako je IPv4. V sítích IPv6 je funkce ARP zajištěna protokolem ND. ARP je protokol fungující na bázi request-response (dotaz-odpověď), komunikuje v rámci jedné sítě a provoz není nikdy směrován přes síťové uzly. Tato vlastnost zařazuje ARP do linkové vrstvy.



Obr. 2.3: ARP Request a ARP Reply

- **Struktura paketu –** ARP používá jednoduchý formát zprávy obsahující jeden ARP dotaz, nebo ARP odpověď. Velikost ARP zprávy závisí na velikosti adresy na linkové a síťové vrstvě. Záhlaví zprávy určuje typy sítí použitých v každé vrstvě a velikost adres na každé vrstvě. Záhlaví zprávy je doplněno operačním kódem pro dotaz (1) a odpověď (2). Užitečné zatížení paketu se skládá ze čtyř adres – hardwarové a protokolové adresy odesílatele a příjemce.

Octet offset	0	1
0	HTYPE	
2	PTYPE	
4	HLEN	PLEN
6	OPER	
8	SHA (první 2 bajty)	
10	další 2 bajty	
12	poslední 2 bajty	
14	SPA (první 2 bajty)	
16	poslední 2 bajty	
18	THA (první 2 bajty)	
20	další 2 bajty	
22	poslední 2 bajty	
24	TPA (první 2 bajty)	
26	poslední 2 bajty	

Obr. 2.4: struktura ARP paketu.

- **HTYPE (Hardware Type) –** specifikace spojovacího hardwaru (např. Ethernet je hodnota 1).
- **PTYPE (Protocol Type) –** číslo protokolu v rámci ARP.
- **HLEN (Hardware Length) –** délka hardwarové adresy v oktetech (např. Ethernet má délku 6).
- **PLEN (Protocol Length) –** délka adresy protokolu (např. IPv4 má 4 oktety).
- **OPER (Operation) –** specifikuje operaci, kterou odesílatel požaduje (1 – dotaz, 2 – odpověď).
- **SHA (Sender Hardware Address) –** fyzická adresa odesílatele – v případě dotazu indikuje adresu uživatele odesílajícího dotaz / v ARP odpovědi uvádí adresu hostitele, pro kterého byl dotaz určen**.**
- **SPA (Sender Protocol Address) –** adresa odesílatele.
- **THA (Target Hardware Address) –** fyzická adresa příjemce – v případě ARP dotazu je toto pole vynecháno / v ARP odpovědi je užito k indikaci adres odesílatele dotazu.
- **TPA (Target Protocol Adress) –** adresa příjemce paketu.

- **IPv6 ND (Neighbour Discovery)** je protokol používaný v IPv6. Je to sada zpráv a procesů, které určují vztahy mezi sousedními uzly. Umožňuje tedy různým

uzlům propagovat jejich existenci svým sousedům, a také jim umožňuje se dozvědět o existenci jejich sousedů. Uzly navíc využívají ND k aktivnímu sledování možnosti dosáhnout sousedů. Pokud selže router (nebo cesta k němu), uzly aktivně hledají alternativy k dosažení cíle. ND koresponduje s kombinací IPv4 protokolů: ARP, ICMP Router Discovery (RDISC) a ICMP Redirect (ICMPv4). Neighbour Discovery ovšem poskytuje mnoho výhod oproti IPv4 protokolům, jako například:

- ► Router Discovery je součástí základní sady protokolů (není třeba „snooping“ směrovacích protokolů).
- ► Propagace routeru (Router Advertisements):
  - obsahují adresy linkové vrstvy (link-layer address), tudíž není potřeba další výměna paketů ke zjištění adresy směrovače.
  - obsahují prefixy, není tedy nutné mít samostatný mechanismus pro konfiguraci masky sítě.
  - umožňují automatickou konfiguraci adresy (Address Autoconfiguration).
- ► „Next-hop determination“ – algoritmus, který uzly používají pro mapování cílové IPv6 adresy na sousední IPv6 adresu, na kterou plánuje odesílat provoz určený cíli.
- ► Detekce duplicitní adresy – uzel určí, zda je adresa již používána jiným uzlem.
- ► Na rozdíl od IPv4 Router Discovery, propagační zprávy routeru neobsahují pole preferencí (preference field). Pole preferencí není třeba ke zvládnutí řízení směrovačů různé „stability“.
- ► „Unreachability Detection“ detekuje nefunkční směrovače a přepne na ty, které jsou funkční.

- **DHCP (Dynamic Host Configuration Protocol)** je protokol správy sítě. Server DHCP dynamicky přiřadí každému zařízení v síti IP adresu a další parametry konfigurace sítě, aby zařízení spolu mohla komunikovat v rámci lokální sítě i se zařízeními jiných sítí protokolu IP. DHCP server umožňuje počítačům automaticky požadovat IP adresy a síťové parametry od ISP, což snižuje potřebu správce sítě nebo uživatele ručně přiřadit IP adresy všem síťovým zařízením. V případě neexistence DHCP serveru musí být počítači nebo jinému zařízení v síti IP adresa přidělena ručně (staticky). DHCP lze implementovat v sítích o velikosti od domácích sítí po velké firemní sítě a sítě regionálních ISP. Směrovač nebo rezidenční gateway (malý směrovač pro spotřebitelské účely, který poskytuje přístup k síti mezi hostiteli sítě LAN do sítě WAN prostřednictvím modemu), lze aktivovat jako server DHCP. Většina směrovačů

přijímá v síti ISP celosvětově jedinečnou IP adresu. V síti LAN přiřadí DHCP server lokální IP adresu každému zařízení, které je k síti připojeno následujícím způsobem (tzv. DHCP handshake):

- **DHCP Discover –** klient tuto zprávu posílá k objevení DHCP serveru/serverů v síti.
- **DHCP Offer –** DHCP server odpovídá nabídkou volné IP adresy ze svého rozsahu a dalšími informacemi.
- **DHCP Request –** klient si vyžádá IP adresu ze serveru.
- **DHCP ACK –** server potvrdí novou IP adresu, která byla nyní určena konkrétnímu zařízení a tím dokončí cyklus „DHCP handshake“.

Protokoly pro definici VLAN

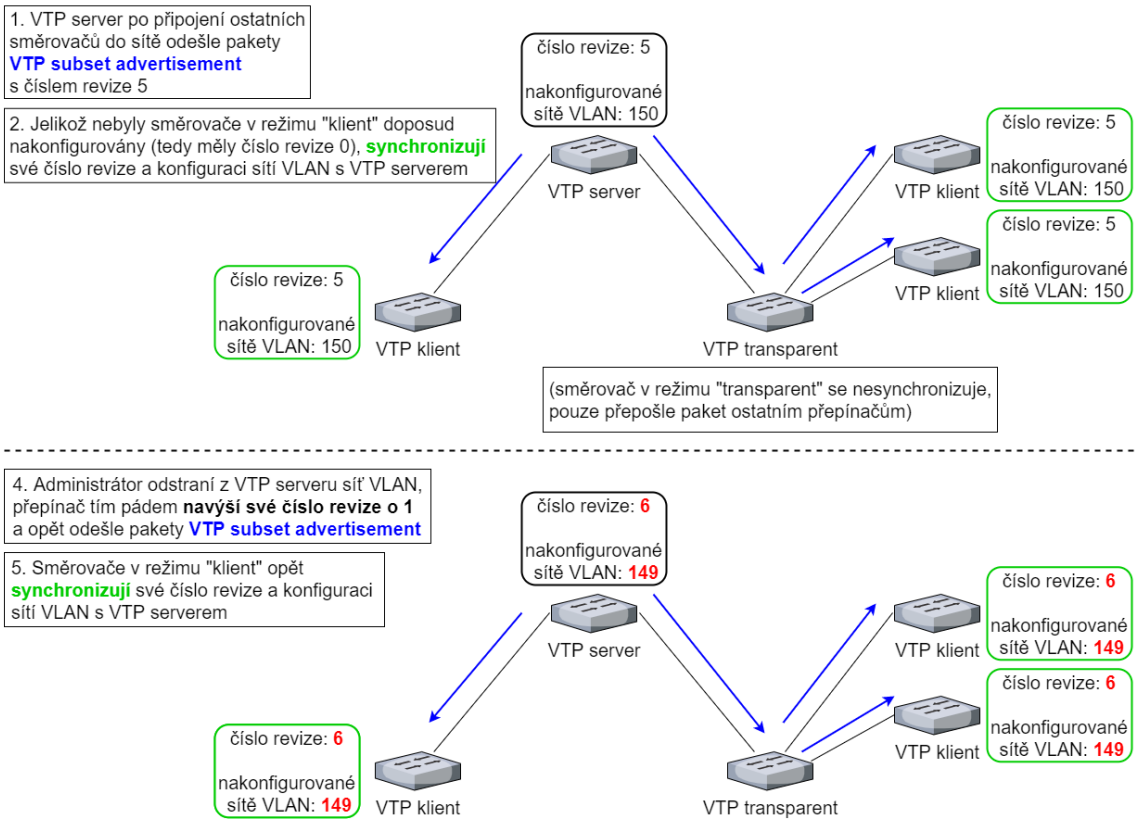
- **Cisco VTP (VLAN Trunking Protocol)** je protokol pro zasílání zpráv linkové vrstvy, který udržuje konzistenci konfigurace VLAN pomocí správy přidávání, mazání a přejmenování VLAN v tzv. VTP doméně. Doména VTP (nazývána také jako doména správy VLAN) je tvořena jedním nebo více síťovými zařízeními, která sdílejí stejný název domény VTP a jsou propojena VLAN trunky. VTP minimalizuje nesprávné konfigurace a nekonzistentní konfigurace, které mohou vést k řadě problémů, např. duplicitní názvy VLAN, nesprávné specifikace typu VLAN a narušení bezpečnosti. S VTP se také dají provádět změny konfigurace centrálně na jednom nebo více síťových zařízeních a nechat tyto změny automaticky poslat všem ostatním zařízením v síti. Synchonizace jednotlivých přepínačů je realizována pomocí čísla revize, což je 32-bitové číslo, které je vytvořeno přepínačem typu server. Při změně názvu domény je toto číslo nastavené na nulu. Při jakékoliv změně (přidání/odebrání/konfigurace) VLAN se revizní číslo zvětší o 1. Existují 3 typy paketů, pomocí kterých spolu přepínače komunikují a 3 režimy přepínačů:
  - **Typy paketů:**
    - **Summary Advertisement (propagace; shrnutí) –** Servery VTP odesílají zprávy každých 300 sekund a také v případě, že dojde ke změně databáze VLAN. Tato zpráva nese informace, jako je verze VTP, název domény, číslo revize, počet následujících VTP zpráv, časové razítko atd. Pokud se změní konfigurace VLAN, jedna nebo více „subset“ zpráv následuje po souhrnné zprávě.
    - **Subset Advertisement –** Servery VTP odesílají „subset“ zprávy po změně konfigurace VLAN. Tyto zprávy obsahují konkrétní změny, které byly provedeny, jako je přidání nebo odstranění sítě

VLAN, změna názvu sítě VLAN atd.

- **Advertisement Request from Clients (propagace; požadavky od klientů) –** Klient VTP může požadovat jakékoli informace o VLAN. Může to být z důvodu, že klientský přepínač byl resetován a ztratil informace o VLAN nebo by mohl dostat vyšší číslo revize, než je lokálně uložené. Přepínač typu server reaguje na tyto požadavky zprávou „Summary Advertisement“, po které následuje „Subset Advertisement“, aby se klient aktualizoval.

► **Režimy přepínačů:**

- **Server** – VTP server je výchozím režimem. V tomto režimu je možno vytvářet, upravovat a mazat VLAN sítě a určovat další konfigurační parametry (jako je např. verze VTP) pro celou VTP doménu. VTP servery inzerují svou VLAN konfiguraci na ostatní přepínače ve stejné doméně VTP a synchronizují svoji VLAN konfiguraci s ostatními přepínači na základě propagací přijatých prostřednictvím trunkových odkazů.
- **Klient** – VTP klienti se chovají stejným způsobem jako servery VTP s tím rozdílem, že VTP klient nemůže vytvářet, měnit ani mazat VLAN sítě.
- **Transparent** – transparentní VTP přepínače se neúčastní VTP. Jinými slovy, transparentní VTP přepínač neautorizuje svoji konfiguraci VLAN a nesynchronizuje svou konfiguraci VLAN na základě přijatých VTP paketů. Transparentní přepínače předávají VTP pakety dalším přepínačům ve VTP doméně.



Obr. 2.5: Příklad VTP v síti

- **GVRP (GARP VLAN Registration Protocol)** nebo také „Generic VLAN Registration Protocol“ je protokol, který usnadňuje řízení sítí VLAN ve větší síti. GVRP odpovídá specifikaci IEEE 802.1Q, která definuje metodu označování rámců konfiguračními daty sítě VLAN. To umožňuje síťovým zařízením dynamicky si vyměňovat informace o konfiguraci VLAN s jinými zařízeními. GVRP je založen na protokolu GARP, což je protokol definující postupy, kterými mohou koncové stanice a přepínače v místní síti (LAN) zaregistrovat a odregistrovat atributy, jako jsou identifikátory nebo adresy, mezi sebou. Každá koncová stanice a přepínač má tedy aktuální záznam o všech ostatních koncových stanicích a přepínačích, se kterými se lze spojit. GVRP, stejně jako GARP, eliminuje zbytečný síťový provoz tím, že brání pokusům o přenos informací neregistrovaným uživatelům. Kromě toho je nutné ručně nakonfigurovat pouze jeden přepínač a všechny ostatní přepínače budou automaticky nakonfigurovány odpovídajícím způsobem.
- **MRP (Multiple Registration Protocol)** je standard IEEE 802.1ak. Tento standard nahradil GARP a určuje protokoly, procedury a spravované objekty, které podporují protokol MRP. MRP umožňuje účastníkům v „MRP Application“ registrovat atributy u ostatních účastníků v Bridged LAN. Jsou

definovány dvě aplikace:

- **MVRP (Multiple VLAN Registration protocol)** – nahradil GVRP a slouží pro automatickou konfiguraci VLAN informací na přepínačích. V síti linkové vrstvy poskytuje MVRP metodu pro dynamické sdílení informací o VLAN a konfigurací VLAN. Například, aby bylo možné přidat port přepínače do VLAN, je třeba překonfigurovat pouze koncový port nebo překonfigurovat síťové zařízení podporující VLAN připojené k přepínači a na ostatních přepínačích podporujících MVRP se dynamicky vytvoří všechny potřebné trunky VLAN. Bez použití MVRP je nutná ruční konfigurace VLAN trunků nebo použití vlastní metody výrobce. Dynamické záznamy VLAN budou aktualizovány ve filtrovací databázi prostřednictvím MVRP. Stručně řečeno, MVRP pomáhá udržovat konfiguraci VLAN dynamicky na základě aktuálních síťových konfigurací. MVRP definuje aplikaci MRP, která poskytuje registrační službu VLAN. MVRP využívá prohlášení „MRP Attribute Statement“ a „MRP Attribute Propagation“, která poskytují popisy společného stavového stroje a společné mechanismy šíření informací definované pro použití v aplikacích založených na MRP. MVRP poskytuje mechanismus pro dynamickou údržbu obsahu dynamických registračních záznamů VLAN pro každou síť VLAN a pro šíření informací na další mosty. Tato informace umožňuje zařízením s podporou MVRP navázat a dynamicky aktualizovat své znalosti sady VLAN. Hlavním účelem MVRP je umožnit přepínačům automaticky získat některé informace o VLAN, které by jinak bylo nutné ručně nakonfigurovat.
- **MMRP (Multiple MAC Registration Protocol) –** protokol pro registraci skupinových MAC adres (tj. multicastového vysílání) na více přepínačích.

Proprietární protokoly

- **LLDP (Link Layer Discovery Protocol)** je vendor-neutral protokol linkové vrstvy používaný síťovými zařízeními pro propagaci jejich identity a sousedů v místní síti založené na technologii IEEE 802, hlavně kabelovém Ethernetu. LLDP vykonává funkce podobné několika proprietárním protokolům, jako je CDP. Informace shromážděné pomocí LLDP lze uložit do „Management Information Database“ zařízení a dotazovat se protokolem SNMP. Topologii sítě podporující LLDP lze zjistit procházením hostitelů a dotazováním se na tuto databázi. Informace, které lze získat, zahrnují název a popis systému, název a popis portu, název VLAN, adresu pro správu IP, možnosti systému (přepínání, směrování atd.) a MAC informace.

- **CDP (Cisco Discovery Protocol)** se používá ke sdílení informací o jiných přímo připojených zařízeních Cisco (např. verze operačního systému a IP adresa). CDP lze také použít pro on-demand routing (směrování na vyžádání). Každé zařízení nakonfigurované pro CDP propaguje alespoň jednu adresu, na které zařízení může přijímat zprávy a odesílat periodické „CDP Advertisements“ (propagace) na všeobecně známou ethernetovou multicastovou adresu (Well-known Ethernet Multicast address) „01:00:0C:CC:CC:CC“ pro protokoly CDP a VTP. Tyto multicastové rámce mohou být přijímány přepínači Cisco a dalšími síťovými zařízeními, které podporují CDP do jejich připojeného síťového rozhraní. Propagace podporované a konfigurované v softwaru Cisco se standardně odesílají každých 60 sekund na rozhraní, která podporují záhlaví protokolu SNAP (Subnetwork Access Protocol). Každé zařízení Cisco, které podporuje CDP, ukládá informace přijaté z jiných zařízení do tabulky, kterou lze zobrazit pomocí příkazu „show cdp neighbours“. Tato tabulka je také přístupná prostřednictvím protokolu SNMP. Informace o tabulce CDP se obnovují pokaždé, když je přijato oznámení a doba čekání pro tento záznam je znovu inicializována. Doba čekání určuje životnost (TTL) záznamu v tabulce – pokud nejsou ze zařízení přijata žádná oznámení po delší dobu, informace o zařízení jsou zahozeny (po 180 sekundách neboli po třech zmeškaných propagacích od tohoto zařízení).

Ostatní protokoly

Další protokoly na linkové vrstvě, které se prozatím nedají zneužít.

- **LACP (Link Aggregation Control Protocol)** ve specifikaci IEEE poskytuje metodu pro řízení svazku několika fyzických portů dohromady za účelem vytvoření jediného logického kanálu. LACP umožňuje síťovému zařízení vyjednat automatické sdružování odkazů zasláním LACP paketů na přímo připojené zařízení, které také implementuje LACP.
- **Ethernet Flow Control** je mechanismus pro dočasné zastavení přenosu dat v počítačových sítích Ethernet. Cílem tohoto mechanismu je zajistit nulovou ztrátu paketů v případě přetížení sítě.

3 Možnosti útoku na linkové vrstvě

Mnoho organizací zajišťuje bezpečnostní opatření ve vyšších vrstvách OSI. Jednou z oblastí, která je obecně opomíjena, je bezpečnost linkové vrstvy. To může otevřít síť mnoha útokům a kompromitacím.

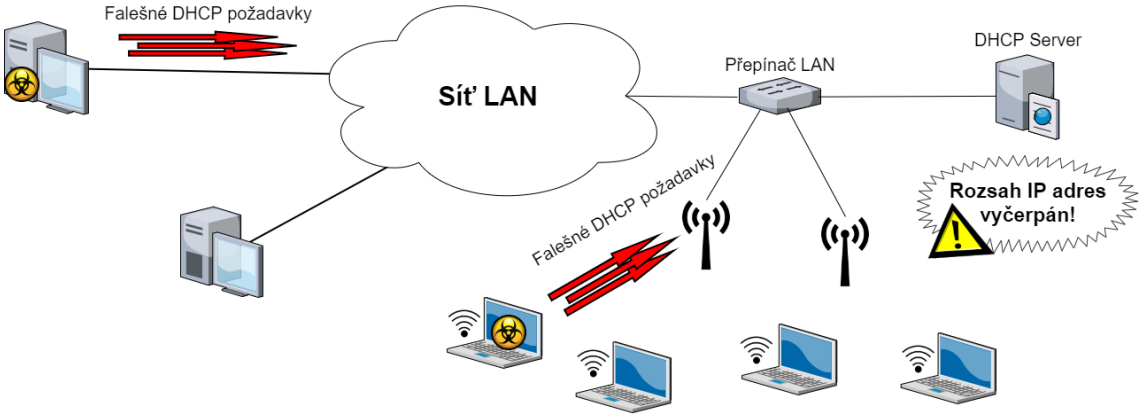
V této kapitole budou probrány bezpečnostní rizika na linkové vrstvě.

3.1 Útoky na DHCP server

Na DHCP servery je možné zaútočit způsobením „vyhladovění“ klientů přijímajících IP adresy z DHCP serveru (DHCP starvation) nebo předstíráním identity DHCP serveru (DHCP spoofing).

3.1.1 DHCP Starvation

Jedná se o zvláštní druh útoku, kdy útočník odešle na DHCP server spoustu požadavků (DHCP Requests) s chybnou MAC adresou. Pokud je síť zaplavena dostatečným množstvím požadavků, může útočník vyčerpat všechny dostupné adresy DHCP serveru. Klienti napadené sítě jsou pak „vyhladověni“ – DHCP server nemá žádné IP adresy, které by mohl přidělit.



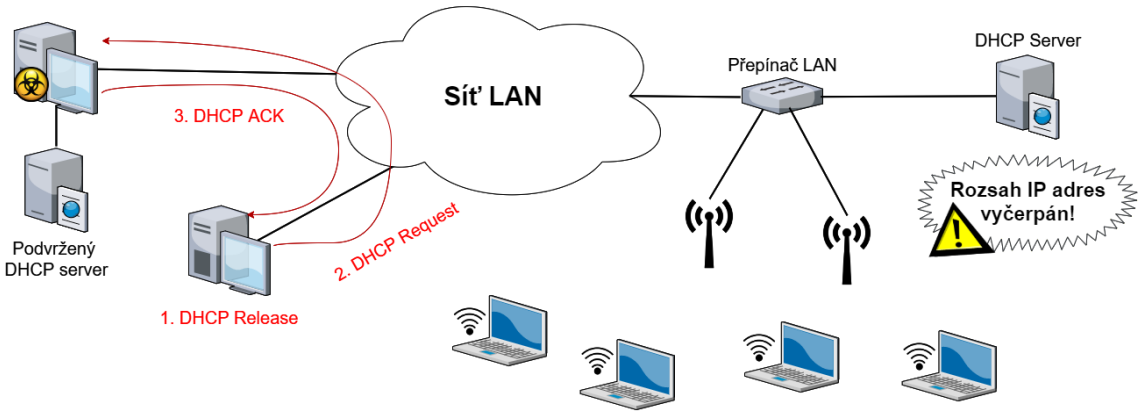
Obr. 3.1: DHCP Starvation

Útočník poté může v síti nastavit podvržený DHCP server a obětem podvrhnout upravené konfigurace IP, zajišťují útočníkovi možnost MITM útoku.

3.1.2 DHCP Spoofing

Při DHCP spoofingu nasadí útočník podvržený DHCP server, který klientům poskytne IP adresy. Když se klienti připojují k síti, nabídne jim podvržený server i legitimní DHCP server IP adresy a výchozí bránu, servery DNS a servery WINS (Windows

Internet Name Services – používané u starších verzí Windows). Pokud se informace poskytované podvrženým DHCP serverem liší od těch legitimních, mohou mít klienti problémy s přístupem k síti, včetně problémů s rychlostí a neschopností komunikace s ostatními klienty v síti. Kromě toho, pokud je podvržený DHCP server nastaven tak, aby jako výchozí brána poskytoval IP adresu počítače, který je obsluhován útočícím uživatelem, potom tento uživatel může sledovat veškerý provoz odeslaný klienty do jiných sítí (MITM útok).



Obr. 3.2: DHCP Spoofing v návaznosti na DHCP Starvation

VMware nebo software virtuálního stroje mohou také působit jako podvržený DHCP server neúmyslně, když jsou spuštěny na klientském počítači připojeném k síti. VMware bude fungovat jako podvržený DHCP server, který přiděluje klientům v síti náhodné IP adresy. Konečným důsledkem může být to, že velké části sítě jsou pak odříznuty od internetu.

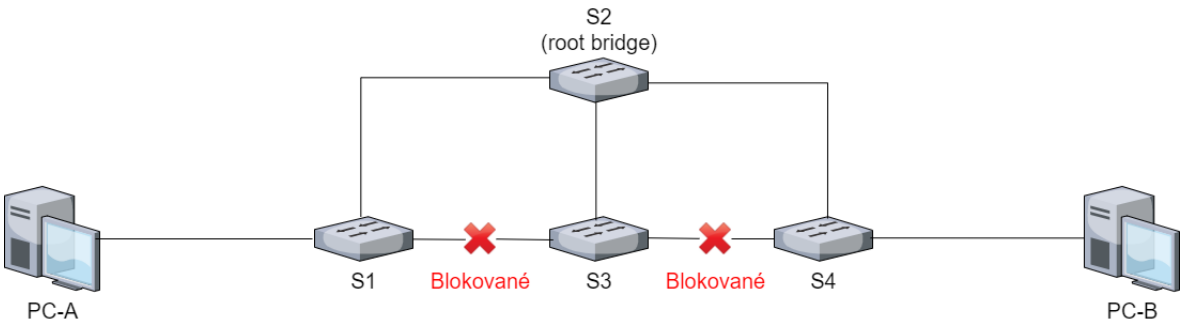
3.2 Napadení STP

Pokud útočník vloží do sítě nové zařízení STP a pokusí se změnit fungování protokolu na tomto zařízení, má tento útok potenciál ovlivnit provoz datového toku přes síť LAN, což má výrazný dopad na použitelnost a bezpečnost síťového provozu.

Pro pochopení zranitelnosti STP, je důležité vědět, jak STP funguje. STP tvoří stromovou topologii s kořenovým mostem (root bridge) na základně. Kořenový most se volí na základě dat sdílených v datových jednotkách STP, tzv. BPDUs (bridge protocol data units). Rámce BPDU jsou zasílány na známé multicastové adresy a obsahují, mimo jiné, MAC adresu přepínače a uživatelem definovanou hodnotu priority. Kombinace těchto hodnot se nazývá ID mostu (bridge ID) a přepínač s nejnižším ID je zvolen jako kořenový most.

Po volbě kořenového mostu najde každý přepínač v síti rozhraní, které vede k nejlepší cestě ke kořenovému mostu a označí jej jako kořenový port (root port), zatímco přebytečná rozhraní jsou přepnuta do blokovacího režimu (blocked port). Všechna aktivní rozhraní na přepínači budou nakonec buď v režimu přesměrování (forwarding), nebo v režimu blokování. Tento proces se nazývá konvergence. *Obr. 3.3* ukazuje

topologii sítě po běžné konvergenci STP. Na tomto obrázku bude provoz z PC-A do PC-B směřován z S1 na kořenový most S2 a poté na S4, zatímco cesty S1 –> S3 a S3 –> S4 jsou blokované, aby se zamezilo tvoření smyček.



Obr. 3.3: Příklad sítě STP

Změny topologie, jako například přidání nových přepínačů mohou způsobit, že bude zvolen nový kořenový most a doména STP bude znovu procházet konvergencí. Čas potřebný k dokončení procesu je výrazný a během této doby se nepředává žádný provoz.

STP navíc sám o sobě nemá absolutně žádné zabezpečovací mechanismy. BPDU jsou vyměňovány v prostém textu (plain text) a neexistuje žádný mechanismus autentizace. Přepínač důvěřuje všem BPDU rámcům, které obdrží. Na základě těchto informací je snadné vydedukovat, že STP lze zneužít následujícími způsoby:

- **DoS útoky –** odesláním „ručně“ vytvořených BPDU není obtížné převzít roli kořenového mostu, což způsobí, že významná část provozu bude přesunuta na zařízení útočníka.

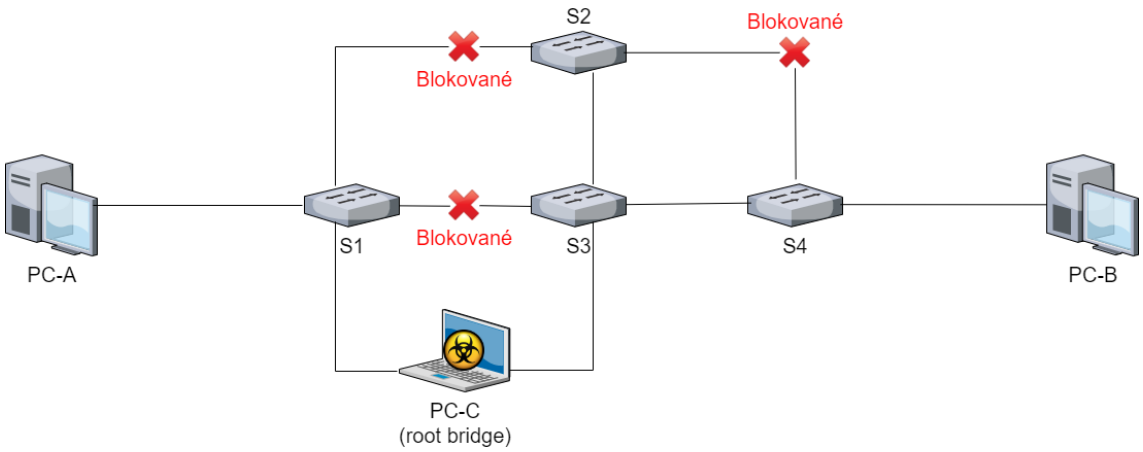
  I v případě nepřevzetí role kořenového mostu útočníkem, je možné (odesláním BPDU s oznámeními o změně topologie v krátkých intervalech) způsobit narušení provozu opakovaným vynucením konvergence.

- **MITM útoky** – v některých případech se může zařízení útočníka (pomocí propagace nízké priority mostu) stát kořenovým mostem. To způsobí, že přes něj projde významná část provozu, kterou lze zkopírovat, upravit a předat do skutečného cíle.

  Na *Obr. 3.4*: Síť STP po útoku MITM

  je vidět ukázka toho, když je útočník schopen vytvořit trunk s S1 a S3 z předchozího příkladu (*Obr. 3.3*: Příklad sítě STP

) a stát se kořenovým mostem inzerováním nižšího ID mostu. Nyní jsou blokovány cesty S1 –> S2 a S2 –> S4, zatímco cesta na lince S3 –> S4 už nebude nadále blokována. Významná část provozu mezi PC-A a PC-B bude nyní protékat kořenovým mostem útočníka PC-C, kde může být zachycen a upraven před tím, než bude přeposlán dále.



Obr. 3.4: Síť STP po útoku MITM

3.3 Útok na protokol ARP

V protokolu ARP neexistuje žádná metoda, kterou by hostitel v síti mohl autentizovat počítač, ze kterého paket pochází. Jedná se o chybu zabezpečení, která umožňuje provádět ARP spoofing.

3.3.1 ARP Spoofing

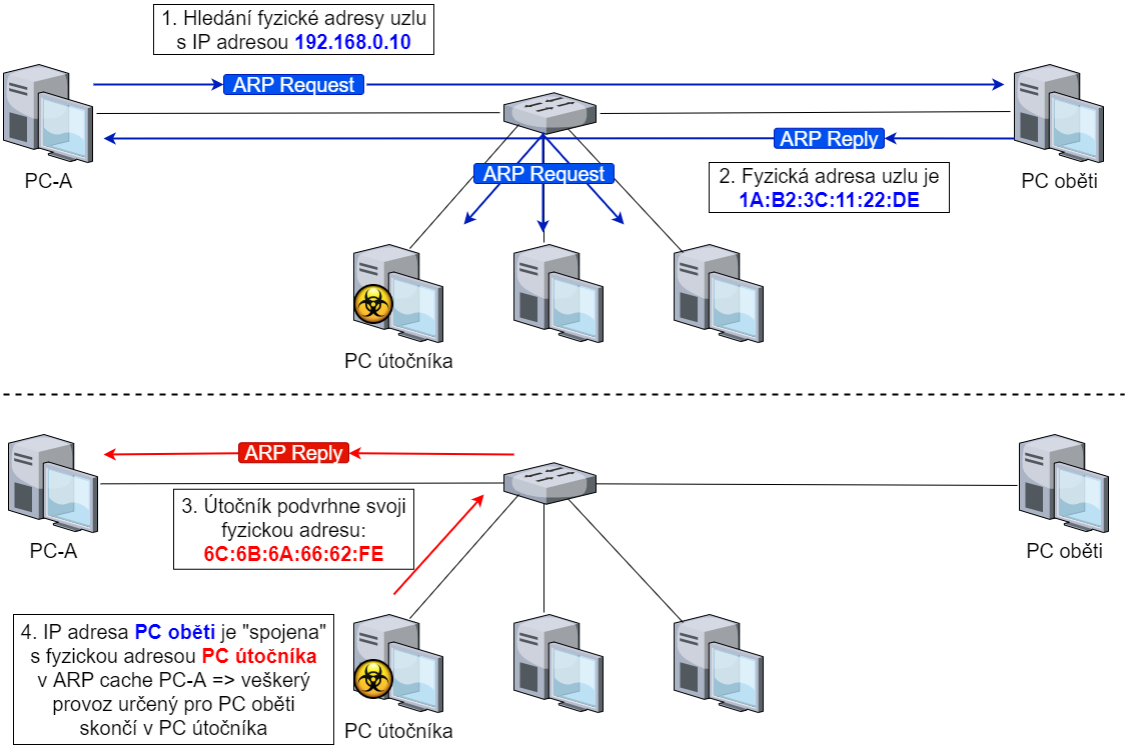
ARP Spoofing (také ARP cache poisoning nebo ARP poison routing) je typ útoku, při kterém útočník odesílá padělané zprávy ARP v lokální síti. To má za následek propojení MAC adresy útočníka s IP adresou legitimního počítače nebo serveru v síti. Jakmile je MAC adresa útočníka spojena s autentizovanou IP adresou, útočník začne přijímat veškerá data, která jsou pro tuto IP adresu určena.

Každý počítač v síti udržuje tabulku zvanou „ARP cache“. Tabulka obsahuje IP adresu a přidružené MAC adresy ostatních zařízení v síti. Protože je ARP „stateless“ protokol (bez informací o aktuální relaci od serveru), pokaždé, když zařízení obdrží „ARP Reply“ od jiného zařízení, přijme jej a aktualizuje svou ARP cache, i přestože neodeslal žádný „ARP Request“. Díky tomuto faktu je možné se jednoduše vydávat za jiná zařízení v síti.

Útok lze použít pouze v sítích, které používají ARP a vyžaduje, aby měl útočník přímý přístup k segmentu místní sítě, která má být napadena. ARP spoofing může umožnit útočníkovi zamaskovat se jako legitimní uživatel a díky tomu zachytit, upravit nebo dokonce i zastavit přenos dat v síti. Účinky útoků typu ARP spoofing mohou mít pro síť, na kterou se útočí, vážné důsledky. Ve své nejzákladnější aplikaci se útoky ARP spoofingu používají k odcizení citlivých informací. Kromě toho se tyto útoky často používají k usnadnění dalších útoků, jako jsou:

- **DoS útoky** – často využívají ARP spoofing k propojení více IP adres s MAC adresou jednoho cíle. V důsledku toho bude přenos, který je určen pro mnoho různých IP adres, přesměrován na MAC adresu cíle a to povede k přetížení cíle nadbytečným provozem.

- **Session hijacking („únos“ relace)** – útočník může pomocí ARP spoofingu ukrást ID relací a poskytnout tak útočníkům přístup k soukromým systémům a datům.
- **MITM útoky** – ARP spoofing je možné využít k zachycení a upravení provozu mezi počítači v napadené síti.



Obr. 3.5: ARP spoofing

3.4 CAM table overflow

Tabulky CAM (content addressable memory), také nazývané tabulky MAC adres, se na přepínačích používají ke sledování, kam se má odesílat provoz pro konkrétní naučené adresy MAC. Pro pochopení skutečného účinku tohoto útoku je třeba porozumět základnímu fungování CAM tabulky a jak optimalizuje chování přepínače při přeposílání dat (forwarding).

Když je přepínač uveden do provozu, má prázdnou CAM tabulku. Neví, která zařízení jsou připojena ke kterým rozhraním, a proto zpočátku odesílá přijatý provoz na všechna rozhraní (flooding). Protože CAM tabulka přijímá provoz v každém rozhraní, vytváří položky pro každou z MAC adres, které vidí a spojuje každou adresu se svým specifickým rozhraním.

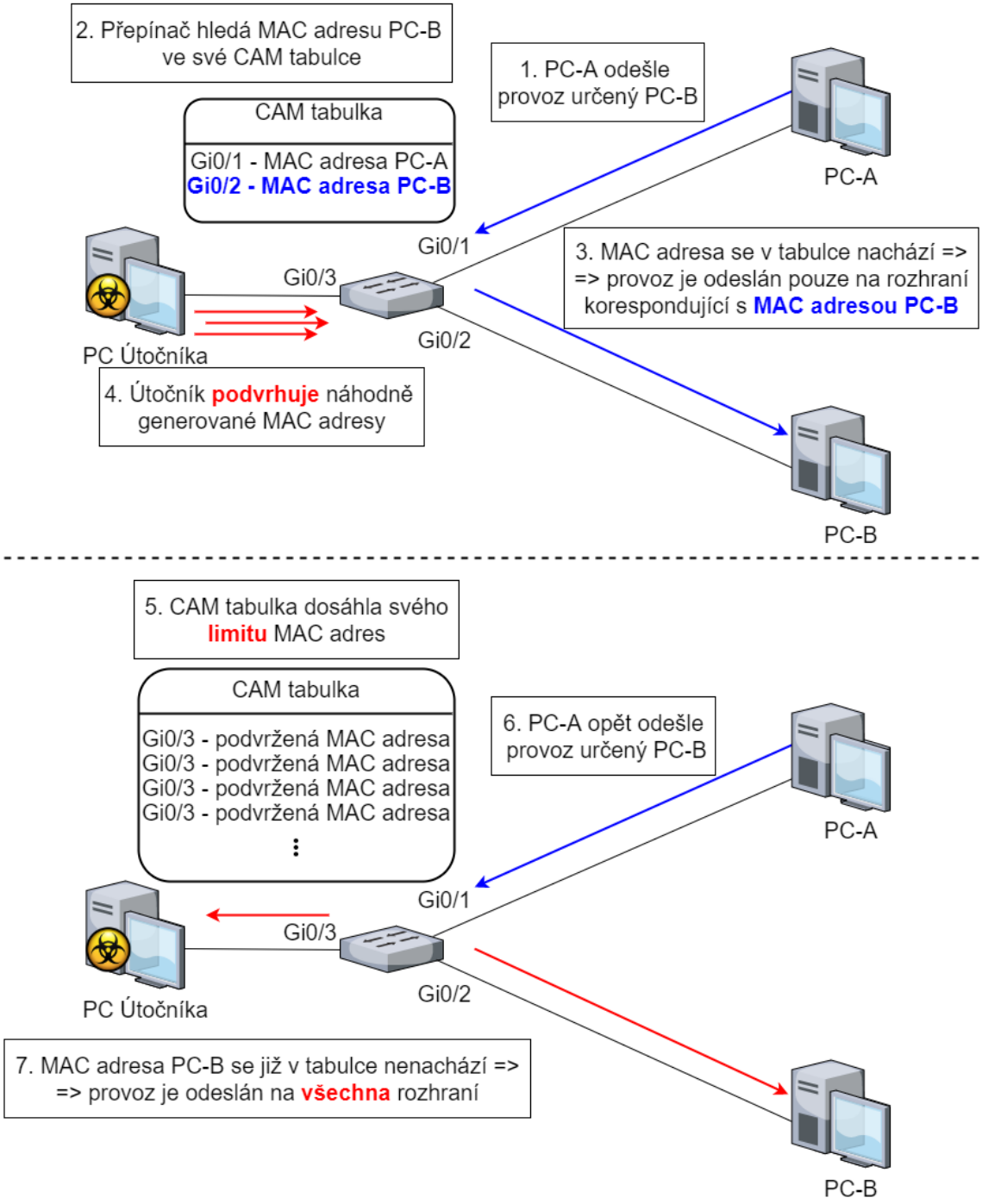
Jakmile má přepínač v CAM tabulce záznam pro konkrétní cílovou MAC adresu, nepřeposílá provoz na všechna rozhraní – místo toho odešle provoz pro tuto

adresu do svého konkrétního naučeného rozhraní. Jakmile jsou MAC adresy všech připojených zařízení naučeny, a tím se zabrání zaplavování, přenos bude odeslán do naučeného rozhraní každého cíle. Tento výsledek výrazně optimalizuje chování přepínače při přeposílání a zvyšuje množství šířky pásma přepínače (za předpokladu, že se jedná o zaneprázdněný přepínač – jde přes něj velké množství provozu).

Každý přepínač má omezený počet MAC adres, které může CAM tabulka pojmout. Pokud je dosaženo limitu tabulky, veškerý provoz sestávající z neznámých MAC adres zaplaví síť. Útok CAM table overflow funguje tak, že jedno (či více) zařízení podvrhuje velké množství MAC adres a odesílá provoz přes přepínač. CAM tabulka přepínače bude zaplněna a veškerý další provoz (obvykle provoz z legitimních zařízení) bude nadbytečný, což způsobí, že přepínač bude velmi zaneprázdněn a potenciálně přetížen. V důsledku toho se síť zpomalí a nakonec se stane nepoužitelnou.

Ve zkratce to tedy znamená tři možnosti:

- V CAM tabulce se **nachází** záznam o cílové MAC adrese – přepínač odešle rámec pouze na rozhraní, na jehož konci je zařízení s danou MAC adresou.
- V CAM tabulce se **nenachází** záznam o cílové MAC adrese – přepínač odešle rámec na všechna svá rozhraní. Pokud z cílové MAC adresy obdrží odpověď, vytvoří si v CAM tabulce nový záznam MAC adresy korespondující s daným rozhraním.
- CAM tabulka je **plná** – nelze vytvořit nový záznam o MAC adrese. Pokud útočník podvrhuje velké množství náhodně generovaných MAC adres, výsledkem bude nejen naplnění kapacity CAM tabulky, ale také „vytlačení“ legitimních MAC adres z tabulky. Další důsledky útoku CAM table overflow jsou následující:
    - ► Zahlcení výpočetní kapacity přepínače (DoS útok).
    - ► Provoz určený pro legitimní uživatele je poslán na všechna rozhraní, tzn. i k útočníkovi, který je schopen pomocí tohoto útoku odposlouchávat veškerý provoz na síti (MITM útok).



Obr. 3.6: CAM table overflow

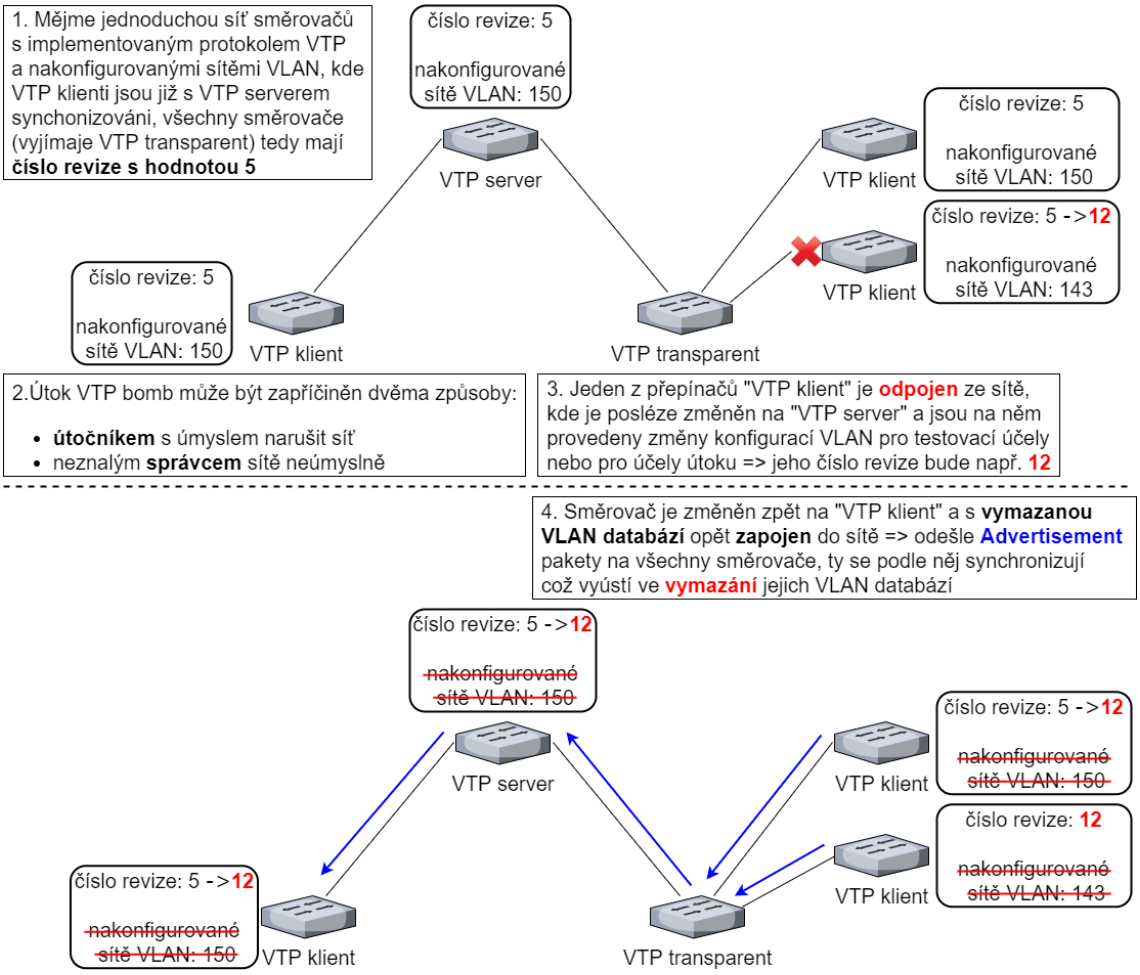
3.5 Útok na protokol VTP

3.5.1 VTP Bomb

Když je do sítě přidán nový přepínač, ve výchozím nastavení je nakonfigurován bez názvu nebo hesla domény VTP, je v režimu serveru VTP. Pokud nebyl nakonfigurován

žádný název domény VTP, předpokládá se název domény z prvního paketu VTP, který přepínač obdrží. Nový přepínač má revizi konfigurace VTP 0, a tak přijme jakékoli číslo revize a přepíše své VLAN informace, pokud se hesla VTP shodují.

Pokud by ovšem byl omylem připojen přepínač k síti se správným názvem a heslem domény VTP, ale s vyšším číslem revize VTP, než má síť aktuálně (např. přepínač, který byl ze sítě odstraněn kvůli údržbě a vrácen s vymazanými VLAN informacemi), pak by celá VTP doména přijala VLAN konfiguraci nového přepínače, což pravděpodobně způsobí ztrátu VLAN informací na všech přepínačích ve VTP doméně, a to následně povede k selhání v síti, protože přepínače Cisco udržují informace o konfiguraci VTP odděleně od běžné konfigurace.



Obr. 3.7: Útok VTP bomb

3.5.2 Falešné VTP zprávy

Útočník může jako VTP server posílat falešné VTP zprávy (neboli VTP advertisements) na trunk porty přepínačů v režimu „klient“ a tím získat privilegium přidávání a odebírání sítí VLAN z VTP domény (např. aby vytvořil STP smyčku). Další škodlivé

VTP zprávy mohou být odeslány bez jakékoliv konfigurace VLAN. Pokud netransparentní přepínač (tzn. v režimu „klient“ nebo „server“) obdrží takovou VTP zprávu, „zdědí“ číslo revize odesílajícího přepínače, což vede k DoS útoku, tedy výmazu všech sítí VLAN nakonfigurovaných ve VLAN databázi napříč celou VTP doménou.

Tento útok ovšem vyžaduje vysoké znalosti útočníka (tj. znalost jména VTP domény, heslo a detaily trunk potrů). Tyto informace mohou být získány skrz sociální inženýrství nebo důkladný průzkum sítě.

3.6 Útok na CDP

Většina směrovačů a přepínačů Cisco má ve výchozí konfiguraci CDP povoleno. CDP informace jsou zasílány v periodických přenosech, které jsou aktualizovány lokálně v CDP databázi každého zařízení. Protože je CDP protokol protokolem linkové vrstvy, směrovače jej nešíří.

CDP obsahuje informace o síťovém zařízení, jako je verze softwaru, IP adresa, platforma, funkce a nativní VLAN. Pokud jsou tyto informace k dispozici útočníkovi, může je použít k nalezení slabin pro útok na síť, obvykle ve formě útoku typu DoS.

Útočník může snadno použít program Wireshark nebo jiný síťový analyzátor k zachycení informací o zařízeních, které CDP odesílá v síti. Zejména verze softwaru Cisco IOS by útočníkovi umožnila zkoumat a určit, zda v dané konkrétní verzi kódu existují zranitelnosti v zabezpečení. Vzhledem k tomu, že CDP nemá žádné zabezpečení autentizací, mohl by útočník vytvořit falešné CDP pakety a nechat je přijmout svým přímo připojeným zařízením Cisco. Pokud útočník může získat přístup ke směrovači buď přes Telnet nebo SNMP, může pomocí informací CDP zjistit celou topologii sítě na linkové, ale i síťové vrstvě, včetně všech úrovní IOS, typů modelů směrovačů a přepínačů a adresování IP. Pokud byl někdo vybaven těmito informacemi a seznamem zranitelností, mohl by proti síti zahájit velmi účinný útok.

3.7 VLAN Hopping

Tento typ útoku umožňuje útočníkovi obejít všechna omezení linkové vrstvy vytvořená k rozdělení hostů v síti. Při správné konfiguraci portu přepínače by se útočník musel dostat přes směrovač a další zařízení síťové vrstvy, aby získal přístup ke svému cíli. Mnoho sítí však má buď špatnou implementaci VLAN, nebo má nesprávné konfigurace, které útočníkům umožní provést tento útok. V rámci VLAN hoppingu existují dva hlavní způsoby útoku: „switched spoofing“ a „double tagging“.

3.7.1 Double Tagging

Double tagging nastane, když útočník přidá a upraví značky (tagy) v Ethernetovém rámci, aby umožnil odesílání paketů prostřednictvím jakékoli sítě VLAN. Tento útok

využívá toho, kolik přepínačů zpracovává značky. Většina přepínačů odstraní pouze vnější značku a předá rámec všem nativním portům VLAN. Tento útok je tedy úspěšný pouze tehdy, pokud je útočník součástí nativní sítě VLAN trunkového spoje (trunk link). Důležitou poznámkou je, že tento útok je striktně jednosměrný, protože je nemožné zapouzdřit vrácený paket.

3.7.2 Switch Spoofing

Útočník nasadí do sítě podvržený přepínač, aby přiměl legitimní přepínač k vytvoření trunkového propojení mezi nimi. Jakmile je trunkové spojení navázáno, má útočník přístup k provozu z jakékoliv sítě VLAN. Tento útok je úspěšný pouze pokud je legitimní přepínač nakonfigurován k vyjednávání trunku (k tomu dochází, když je rozhraní nakonfigurováno v režimu – switchport mode „dynamic desirable“, „dynamic auto“ nebo „trunk“). Pokud má cílový přepínač na daném rozhraní nakonfigurovaný jeden z těchto režimů, může útočník vygenerovat ze svého počítače zprávu DTP (Dynamic Trunking Protocol) a může být vytvořen trunkový spoj.

3.8 ICMP Redirect

ICMP redirect (přesměrování) je funkce protokolu IP, která umožňuje směrovači informovat zařízení o tom, že existuje efektivnější cesta do cíle a že by zařízení mělo odpovídajícím způsobem upravit svoji směrovací tabulku. V zásadě se ICMP redirect jeví jako užitečná funkce v důvěryhodné lokální síti, ale na veřejném internetu, kde je spousta skrytých hrozeb, může mít fatální následky mít přesměrovaný provoz falešnou ICMP zprávou od útočníka. I přesto je však ICMP redirect systému Linux ve výchozím nastavení povolen.

Díky tomu, že ICMP je postarší protokol (rok 1981), může tento typ útoku výrazně narušit chod sítě. Odesláním falešného přesměrování nedojde ihned k uložení falešné trasy do mezipaměti tras (tzv. route cache). Ovšem při následovném pokusu kontaktovat zařízení (na které je provoz přesměrován) se v mezipaměti tras objeví falešný záznam, který brání v kontaktování tohoto zařízení. Kromě toho, jakmile se záznam dostane do mezipaměti tras, není snadné se ho zbavit. I když se mezipamět vymaže, falešný záznam se při příštím pokusu kontaktovat cílové zařízení opět objeví, což je nejspíše způsobeno faktem, že jádro systému (kernel) v sobě uchovává nějaký samostatný stav přesměrovaných záznamů o trase. Z toho vyplývá, že jediným účinným řešením je obnovení a restartování postiženého zařízení.

Je tedy zřejmé, že ICMP redirect lze použít k útokům DoS. Při snaze zabránit určitému zařízení (oběti) kontaktovat jiné zařízení (cíl), stačí oběti poslat falešné přesměrování. Jediným omezením je, že oběť musí kontaktovat cíl v určitém čase od přijetí přesměrování, aby DoS útok fungoval. To lze ovšem snadno vyřešit. Stačí přesměrování odeslat, když se má oběť pravděpodobně spojit s cílem nebo jednoduše odesílat nové přesměrování např. každých 10 minut.

ICMP redirect lze i snadno využít k útokům MITM pomocí přesměrování provozu zařízení oběti přes zařízení útočníka.

4 Možnosti detekce útoků na linkové vrstvě a obrana proti nim

4.1 Zabezpečení DHCP

4.1.1 DHCP Snooping

DHCP snooping je bezpečnostní technologie linkové vrstvy zabudovaná do operačního systému síťového přepínače, který zahazuje provoz DHCP, který je považován za nepřijatelný. Základním principem použití DHCP snoopingu je zabránit podvrženým DHCP serverům nabízet IP adresy klientům DHCP. Podvržené DHCP servery jsou často používány k MITM nebo DoS útokům.

DHCP snooping ukládá svá pozorování do databáze obsahující klientskou MAC adresu, IP adresu přiřazenou DHCP, zbývající dobu pronájmu adresy, VLAN a switchport. Databáze je jednoduchý soubor, který lze uložit do flash zařízení. Velikost flash je však omezená; proto se považuje za osvědčený postup ukládání DHCP snooping na vzdáleném místě, například na serveru TFTP. Uložení také zaručuje, že databáze přežije selhání přepínače.

Když služba DHCP snoopingu zjistí narušení, paket je zahozen a je zaznamenána zpráva, která obsahuje text „DHCP_SNOOPING“. Pokud je přepínač nakonfigurován tak, aby odesílal protokoly (provozní záznamy) na server syslog, je možné zvážit eskalaci upozornění na DHCP snooping, protože některé druhy zneužití vyžadují další šetření.

DHCP snooping zahodí následující provoz v síti:

- DHCP snooping zahodí DHCP zprávy z DHCP serveru, který není důvěryhodný. Důvěryhodné DHCP servery jsou identifikovány konfigurací stavu důvěryhodnosti DHCP snoopingu přepínače. Zprávy DHCP serveru mohou probíhat přes přepínače, které mají důvěryhodný stav DHCP snoopingu. Zprávy DHCP serveru budou zahozeny, pokud procházejí přes port, který není důvěryhodný.
- Zprávy DHCP, u kterých se zdrojový MAC a hardwarový MAC integrovaného klienta neshodují, budou také zahozeny, ačkoli tuto ochranu lze zrušit – špatně napsaná implementace IP dodavatele může způsobit, že k tomu dojde ve větší frekvenci, přičemž nejběžnějším scénářem je DHCP požadavek na jedno rozhraní, které se předává přes jiné rozhraní na stejném zařízení.
- DHCP snooping také zahodí zprávy, které uvolňují pronájem nebo odmítají nabídku, pokud je zpráva o uvolnění nebo odmítnutí přijata na jiném přepínacím portu, než je port, na kterém se konala původní DHCP konverzace. To brání třetí straně ukončit pronájem nebo odmítnout DHCP nabídku jménem skutečného DHCP klienta.

4.2 Prevence a obrana proti útokům na STP

4.2.1 Root Guard

Root Guard omezuje porty přepínačů, z nichž lze vyjednat root bridge. Pokud port „root-enabled“ přijme BPDU, které jsou nadřazené těm, které odesílá aktuální kořenový most, pak se tento port přesune do stavu „root-inconsistent“ a přes tento port se už nepřeposílá žádný datový provoz. Root guard je nejčastěji nasazen na porty, které se připojují k přepínačům, u nichž se neočekává převzetí root bridge.

4.2.2 BPDU Guard

BPDU Guard se používá k ochraně sítě před problémy, které mohou být způsobeny přijetím BPDU na přístupových portech. Toto jsou porty, které by neměly přijímat žádné BDPUs. Ochrana BPDU guard je nejčastěji nasazen na porty, ke kterým mají přístup uživatelé, aby se zabránilo připojení útočníka.

4.2.3 PortFast

PortFast může být použit na portech přepínačů nebo trunků, které jsou připojeny k jediné pracovní stanici, přepínači nebo serveru, aby se tato zařízení mohla připojit k síti okamžitě, místo čekání na přechod portu ze stavu listening a learning do stavu forwarding.

Když se přepínač zapne nebo když je zařízení připojeno k portu, port přejde do stavu listening. Když vyprší „forward delay timer“ (časovač zpoždění), port přejde do stavu learning. Když vyprší „forward delay timer“ podruhé, port se přepne do stavu forwarding nebo blocking.

PortFast se dá použít k připojení jedné koncové stanice nebo přepínacího portu k přepínacímu portu. Pokud povolíte PortFast na portu, který je připojen k jinému L2 zařízení, například k přepínači, mohou vzniknout síťové smyčky.

4.3 Ochrana protokolu ARP

Metoda zabezpečení portu může zabránit útokům typu MAC flooding. Nezabrání však ARP spoofingu. Zabezpečení portu ověřuje „MAC source address“ (zdrojovou adresu MAC) v záhlaví rámce, ale ARP rámce obsahují další „MAC source field“ (zdrojové pole MAC) v „data payload“ (datový obsah) a hostitel používá toto pole k naplnění své ARP cache. Některé metody, jak zabránit ARP spoofingu, jsou uvedeny níže:

- **Statické záznamy ARP** – jednou z doporučených akcí je použití statických záznamů ARP v ARP cache. Statické záznamy ARP jsou trvalé, tedy neměnné. Tato metoda je však nepraktická. Rovněž neumožňuje použití protokolu DHCP, protože statická IP adresa musí být použita pro všechny hostitele v síti.
- **Dynamic ARP inspection** – tato prevence útoku ARP spoofing je podobná metodě DHCP snooping. Používá důvěryhodné a nedůvěryhodné porty. ARP odpovědi jsou povoleny do rozhraní přepínače pouze na důvěryhodných portech.

Pokud na přepínač na nedůvěryhodném portu přijde odpověď ARP, porovná se obsah paketu odpovědí ARP s vazebnou tabulkou DHCP, aby se ověřila přesnost paketu. Pokud odpověď ARP není platná, odpověď ARP se zruší a port je blokován.

- **Packet filtering** – filtry paketů kontrolují pakety při jejich přenosu v síti. Filtry paketů jsou užitečné v prevenci ARP spoofingu, protože jsou schopny filtrovat a blokovat pakety s konfliktními informacemi o zdrojové adrese (pakety zvnějšku sítě, které zobrazují zdrojové adresy zevnitř sítě a naopak).
- **Blokování trust relationships** – organizace by měly vyvíjet protokoly, které se spoléhají na „trust relationships“ (práva uživatelů jedné domény jsou automaticky sdílena s dalšími) co nejméně. Trust relationships se při ověřování spoléhají pouze na adresy IP, což útočníkům výrazně usnadňuje provádění útoků typu spoofing ARP, pokud jsou na místě.
- **Systém detekce ARP spoofingu** – existuje mnoho programů, které pomáhají detekovat útoky ARP spoofingu. Tyto programy fungují na principu kontroly a certifikace dat před jejich přenosem a blokováním dat, která se zdají být podvržena. Tyto systémy jsou však náchylné k hlášení „false positive“ (falešný poplach).

4.4 Ochrana proti CAM table overflow

4.4.1 Port Security

Přepínače Cisco umožňují řídit, jak port přepínače ukládá MAC adresy korespondující s určitým rozhraním. Hlavním použitím příkazu „port security“ je nastavení limitu na maximální počet souběžných MAC adres, které lze přiřadit jednotlivým portům přepínače.

Pokud útočník začne generovat velké množství MAC adres a podvrhovat je přepínači, je výchozí akcí Port Security vypnutí rozhraní přepínače. Přesto je možné přepínač nakonfigurovat tak, aby zahodil všechny budoucí rámce přijaté z falešných MAC adres.

4.5 Ochrana VTP

Doména VTP může být zabezpečena zabudovaným heslem, které je nakonfigurováno na všech přepínačích ve VTP doméně. Hesla jsou použita k autentizaci VTP zpráv. Je ovšem nutno poznamenat, že VTP heslo nebude zobrazeno v konfiguračním souboru přepínače (je uloženo ve VLAN databázi). Heslo je taktéž téměř nemožné považovat za bezpečné, protože může být zobrazeno v nezašifrovaném formátu pomocí příkazů „show vtp status“ a „show vtp password“.

4.6 Ochrana proti CDP spoofingu

4.6.1 Zablokování CDP

Pokud se uvažuje o deaktivaci CDP z bezpečnostních důvodů, je nutno zvážit deaktivaci na celém směrovači, nikoli jen na některých rozhraních. Pokud je CDP zakázán na jednom rozhraní, zabrání se pouze ve čtení CDP zpráv (tzv. CDP advertisements), ale tabulka CDP bude stále existovat a bude snadno dostupná prostřednictvím SNMP nebo Telnet. Sondování bude tedy stále možné.

Bezpečnostní riziko může hrozit ze dvou bodů. Útok lze spustit zevnitř sítě nebo z přímo připojené sítě. Je tudíž jasné, že CDP musí být deaktivováno na jakémkoli směrovači, který se připojuje k externím sítím, a především na směrovači, který se připojuje k internetu. Útoky zevnitř sítě jsou zahájeny uživateli fyzicky připojenými k síti s předpokladem, že se jedná o legitimní uživatele. Je těžké odhalit útočníka ve skupině uživatelů, z nichž všichni jsou chápáni jako důvěryhodní. Škodlivost útoku pak předčí užitečnost CDP. Zablokování, nebo užívání CDP v takové situaci záleží na tom, do jaké míry jsou uživatelé s přístupem k síti důvěryhodní.

5 Provedení jednotlivých útoků

V následující kapitole se nachází shrnutí základních útoků na linkové vrstvě, které nejlépe vystihují zranitelnosti této vrstvy.

5.1 ARP Spoofing

5.1.1 Popis útoku

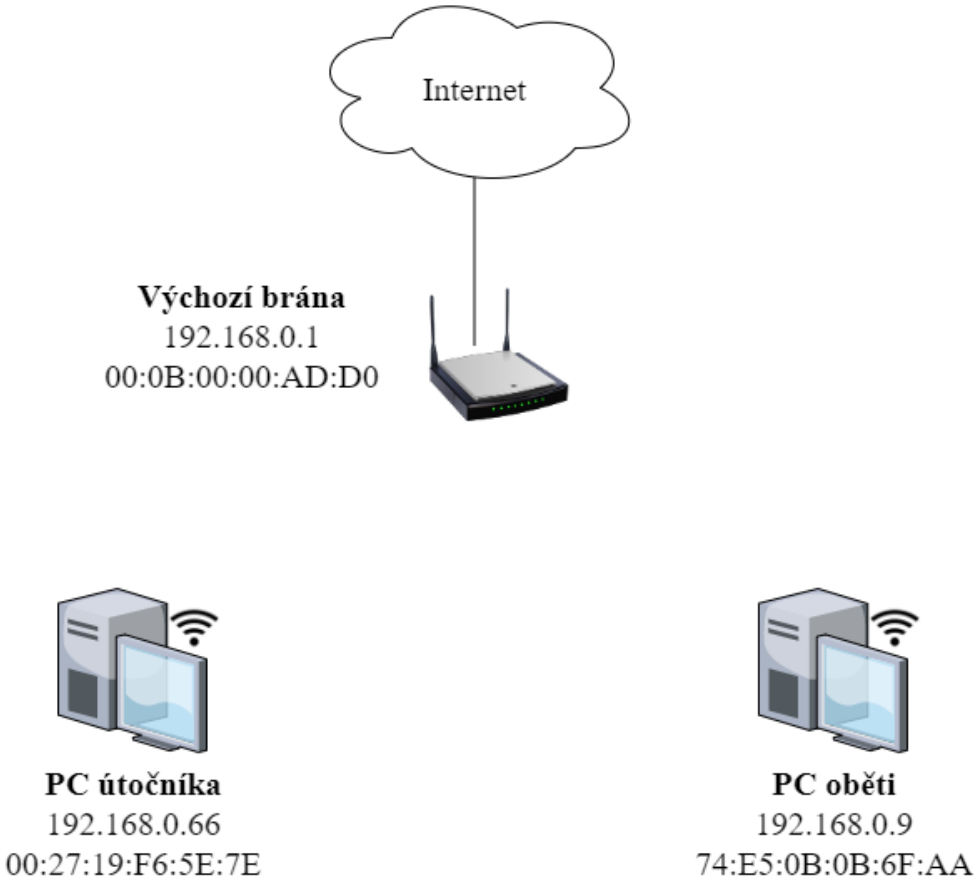
Útočník může zneužít protokolu ARP tím, že odpoví na požadavek ARP (např. od směrovače, který potřebuje zjistit MAC adresu počítače, který se chce dostat na určitou webovou stránku). Útočník se tedy vydává za počítač, jehož provoz chce „odposlouchávat“. Po spojení MAC adresy útočníka s autentickou IP adresou oběti začne útočník přijímat veškerá data, která jsou určena pro tuto legitimní IP adresu. Nyní může útočník zahájit útok typu MITM (tedy začít zachytávat síťový provoz se všemi citlivými uživatelskými daty).

Útočník může také vysílat tzv „Gratuitous ARP“ zprávu s IP adresou výchozí brány. „Gratuitous ARP“ je broadcastový paket používaný síťovými zařízeními k oznámení jakékoli změny jejich IP adresy nebo MAC adresy. Odesláním „Gratuitous ARP“ s IP adresou výchozí brány může útočník fingovat výchozí bránu a zachytit veškerý síťový provoz pohybující se mimo lokální síť.

5.1.2 Použité nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **PC oběti (Win 10)**
- **Síťové karty** umožňující připojení k bezdrátové síti WiFi
- **Bezdrátový směrovač** umožňující přístup k internetu
- **Ettercap (0.8.3)** – nástroj užitečný nejen k provedení útoku ARP spoofing, ale i mnoho dalších. Ettercap se používá především pro útoky typu MITM. Software podporuje různé distribuce Linuxu i Mac OS X. Instalace na systému Windows je možná, ale vyžaduje přídavné konfigurace. Útoky jako „sniffing“, ARP spoofing a shromažďování hesel jsou v tomto nástroji automatizovány. Ettercap může manipulovat se zachycenými daty a útočit i na sítě, které jsou zabezpečeny pomocí SSH nebo SSL. Program je oficiálně nabízen jako bezpečnostní software a používá se při testování zranitelností
- **Wireshark** pro odchycení podvržených ARP odpovědí (gratuitous ARP)

5.1.3 Topologie sítě



Obr. 5.1: ARP Spoofing – Topologie sítě

5.1.4 Provedení útoku

Útok ARP spoofing je proveden následovně:

- před započetím samotného útoku je třeba mít správně nakonfigurovaná zařízení v síti (statický nebo dynamický protokol IPv4 na obou PC) a dále ověřit konektivitu všech zařízení, se kterými se bude pracovat (např. pomocí příkazu ping). Také je možno vypsat ARP cache obou PC (pomocí příkazu „arp“ pro Kali Linux a „arp -a“ pro Windows).

```
root@kaliLinux:~# arp
Adresa                   HWtyp   HWadresa           Příz. Maska             Rozhr
192.168.0.1              ether   00:0b:00:00:ad:d0   C                       eth0
192.168.0.9              ether   74:e5:0b:0b:6f:aa   C                       eth0
```

Obr. 5.2: ARP Spoofing – ARP cache PC útočníka

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.0.9 --- 0xf
  Internet Address      Physical Address      Type
  192.168.0.1           00-0b-00-00-ad-d0     dynamic
  192.168.0.66          00-27-19-f6-5e-7e     dynamic
```

Obr. 5.3: ARP Spoofing – ARP cache PC oběti

- nyní je možno začít s útokem. Po spuštění grafického rozhraní nástroje Ettercap je možné provést oskenování a výpis všech zařízení v lokální síti (tzn. Ettercap vypíše IP adresy a MAC adresy všech zařízení v lokální síti). Poté je nutné přidat PC oběti jako „Target 1“ a výchozí bránu jako „Target 2“.

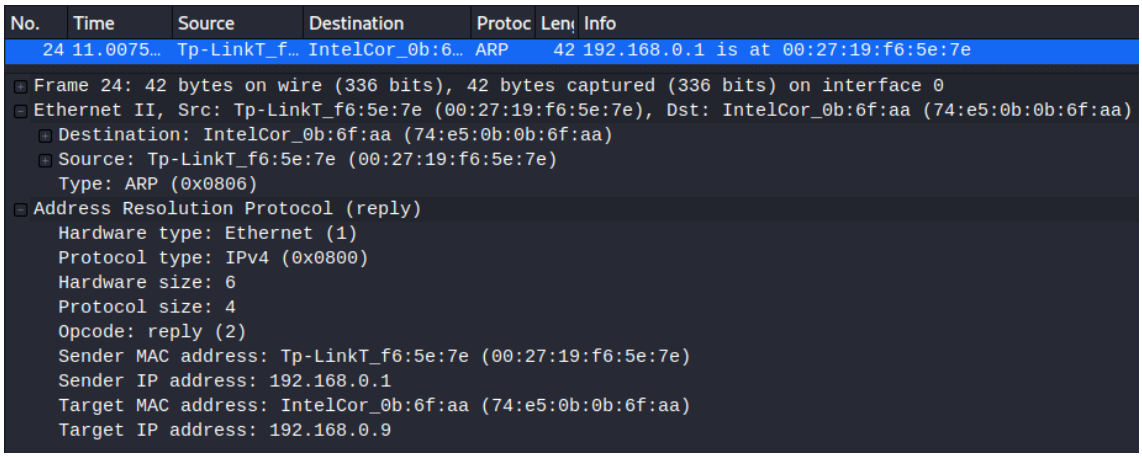
IP Address	MAC Address	Description
192.168.0.1	00:0B:00:00:AD:D0	
192.168.0.5	00:26:C6:51:33:EC	
192.168.0.8	E4:E0:C5:80:F9:97	
192.168.0.9	00:21:CC:67:BF:AF	
192.168.0.15	94:3B:B1:55:C6:D6	
192.168.0.55	04:95:E6:45:BF:70	
192.168.0.56	04:95:E6:23:E9:D0	
192.168.0.61	00:D8:61:14:69:37	

Obr. 5.4: ARP Spoofing – Výpis seznamu zařízení v síti

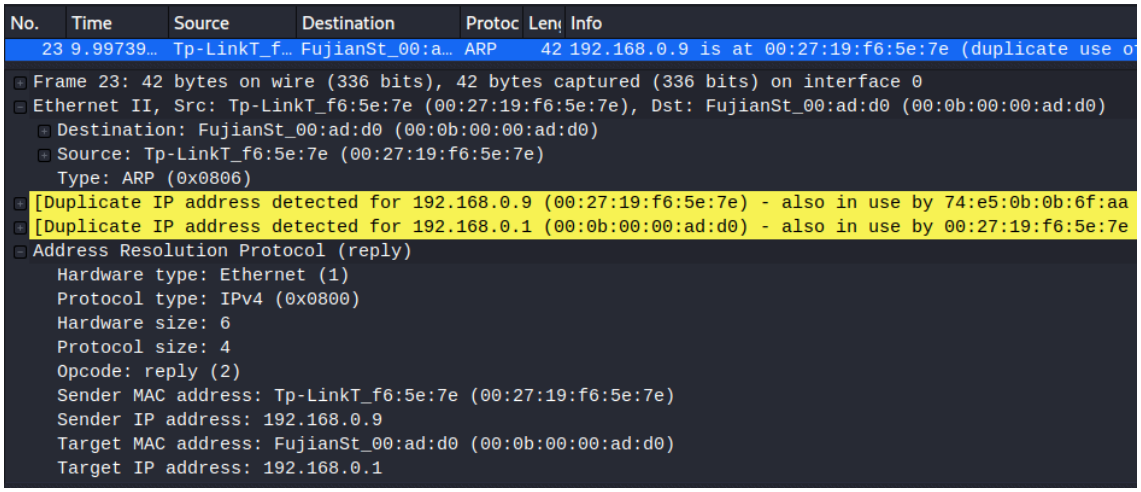
- následovně se útočník pomocí „MITM menu –> ARP poisoning…“ vydává jak za PC oběti (donutí směrovač veškerý provoz určený PC oběti posílat skrze PC útočníka), tak za směrovač (to samé, jen naopak) a je tedy schopen odposlouchávat komunikaci mezi útočníkem a směrovačem (MITM útok), protože byly změněny záznamy v ARP cache jak PC oběti, tak směrovače.

```
Interface: 192.168.0.9 --- 0xf
  Internet Address      Physical Address      Type
  192.168.0.1           00-27-19-f6-5e-7e     dynamic
  192.168.0.66          00-27-19-f6-5e-7e     dynamic
```

Obr. 5.5: ARP Spoofing – ARP cache PC oběti v průběhu útoku

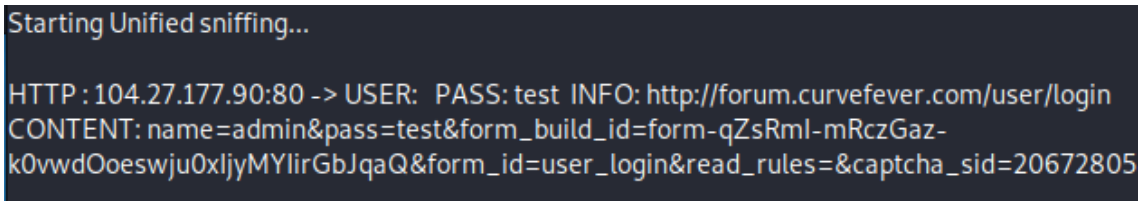


Obr. 5.6: ARP Spoofing – Falešná ARP odpověď určená PC oběti



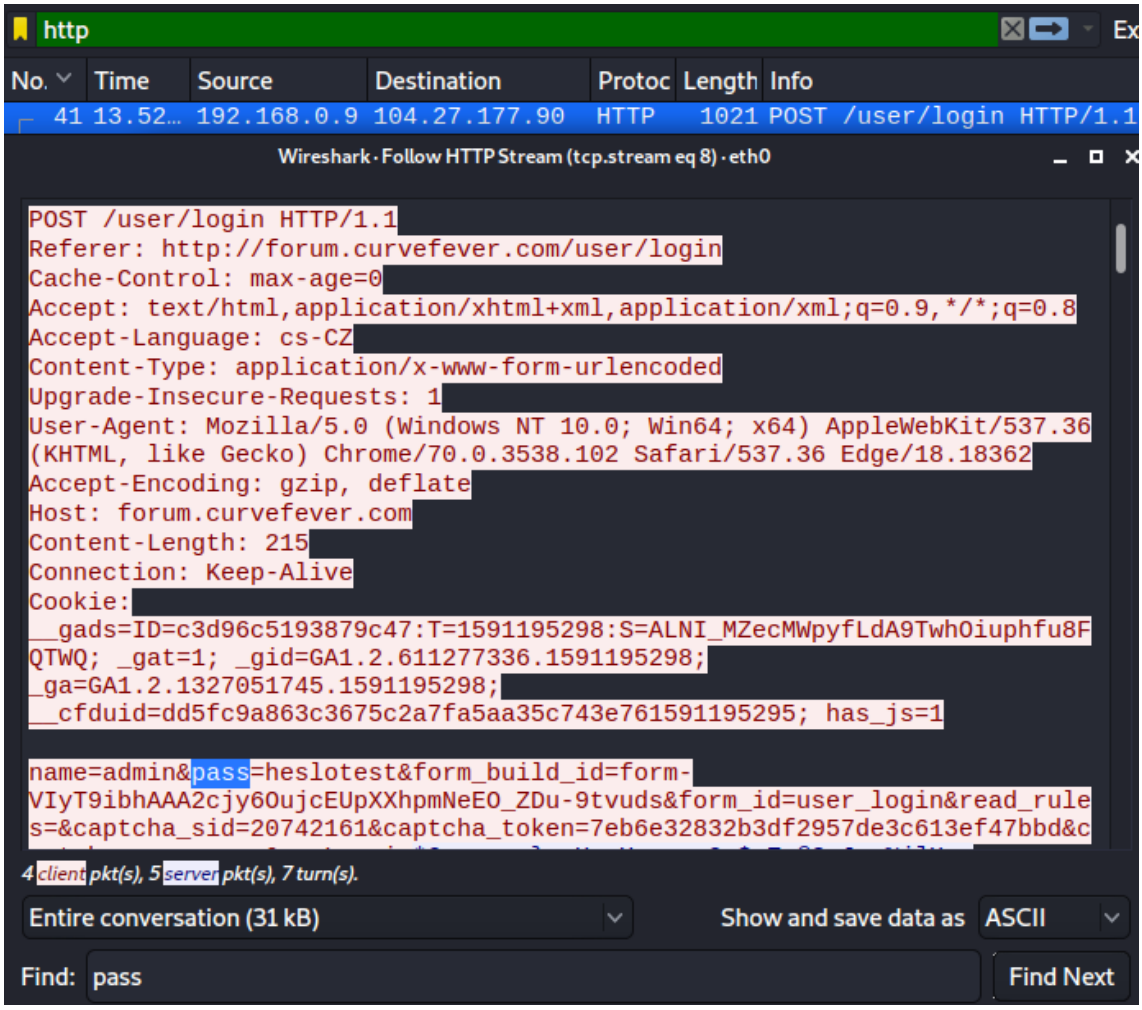
Obr. 5.7: ARP Spoofing – Falešná ARP odpověď určená výchozí bráně

- v nástroji Wireshark lze pozorovat ARP zprávy, které útočník generuje v určitých intervalech a posílá je oběti (Obr. 5.6) a výchozí bráně (Obr. 5.7).
- nástroj Ettercap poté vypisuje všechny důležité informace o aktivitě PC oběti na internetu (např. přihlašovací údaje na nezabezpečené stránce, komunikace přes Telnet, FTP atd.).



Obr. 5.8: ARP Spoofing – Odposlech hesla na nezabezpečené stránce

- heslo se dá také odposlechnout pomocí programu Wireshark. Zádáním „http“ do filtru, poté kliknutím pravým tlačítkem na paket „/user/login“ a dále na „Follow –> HTTP Stream“, kde se dá najít hledané slovo (např. pass).



Obr. 5.9: ARP Spoofing – Odposlech hesla pomocí Wireshark

5.1.5 Detekce útoku a ochranná opatření proti němu

Existuje spousta metod k detekci tohoto útoku, jako například statické záznamy ARP, dynamic ARP inspection, packet filtering, blokování trust relationships a systémy detekce ARP spoofingu. Tyto metody jsou ovšem buď neefektivní nebo náchylné k hlášení falešných poplachů. Útok se dá také detekovat o dost jednodušeji, a to buď vypsáním arp cache (pomocí příkazu „arp -a“ pro Windows a příkazu „arp“ pro Linux), kde uvidíme stejnou MAC adresu pro výchozí bránu a PC útočníka, anebo odposlouchávat ARP zprávy pomocí nástroje Wireshark. Nejúčinnější zaručenou ochranou je ovšem používání zabezpečených protokolů (SSH, HTTPS atd.).

5.1.6 Shrnutí

Případ útoku ARP spoofing může kriticky ohrozit uživatele, na kterého je útok směřován, protože je všechen jeho provoz přeposílán přes útočníka, který z nezabezpečeného provozu může vyčíst mnohé soukromé údaje (jako jsou přihlašovací jména, hesla atd.). Tento útok je nejjednodušší provést na bezplatných sítích WiFi, proto je nutné na takových sítích nikdy nepoužívat nezabezpečené protokoly (či

v nejlepším případě nevyužívat bezplatných WiFi vůbec, protože ARP spoofing je jen jedním z mnoha útoků, které mohou kohokoliv na takové síti postihnout). Dále je tu možnost útoku na firemní síť, což už se provádí hůře, protože k jeho realizaci je nutný fyzický přístup k síti.

5.2 Podvržený DHCP server

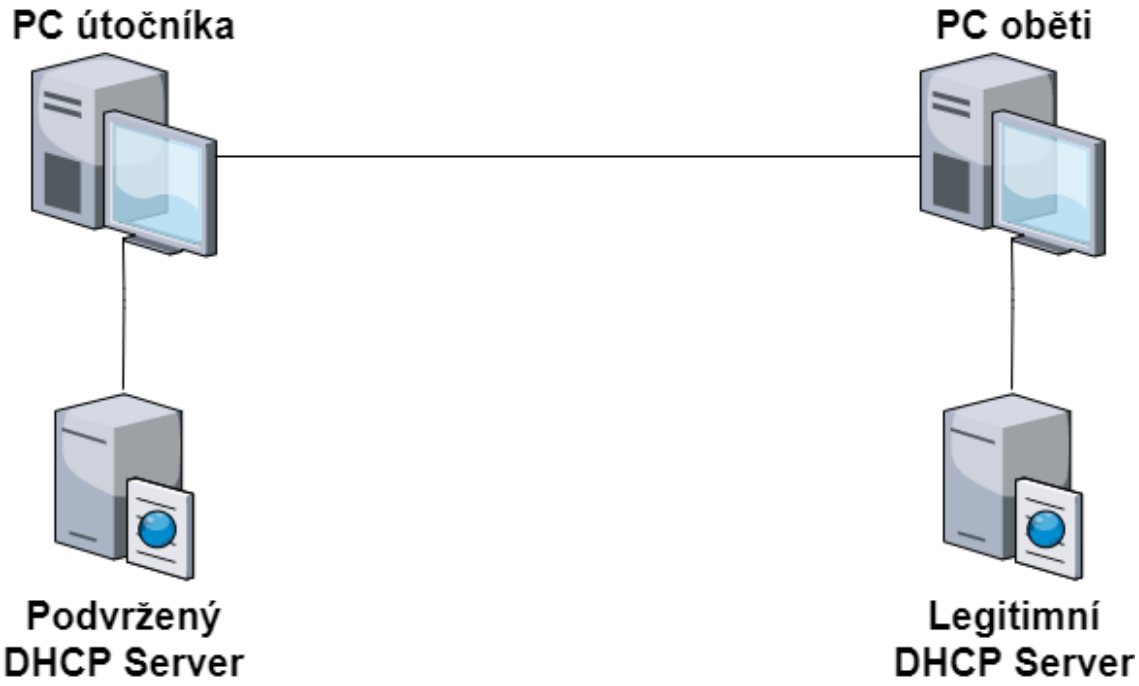
5.2.1 Popis útoku

V následující kapitole bude znázorněn příklad útoku podvrženého DHCP serveru. Útočník (kali Linux) vytvoří podvržený DHCP server pomocí programu Yersinia, který způsobí, že po vypršení „lease time“ u IP adresy PC oběti (Windows 10 x86) je podvržený DHCP server vnucen PC oběti a bude se vydávat za jeho legitimní DHCP server.

5.2.2 Použité nástroje

- **Oracle VM VirtualBox** je open-source software pro virtualizaci počítačové architektury x86. Funguje jako hypervisor a vytváří virtuální počítač VM, ve kterém může uživatel provozovat jiný operační systém. Operační systém, ve kterém běží VirtualBox, se nazývá „hostitelský“ operační systém.
- **Wireshark** je open-source software pro analýzu paketů. Používá se pro řešení problémů v síti, analýzu softwaru, vývoj softwaru a komunikačních protokolů a pro vzdělávání.
- **Yersinia s**louží k realizaci různých útoků proveditelných na linkové vrstvě, které využívají slabiny protokolů na této vrstvě. Pentester (člověk, který testuje bezpečnost pomocí útoků na síť) díky tomuto nástroji může identifikovat zranitelnosti v síti. Během penetračních testů se Yersinia používá k iniciaci útoků na různá zařízení a protokoly linkové vrstvy, jako jsou přepínače, DHCP servery atd. V současné době Yersinia podporuje následující protokoly: STP, CDP, DTP, DHCP, VTP, IEEE 802.1Q a IEEE 802.1X atd.
- **RogueChecker** – nástroj Microsoft Rogue DHCP Checker umožňuje rychle a snadno zkontrolovat, zda v síti existují další servery DHCP a tudíž je užitečný při detekci podvržených DHCP serverů.

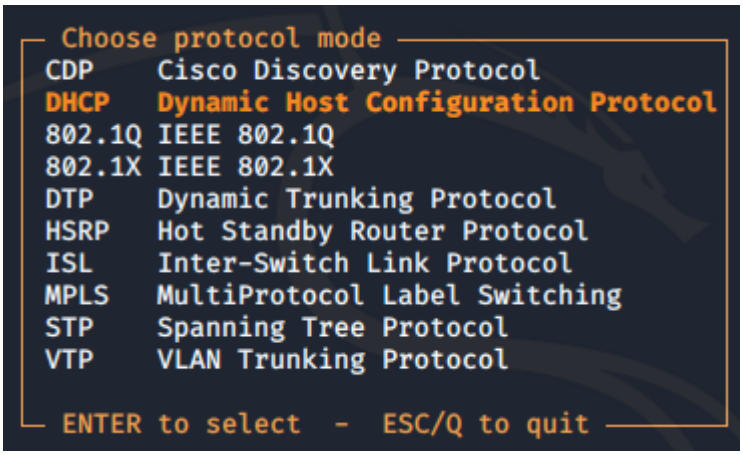
5.2.3 Topologie sítě



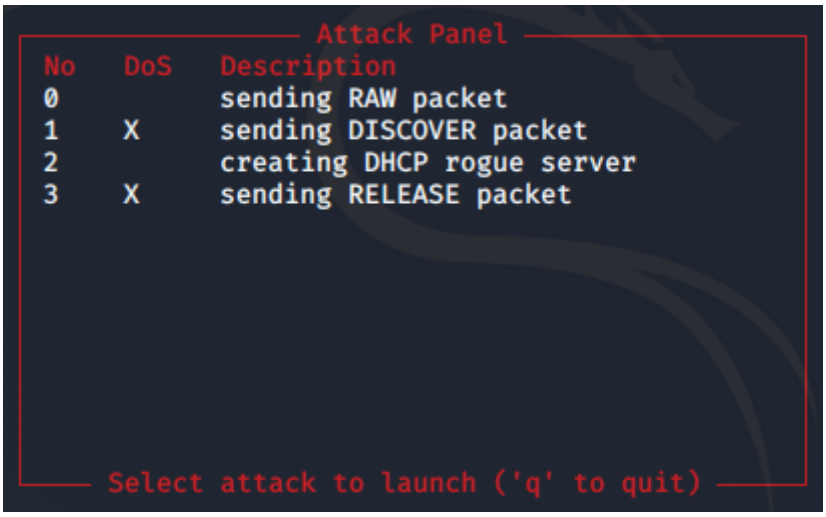
Obr. 5.10: DHCP Spoofing – Topologie sítě

5.2.4 Provedení útoku

Útočník do sítě podvrhne svůj DHCP server následujícím způsobem:



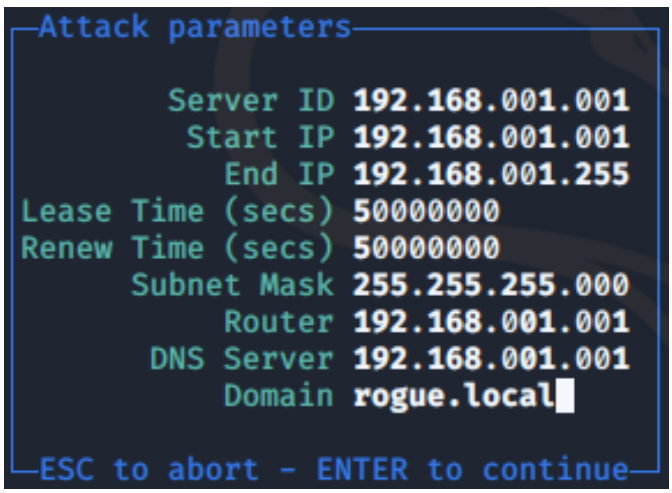
Obr. 5.11: DHCP Spoofing – Rozhraní nástroje Yersinia



Obr. 5.12: DHCP Spoofing – Možnosti útoků na DHCP

Pomocí nástroje Yersinia se dají nastavit všechny parametry podvrženého DHCP serveru podle vlastní potřeby:

- **Server IP** – adresa podvrženého DHCP serveru (např. 192.168.1.1).
- **Start IP** – počáteční IP adresa z rozsahu DHCP serveru (např. 192.168.1.2).
- **End IP** – koncový rozsah IP adres poskytovaných DHCP serverem (např. 192.168.1.254).
- **Lease Time (secs)** – čas trvání pronájmu IP adresy konkrétnímu zařízení.
- **Renew Time (secs)** – čas, po kterém je nutno obnovit pronájem IP adresy.
- **Subnet mask** – maska sítě (např. 255.255.255.0).
- **Router** – IP adresa falešného směrovače (např. 192.168.1.66).
- **DNS Server** – IP adresa falešného DNS serveru (např. 192.168.1.66).
- **The Domain** – doménové jméno lokální sítě (např. rouge.local).



Obr. 5.13: DHCP Spoofing – Konfigurace podvrženého DHCP serveru

Poté už jen stačí potvrdit konfiguraci podvrženého DHCP serveru a započít útok (stačí jen počkat na připojení nových klientů k síti nebo počkat na vypršení „lease time“ stávajících klientů). Následkem je MITM útok a tím pádem možnost odposlouchávat vzájemný provoz zařízení v lokální síti nebo jejich komunikaci přes internet.

SIP	DIP	MessageType	Iface	Last seen
192.168.56.102	192.168.56.100	REQUEST	eth0	21 Dec 22:06:22
192.168.56.100	192.168.56.102	ACK	eth0	21 Dec 22:06:22
192.168.56.102	192.168.56.100	REQUEST	eth0	21 Dec 22:16:22
192.168.56.100	192.168.56.102	ACK	eth0	21 Dec 22:16:22
0.0.0.0	255.255.255.255	DISCOVER	eth0	21 Dec 22:25:16
192.168.56.100	255.255.255.255	OFFER	eth0	21 Dec 22:25:16
0.0.0.0	255.255.255.255	REQUEST	eth0	21 Dec 22:25:16
192.168.56.100	255.255.255.255	ACK	eth0	21 Dec 22:25:16
192.168.1.1	255.255.255.255	ACK	eth0	21 Dec 22:25:16

Obr. 5.14: DHCP Spoofing – Handshake PC oběti s podvrženým DHCP serverem

5.2.5 Detekce útoku a ochranná opatření proti němu

Účinnou obranou proti podvrženému DHCP serveru je DHCP Snooping. Je to bezpečnostní technologie linkové vrstvy začleněná do operačního systému kompatibilního přepínače, který zahazuje nelegitimní DHCP provoz. Funkce DHCP Snooping provádí následující činnosti:

- ověřuje zprávy DHCP z nedůvěryhodných zdrojů a filtruje neplatné zprávy.
- vytváří a udržuje DHCP Snooping databázi, která obsahuje informace o nedůvěryhodných zařízeních s pronajatými IP adresami. Tuto databázi následovně využívá k identifikaci DHCP požadavků od nedůvěryhodných zařízení.

Discovered DHCP Servers in the subnet

	Valid DHCP Server	Server IP	Offered Client IP	Gateway Address	Response Time
	☑	192.168.56.100	192.168.56.105	0.0.0.0	0
❗	☐	192.168.1.1	192.168.1.1	192.168.1.1	39

Obr. 5.15: DHCP Spoofing – RougueChecker; detekce podvrženého DHCP serveru

bootp — Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
20	165.521698	192.168.1.1	255.255.255.255	DHCP	335	DHCP ACK
23	223.352648	192.168.56.104	192.168.56.100	DHCP	342	DHCP Release
44	227.464934	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover
45	227.465237	192.168.56.100	255.255.255.255	DHCP	590	DHCP Offer
46	227.465469	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request
47	227.467622	192.168.56.100	255.255.255.255	DHCP	590	DHCP ACK

Obr. 5.16: DHCP Spoofing – Wireshark; detekce podvrženého DHCP serveru

5.2.6 Shrnutí

Případ útoku podvrženého DHCP serveru může kriticky ochromit síť, která nemá

dostatečné prostředky na detekci útoku tohoto typu útoku a účinnou obranu proti němu. Menší firmy mohou být tímto útokem zasaženy celkem jednoduše pokud používají staré přepínače a směrovače. Ve velkých společnostech je ovšem tento útok skoro nemožný z důvodu novějších technologií a větší obezřetnosti v oblasti zabezpečení sítě.

5.3 ICMP Redirect

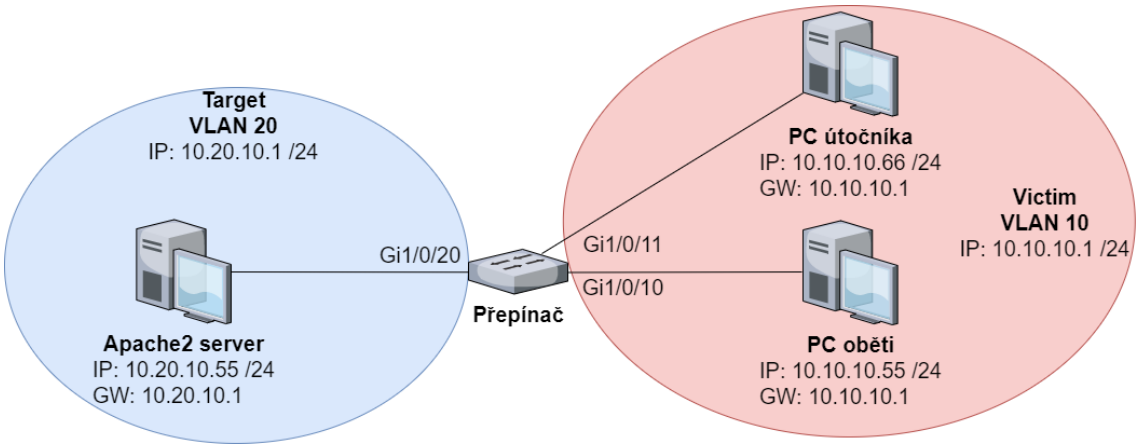
5.3.1 Popis útoku

Případ útoku ICMP redirect se dá velice jednoduše zneužít k MITM útoku. Útočník může komukoliv podvrhnout paket ICMP redirect a tím pádem přes sebe směrovat veškerý provoz, který oběť posílá do internetu, nebo do lokální sítě. Protože je ICMP redirect v systémech Linux i Windows ve výchozím nastavení povolen a málo kdo o něm ví, je možné ho jednoduše zneužít.

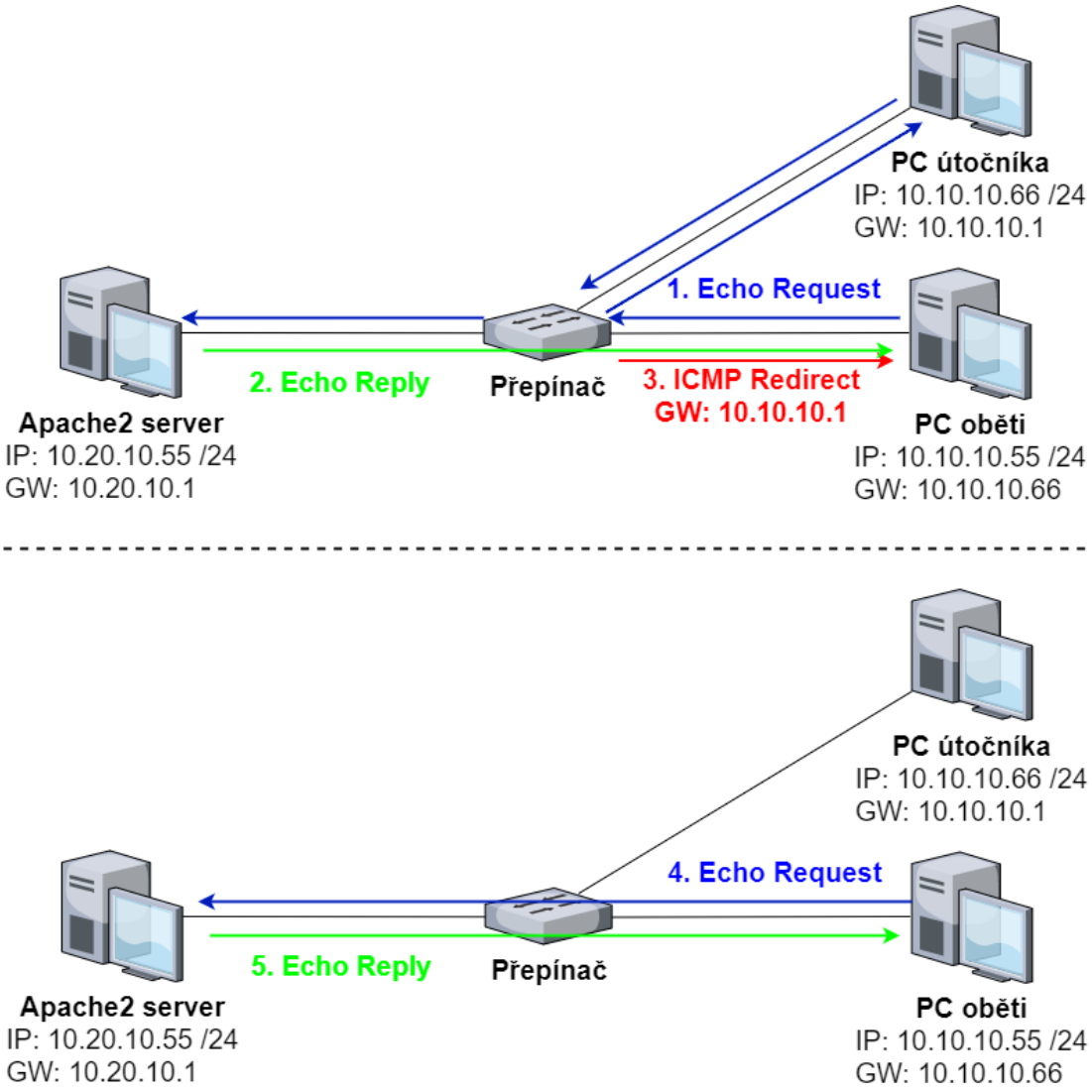
5.3.2 Použité nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **PC oběti (Win10)**
- **PC s web serverem Apache2 (Linux Mint)** na který se bude obět přihlašovat a útočník heslo bude schopen odposlechnout přihlašovací údaje.
- **Přepínač (Cisco Catalyst 3650X)**
- **Wireshark**
- **Hping3** užitý ke generování paketů ICMP redirect.

5.3.3 Topologie sítě



Obr. 5.17: ICMP Redirect – Topologie sítě



Obr. 5.18: ICMP Redirect – Ukázka funkčnosti ICMP redirect

5.3.4 Provedení útoku

Pro provedení útoku bylo nutné povolit funkci přesměrování v systému Kali Linux.

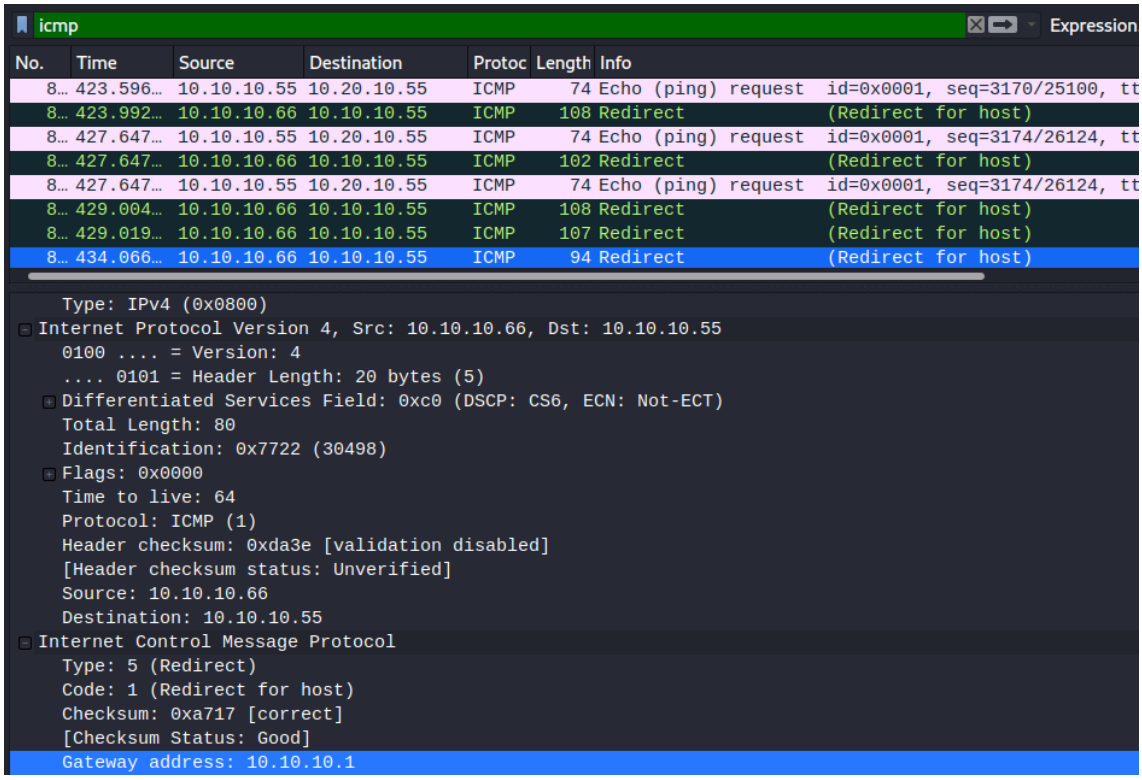
```
root@kaliLinux:~# sysctl net.ipv4.conf.all.forwarding
net.ipv4.conf.all.forwarding = 0
root@kaliLinux:~# sysctl net.ipv4.conf.all.forwarding=1
net.ipv4.conf.all.forwarding = 1
```

Obr. 5.19: ICMP Redirect – Povolení přesměrování

Před započetím samotného útoku lze vyzkoušet funkci ICMP redirect ke zjištění, zda funguje. Pro tento účel byla výchozí brána PC oběti změněna na „10.10.10.66“, tedy na IP adresu PC útočníka. Posléze byl na PC oběti zadán příkaz „ping 10.20.10.55 -t“. Echo request byl poslán následující cestou:

PC oběti –> Přepínač –> PC útočníka –> Přepínač –> Apache2 server. Na základě toho

přepínač vygeneroval ICMP redirect pomocí kterého sdělil PC oběti skutečnost, že existuje výhodnější cesta přes výchozí bránu „10.10.10.1“, poslal redirect PC oběti a další pakety typu Echo request už tím pádem směřovaly cestou: PC oběti –> Přepínač –> Apache2 server.



Obr. 5.20: ICMP Redirect – Wireshark; přesměrování provozu na výhodnější cestu

Samotný útok byl proveden pomocí nástroje „hping3“ (měl by být součástí nástrojů obsažených v OS Kali Linux), který umožňuje vygenerování paketu ICMP redirect a jeho nepřetržité posílání v určitém intervalu, dokud není příkaz přerušen.

```
root@kaliLinux:~# hping3 10.10.10.55 -C 5 -K 1 -a 10.10.10.1 --icmp-gw 10.10.10.66 --icmp
-ipdst 10.20.10.55 --icmp-ipsrc 10.10.10.55
HPING 10.10.10.55 (eth0 10.10.10.55): icmp mode set, 28 headers + 0 data bytes
```

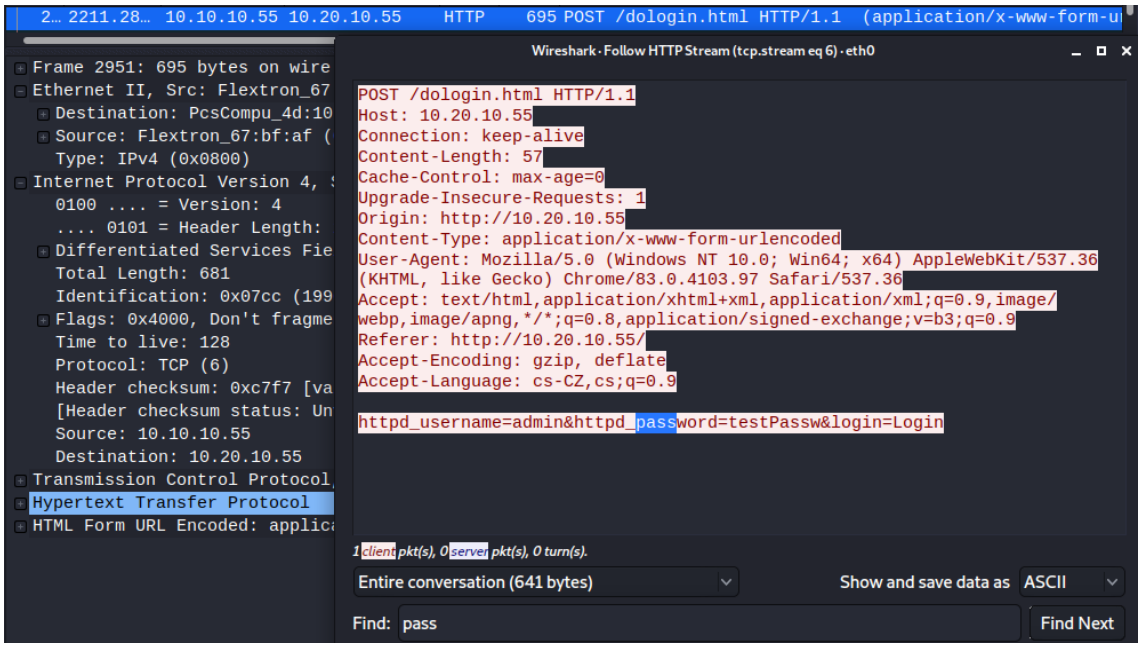
Obr. 5.21: ICMP Redirect – Použití nástroje hping3

Následně byly z PC oběti poslány pakety ICMP Echo směrem k serveru Apache2, které byly za normálních okolností směrovány skrze přepínač. Tento provoz byl po provedení příkazu „hping3“ následně přesměrován na PC útočníka, kde ho bylo možné pozorovat pomocí nástroje Wireshark.

```
2… 2058.65… 10.10.10.1  10.10.10.55  ICMP   70 Redirect            (Redirect for host)
2… 2059.03… 10.10.10.55 10.20.10.55  ICMP   74 Echo (ping) request id=0x0001, seq=6330/47640,
2… 2059.03… 10.10.10.55 10.20.10.55  ICMP   74 Echo (ping) request id=0x0001, seq=6330/47640,
2… 2059.65… 10.10.10.1  10.10.10.55  ICMP   70 Redirect            (Redirect for host)
2… 2060.04… 10.10.10.55 10.20.10.55  ICMP   74 Echo (ping) request id=0x0001, seq=6331/47896,
2… 2060.04… 10.10.10.55 10.20.10.55  ICMP   74 Echo (ping) request id=0x0001, seq=6331/47896,
2… 2060.65… 10.10.10.1  10.10.10.55  ICMP   70 Redirect            (Redirect for host)
2… 2061.06… 10.10.10.55 10.20.10.55  ICMP   74 Echo (ping) request id=0x0001, seq=6332/48152,
2… 2061.06… 10.10.10.55 10.20.10.55  ICMP   74 Echo (ping) request id=0x0001, seq=6332/48152,
```

Obr. 5.22: ICMP Redirect – Sledování provozu určeného serveru Apache2

Dále bylo vyzkoušeno pomocí webového prohlížeče z PC oběti připojení na Apache2 server a vyplnění náhodných přihlašovacích údajů (např. username: admin, password: testPassw). V nástroji Wireshark s filtrem „http“ bylo poté možné na PC útočníka pozorovat paket (kliknutím pravým tlačítkem myši na paket a vybráním volby „Follow –> HTTP Stream“) s přihlašovacími údaji.



Obr. 5.23: ICMP Redirect – Sledování hesla v nástroji Wireshark

5.3.5 Detekce útoku a ochranná opatření proti němu

Jedinou účinnou ochranou je zakázání funkce ICMP redirect (v regedit - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

\EnableICMPRedirect nastavit hodnotu na 0 pro Windows) a pro Linux se dá deaktivovat pomocí příkazů:

```
sysctl net.ipv4.conf.eth0.accept_redirects=0
sysctl net.ipv4.conf.eth0.send_redirects=0
```

5.3.6 Shrnutí

Tento případ útoku může být velice účinný pro ty, kteří neví o jeho existenci. Dá se ovšem zužitkovat pouze v případě, že ten, na koho se útočí není obezřetný a přistupuje na nezabezpečené webové stránky nebo používá komunikaci přes nezabezpečené protokoly jako např. telnet.

5.4 CAM Table Overflow

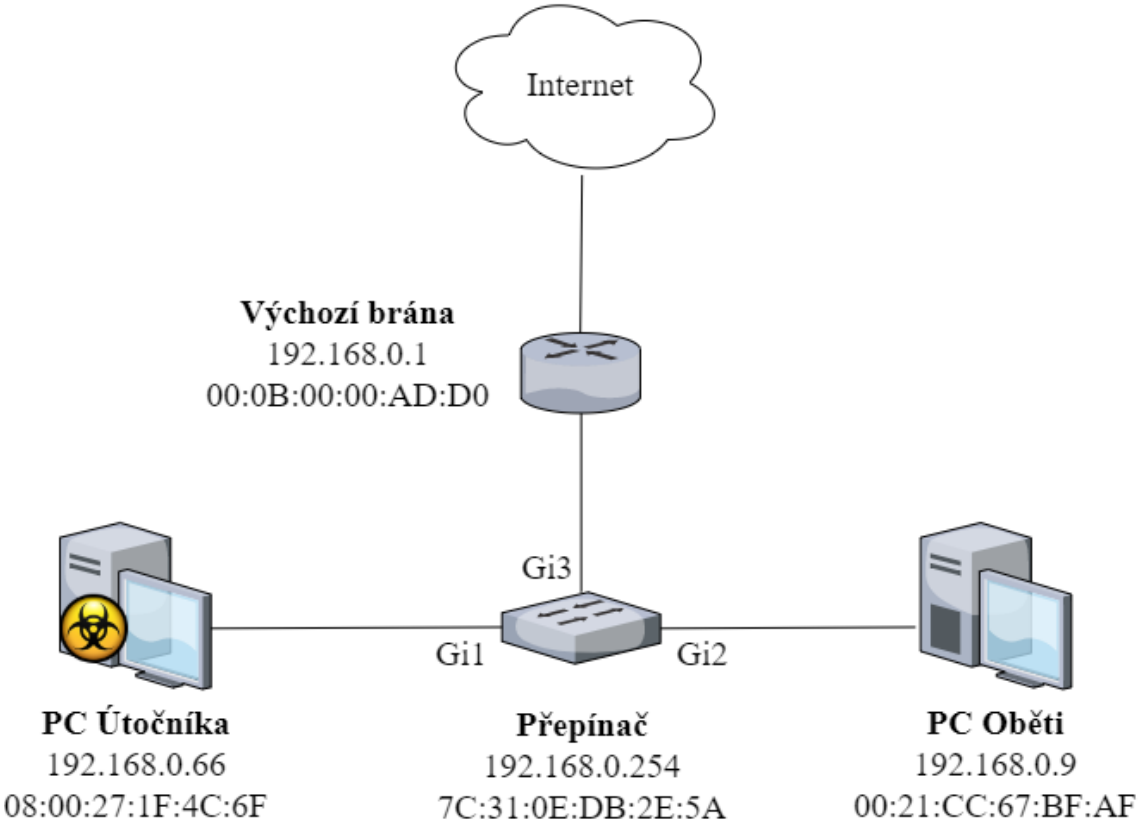
5.4.1 Popis útoku

Při tomto typu útoku je naprosto vyčerpána CAM tabulka a tím pádem je dosaženo DoS útoku. Ovšem, tohle byl výsledek napadení přepínače Cisco SG250 a je jasné, že jiné typy přepínačů by mohly reagovat odlišně (např. by se začaly po vyčerpání CAM tabulky chovat jako hub).

5.4.2 Použité nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **PC oběti (Win 10)**
- **Přepínač (Cisco SG250)**
- **Směrovač** spojující lokální síť s internetem.
- **Dsniff** k provedení samotného útoku (pomocí příkazu „apt-get install dsniff“).
- **PuTTY** ke konfiguraci přepínače pomocí SSH.

5.4.3 Topologie sítě



Obr. 5.24: CAM Table Overflow – Topologie sítě

5.4.4 Provedení útoku

Před započetím samotného útoku je možné vypsat na přepínači CAM tabulku pomocí příkazu „show mac address-table“ a také vypsat maximální množství MAC adres, které je schopna tabulka určitého přepínače zapsat pomocí příkazu „show mac address-table count“.

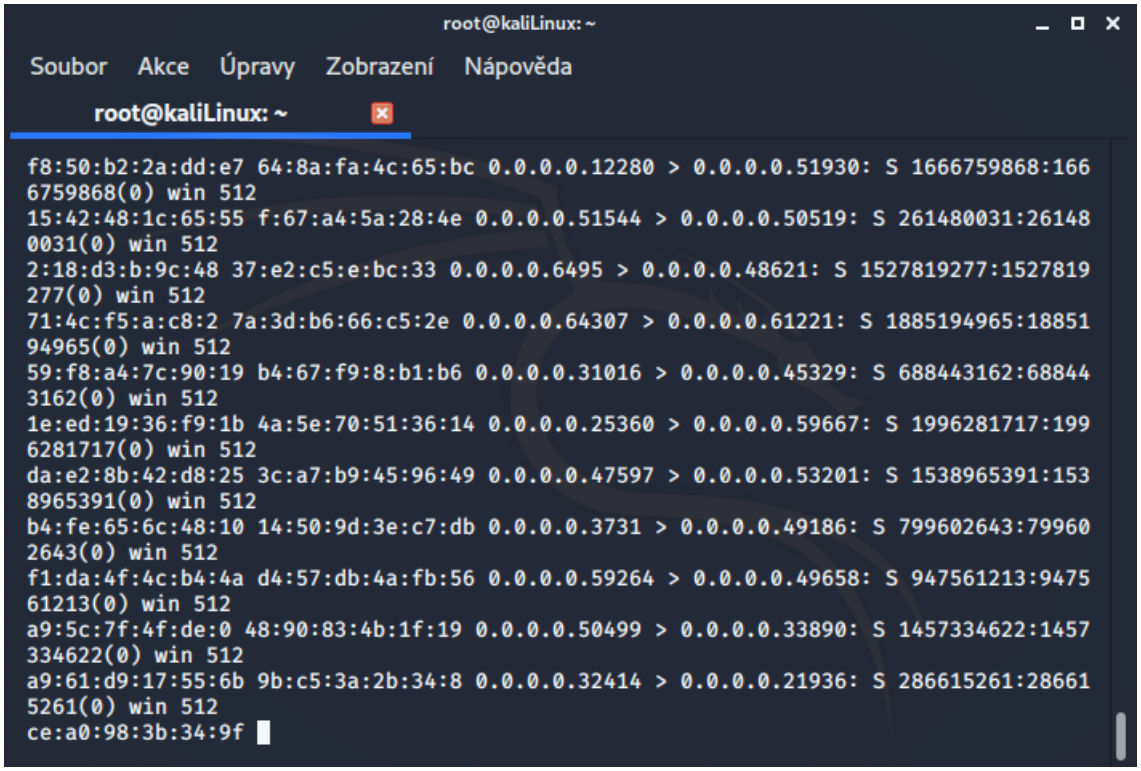
```
Switch#show mac address-table
Flags: I - Internal usage VLAN
Aging time is 300 sec

    Vlan          Mac Address          Port       Type
----------- -------------------- ---------- ----------
     1          00:0b:00:00:ad:d0       gi3      dynamic
     1          00:21:cc:67:bf:af       gi2      dynamic
     1          00:d8:61:14:69:37       gi1      dynamic
     1          08:00:27:1f:4c:6f       gi1      dynamic
     1          7c:31:0e:db:2e:5a         0       self
```

Obr. 5.25: CAM Table Overflow – Výpis CAM tabulky

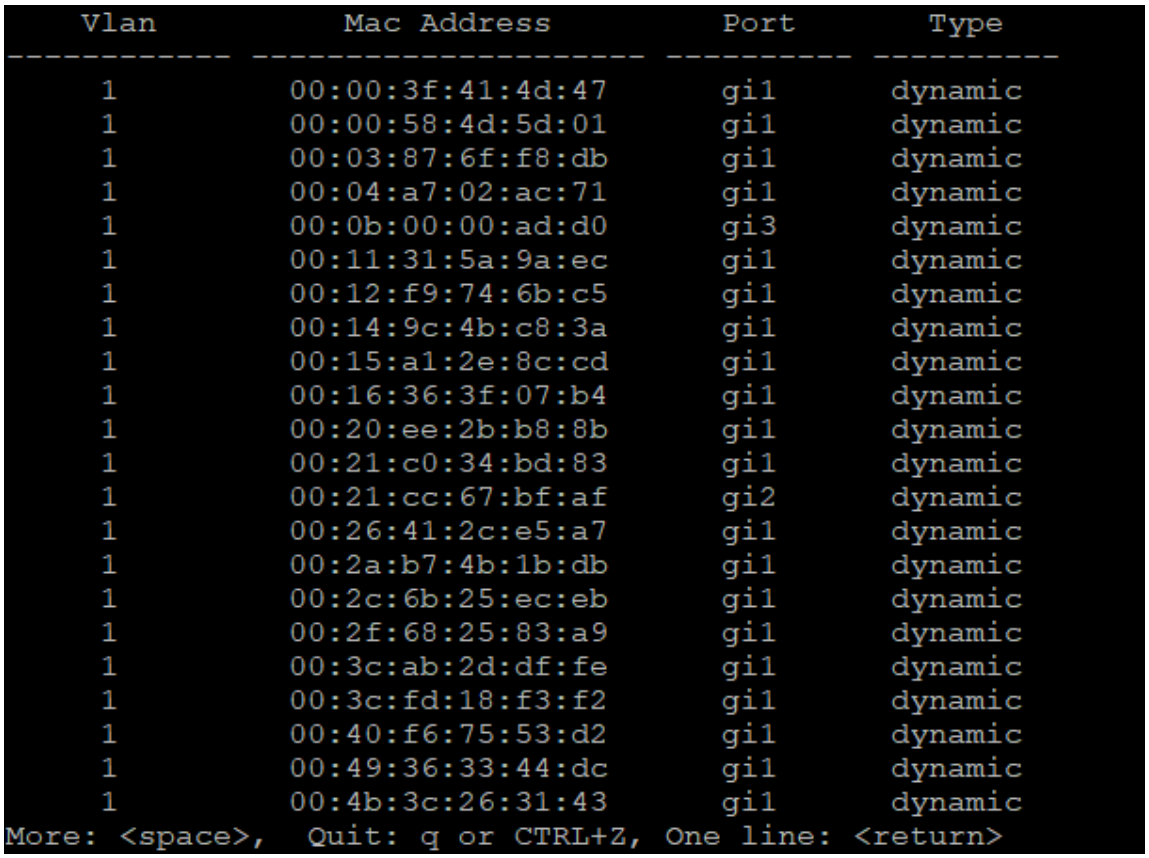
```
Switch#show mac address-table count
Capacity          : 8192
Free              : 8181
Used unicast      : 10
Used multicast    : 1
Used IPv4 hosts   : 0
Used IPv6 hosts   : 0
Secure            : 0
Dynamic unicast   : 9
Static unicast    : 0
Internal          : 1
```

Obr. 5.26: CAM Table Overflow – Výpis maximálního počtu MAC adres

Nyní k samotnému útoku. Stačí jeden příkaz, a to „macof -i eth0“ (v tomto konkrétním případě je rozhraní „eth0“, pokud příkaz nefunguje, dá se rozhraní zjistit např. pomocí příkazu „ifconfig“). Pomocí příkazu „macof“ je možno generovat stovky falešných MAC adres za sekundu, přepínač tedy bude mít během krátkého času přeplněnou svoji CAM tabulku a nakonec budou přepsány i původně uložené adresy z důvodu neustálého podvrhování dalších MAC adres.



Obr. 5.27: CAM Table Overflow – Podvrhování náhodně generovaných MAC adres



Vlan	Mac Address	Port	Type
1	00:00:3f:41:4d:47	gi1	dynamic
1	00:00:58:4d:5d:01	gi1	dynamic
1	00:03:87:6f:f8:db	gi1	dynamic
1	00:04:a7:02:ac:71	gi1	dynamic
1	00:0b:00:00:ad:d0	gi3	dynamic
1	00:11:31:5a:9a:ec	gi1	dynamic
1	00:12:f9:74:6b:c5	gi1	dynamic
1	00:14:9c:4b:c8:3a	gi1	dynamic
1	00:15:a1:2e:8c:cd	gi1	dynamic
1	00:16:36:3f:07:b4	gi1	dynamic
1	00:20:ee:2b:b8:8b	gi1	dynamic
1	00:21:c0:34:bd:83	gi1	dynamic
1	00:21:cc:67:bf:af	gi2	dynamic
1	00:26:41:2c:e5:a7	gi1	dynamic
1	00:2a:b7:4b:1b:db	gi1	dynamic
1	00:2c:6b:25:ec:eb	gi1	dynamic
1	00:2f:68:25:83:a9	gi1	dynamic
1	00:3c:ab:2d:df:fe	gi1	dynamic
1	00:3c:fd:18:f3:f2	gi1	dynamic
1	00:40:f6:75:53:d2	gi1	dynamic
1	00:49:36:33:44:dc	gi1	dynamic
1	00:4b:3c:26:31:43	gi1	dynamic

More: <space>, Quit: q or CTRL+Z, One line: <return>

Obr. 5.28: CAM Table Overflow – CAM tabulka s falešnými MAC adresami

```
C:\Windows\system32>ping vutbr.cz

Pinging vutbr.cz [147.229.2.90] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 147.229.2.90:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Obr. 5.29: CAM Table Overflow – Následek útoku (DoS)

5.4.5 Detekce útoku a ochranná opatření proti němu

Účinnou obranou proti tomuto útoku je nastavení maximálního počtu MAC adres na jedno rozhraní na přepínači pomocí „port security“.

Případ přepínačů Cisco Catalyst - rozhraní je nutné přepnout do access mode pomocí příkazu „switchport mode access“. Poté je nutné zadání příkazů „switchport port-security maximum 5“ a „switchport port-security“. Tímto je počet MAC adres na rozhraní omezen na 5. Při dalším provedení útoku tedy bude možné podvrhnout do

CAM tabulky maximálně 5 MAC adres.

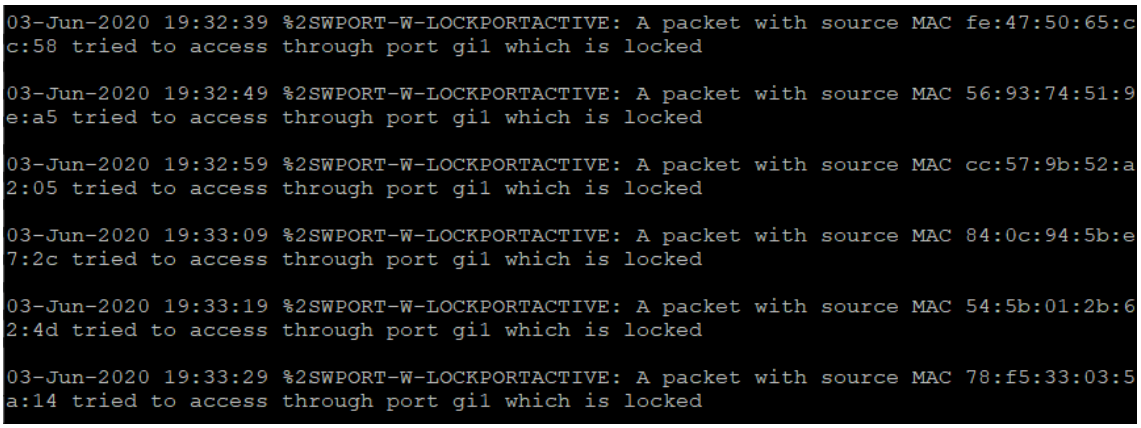
Případ přepínače Cisco SG250 – v konfiguračním terminálu je nutné zadat příkaz „interface gi1“ a poté „port security max 5“, „port security trap 10“ a „port security discard“. Posléze je možné vypsat tabulku zabezpečení portů pomocí příkazu „show ports security“. Tímto nastavením zabezpečení bylo zajištěno, že lze do CAM tabulky k rozhraní Gi1 zapsat maximálně 5 MAC adres, zbytek bude zahozen s upozorněním každých 10 sekund.

```
Switch(config-if)#port security max 5
Switch(config-if)#port security trap 10
Switch(config-if)#port security discard
Switch(config-if)#end
Switch#show ports security

 Port      status      Learning       Action    Maximum    Trap    Frequency
--------- ---------- -------------- ---------- --------- -------- ----------
  gi1     Enabled    Max-Addresses   Discard       5     Enabled      10
  gi2     Disabled       Lock            -         1     Disabled     -
  gi3     Disabled       Lock            -         1     Disabled     -
  gi4     Disabled       Lock            -         1     Disabled     -
  gi5     Disabled       Lock            -         1     Disabled     -
  gi6     Disabled       Lock            -         1     Disabled     -
  gi7     Disabled       Lock            -         1     Disabled     -
  gi8     Disabled       Lock            -         1     Disabled     -
```

Obr. 5.30: CAM Table Overflow – Výpis port security

```
   Vlan          Mac Address          Port        Type
------------ --------------------- ---------- ----------
     1         00:0b:00:00:ad:d0       gi3      dynamic
     1         00:21:cc:67:bf:af       gi2      dynamic
     1         00:26:c6:51:33:ec       gi3      dynamic
     1         00:d8:61:14:69:37       gi1      dynamic
     1         04:95:e6:23:e9:d0       gi3      dynamic
     1         04:95:e6:45:bf:70       gi3      dynamic
     1         10:75:46:52:31:c8       gi1      dynamic
     1         34:e1:f5:6e:a1:da       gi1      dynamic
     1         62:8d:c8:11:e2:75       gi1      dynamic
     1         7c:31:0e:db:2e:5a        0        self
     1         ca:3e:c3:20:4f:0b       gi1      dynamic
     1         e4:e0:c5:80:f9:97       gi3      dynamic
```

Obr. 5.31: CAM Table Overflow – Útok po nastavení port security



Obr. 5.32: CAM Table Overflow – Upozornění port security

5.4.6 Shrnutí

Přeplněním CAM tabulky se velice snadno dosáhne DoS útoku. Záleží ovšem na druhu přepínače. V tomto konkrétním případě nebyl přepínač schopen zvládat přeposílání jakýchkoliv paketů. Útoku lze ovšem velmi jednoduše zabránit nastavením „port security“ a je možné i nastavení upozornění, což napomáhá snadnějšímu odhalení útočníka.

5.5 VTP Bomb

5.5.1 Popis útoku

Vygenerováním falešné VTP zprávy je možno dosáhnout útoku VTP Bomb. Tento útok má za následek vymazání všech sítí VLAN nakonfigurovaných na přepínači. Pomocí falešných VTP zpráv se ovšem dají i přidávat a odebírat konkrétní sítě VLAN.

5.5.2 Použité nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **Yersinia (0.8.3)** k vygenerování falešné VTP zprávy.
- **Přepínač (Cisco Catalyst 3650X)** s možností konfigurace VTP.
- **PuTTY** pro připojení k přepínači pomocí sériové linky.
- **Wireshark** ke sledování falešných VTP zpráv.

5.5.3 Topologie sítě

Obr. 5.33: VTP Bomb – Topologie sítě

5.5.4 Provedení útoku

Před útokem je možné vypsat si informace o sítích VLAN a informace o samotné VTP doméně po konfiguraci náhodných sítí VLAN.

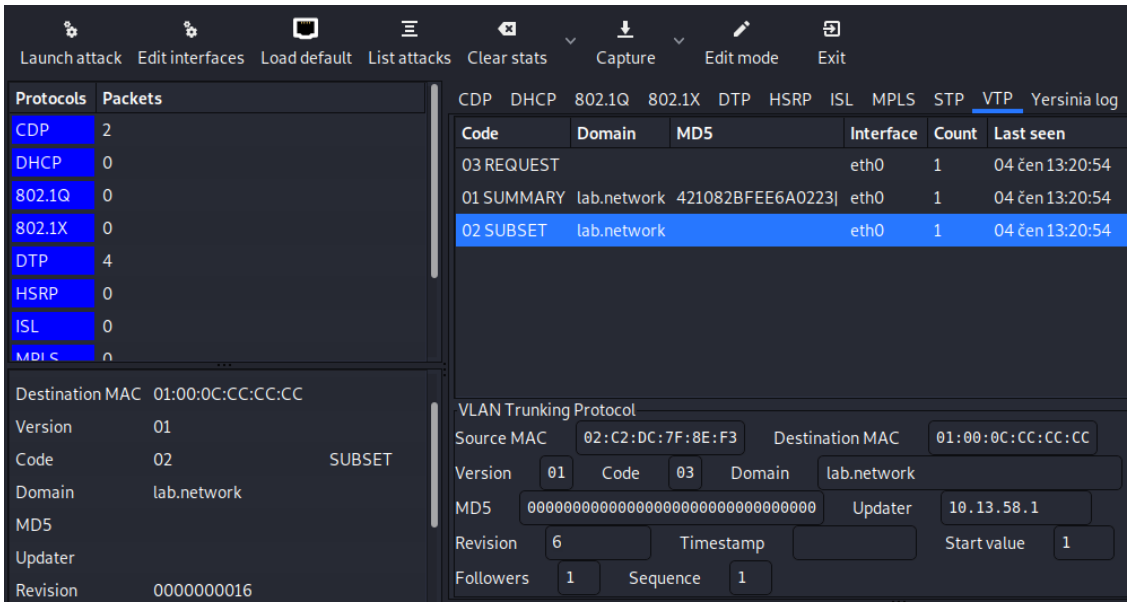
```
10   User                             active
20   Management                       active
30   Financial                        active
40   Student                          active

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
50   vlan50                           active
```

Obr. 5.34: VTP Bomb – Výpis sítí VLAN před útokem

```
Switch#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : lab.network
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 70ca.9b80.f100
Configuration last modified by 0.0.0.0 at 1-8-06 02:17:34
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 6
Configuration Revision            : 5
MD5 digest                        : 0x2A 0x83 0xD6 0x32 0xBB 0x26 0xB7 0xEA
                                    0xCE 0xE8 0xC7 0x6D 0x13 0xF4 0xC0 0xFA
```

Obr. 5.35: VTP Bomb – Vypsání informací o VTP

Pomocí „Launch attack“ a vybráním „Sending VTP packet“ v nástroji Yersinia se dají zjistit informace o VTP doméně.

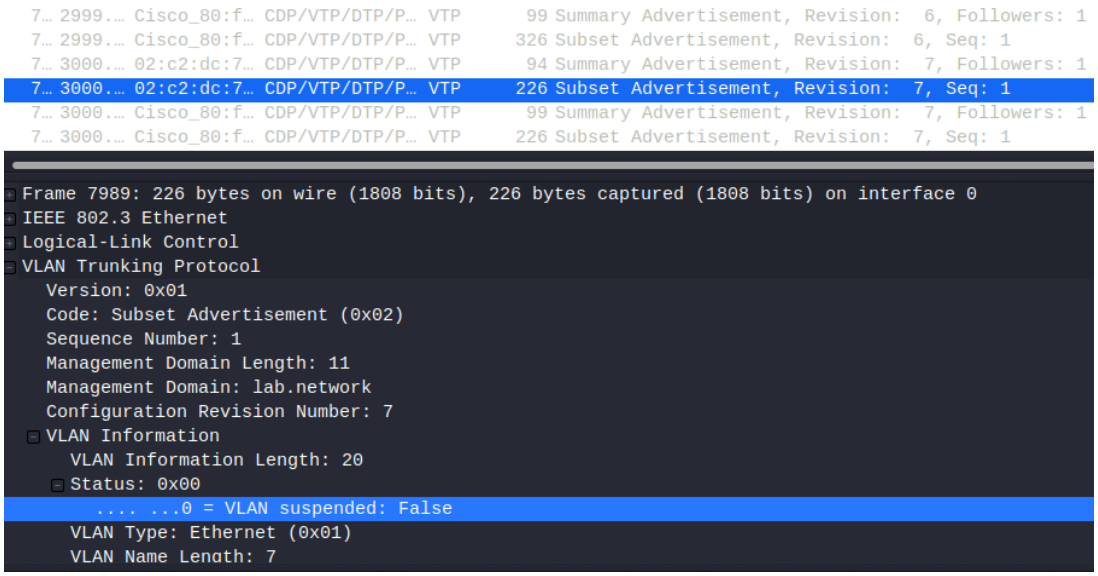


Obr. 5.36: VTP Bomb – Yersinia; informace o VTP doméně

Pomocí nástroje Yersinia se vygeneruje falešná VTP zpráva s vyšším číslem revize, než má přepínač, tudíž se přepínač synchronizuje podle této zprávy.

```
Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 1
Configuration Revision            : 6
MD5 digest                        : 0x84 0xDE 0xAB 0xD0 0x0E 0x8B 0xC5 0x25
                                    0x17 0x5E 0x90 0x0E 0x46 0x52 0xA0 0xF9
```

Obr. 5.37: VTP Bomb – Vypsání informací VTP po provedení útoku



Obr. 5.38: VTP Bomb – Wireshark; odeslání falešných VTP zpráv

5.5.5 Detekce útoku a ochranná opatření proti němu

Nejúčinnější a nejspolehlivější obranou je nepoužívání VTP, neboť poskytuje více rizik než výhod. Další ochranou by mohlo být nastavení dostatečně bezpečného hesla VTP domény, ale heslo je zobrazeno v nezašifrované podobě, což znamená další bezpečnostní riziko.

5.5.6 Shrnutí

Tento útok může vážně poškodit např. firemní síť, která tento protokol používá a pokud nejsou správci sítě obezřetní a nedělají zálohy konfigurací VLAN, tak se nabízí možnost velice účinného DoS útoku.

5.6 Napadení protokolu STP

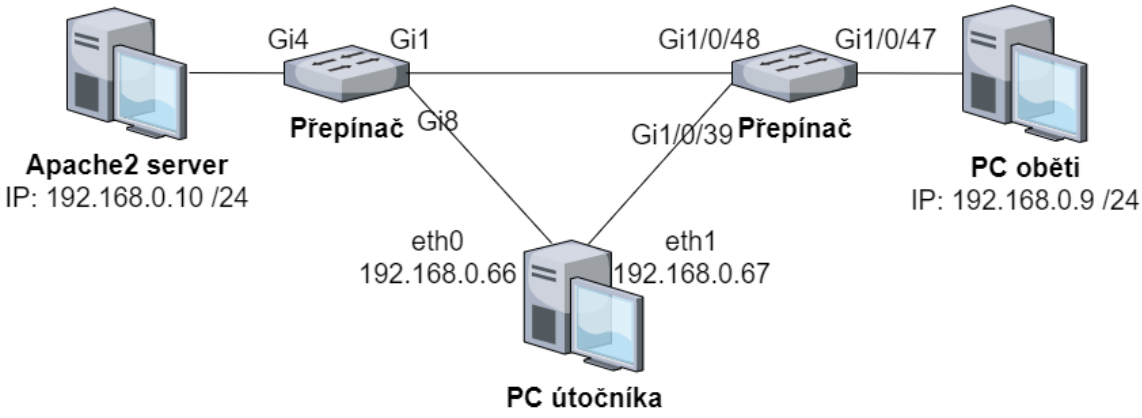
5.6.1 Popis útoku

Tento útok je proveden pomocí převzetí role „root bridge“ v síti využívající STP. Z PC útočníka lze tento útok realizovat vytvořením „síťového mostu“ v síťových nastaveních. Tento most zajišťuje, že všechny pakety, které jsou přijaty jednou síťovou kartou PC útočníka, jsou dále odeslány druhou síťovou kartou (tedy se chová jako přepínač v STP doméně).

5.6.2 Použité nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)** se dvěma síťovými kartami.
- **PC oběti (Win 10)**
- **PC cíle (Linux Mint)** se serverem Apache2.
- **Přepínač (Cisco Catalyst 3650X)**
- **Přepínač (Cisco SG 250)**
- **Yersinia** k vytvoření paketu na převzetí root bridge.
- **Wireshark** k odchytávání provozu na síti.
- **Bridge utils** k vytvoření síťového mostu na PC útočníka.
- **Bittwist** k odeslání paketu zachyceného wiresharkem díky kterému PC útočníka získá roli root bridge.
- **PuTTY** ke konfiguraci přepínačů.

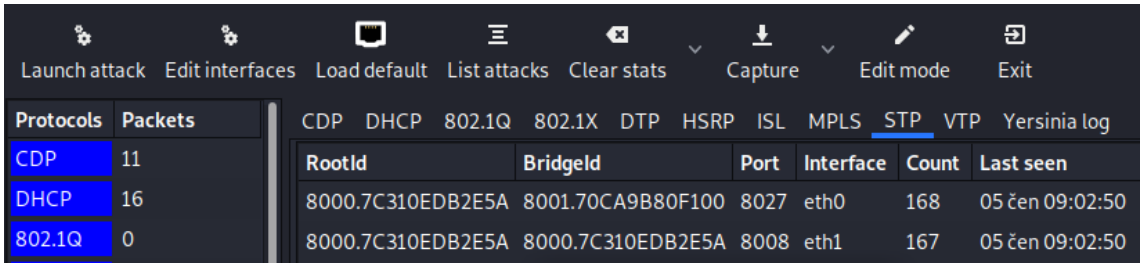
5.6.3 Topologie sítě



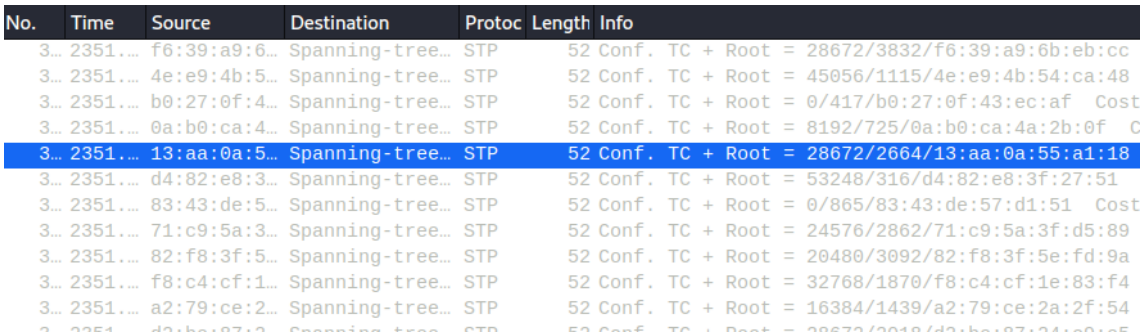
Obr. 5.39: STP – Topologie sítě

5.6.4 Provedení útoku

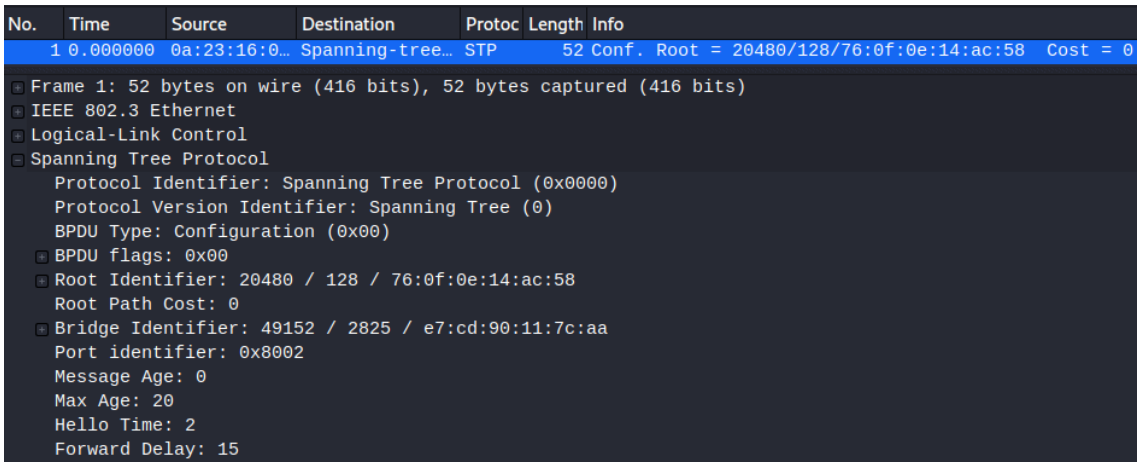
Pomocí nástroje Yersinia je možné generovat pakety, díky kterým lze převzít roli root bridge. Tento nástroj je ovšem schopen generovat buď pouze jeden paket, což má za následek zvolení PC útočníka do role root bridge na 2 sekundy (hello time – interval odesílání STP zpráv) anebo je možno generovat přehnaně velké množství těchto paketů, což pro provedení MITM útoku není ideální (jedná se spíše o DoS útok, protože vytížení CPU obou směrovačů při simulaci tohoto typu útoku dosahovalo až 99%).



Obr. 5.40: STP – Rozhraní nástroje Yersinia



Obr. 5.41: STP – DoS útok



Obr. 5.42: STP – Zachycení jediného paketu; převzetí root bridge

Pro dosažení požadovaného cíle byl použit nástroj Wireshark k odchycení paketu, který měl za následek převzetí role root bridge. Tento paket byl posléze uložen jako soubor „.pcap“ a bylo možné jej odesílat nepřetržitě v intervalu 2 sekund pomocí příkazu „watch bittwist -i br0 /root/STPConfPacket.pacp“.

```
Every 2,0s: bittwist -i br0 /root/STPConfPacket.pcap  kaliLinux: Fri Jun  5 13:55:03 2020

sending packets through br0
trace file: /root/STPConfPacket.pcap
1 packets (52 bytes) sent
Elapsed time = 0.000191 seconds
```

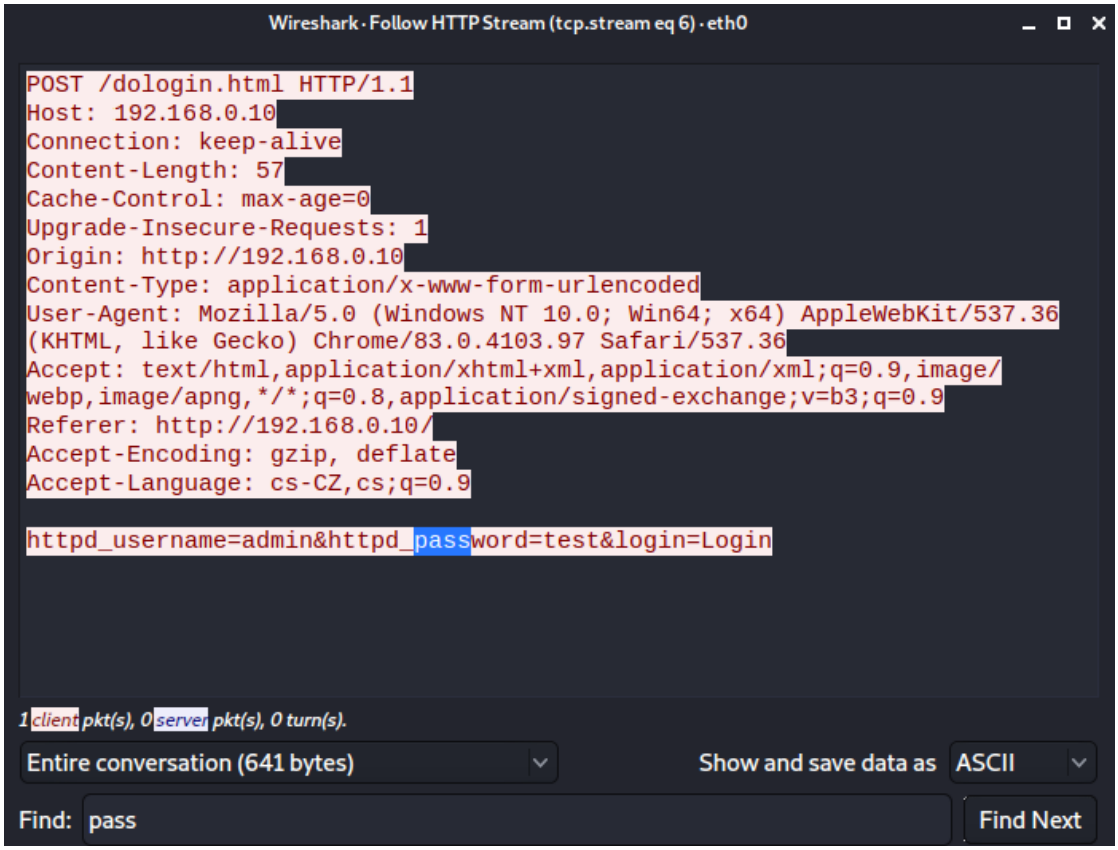
Obr. 5.43: STP – Odesílání paketů k převzetí root bridge v intervalu 2 sek.

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    20608
              Address     760f.0e14.ac58
              Cost        4
              Port        39 (GigabitEthernet1/0/39)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     70ca.9b80.f100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/39            Root FWD 4         128.39   P2p Peer(STP)
Gi1/0/47            Desg FWD 4         128.47   P2p
Gi1/0/48            Altn BLK 4         128.48   P2p
```

Obr. 5.44: STP – Vypsání informací o spanning tree v průběhu útoku

Následně bylo možné pomocí nástroje Wireshark sledovat veškerý provoz, který

např. PC oběti poslal na server Apache2 (při tomto konkrétním útoku byly odchyceny přihlašovací údaje).



Obr. 5.45: STP – Wireshark; odchycení hesla

5.6.5 Detekce útoku a ochranná opatření proti němu

Jsou dva způsoby, kterými se dá bránit proti útoku převzetí root bridge. Tyto byly vyzkoušeny a bylo možné sledovat jejich efekt vypsáním informací o spanning tree („show spanning-tree“) po provedení útoku (oba typy „zabezpečení“ byly konfigurovány na rozhraní Gi1/0/39):

- **BPDU Filter** – dá se nastavit na určitém portu příkazem „spanning-tree bpdufilter enable“. Principem tohoto způsobu obrany je, že po přijetí jakéhokoliv BPDU paketu na port, je tento následně zahozen. Tento způsob obrany měl bohužel za následek selhání topologie sítě STP kvůli vytvoření smyčky v síti (všechny porty byly ve stavu forwarding).

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/39            Desg FWD 3         128.39   P2p
Gi1/0/47            Desg FWD 4         128.47   P2p
Gi1/0/48            Root FWD 4         128.48   P2p


Switch(config-if)#
*Jan  9 04:57:31.113: %SW_MATM-4-MACFLAP_NOTIF: Host 0021.cc67.bfaf in vlan 1 is
 flapping between port Gi1/0/48 and port Gi1/0/39
Switch(config-if)#
*Jan  9 04:57:33.378: %SW_MATM-4-MACFLAP_NOTIF: Host 0021.cc67.bfaf in vlan 1 is
 flapping between port Gi1/0/39 and port Gi1/0/48
*Jan  9 04:57:33.378: %SW_MATM-4-MACFLAP_NOTIF: Host 7c31.0edb.2e5a in vlan 1 is
 flapping between port Gi1/0/39 and port Gi1/0/48
```

Obr. 5.46: STP – BPDU filtr

- **BPDU Guard** – na určitém portu se dá nastavit pomocí „spanning-tree bpduguard enable“. BPDU guard měl za následek přepnutí portu do stavu blokování ihned po přijetí paketu BPDU.

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32768
              Address     7c31.0edb.2e5a
              Cost        4
              Port        48 (GigabitEthernet1/0/48)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     70ca.9b80.f100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/47            Desg BLK 4         128.47   P2p
Gi1/0/48            Root FWD 4         128.48   P2p
```

Obr. 5.47: STP – BPDU guard

5.6.6 Shrnutí

Tento typ útoku je velice účinný v DoS i MITM útocích. V lokální síti s STP doménou se tedy dá velice jednoduše zneužít k získávání citlivých informací, pokud nejsou na síti zavedena potřebná bezpečnostní opatření. BPDU filtr měl za následek spíše zhoršení nežli zlepšení. BPDU guard se na druhou stranu jevil jako dostatečně účinný k prevenci tohoto útoku.

6 Závěr

Tato bakalářská práce je zaměřena na zabezpečení lokálních sítí na linkové vrstvě. V teoretické části jsou poskytnuty jak základní, tak i hlubší informace související s tímto tématem. V první části teorie je zahrnut popis základních informací pro pochopení fungování linkové vrstvy a výčet všech významných protokolů s linkovou vrstvou spojených. Ve druhé části jsou popsány možnosti zneužití protokolů a funkcí linkové vrstvy. Třetí část teorie obsahuje informace o účinných metodách obrany proti útokům na linkové vrstvě.

Praktická část již popisuje provedení těchto útoků. Dále je praktická část rozdělena na šest ukázek provedení útoku v laboratorním prostředí. Každá z těchto ukázek je rozdělena na jednotlivé části: použité nástroje, topologii sítě, na které byl útok simulován, provedení samotného útoku, vyzkoušení ochranných opatření proti útoku a krátké shrnutí dopadů útoku. První ukázka obsahuje provedení útoku ARP spoofing, následují ukázky obsahují provedení útoků DHCP spoofing, ICMP redirect, CAM table overflow, VTP bomb a nakonec útok na STP.

V poslední řadě jsou součástí bakalářské práce přílohy, které obsahují šest návrhů zapojení laboratorní úlohy. Cílem návrhu těchto laboratorních úloh je jejich případné budoucí využití ať už studenty nebo kýmkoliv, koho tohle téma zajímá. Podle laboratorních úloh je možné vyzkoušet si na vlastní pěst provedení nejznámějších útoků na linkové vrstvě.

Literatura

[1] *ARP Spoofing: Attacks from the internal network* [online]. 2020, [cit. 3. 4. 2020]. Dostupné z URL: <https://www.ionos.com/digitalguide/server/security/arp-spoofing-attacks-from-the-internal-network/>.

[2] *Attacking the Spanning Tree Protocol* [online]. 2020, [cit. 23. 4. 2020]. Dostupné z URL: <http://ptgmedia.pearsoncmg.com/images/9781587052569/samplechapter/1587052563_CH03.pdf>.

[3] *Attacks at Data Link Layer of OSI Model: An Owerview* [online]. 2019, [cit. 10. 11. 2019]. Dostupné z URL: < http://ijates.com/images/short_pdf/1422442328_357.pdf>.

[4] *Attacks at the Data Link Layer* [online]. 2019, [cit. 7. 11. 2019]. Dostupné z URL: <https://www.researchgate.net/publication/34492903_Attacks_at_the_Data_Link_Layer>.

[5] *CAM Overflow* [online]. 2019, [cit. 30. 11. 2019]. Dostupné z URL:< http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=2>.

[6] *CAM table overflow útok v Javě* [online]. 2020, [cit. 11. 5. 2020]. Dostupné z URL: <https://www.soom.cz/clanky/1125-CAM-table-overflow-utok-v-Jave>.

[7] *Catalyst 6500 Release 12.2SX Software Configuration Guide* [online]. 2019, [cit. 15.11.2019]. Dostupné z URL:<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vtp.html>.

[8] *CDP Attacks* [online]. 2019, [cit. 25. 11. 2019]. Dostupné z URL:<https://howdoesinternetwork.com/2011/cdp-attack>.

[9] *Cisco: Securing the Control Plane Infrastructure security* [online]. 2020, [cit. 30. 4. 2020]. Dostupné z URL: <https://oracle-patches.com/en/security/4151-cisco-securing-the-control-plane-of-infrastructure-security>.

[10] *DHCP Snooping* [online]. 2019, [cit. 25. 11. 2019]. Dostupné z URL:<https://packetpushers.net/five-things-to-know-about-dhcp-snooping/>.

[11] *Ettercap Tutorial For Network Sniffing and Man In The Middle* [online]. 2020, [cit. 30. 3. 2020]. Dostupné z URL: <https://www.poftut.com/ettercap-tutorial-network-sniffing-man-middle/>.

[12] *GARP* [online]. 2019, [cit. 16. 11. 2019]. Dostupné z URL: <https://searchnetworking.techtarget.com/definition/GARP-Generic-Attribute-Registration-Protocol>.

[13] *GVRP* [online]. 2019, [cit. 16. 11. 2019]. Dostupné z URL: <https://searchnetworking.techtarget.com/definition/GVRP>.

[14] *ICMP Redirect Attacks in the Wild* [online]. 2020, [cit. 23. 3. 2020]. Dostupné z URL: <https://www.agwa.name/blog/post/icmp_redirect_attacks_in_the_wild>.

[15] *Information Security Training* [online]. [cit. 23. 5. 2020]. Dostupné z URL: <https://www.sans.org/reading-room/whitepapers/threats/icmp-attacks-illustrated-477>.

[16] *IPv6 Neighbor Discovery Overview* [online]. 2020, [cit. 20. 5. 2020]. Dostupné z URL: <https://www.juniper.net/documentation/en_US/junos/topics/concept/neighbor-discovery-routing-overview.html>.

[17] *Layer 2 switching* [online]. 2020, [cit. 20. 5. 2020] Dostupné z URL: <https://study-ccna.com/layer-2-switching/>.

[18] *Loop Guard* [online]. 2019, [cit. 16. 11. 2019]. Dostupné z URL: < https://ccieblog.co.uk/spanning-tree/loop-guard-and-udld>.

[19] *Neighbour Discovery for IP version 6 (IPv6)* [online]. 2007, [cit. 27. 5. 2020]. Dostupné z URL: <https://tools.ietf.org/html/rfc4861>.

[20] *Network Security – Data Link Layer* [online]. 2019, [cit. 20. 11. 2019]. Dostupné z URL: <https://www.tutorialspoint.com/network_security/network_security_data_link_layer.htm>.

[21] *Securing ARP and DHCP for mitigating link layer attacks* [online]. 2019, [cit. 7. 11. 2019]. Dostupné z URL: <https://www.ias.ac.in/article/fulltext/sadh/042/12/2041-2053>.

[22] STALLINGS, William, Lawrie BROMWN, Michael D. BAUER a Michael HOWARD.: *Computer Security: principles and practice*. Upper Saddle River, N.J.: Prentice Hall, C2008. ISBN 0-13-600424-5.

[23] *Understanding VLAN Trunking Protocol* [online]. 2019, [cit. 30. 11. 2019]. Dostupné z URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html>.

[24] *VTP Advertisements - Knowledge Base* [online]. 2020, [25. 3. 2020]. Dostupné z URL: <https://sites.google.com/site/amitsciscozone/home/switching/vtp-advertisements>.

[25] *What Is DHCP Snooping and How It Works?* [online]. 2020, [cit. 12. 4. 2020]. Dostupné z URL: <https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html>.

Seznam symbolů, veličin a zkratek

ACK	Acknowledge
BPDU	Bridge Protocol Data Unit
BPDUs	Bridge Protocol Data Units
CAM	Content Adressable Memory
CDP	Cisco Discovery Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DoS	Denial of Service
DTP	Dynamic Trunking Protocol
GARP	Generic Attribute Registration Protocol
GVRP	Generic VLAN Registration Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
L2	Layer 2
LACP	Link Aggregation Control Protocol
LAN	Local area network
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MITM	Man-in-the-middle
MRP	Multiple Registration Protocol
ND	Neighbour Discovery
NIC	Network Interface Controller
OS	Operační systém
OSI	Open Systems Interconnection model
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time to live
VLAN	Virtual local area network

VM	Virtual Machine
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WINS	Windows Internet Name Service

Seznam příloh

A Návrh na zapojení laboratorní úlohy – LAB 1

Upozornění: Nezkoušejte následující útoky v žádné veřejné ani jiné síti kromě laboratoře!

A.1 ARP Spoofing

Cíl laboratorní úlohy

Cílem této úlohy je vyzkoušet si provedení útoku ARP spoofing v laboratorním prostředí. Výsledkem by měla být možnost odposlouchávat provoz PC oběti pomocí nástroje Ettercap (např. přihlašovací údaje zadané na nezabezpečené webové stránce).

Teoretický úvod

ARP je komunikační protokol používaný pro objevování adres na linkové vrstvě, jako je MAC adresa spojená s danou adresou ze sady TCP/IP, obvykle IPv4 adresou. Toto mapování je kritickou funkcí v sadě internetových protokolů. ARP byl implementován s mnoha kombinacemi technologií síťových a datových spojů, jako je IPv4. V sítích IPv6 je funkce ARP zajištěna protokolem ND. ARP je protokol fungující na bázi request-response (dotaz-odpověď).

ARP Spoofing (také ARP cache poisoning nebo ARP poison routing) je typ útoku, při kterém útočník odesílá padělané zprávy ARP v lokální síti. To má za následek propojení MAC adresy útočníka s IP adresou legitimního počítače nebo serveru v síti. Jakmile je MAC adresa útočníka spojena s autentizovanou IP adresou, útočník začne přijímat veškerá data, která jsou pro tuto IP adresu určena.

Každý počítač v síti udržuje tabulku zvanou „ARP cache“. Tabulka obsahuje IP adresu a přidružené MAC adresy ostatních zařízení v síti. Protože je ARP „stateless“ protokol (bez informací o aktuální relaci od serveru), pokaždé, když zařízení obdrží „ARP Reply“ od jiného zařízení, přijme jej a aktualizuje svou ARP cache, i přestože neodeslal žádný „ARP Request“. Díky tomuto faktu je možné se jednoduše vydávat za jiná zařízení v síti.

ARP spoofing se dá použít k následujícím útokům:

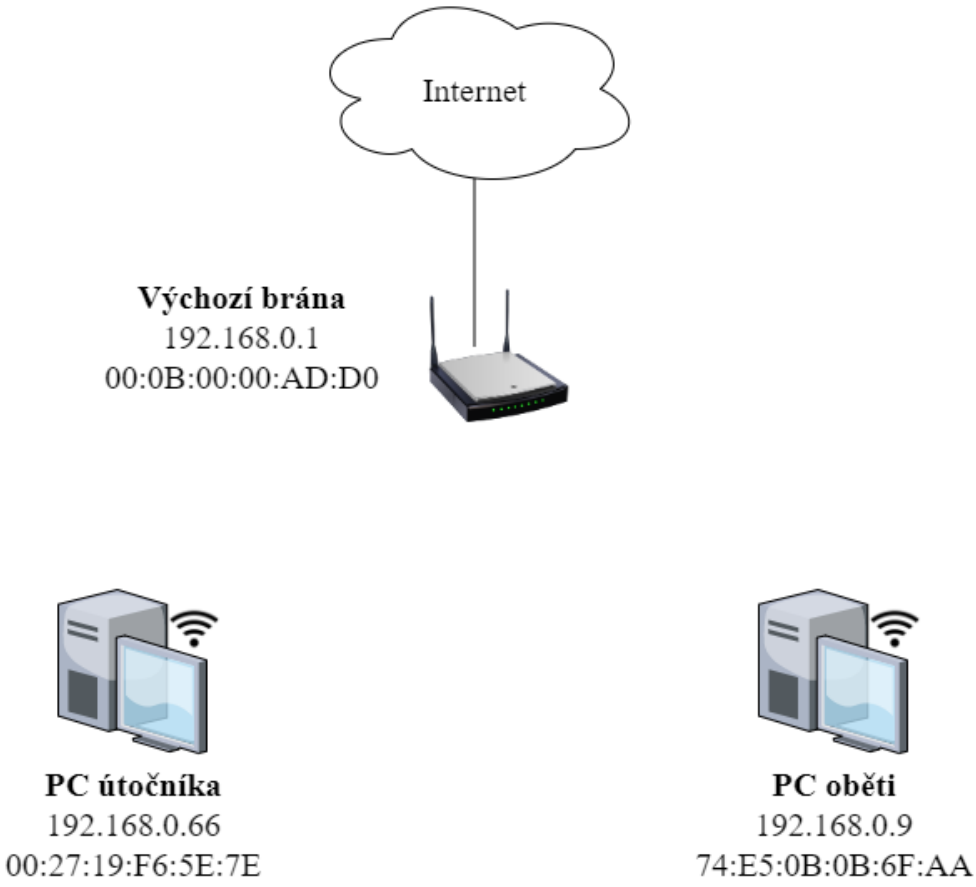
- **DoS útoky** – často využívají ARP spoofing k propojení více IP adres s MAC adresou jednoho cíle. V důsledku toho bude přenos, který je určen pro mnoho různých IP adres, přesměrován na MAC adresu cíle a to povede k přetížení cíle nadbytečným provozem.
- **Session hijacking („únos“ relace)** – útočník může pomocí ARP spoofingu ukrást ID relací a poskytnout útočníkům přístup k soukromým systémům a datům.
- **MITM útoky** – je možné ARP spoofing využít k zachycení a upravení provozu mezi počítači v napadené síti.

Potřebné nástroje

K provedení laboratorní úlohy budeme potřebovat následující:

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **PC oběti (Win10)**
- **Síťové karty** umožňující připojení k bezdrátové síti WiFi
- **Bezdrátový směrovač** umožňující přístup k internetu
- **Ettercap (0.8.3)** – nástroj užitečný nejen k provedení útoku ARP spoofing, ale i mnoho dalších. Ettercap se používá především pro útoky typu MITM. Software podporuje různé distribuce Linuxu i Max OS X. Instalace na systému Windows je možná, ale vyžaduje přídavné konfigurace. Útoky jako „sniffing“, ARP spoofing a shromažďování hesel mohou být automatizovány. Ettercap může manipulovat se zachycenými daty a útočit i na sítě, které jsou zabezpečeny pomocí SSH nebo SSL. Program je oficiálně nabízen jako bezpečnostní software a používá se při testování zranitelností.

Topologie sítě



Obr. A.1: ARP Spoofing – Topologie sítě

Konfigurace PC oběti

Pro PC oběti nastavíme síťový adaptér pro IPv4 na statickou IP adresu a ostatní parametry v nastavení sítě.**Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.**

Konfigurace PC útočníka

Pro PC útočníka (jelikož běží ve virtuálním prostředí) bude nutné nakonfigurovat síťové nastavení ve VM VirtualBox na síťový most pro Kali Linux a IP adresu v „Rozšířená nastavení sítě“.

Dalším krokem potom bude napsání několika příkazů do konfiguračního terminálu:

- „apt-get update“ pro aktualizaci systému
- „apt-get install ettercap-graphical“ pro instalaci nástroje Ettercap s grafickým rozhraním

Příprava útoku

Pomocí příkazů „ping“ ověříme konektivitu obou zařízení. Pokud budou pingy úspěšné, vytvoří si tím PC útočníka záznam v ARP cache o PC oběti a naopak. Záznam ARP cache lze vypsat pomocí příkazů „arp“ pro Kali Linux a „arp -a“ pro Win10. Záznamy tedy budou vypadat následovně:

```
root@kaliLinux:~# arp
Adresa                   HWtyp   HWadresa           Příz. Maska             Rozhr
192.168.0.1              ether   00:0b:00:00:ad:d0  C                       eth0
192.168.0.9              ether   74:e5:0b:0b:6f:aa  C                       eth0
```

Obr. A.2: ARP Spoofing – ARP cache PC útočníka

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.0.9 --- 0xf
  Internet Address      Physical Address      Type
  192.168.0.1           00-0b-00-00-ad-d0     dynamic
  192.168.0.66          00-27-19-f6-5e-7e     dynamic
```

Obr. A.3: ARP Spoofing – ARP cache PC oběti

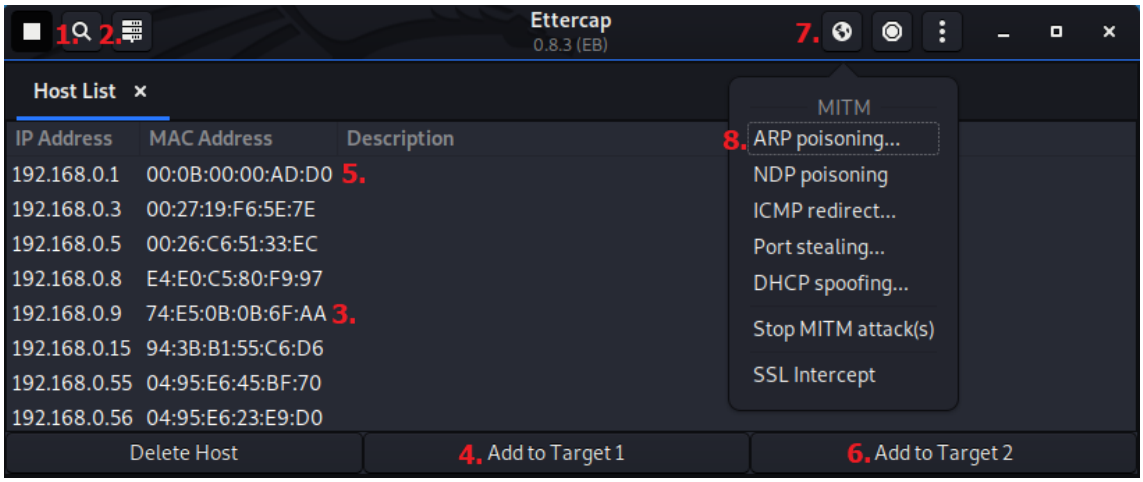
Provedení útoku

V terminálu PC útočníka zadáme příkaz „ettercap -G“ pro spuštění grafického rozhraní.

Objeví se tabulka, ve které je nutné zvolit síťové rozhraní (v našem případě to bude rozhraní „eth0“) a tuto volbu potvrdit.

Nyní začneme prohledávat síť pomocí znaku lupy „Scan for hosts“. Po dokončení prohledávání sítě klikneme na vedlejší tlačítko „Hosts list“ a zobrazí se tabulka, ve které bychom měli vidět všechna zařízení v lokální síti. Dále už jen stačí vybrat IP adresu PC oběti a označit ji jako „Target 1“ pomocí „Add to Target 1“, respektive vybrat IP adresu výchozí brány a označit ji jako „Target 2“ pomocí „Add to Target 2“. Poté už jen

zvolíme „MITM menu –> ARP poisoning…“, kde zaškrtneme „Sniff remote connections“ a potvrdíme. Odposlouchávání sítě lze korigovat tlačítkem nalevo od lupy „Start/Stop Sniffing“.



Obr. A.4: ARP Spoofing – Provedení útoku v nástroji Ettercap

Nyní se vraťme k PC oběti zjistit, zda útok funguje. Stačí najít jakoukoliv webovou stránku bez zabezpečeného připojení (např. http://forum.curvefever.com/user/login), kde se zkusíme přihlásit s uživatelským jménem „admin“ a heslem „test“. V nástroji Ettercap poté uvidíme následující výpis provozu:

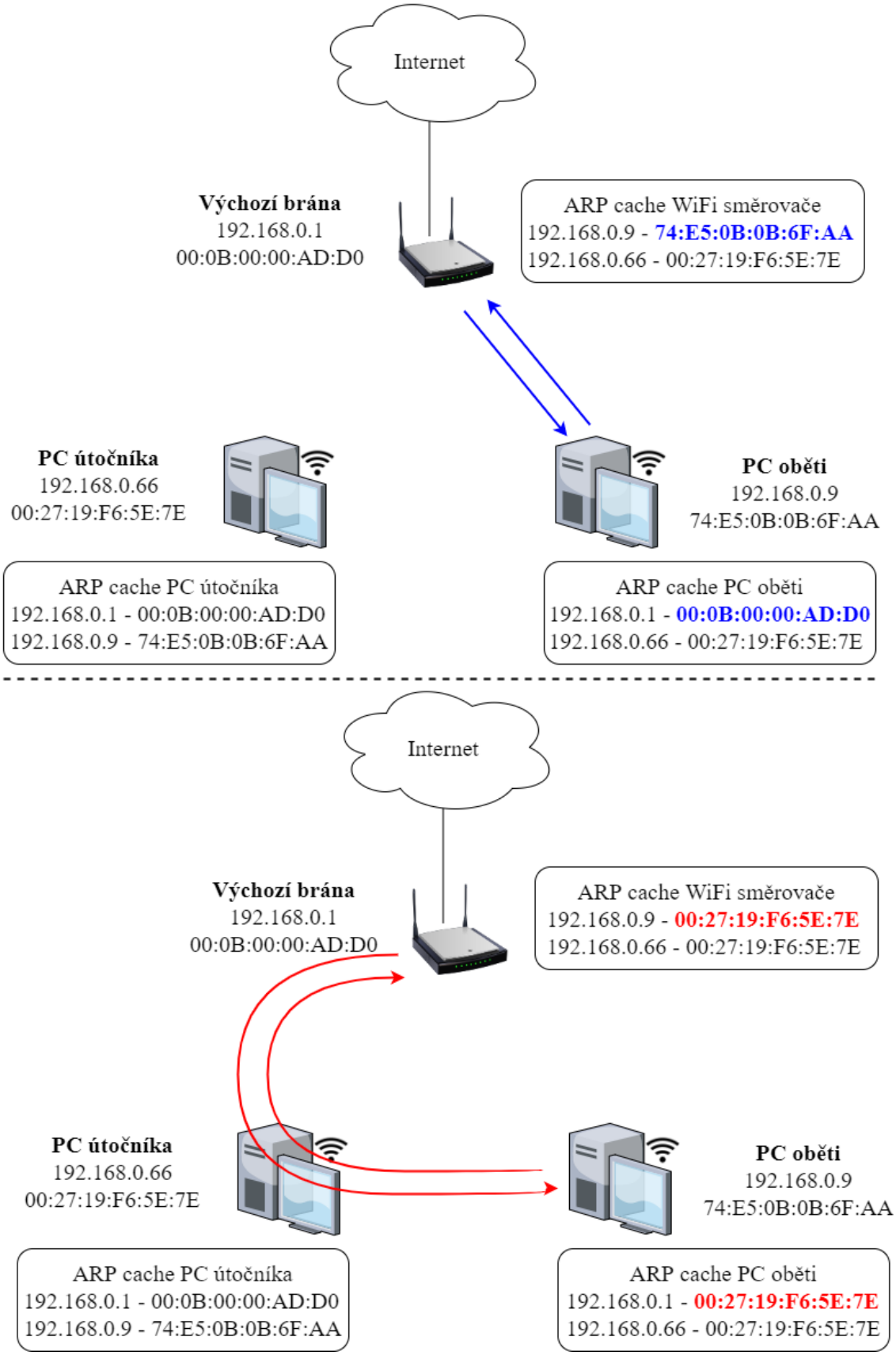
```
Starting Unified sniffing...

HTTP : 104.27.177.90:80 -> USER:  PASS: test  INFO: http://forum.curvefever.com/user/login
CONTENT: name=admin&pass=test&form_build_id=form-qZsRml-mRczGaz-
k0vwdOoeswju0xljyMYlirGbJqaQ&form_id=user_login&read_rules=&captcha_sid=20672805
```

Obr. A.5: ARP Spoofing – Odposlech uživatelského jména a hesla PC oběti

Útok tedy funguje perfektně. Dále je možné vyzkoušet odposlechnout uživatelské jméno a heslo zadané na jakoukoliv zabezpečenou webovou stránku (např. https://www.vutbr.cz/login) a můžeme vidět, že Ettercap nic nevypíše. Odposlech takového provozu se sice dá zajistit pomocí programu Wireshark, ale v případě zabezpečeného připojení není možné z něj cokoliv vyčíst.

```
Interface: 192.168.0.9 --- 0xf
  Internet Address      Physical Address      Type
  192.168.0.1           00-27-19-f6-5e-7e     dynamic
  192.168.0.66          00-27-19-f6-5e-7e     dynamic
```

Obr. A.6: ARP Spoofing – Výpis ARP cache PC oběti po provedení útoku



Obr. A.7: ARP Spoofing – Síť před útokem a po útoku

Kontrolní otázky

Jak se nazývají dvě zprávy protokolu ARP, pomocí kterých spolu v rámci protokolu zařízení komunikují?

Jsou ARP zprávy stejného typu provozu (unicast, broadcast)? Pokud ne, jaká zpráva je jakého typu a proč to takhle funguje?

K jakým typům útoků lze ARP spoofing využít?

Znáte jiné programy/způsoby, pomocí kterých se dá ARP spoofing provést?

Na jakém typu sítě by se dal tento útok v praxi provést nejjednodušeji?

A.2 DHCP Spoofing

Cíl laboratorní úlohy

Cílem laboratorní úlohy je simulovat útok pomocí podvrženého DHCP serveru a následně vyzkoušet si detekci podvrženého DHCP serveru. Útočník (kali Linux) podvrhne DHCP server pomocí programu Yersinia, který způsobí, že po vypršení „lease time“ u IP adresy PC oběti (Windows 10 x86) se podvržený DHCP server „vnutí“ oběti a bude předstírat jeho původní DHCP server.

Teoretický úvod

DHCP je protokol správy sítě. Server DHCP dynamicky přiřadí každému zařízení v síti IP adresu a další parametry konfigurace sítě, aby zařízení mohla komunikovat spolu v rámci lokální sítě i se zařízeními jiných sítí protokolu IP. DHCP server umožňuje počítačům automaticky požadovat IP adresy a síťové parametry od ISP, což snižuje potřebu správce sítě nebo uživatele ručně přiřadit IP adresy všem síťovým zařízením. V případě neexistence DHCP serveru musí být počítači nebo jinému zařízení v síti IP adresa přidělena ručně nebo musí být přiřazena adresa APIPA, která neumožňuje komunikaci mimo místní podsíť. DHCP lze implementovat v sítích o velikosti od domácích sítí po velké firemní sítě a sítě regionálních ISP. Směrovač nebo rezidenční gateway (malý směrovač pro spotřebitelské účely, který poskytuje přístup k síti mezi hostiteli sítě LAN do sítě WAN prostřednictvím modemu) lze aktivovat jako server DHCP. Většina směrovačů přijímá v síti ISP celosvětově jedinečnou IP adresu. V síti LAN přiřadí DHCP server lokální IP adresu každému zařízení, které je k síti připojeno následujícím způsobem (tzv. DHCP handshake):

- **DHCP Discover –** klient tuto zprávu posílá k objevení DHCP serveru/serverů v síti.
- **DHCP Offer –** DHCP server odpovídá nabídkou volné IP adresy ze svého rozsahu a dalšími informacemi.
- **DHCP Request –** klient si vyžádá IP adresu ze serveru.
- **DHCP ACK –** server potvrdí novou IP adresu, která byla nyní určena konkrétnímu zařízení a tím dokončí cyklus „DHCP handshake“.

Protokolu DHCP se dá zneužít dvěma způsoby:

- **DHCP Starvation** – jedná se o zvláštní druh útoku, kdy útočník odešle na DHCP server spoustu požadavků (DHCP Requests) s chybnou MAC adresou. Pokud je síť zaplavena dostatečným množstvím požadavků, může útočník vyčerpat všechny dostupné adresy DHCP serveru. Klienti napadené sítě jsou pak „vyhladověni“ – DHCP server nemá žádné IP adresy, které by mohl přidělit. Útočník poté může v síti nastavit podvržený DHCP server a obětem odpovědět na upravené konfigurace IP. Tyto parametry zajišťují útočníkovi možnost MITM útoku.

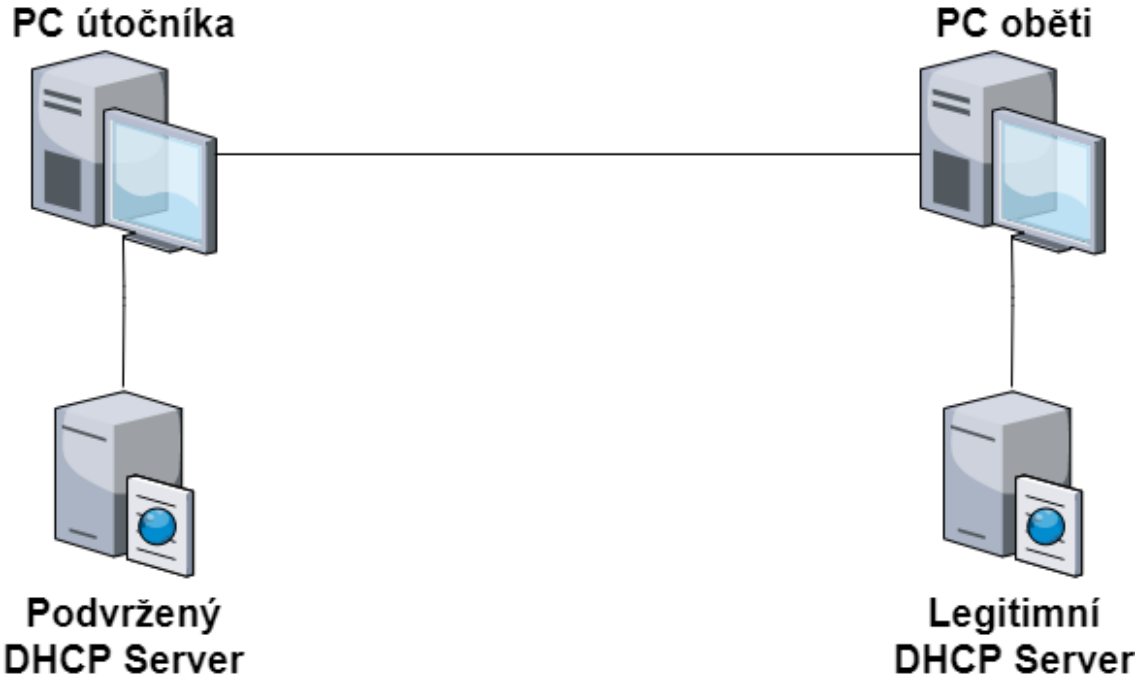
- **DHCP spoofing** – útočník do sítě nasadí podvržený DHCP server, který klientům poskytne IP adresy. Když se klienti připojují k síti, nabídne jim podvržený server i legitimní DHCP server IP adresy a výchozí bránu, servery DNS a servery WINS. Pokud se informace poskytované podvrženým DHCP serverem liší od těch legitimních, mohou klienti mít problémy s přístupem k síti, včetně problémů s rychlostí a neschopností dosáhnout ostatních klientů v síti.

  Kromě toho, pokud je podvržený DHCP server nastaven tak, aby jako výchozí brána poskytoval IP adresu počítači, který je obsluhován útočícím uživatelem, potom tento uživatel může „čichat“ veškerý přenos odeslaný klienty do jiných sítí, což porušuje zásady zabezpečení sítě a soukromí uživatelů (MITM útok).

Potřebné nástroje

- **Oracle VM VirtualBox** je open-source software pro virtualizaci počítačové architektury x86. Funguje jako hypervisor a vytváří virtuální počítač VM, ve kterém může uživatel provozovat jiný operační systém. Operační systém, ve kterém běží VirtualBox, se nazývá „hostitelský“ operační systém.
- **Wireshark** je open-source software pro analýzu paketů. Používá se pro řešení problémů v síti, analýzu softwaru, vývoj softwaru a komunikačních protokolů a pro vzdělávání.
- **Yersinia s**louží k realizaci různých útoků proveditelných na linkové vrstvě, které využívají slabiny protokolů na této vrstvě. Pentester (člověk, který testuje bezpečnost útoky na síť) pomocí tohoto nástroje může identifikovat zranitelnosti v síti. Během penetračních testů se yersinia používá k iniciaci útoků na různá zařízení a protokoly linkové vrstvy, jako jsou přepínače, dhcp servery STP atd. V současné době yersinia podporuje následující protokoly: STP, CDP, DTP, DHCP, VTP, HSPR, ISL, IEEE 802.1Q a IEEE 802.1X.
- **RogueChecker** – nástroj Microsoft Rogue DHCP Checker umožňuje rychle a snadno zkontrolovat, zda v síti existují další servery DHCP a tudíž je užitečný při detekci podvržených DHCP serverů.

Topologie sítě



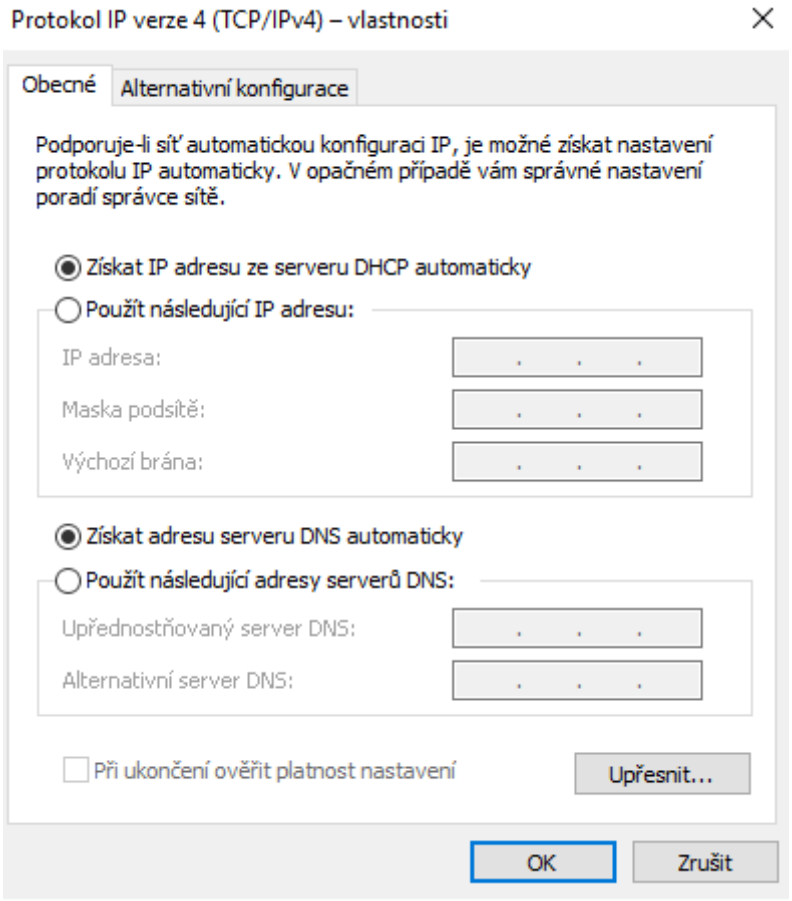
Obr. A.8: DHCP Spoofing – Topologie sítě

Konfigurace VM VirtualBox a příprava virtuálních PC

Po nainstalování virtuálních strojů kali Linux a Windows 10 na VirtualBox si před jejich spuštěním nakonfigurujeme síťová rozhraní – v nastavení obou virtuálních strojů na síťové kartě zvolíme „Síť pouze s hostem“, tím zaručíme spojení mezi dvěma stroji.

Nyní můžeme virtuální stroje spustit a nainstalovat potřebný software (tj. na kali Linux program Yersinia a na Windows 10 programy RogueChecker a Wireshark). Kali Linux před instalací updatujeme, aby se zamezilo možným potížím pomocí příkazu „sudo apt-get update -y“ s flagem „-y“ pro případné odsouhlasení všech dotazů. Po updatování systému můžeme nainstalovat program Yersinia pomocí příkazu „sudo apt-get install -y yersinia“. Na počítači oběti nainstalujeme programy RogueChecker a Wireshark.

Po instalaci potřebného software se ujistíme, že u počítače oběti je v síťovém nastavení vybrána možnost „Získat IP adresu ze serveru DHCP automaticky“.

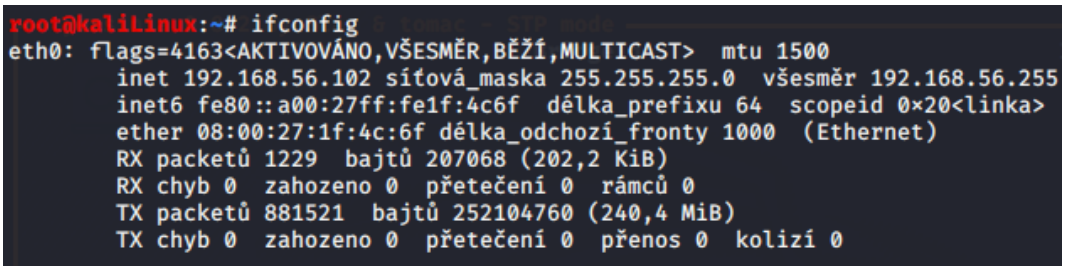


Obr. A.9: DHCP Spoofing – Získání IP adresy ze serveru DHCP

Nyní zjistíme IP adresy obou PC pomocí příkazu „ipconfig“ ve Win 10 command prompt, respektive „ifconfig“ v emulátoru terminálu kali Linux a zkusíme vzájemnné propojení PC pomocí příkazu ping. Pokud spolu stroje komunikují, zjistíme IP adresu počítače útočníka a oběti.

```
C:\Users\win>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c1a5:4ec5:e53f:6902%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Obr. A.10: DHCP Spoofing – IP adresa PC oběti



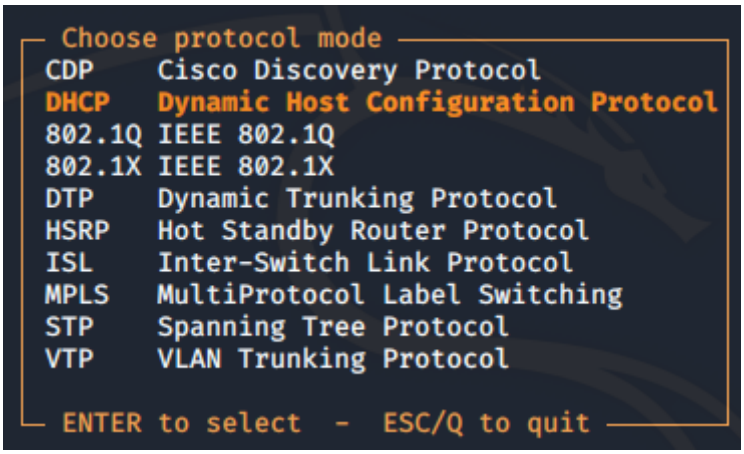
Obr. A.11: DHCP Spoofing – IP adresa PC útočníka

V našem případě je IP adresa 192.168.56.104 na PC oběti a 192.168.56.102 na PC útočníka.

Provedení útoku

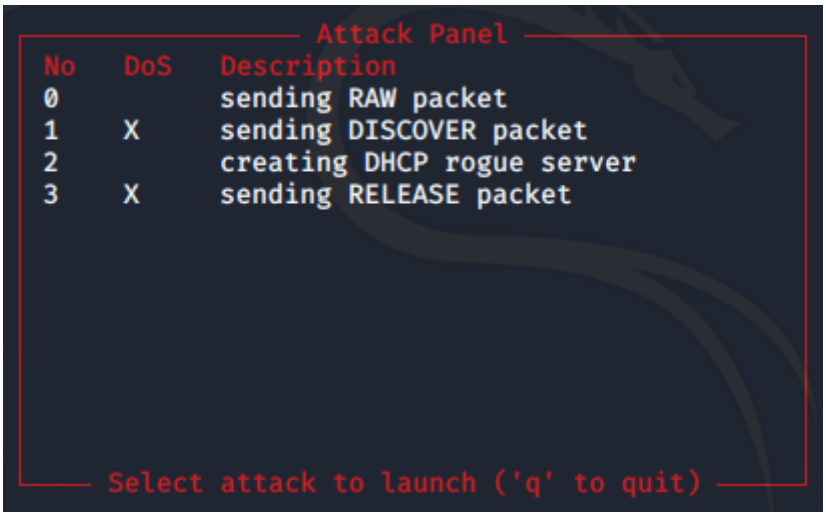
Spustíme na PC útočníka program Yersinia pomocí příkazu „yersinia -I“. Dále vybereme správné rozhraní (tj. v síti s počítačem oběti – např eth0) pomocí klávesy „I“.

Po konfiguraci správného rozhraní otevřeme nabídku útoků klávesou „G“ nabídku protokolů, které se dají napadnout a vybereme protokol DHCP.



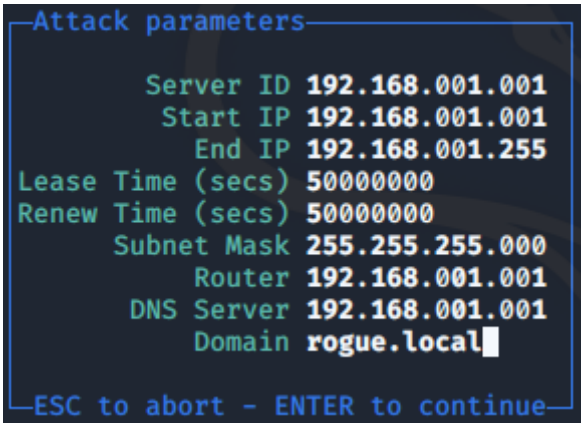
Obr. A.12: DHCP Spoofing – Yersinia; výběr protokolu DHCP

Výběr potvrdíme pomocí klávesy „ENTER“ a stiskneme „X“ k provedení útoku. Zobrazí se nám nabídka možností útoku, zvolíme možnost „creating DHCP rouge server“ pomocí klávesy „num 2“.



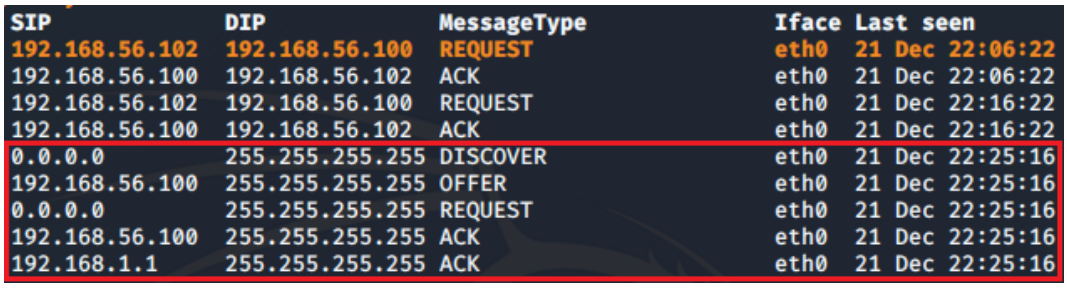
Obr. A.13: DHCP Spoofing – Yersinia; panel útoků pro DHCP server

Zobrazí se nám tabulka s parametry podvrženého DHCP serveru, kterou nakonfigurujeme následovně (Server ID může být jakékoliv, záleží na tom, jakou síť chce útočník vytvořit a z jakého rozsahu chce rozdělovat IP adresy – Start IP-End IP, dále Router a DNS Server jsou adresy falešného DNS serveru a routeru). Konfiguraci potvrdíme.



Obr. A.14: DHCP Spoofing – Yersinia; konfigurace podvrženého DHCP serveru

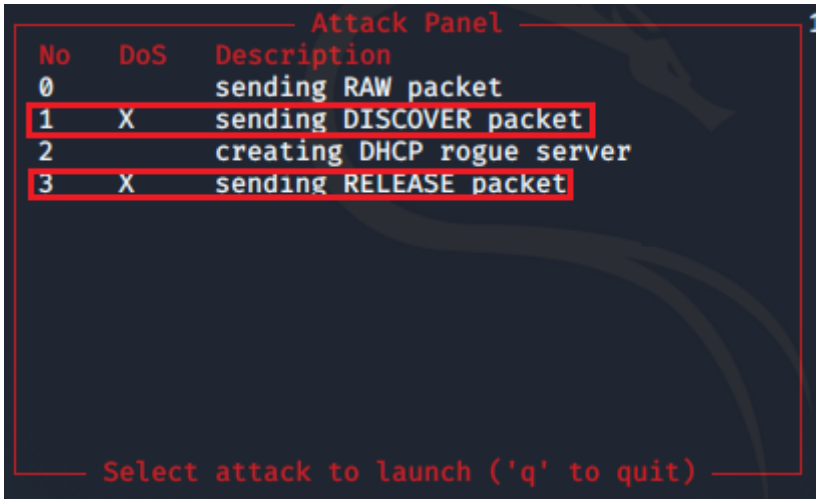
Nyní je podvržený DHCP server v provozu a jediné, co útočník potřebuje, je počkat na obnovení IP adresy oběti (vypršení lease time), či restart PC oběti – v našem případě tuto akci urychlíme pomocí zadání příkazů „ipconfig /release“ a „ipconfig /renew“ na počítači oběti. Po obnovení IP adresy obdrží PC oběti novou IP adresu z nastaveného rozsahu podvrženého DHCP serveru – to ověříme kontrolou, zda proběhl nový „handshake“ DHCP serveru.



SIP	DIP	MessageType	Iface	Last seen
192.168.56.102	192.168.56.100	REQUEST	eth0	21 Dec 22:06:22
192.168.56.100	192.168.56.102	ACK	eth0	21 Dec 22:06:22
192.168.56.102	192.168.56.100	REQUEST	eth0	21 Dec 22:16:22
192.168.56.100	192.168.56.102	ACK	eth0	21 Dec 22:16:22
0.0.0.0	255.255.255.255	DISCOVER	eth0	21 Dec 22:25:16
192.168.56.100	255.255.255.255	OFFER	eth0	21 Dec 22:25:16
0.0.0.0	255.255.255.255	REQUEST	eth0	21 Dec 22:25:16
192.168.56.100	255.255.255.255	ACK	eth0	21 Dec 22:25:16
192.168.1.1	255.255.255.255	ACK	eth0	21 Dec 22:25:16

Obr. A.15: DHCP Spoofing – Handshake PC oběti s podvrženým DHCP serverem

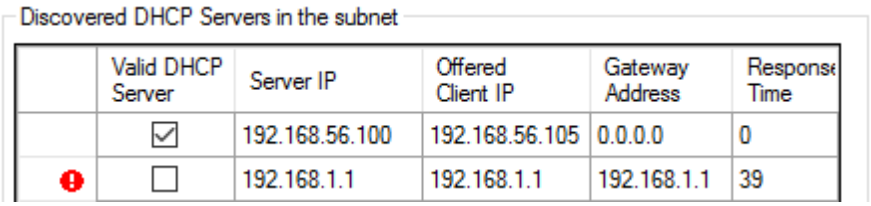
Počítači oběti byla tímto přidělena IP adresa z rozsahu podvrženého DHCP serveru s tím, že při opětovném zadání příkazu „ipconfig“ nepozná rozdíl, protože se DHCP server zamaskuje jako pravý DHCP server a podvrhne stejné údaje síťové konfigurace. Nyní můžeme na počítač oběti spustit například útok DoS pomocí opětovného stisknutí klávesy „X“ a výběrem možnosti „sending DISCOVER packet“, nebo „sending RELEASE packet“. Tímto bude počítač oběti neschopen se připojit k internetu, či k ostatním zařízením v síti (útok DHCP Starvation).



Obr. A.16: DHCP Spoofing – Yersinia; provedení DoS útoku

Detekce útoku

Detekci útoku provedeme nejprve pomocí programu RogueChecker, který nám přímo ukáže, že se v naší síti vyskytl nový DHCP server. Program spustíme a klikneme na „detect rogue servers“.

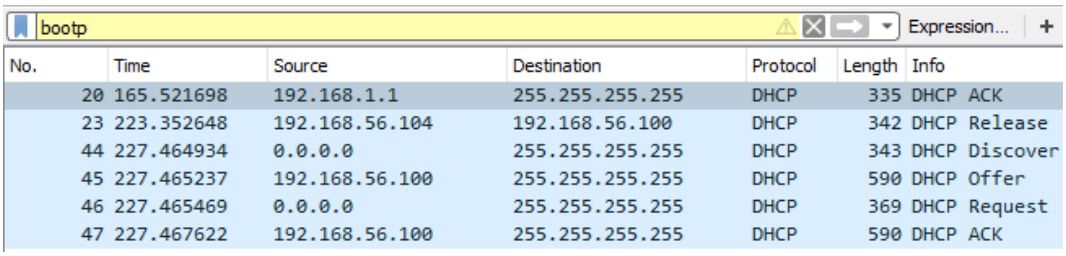


Obr. A.17: DHCP Spoofing – RogueChecker; detekce podvrženého DHCP serveru

Můžeme vidět, že program RogueChecker nám ukázal dva různé DHCP servery, první správný s IP adresou 192.168.56.100 a druhý podvržený s námi nakonfigurovanou IP adresou.

Dále si vyzkoušíme detekci útoku pomocí Wireshark. Program zapneme a zvolíme síťové rozhraní, které chceme odposlouchávat.

Pro jednodušší odhalení podvrženého DHCP serveru si zobrazíme filtr „bootp“. Poté zopakujeme obnovení IP adresy na PC oběti pomocí „ipconfig /release“ a „ipconfig /renew“ a ve Wiresharku uvidíme IP adresu nelegitimního DHCP serveru, tj. 192.168.1.1.



Obr. A.18: DHCP Spoofing – Wireshark; detekce podvrženého DHCP serveru

Kontrolní otázky

Co všechno má na starost DHCP server (jaké parametry přiděluje zařízením v síti)?

Jak probíhá DHCP handshake?

K jakým typům útoků se dá DHCP spoofing využít?

Z jakého důvodu poskytuje DHCP server IP adresy ze svého rozsahu jen po určitou dobu (lease time)?

Pomocí jakých dvou příkazů lze zahodit momentálně přidělenou IP adresu od DHCP serveru a vyžádat si novou? (berme v potaz příkazový řádek systému Windows)

A.3 ICMP Redirect

Cíl laboratorní úlohy

Cílem této laboratorní úlohy je provést ICMP redirect k dosažení MITM útoku.

Teoretický úvod

ICMP redirect (přesměrování) je funkce protokolu IP, která umožňuje směrovači informovat zařízení o tom, že existuje efektivnější cesta do cíle a že by zařízení mělo odpovídajícím způsobem upravit svoji směrovací tabulku. V zásadě se ICMP redirect jeví jako užitečná funkce v důvěryhodné lokální síti, ale na veřejném internetu, kde je spousta skrytých hrozeb, může mít fatální následky mít přesměrovaný provoz falešnou ICMP zprávou od útočníka. I přesto je však ICMP redirect systému Linux a Windows ve výchozím nastavení povolen.

Díky tomu, že ICMP je postarší protokol (1981), může tento typ útoku výrazně narušit chod sítě, kde je povolen bez vědomí, že se dá jednoduše zneužít. Odesláním falešného přesměrování nedojde ihned k uložení falešné trasy do mezipaměti tras (tzv. route cache). Ovšem při následovném pokusu kontaktovat zařízení (na které je provoz přesměrován) se v mezipaměti tras objeví falešný záznam, který brání v kontaktování tohoto zařízení. Kromě toho, jakmile se záznam dostane do mezipaměti tras, není snadné se ho zbavit. I když se mezipamět vymaže, falešný záznam se při příštím pokusu kontaktovat cílové zařízení opět objeví, což je nejspíše způsobeno faktem, že jádro systému (kernel) v sobě uchovává nějaký samostatný stav přesměrovaných záznamů o trase. Z toho vyplývá, že jediným účinným řešením je obnovení a restartování postiženého serveru.

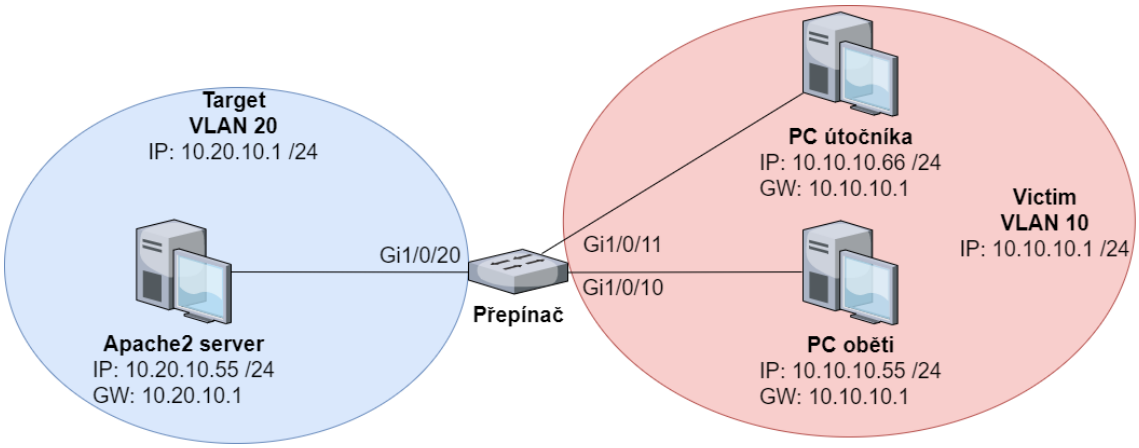
Je tedy zřejmé, že jde ICMP redirect použít k útokům DoS. Při snaze zabránit určitému zařízení (oběti) kontaktoval jiné zařízení (cíl), stačí oběti poslat falešné přesměrování pro cíl. Jediným omezením je, že oběť musí kontaktovat cíl v určitém čase od přijetí přesměrování, aby DoS útok fungoval. To lze ovšem snadno vyřešit. Stačí přesměrování odeslat, když se má oběť pravděpodobně spojit s cílem nebo jednoduše odesílat nové přesměrování např. každých 10 minut.

ICMP redirect lze i snadno využít k útokům MITM pomocí přesměrování provozu zařízení oběti přes zařízení útočníka.

Potřebné nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **PC oběti (Win10)**
- **PC s web serverem Apache2 (Linux Mint)** na který se bude obět přihlašovat a útočník heslo bude schopen odposlechnout přihlašovací údaje
- **Přepínač (Cisco Catalyst 3650X)**
- **Wireshark** k monitorování provozu (apt-get install wireshark)

Topologie sítě



Obr. A.19: ICMP Redirect – Topologie sítě

Konfigurace PC oběti

Pro PC oběti nastavíme síťový adaptér pro IPv4 na statickou IP adresu 10.10.10.55 s maskou sítě 255.255.255.0.**Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.Chyba! Nenalezen zdroj odkazů.**

Konfigurace PC útočníka

Pro PC útočníka (jelikož běží ve virtuálním prostředí) bude nutné nakonfigurovat síťové nastavení ve VM VirtualBox pro Kali Linux (síťový most) a IP adresu v „Rozšířená nastavení sítě“ 10.10.10.66 s maskou sítě 255.255.255.0. Dále je nutné na PC útočníka povolit přesměrování provozu (forwarding), aby PC oběti po poslání ICMP redirect nepřišlo o spojení s cílovým zařízením. Zda je přesměrování povolené, což lze zjistit pomocí příkazu „sysctl net.ipv4.conf.all.forwarding“. Pokud je hodnota „0“, lze přesměrování povolit pomocí stejného příkazu s koncovkou „=1“ bez mezer.

```
root@kaliLinux:~# sysctl net.ipv4.conf.all.forwarding
net.ipv4.conf.all.forwarding = 0
root@kaliLinux:~# sysctl net.ipv4.conf.all.forwarding=1
net.ipv4.conf.all.forwarding = 1
```

Obr. A.20: ICMP Redirect – Povolení přesměrování

Konfigurace serveru Apache2

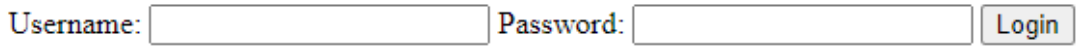
Na počítači, na kterém bude server Apache2, nakonfigurujeme IP adresu 10.20.10.55 s maskou sítě 255.255.255.0 a nainstalujeme server Apache2 pomocí příkazu „apt-get install apache2“. Po instalaci by měl být server přístupný z jakéhokoliv webového prohlížeče na URL „http://10.20.10.55“. Pro účel této laboratorní práce si na úvodní stránce serveru Apache2 nakonfigurujeme jednoduché přihlašovací rozhraní, na které se bude „přihlašovat“ PC oběti. Webový server můžeme upravit pomocí textového editoru

„nano /var/www/html/index.html“.

```
  GNU nano 2.5.3         File: /var/www/html/index.html

<form method="POST" action="/dologin.html">
  Username: <input type="text" name="httpd_username" value="" />
  Password: <input type="password" name="httpd_password" value="" />
  <input type="submit" name="login" value="Login" />
</form>
```

Obr. A.21: ICMP Redirect – Konfigurace serveru Apache2

Dále server restartujeme pomocí příkazu „service apache2 restart“ a pomocí webového prohlížeče přejdeme na „http://10.20.10.55“. Měla by se zobrazit následující stránka:



Obr. A.22: ICMP Redirect – Ukázka úvodní stránky serveru Apache2

Konfigurace přepínače

Na přepínači nakonfigurujeme dvě sítě VLAN, přiřadíme k nim porty a následovně si pro kontrolu vypíšeme přehled sítí VLAN pomocí příkazů:

```
Switch#conf t
Switch(config)#vlan 10
Switch(config-if)#name Victim
Switch(config-if)#vlan 20
Switch(config-if)#name Target
Switch(config-if)#exit
Switch(config)#int range g1/0/10-11
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int g1/0/20
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
Switch#show vlan brief
```

```
10   Victim                           active    Gi1/0/10, Gi1/0/11
20   Target                           active    Gi1/0/20
```

Obr. A.23: ICMP Redirect – Výpis sítí VLAN

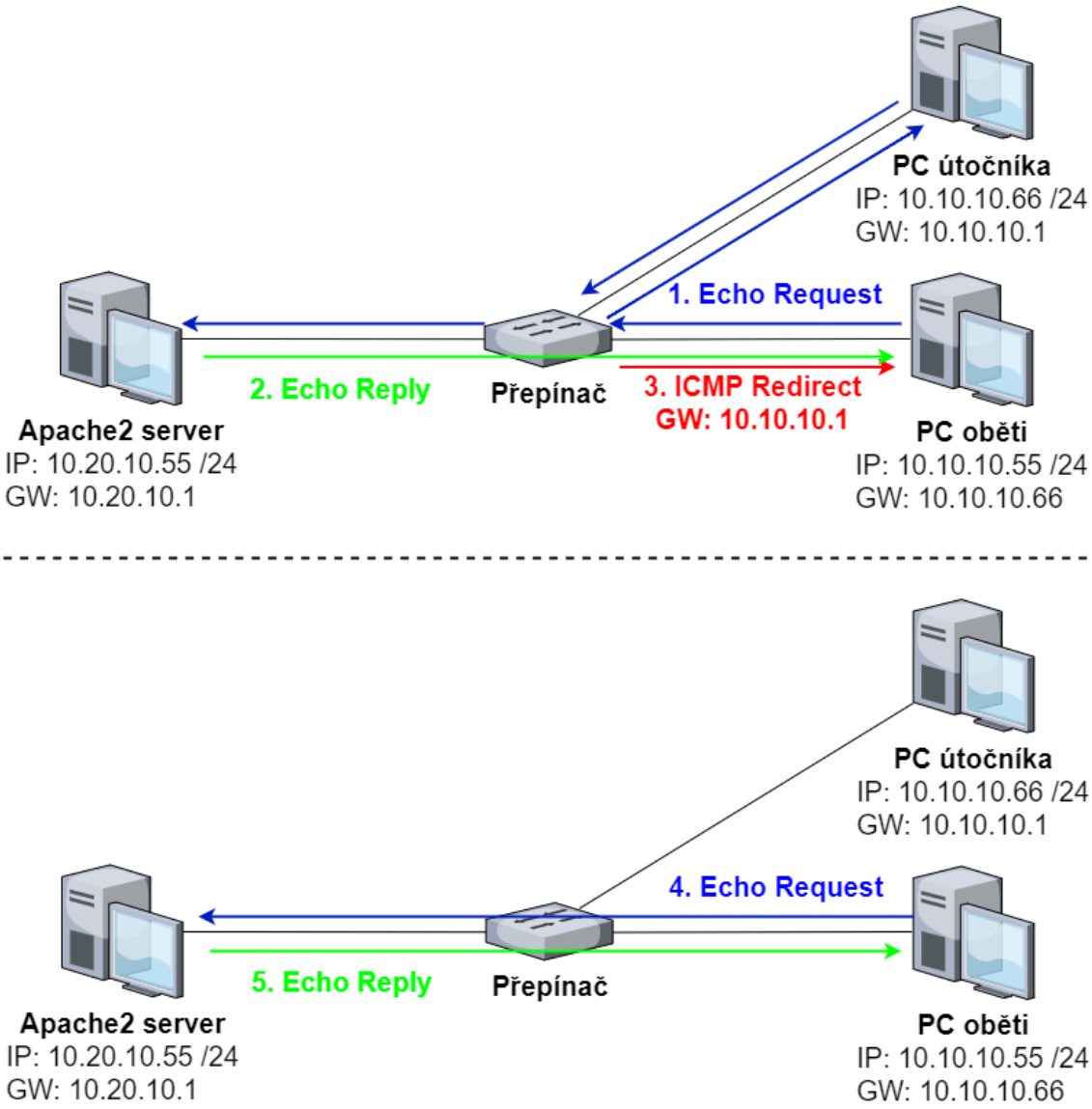
Příprava útoku

Nejprve ověříme konektivitu všech zařízení v síti pomocí příkazu ping. Pokud jsou pingy úspěšné, můžeme pokračovat dále. Pokud ne, nejspíše bude chyba někde v konfiguraci IP adres a výchozích bran.

Před provedením samotného útoku zjistíme, zda ICMP redirect funguje. Na PC oběti

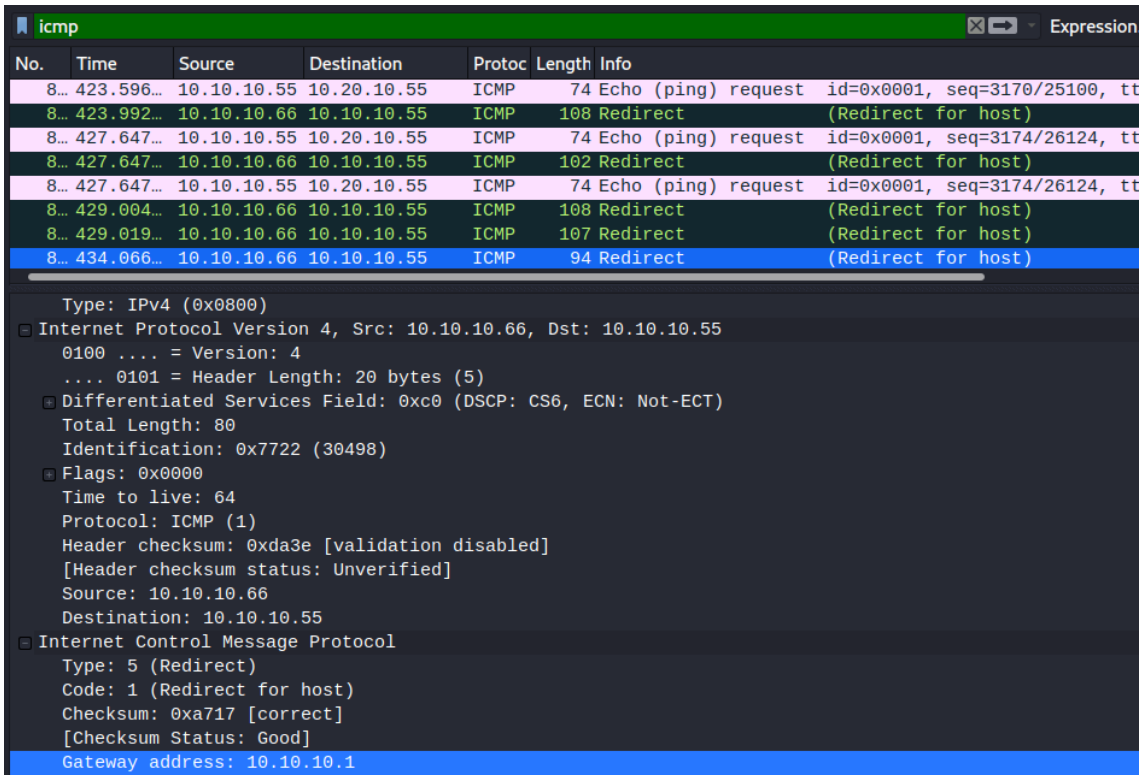
nastavíme výchozí bránu na „10.10.10.66“, tedy na PC útočníka. Posléze na PC oběti zadáme příkaz „ping 10.20.10.55 -t“. Echo request půjde následující cestou:

PC oběti –> Přepínač –> PC útočníka –> Přepínač –> Apache2 server. Na základě toho přepínač vygeneruje ICMP redirect s výhodnější cestou přes výchozí bránu „10.10.10.1“, pošle jej PC oběti a další Echo requesty už tím pádem půjdou cestou: PC oběti –> Přepínač –> Apache2 server.



Obr. A.24: ICMP Redirect – Test funkčnosti ICMP redirect

Samotný paket ICMP redirect můžeme sledovat ve Wiresharku s filtrem „icmp“.



Obr. A.25: ICMP Redirect – Wireshark; paket ICMP redirect

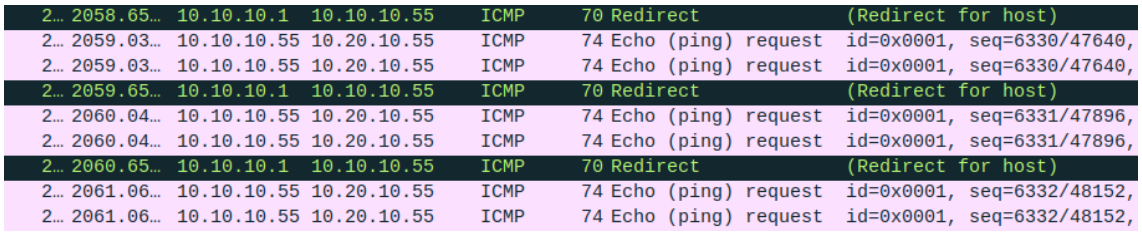
Pokud tahle zkouška funguje, nastavíme výchozí bránu PC oběti zpět na „10.10.10.1“ a můžeme se přesunout k samotnému útoku.

Provedení útoku

K provedení útoku použijeme nástroj „hping3“ pomocí kterého vygenerujeme paket ICMP redirect následujícím způsobem:

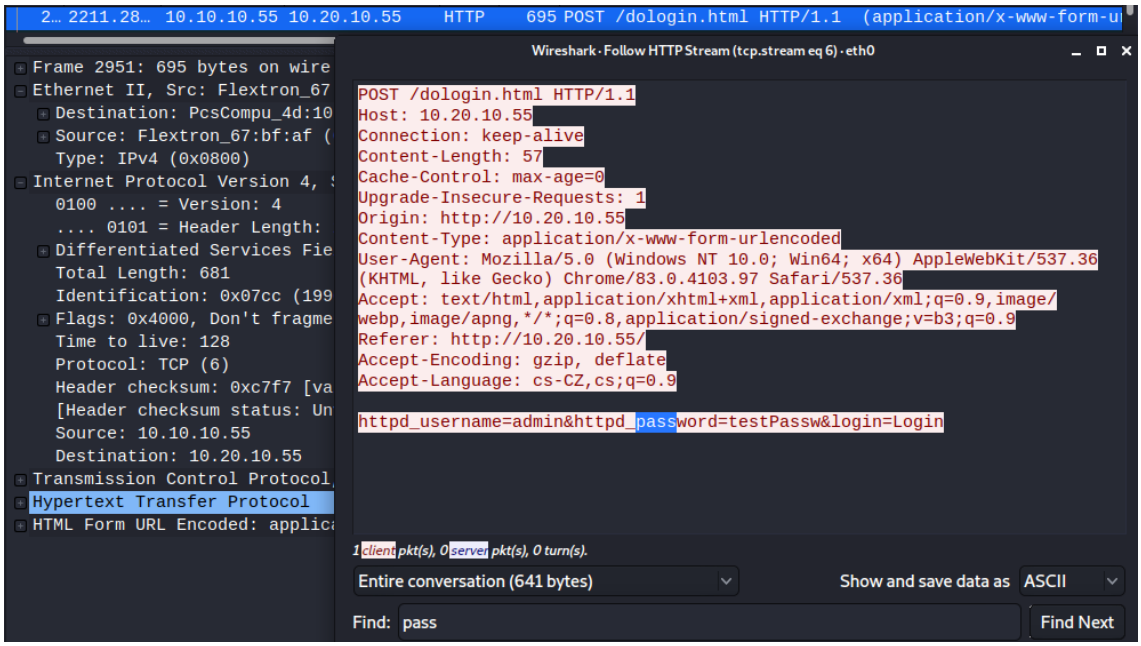
root@kaliLinux:~# hping3 10.10.10.55 -C 5 -K 1 -a 10.10.10.1 --icmp-gw 10.10.10.66 --icmp-ipdst 10.20.10.55 --icmp-ipsrc 10.10.10.55

Po zadání tohoto příkazu se začnou po určitých intervalech posílat pakety ICMP redirect na PC oběti, dokud příkaz nepřerušíme pomocí „Ctrl+C“. Můžeme opět vyzkoušet, zda přesměrování funguje pomocí příkazů ping z PC oběti na Apache2 server (ping 10.20.10.55 -t) a sledovat na PC útočníka pomocí Wiresharku, zda vše probíhá, jak má.



Obr. A.26: ICMP Redirect – Wireshark; přesměrování provozu na PC útočníka

Dále, pokud vše proběhlo vpořádku, se pomocí webového prohlížeče z PC oběti připojíme na Apache2 server a vyplníme náhodně přihlašovací údaje (např. username: admin, password: testPassw). Ve Wiresharku s filtrem „http“ je poté na PC útočníka pozorovat paket (kliknutím pravým tlačítkem myši na paket a vybráním volby „Follow –> HTTP Stream“) s přihlašovacími údaji.



Obr. A.27: ICMP Redirect – Wireshark; paket s přihlašovacími údaji

Kontrolní otázky

Na základě čeho je generován legitimní ICMP redirect?

Jak se dá ICMP redirectu zneužít?

Znáte jiné nástroje, které by se daly využít ke generování paketů ICMP redirect?

Jaké IP adresy je třeba znát k provedení tohoto útoku?

B Návrh na zapojení laboratorní úlohy – LAB 2

Upozornění: Nezkoušejte následující útoky v žádné veřejné ani jiné síti kromě laboratoře!

B.1 CAM Table Overflow

Cíl laboratorní úlohy

Cílem laboratorní úlohy je vyzkoušet si provedení útoku CAM table overflow, tedy zahltit CAM tabulku přepínače (k provedení DoS útoku) a následně na tomto přepínači nakonfigurovat ochranné opatření proti tomuto typu útoku.

Teoretický úvod

Tabulky CAM (content addressable memory), také nazývané tabulky MAC adres, se na přepínačích používají ke sledování, kam se má odesílat provoz pro konkrétní naučené adresy MAC. Pro pochopení skutečného účinku tohoto útoku je třeba porozumět základnímu fungování CAM tabulky a jak optimalizuje chování přepínače při přeposílání dat (forwarding).

Když je přepínač uveden do provozu, má prázdnou CAM tabulku. Neví, která zařízení jsou připojena ke kterým rozhraním, a proto zpočátku odesílá přijatý provoz na všechna rozhraní (flooding). Protože CAM tabulka přijímá provoz v každém rozhraní, vytváří položky pro každou z MAC adres, které vidí a spojuje každou adresu se svým specifickým rozhraním.

Jakmile má přepínač v CAM tabulce záznam pro konkrétní cílovou MAC adresu, nepřeposílá provoz na všechna rozhraní – místo toho odešle provoz pro tuto adresu do svého konkrétního naučeného rozhraní. Jakmile jsou MAC adresy všech připojených zařízení naučeny, a tím se zabrání zaplavování – přenos bude odeslán do naučeného rozhraní každého cíle. Tento výsledek výrazně optimalizuje chování přepínače při přeposílání a zvyšuje množství šířky pásma přepínače (za předpokladu, že se jedná o zaneprázdněný přepínač – jde přes něj velké množství provozu).

Každý přepínač má omezený počet MAC adres, které může CAM tabulka pojmout. Pokud je dosaženo limitu tabulky, veškerý provoz sestávající z neznámých MAC adres zaplaví síť. Útok CAM table overflow funguje tak, že jedno (či více) zařízení podvrhuje velké množství MAC adres a odesílá provoz přes přepínač. CAM tabulka přepínače bude zaplněna a veškerý další provoz (obvykle provoz z legitimních zařízení) bude nadbytečný, což způsobí, že přepínač bude velmi zaneprázdněn a potenciálně přetížen. V důsledku toho se síť zpomalí a nakonec se stane nepoužitelnou.

Ve zkratce to tedy znamená tři možnosti:

- V CAM tabulce se **nachází** záznam o cílové MAC adrese – přepínač odešle rámec pouze na rozhraní, na jehož konci je zařízení s danou MAC adresou.
- V CAM tabulce se **nenachází** záznam o cílové MAC adrese – přepínač odešle

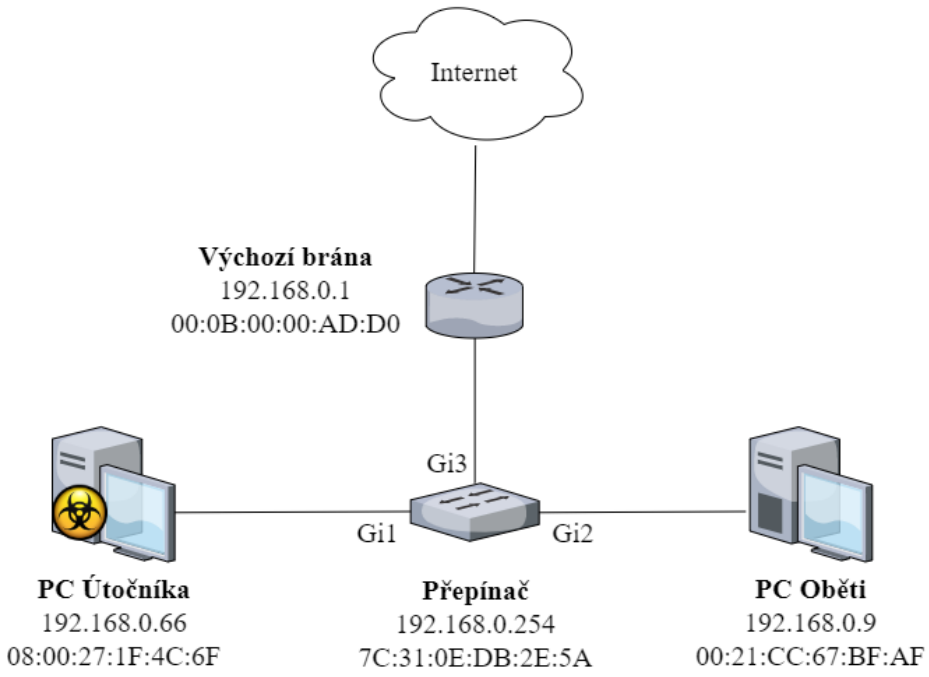
rámec na všechna svá rozhraní. Pokud z cílové MAC adresy obdrží odpověď, vytvoří si v CAM tabulce nový záznam MAC adresy korespondující s daným rozhraním.

- CAM tabulka je **plná** – nelze vytvořit nový záznam o MAC adrese. Pokud útočník podvrhuje velké množství náhodně generovaných MAC adres, výsledkem bude nejen naplnění kapacity CAM tabulky, ale také „vytlačení" legitimních MAC adres z tabulky. Další důsledky útoku CAM table overflow jsou následující:
  - ► Zahlcení výpočetní kapacity přepínače (DoS útok).
  - ► Provoz určený pro legitimní uživatele je poslán na všechna rozhraní (přepínač začne fungovat jako hub, tzn. veškerý přijatý provoz přeposílá na všechna rozhraní), tudíž i k útočníkovi, který je schopen pomocí tohoto útoku odposlouchávat veškerý provoz na síti (MITM útok).

Potřebné nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **PC oběti (Win 10)**
- **Přepínač (Cisco SG250)** na který budeme útočit
- **Směrovač** spojující lokální síť s internetem
- **Dsniff** k provedení samotného útoku (pomocí příkazu „apt-get install dsniff")
- **PuTTY** ke konfiguraci přepínače pomocí SSH

Topologie sítě



Obr. B.1: CAM Table Overflow – Topologie sítě

Konfigurace

Po sestavení topologie sítě je jediná důležitá věc, a to mít nastavené IP adresy v rozsahu lokální sítě. V tomto konkrétním případě jsou IP adresy obou PC (viz Obr. B.1) nastavené staticky a na síťových zařízeních vypnut protokol IPv6. Pokud máte nastavené přidělení IPv4 adresy automaticky, není co řešit, jen je třeba zjistit konkrétní přidělené IP adresy.

Dále je nutné nakonfigurovat IP adresu přepínače (pokud má nastavenou statickou IP adresu) pomocí příkazu „interface vlan 1“ v konfiguračním terminálu a následným zadáním „ip address 192.168.0.254 255.255.255.0“ (je nutné mít na paměti, že pro přístup pomocí SSH musí být počítač a přepínač na **stejné síti**, tedy pokud je IP adresa přepínače např. 192.168.100.254, je nutné nastavit IP adresu počítače z rozsahu sítě 192.168.100.0, tedy např. 192.168.100.66).

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.0.254
```

Obr. B.2: CAM Table Overflow – Nastavení IP adresy přepínače

Ve VM VirtualBox je ještě nutné nakonfigurovat síťové nastavení u Kali Linuxu pomocí „nastavení –> síť“ na síťový most.

Příprava útoku

Pomocí příkazu „ping“ vyzkoušíme konektivitu všech zařízení v lokální síti. Pokud je vše funguje jak má, vypíšeme si CAM tabulku na přepínači pomocí příkazu „show mac adress-table“.

```
Switch#show mac address-table
Flags: I - Internal usage VLAN
Aging time is 300 sec

    Vlan          Mac Address          Port       Type
------------ --------------------- ---------- ----------
       1          00:0b:00:00:ad:d0      gi3      dynamic
       1          00:21:cc:67:bf:af      gi2      dynamic
       1          00:d8:61:14:69:37      gi1      dynamic
       1          08:00:27:1f:4c:6f      gi1      dynamic
       1          7c:31:0e:db:2e:5a       0         self
```

Obr. B.3: CAM Table Overflow – Výpis CAM tabulky před útokem

Můžeme si všimnout, že s každým rozhraním je spjata jedna MAC adresa (pro Gi1 jsou to ovšem dvě, protože se bere v potaz síťová karta fyzického i virtuálního PC.

Dále můžeme zjistit limit CAM tabulky na přepínači pomocí příkazu „show mac address-table count“. V našem konkrétním případě je přepínač schopen pojmout 8192

MAC adres.

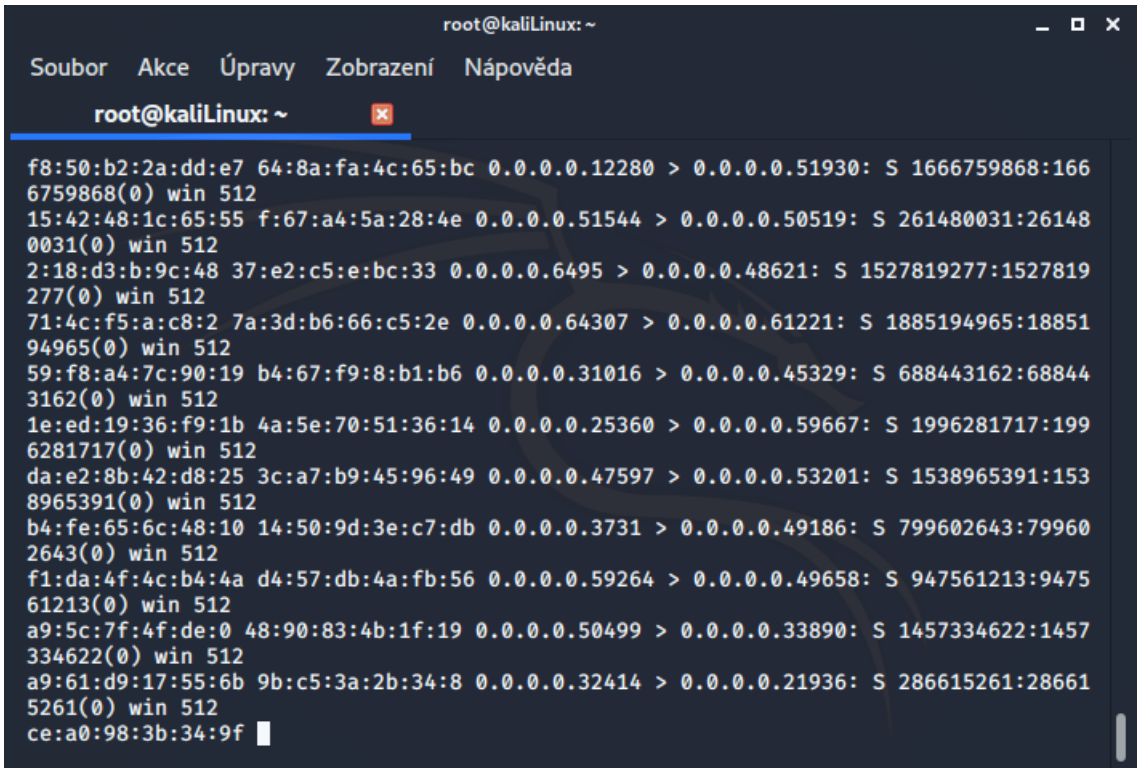
```
Switch#show mac address-table count
Capacity          : 8192
Free              : 8181
Used unicast      : 10
Used multicast    : 1
Used IPv4 hosts   : 0
Used IPv6 hosts   : 0
Secure            : 0
Dynamic unicast   : 9
Static unicast    : 0
Internal          : 1
```

Obr. B.4: CAM Table Overflow – Výpis počtu možných MAC adres v CAM tabulce

Na PC útočníka otevřeme konfigurační terminál a nainstalujeme balíček dSniff pomocí příkazu „apt-get install dsniff“, jehož součástí je utilita „macof“, kterou použijeme ke generování náhodných MAC adres, tedy k provedení útoku. Pomocí „macof -h“ je možné vypsat verzi programu a všechny příkazy, které „macof“ podporuje.

Provedení útoku

Nyní k samotnému útoku. Stačí jeden příkaz, a to „macof -i eth0“ (v našem případě je rozhraní „eth0“, pokud tento příkaz nefunguje, rozhraní se dá zjistit např. pomocí příkazu „ifconfig“).



Obr. B.5: CAM Table Overflow – Generování MAC adres

Následkem bude zahlcení přepínače falešnými MAC adresami, které budou všechny náležet rozhraní Gi1 (rozhraní, pomocí kterého je útočník připojen).

```
    Vlan          Mac Address          Port       Type
----------- -------------------- ---------- ----------
     1          00:00:3f:41:4d:47      gi1      dynamic
     1          00:00:58:4d:5d:01      gi1      dynamic
     1          00:03:87:6f:f8:db      gi1      dynamic
     1          00:04:a7:02:ac:71      gi1      dynamic
     1          00:0b:00:00:ad:d0      gi3      dynamic
     1          00:11:31:5a:9a:ec      gi1      dynamic
     1          00:12:f9:74:6b:c5      gi1      dynamic
     1          00:14:9c:4b:c8:3a      gi1      dynamic
     1          00:15:a1:2e:8c:cd      gi1      dynamic
     1          00:16:36:3f:07:b4      gi1      dynamic
     1          00:20:ee:2b:b8:8b      gi1      dynamic
     1          00:21:c0:34:bd:83      gi1      dynamic
     1          00:21:cc:67:bf:af      gi2      dynamic
     1          00:26:41:2c:e5:a7      gi1      dynamic
     1          00:2a:b7:4b:1b:db      gi1      dynamic
     1          00:2c:6b:25:ec:eb      gi1      dynamic
     1          00:2f:68:25:83:a9      gi1      dynamic
     1          00:3c:ab:2d:df:fe      gi1      dynamic
     1          00:3c:fd:18:f3:f2      gi1      dynamic
     1          00:40:f6:75:53:d2      gi1      dynamic
     1          00:49:36:33:44:dc      gi1      dynamic
     1          00:4b:3c:26:31:43      gi1      dynamic
More: <space>,  Quit: q or CTRL+Z, One line: <return>
```

Obr. B.6: CAM Table Overflow – CAM tabulka s falešnými MAC adresami

Tento případ vede k DoS útoku. Přepínač není schopen zvládat spojení PC oběti s internetem.

```
C:\Windows\system32>ping vutbr.cz

Pinging vutbr.cz [147.229.2.90] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 147.229.2.90:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Obr. B.7: CAM Table Overflow – Následek útoku (DoS)

Obrana proti útoku

Účinnou obrannou proti tomuto útoku je nastavení maximálního počtu MAC adres na jedno rozhraní na přepínači pomocí „port security“.

Případ přepínačů Cisco Catalyst - rozhraní je nutné přepnout do access mode pomocí příkazu „switchport mode access“. Poté zadáme příkazy „switchport port-security maximum 5“ a „switchport port-security“. Tímto je počet MAC adres na rozhraní Gi1 omezen na 5. Při dalším provedením útoku tedy nebude možné podvrhnout do CAM tabulky maximálně 5 MAC adres.

Případ přepínače Cisco SG250 – v konfiguračním terminálu zadáme příkaz „interface gi1“ a poté „port security max 5“, „port security trap 10“ a „port security discard“. Posléze vypíšeme tabulku zabezpečení portů pomocí příkazu „show ports security“. Tímto nastavením zabezpečení jsme způsobili, že lze do CAM tabulky k rozhraní Gi1 zapsat jen 5 MAC adres, zbytek bude zahozen s upozorněními každých 10 sekund.

```
Switch(config-if)#port security max 5
Switch(config-if)#port security trap 10
Switch(config-if)#port security discard
Switch(config-if)#end
Switch#show ports security

 Port      status      Learning       Action    Maximum    Trap    Frequency
-------- ---------- --------------- ---------- -------- -------- ----------
  gi1     Enabled    Max-Addresses   Discard       5     Enabled      10
  gi2     Disabled       Lock           -         1     Disabled     -
  gi3     Disabled       Lock           -         1     Disabled     -
  gi4     Disabled       Lock           -         1     Disabled     -
  gi5     Disabled       Lock           -         1     Disabled     -
  gi6     Disabled       Lock           -         1     Disabled     -
  gi7     Disabled       Lock           -         1     Disabled     -
  gi8     Disabled       Lock           -         1     Disabled     -
```

Obr. B.8: CAM Table Overflow – Port security

```
   Vlan          Mac Address          Port        Type
------------ --------------------- ---------- ----------
     1         00:0b:00:00:ad:d0       gi3      dynamic
     1         00:21:cc:67:bf:af       gi2      dynamic
     1         00:26:c6:51:33:ec       gi3      dynamic
     1         00:d8:61:14:69:37       gi1      dynamic
     1         04:95:e6:23:e9:d0       gi3      dynamic
     1         04:95:e6:45:bf:70       gi3      dynamic
     1         10:75:46:52:31:c8       gi1      dynamic
     1         34:e1:f5:6e:a1:da       gi1      dynamic
     1         62:8d:c8:11:e2:75       gi1      dynamic
     1         7c:31:0e:db:2e:5a        0        self
     1         ca:3e:c3:20:4f:0b       gi1      dynamic
     1         e4:e0:c5:80:f9:97       gi3      dynamic
```

Obr. B.9: CAM Table Overflow – Útok po nastavení port security

```
03-Jun-2020 19:32:39 %2SWPORT-W-LOCKPORTACTIVE: A packet with source MAC fe:47:50:65:c
c:58 tried to access through port gi1 which is locked

03-Jun-2020 19:32:49 %2SWPORT-W-LOCKPORTACTIVE: A packet with source MAC 56:93:74:51:9
e:a5 tried to access through port gi1 which is locked

03-Jun-2020 19:32:59 %2SWPORT-W-LOCKPORTACTIVE: A packet with source MAC cc:57:9b:52:a
2:05 tried to access through port gi1 which is locked

03-Jun-2020 19:33:09 %2SWPORT-W-LOCKPORTACTIVE: A packet with source MAC 84:0c:94:5b:e
7:2c tried to access through port gi1 which is locked

03-Jun-2020 19:33:19 %2SWPORT-W-LOCKPORTACTIVE: A packet with source MAC 54:5b:01:2b:6
2:4d tried to access through port gi1 which is locked

03-Jun-2020 19:33:29 %2SWPORT-W-LOCKPORTACTIVE: A packet with source MAC 78:f5:33:03:5
a:14 tried to access through port gi1 which is locked
```

Obr. B.10: CAM Table Overflow – Upozornění port security

Kontrolní otázky

K čemu slouží CAM tabulka?

Jakým způsobem se dá docílit zahlcení přepínače?

Jak se dá proti tomuto útoku bránit?

Jaký je rozdíl mezi přepínačem a hubem?

B.2 VTP Bomb

Cíl laboratorní úlohy

Cílem laboratorní úlohy je zkusit pomocí falešných VTP zpráv upravovat konfiguraci VLAN na přepínači.

Teoretický úvod

VLAN je jakákoli broadcastová doména, která je rozdělena a izolována v počítačové síti na linkové vrstvě – realizuje se na přepínačích. Sítě VLAN fungují tak, že aplikují tagy na síťové rámce a manipulují s těmito tagy v síťových systémech – vytvářejí vzhled a funkčnost síťového provozu, který je fyzicky v jediné síti, ale funguje tak, jako by byl rozdělen na samostatné sítě. Tímto způsobem mohou sítě VLAN udržovat síťové aplikace oddělené, přestože jsou připojeny ke stejné fyzické síti, a to bez nutnosti nasazení více sad kabelů a síťových zařízení. VLAN umožňuje správcům sítě seskupovat zařízení společně, i když nejsou přímo připojeni ke stejnému přepínači. Protože členství ve VLAN lze konfigurovat pomocí softwaru, může to výrazně zjednodušit návrh a realizaci zapojení sítě.

Když je do sítě přidán nový přepínač, ve výchozím nastavení je nakonfigurován bez názvu nebo hesla domény VTP, je v režimu serveru VTP. Pokud nebyl nakonfigurován žádný název domény VTP, předpokládá se název domény z prvního paketu VTP, který přepínač obdrží. Nový přepínač má revizi konfigurace VTP 0, a tak přijme jakékoli číslo revize a přepíše své VLAN informace, pokud se hesla VTP shodují.

Pokud by ovšem byl omylem připojen přepínač k síti se správným názvem a heslem domény VTP, ale s vyšším číslem revize VTP, než má síť aktuálně (např. přepínač, který byl ze sítě odstraněn kvůli údržbě a vrácen s vymazanými VLAN informacemi), pak by celá VTP doména přijala VLAN konfiguraci nového přepínače, což pravděpodobně způsobí ztrátu VLAN informací na všech přepínačích ve VTP doméně, a to následně povede k selhání v síti, protože přepínače Cisco udržují informace o konfiguraci VTP odděleně od běžné konfigurace.

Útočník může jako VTP server posílat falešné VTP zprávy (neboli VTP advertisements) na trunk porty přepínačů v režimu „klient“ a tím získat privilegium přidávání a odebírání sítí VLAN z VTP domény (např. aby vytvořil STP smyčku). Další škodlivé mohou být odeslány VTP zprávy bez jakékoliv konfigurace VLAN. Pokud netransparentní přepínač (tzn. v režimu „klient“ nebo „server“) obdrží takovou VTP zprávu, „zdědí“ číslo revize odesílajícího přepínače, což vede k DoS útoku, tedy výmazu všech sítí VLAN nakonfigurovaných ve VLAN databázi napříč celou VTP doménou.

Tento útok ovšem vyžaduje vysoké znalosti útočníka (tj. znalost jména VTP domény, heslo a detaily trunk potrů). Tyto informace mohou být získány skrz sociální inženýrství nebo důkladný průzkum sítě.

Potřebné nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)**
- **Yersinia (0.8.3)** k vygenerování falešné VTP zprávy
- **Přepínač (Cisco Catalyst 3650X)** s možností konfigurace VTP
- **PuTTY** pro připojení k přepínači pomocí sériové linky
- **Wireshark** ke sledování falešných VTP zpráv

Topologie sítě

Obr. B.11: VTP Bomb – Topologie sítě

Konfigurace PC útočníka

Pro instalaci všech potřebných nástrojů zadáme v konfiguračním terminálu sled příkazů „apt-get update“, „apt-get install yersinia“, „apt-get install putty“ a nakonec „apt-get install wireshark“.

Konfigurace směrovače

Pomocí nástroje PuTTY se sériovou linkou připojíme k přepínači pro jeho následovnou konfiguraci.

Aby tento útok fungoval, je důležité přepnout port na přepínači, ke kterému jsme s PC útočníka připojení, nakonfigurovat rozhraní (v našem případě „interface GigabitEternet1/0/39) na trunk mode (bez tohoto nastavení se neodesílají VTP zprávy) pomocí příkazu „switchport mode trunk“ (pokud přepínač hlásí chybu, je nutné změnit encapsulation na dot1q pomocí příkazu „switchport trunk encapsulation dot1q“).

Nyní je třeba konfigurace VTP pomocí příkazů „configure terminal“ pro spuštění konfiguračního terminálu, „set vtp domain lab.network“ pro nastavení VTP domény, „set vtp mode server“ pro režim VTP serveru a „vtp version 1“ pro nastavení VTP verze 1. Konfiguraci VTP lze vypsat pomocí příkazu „show vtp status“. Po výpisu si můžeme všimnout, že číslo revize je 0, jelikož nebyly zatím provedeny žádné konfigurace VLAN.

```
Switch#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : lab.network
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 70ca.9b80.f100
Configuration last modified by 0.0.0.0 at 1-8-06 02:17:34
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 1
Configuration Revision          : 0
MD5 digest                      : 0x2A 0x83 0xD6 0x32 0xBB 0x26 0xB7 0xEA
                                  0xCE 0xE8 0xC7 0x6D 0x13 0xF4 0xC0 0xFA
```

Obr. B.12: VTP Bomb – Výpis VTP statusu

Dále k vytvoření sítí VLAN. Stačí náhodně vytvořit např. 5 sítí VLAN (v našem případě VLAN 10, 20, 30, 40 a 50). Zkontrolovat sítě VLAN posléze můžeme pomocí příkazu „show vlan brief“.

Tím pádem se číslo revize a počet sítí VLAN navýší o 5.

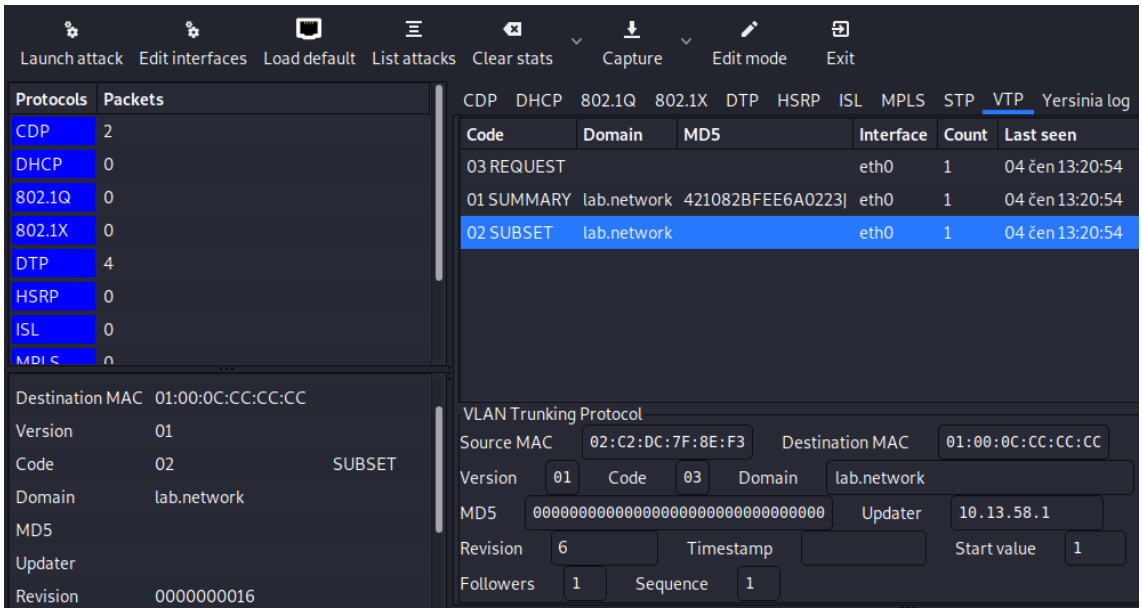
```
Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 6
Configuration Revision          : 5
MD5 digest                      : 0x2A 0x83 0xD6 0x32 0xBB 0x26 0xB7 0xEA
                                  0xCE 0xE8 0xC7 0x6D 0x13 0xF4 0xC0 0xFA
```

Obr. B.13: VTP Bomb – Navýšení čísla revize

Příprava útoku

Na PC útočníka spustíme grafické rozhraní nástroje Yersinia pomocí příkazu „yersinia -G“. V záložce „Edit interfaces“ zaškrtneme aktuálně používané rozhraní (např. eth0). Přepneme na záložku „VTP“, zvolíme „Launch attack“ a vybereme možnost „sending VTP packet“ ke zjištění, zda komunikace s VTP serverem funguje.

VTP server by měl na tento paket odpovědět, v nástroji Yersinia se tedy objeví záznamy o VTP doméně.



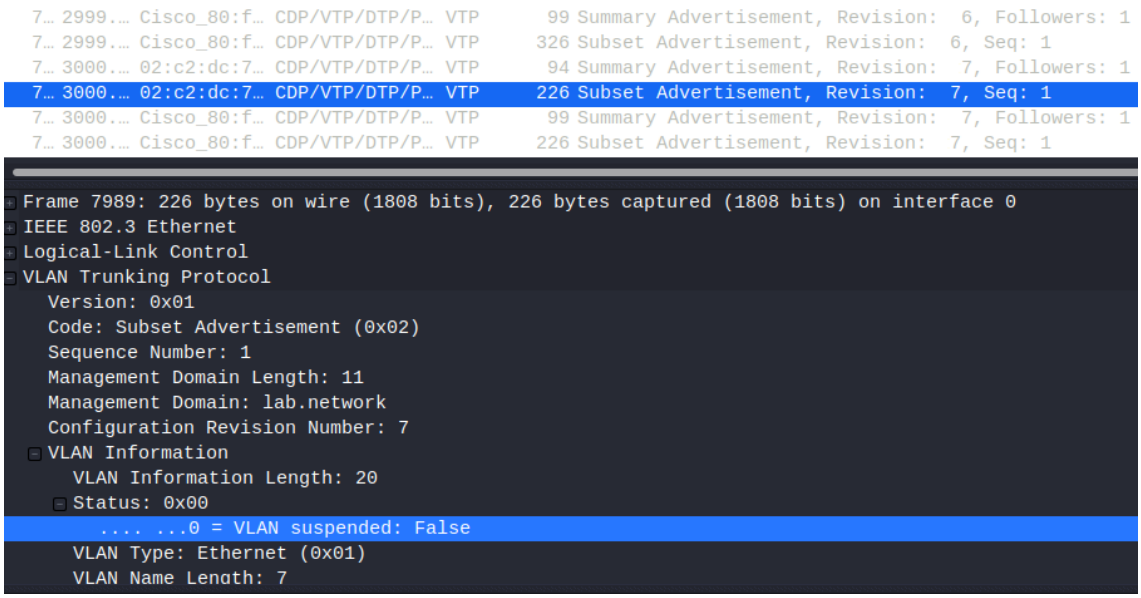
Obr. B.14: VTP Bomb – Informace o VTP doméně

Provedení útoku

Pro smazání veškerých sítí VLAN vybereme volbu „deleting all VTP vlans“ v Launch attack. Poté je nutné zvolit „sending VTP packet“, následně bude odeslána falešná VTP zpráva s číslem revize 6, která bude mít za následek vymazání všech sítí VLAN.

```
Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 1
Configuration Revision            : 6
MD5 digest                        : 0x84 0xDE 0xAB 0xD0 0x0E 0x8B 0xC5 0x25
                                    0x17 0x5E 0x90 0x0E 0x46 0x52 0xA0 0xF9
```

Obr. B.15: VTP Bomb – Vymazání všech sítí VLAN



Obr. B.16: VTP Bomb – Záznam VTP zpráv v nástroji Wireshark

Je také možné otestovat přidání podvržených sítí VLAN pomocí „adding one vlan“ nebo „deleting one vlan“ v Launch attack, kde vybereme VLAN ID (pro přidání i odebrání) a název VLAN (pouze u přidávání). Stejně jako u odstraňování všech sítí VLAN se v „List attacks“ vytvoří fronta zadaných útoků, které jsou uskutečněny po odeslání další falešné VTP zprávy (u přidávání sítí VLAN se ovšem přidá vždy pouze jedna, ikdyž je jich ve frontě víc).

Kontrolní otázky

Stručně popište základní fungování VTP

Jaký je rozdíl mezi režimy VTP (transparent, client, server)?

Jak může neznalý uživatel bez úmyslu uškodit síti a provést útok VTP bomb?

K čemu slouží sítě VLAN?

B.3 Útok na STP

Cíl laboratorní úlohy

Cílem této laboratorní úlohy je stát se kořenovým mostem v topologii STP a tím pádem moci odchytávat provoz v síti.

Teoretický úvod

STP (Spanning Tree Protocol) je síťový protokol, který vytváří logickou topologii bez smyček pro sítě Ethernet. Základní funkcí STP je zabránit přemostění smyček a broadcastovému vysílání, které z nich vyplývá. Spanning tree také umožňuje, aby návrh sítě zahrnoval záložní odkazy, které poskytují odolnost proti chybám, pokud aktivní spojení selže. Jak název napovídá, STP vytváří kostru grafu (spanning tree) v síti propojených mostů linkové vrstvy a zakáže ty odkazy, které nejsou součástí kostry grafu, a ponechává jedinou aktivní cestu mezi dvěma libovolnými síťovými uzly. Potřeba STP vznikla, protože přepínače v lokálních sítích jsou často propojeny pomocí redundantních odkazů, aby se zlepšila odolnost v případě selhání jednoho spojení. Tato konfigurace připojení však vytváří přepínací smyčku vedoucí k „broadcast radiation“ (kumulace broadcastového a multicastového provozu v síti) a nestabilitě tabulky MAC adres. Pokud se pro připojení přepínačů používají redundantní (přebytečná) spojení, je třeba se vyhnout přepínacím smyčkám. Aby se předešlo problémům spojeným s redundantními spoji v přepínané LAN, je do přepínačů implementován STP pro sledování topologie sítě. Každá vazba mezi přepínači, zejména nadbytečné propojení, je katalogizována. STP pak deaktivuje nadbytečná spojení nastavením jednoho preferovaného spojení mezi přepínači v síti LAN. Toto preferované spojení se používá pro všechny rámce Ethernet, pokud ovšem neselže. V takovém případě je povoleno nepreferované redundantní spojení. Když je implementován v síti, STP označí jeden přepínač jako root bridge (kořenový most). Na tomto kořenovém mostu se vypočítají preferovaná a nepreferovaná spojení. Přepínač, zvolený jako kořenový most, neustále komunikuje s ostatními přepínači v síti LAN pomocí BPDUs.

Primární funkcí STP je tedy odstranění potenciálních smyček v síti. Bez STP by v mnoha případech L2 LAN sítě jednoduše přestaly fungovat, protože smyčky vytvořené v síti zaplavily přepínače nadbytečným provozem. Optimalizovaný provoz a konfigurace STP zajišťuje, že síť LAN zůstává stabilní a že provoz vede po síti nejoptimalizovanější cestou. Všechny porty přepínačů v síti, kde je STP nastaven, jsou kategorizovány:

- **Root** – port s nejnižší cenou cesty k root bridge
- **Blocking** – blokovaný port, který by způsobil přepínací smyčku, kdyby byl aktivní. Aby se zabránilo použití smyčkových cest, nejsou přes blocking port odesílána ani přijímána žádná uživatelská data. Data BPDU jsou stále přijímána v stavu blocking. Blokovaný port může přejít do režimu forwarding, pokud

ostatní používané odkazy selžou a algoritmus STP určí, že port může přejít do stavu forwarding.

- **Listening** – přepínač zpracovává BPDU a čeká na možné nové informace, které by způsobily návrat do stavu blocking. Nezaplňuje tabulku MAC a nepředává rámce.
- **Learning** – zatímco port ještě nepředává rámce, učí se zdrojové adresy z přijatých rámců a přidává je do tabulky MAC.
- **Forwarding** – port v normálním provozu, který přijímá a předává rámce. Port monitoruje příchozí BPDUs, které by naznačovaly, že by se měl vrátit do stavu blocking, aby se zabránilo smyčce.
- **Disabled** – správce sítě ručně port manuálně zakázal

Pokud útočník vloží do sítě nové zařízení STP a pokusí se změnit fungování protokolu na tomto zařízení, má tento útok potenciál ovlivnit provoz datového toku přes síť LAN, což má výrazný dopad použitelnost a bezpečnost síťového provozu.

Pro pochopení zranitelnosti STP, je důležité vědět, jak STP funguje. STP tvoří stromovou topologii s kořenovým mostem (root bridge) na základně. Kořenový most se volí na základě dat sdílených v datových jednotkách STP, tzv. BPDUs (bridge protocol data units). Rámce BPDU jsou zasílány na známé multicastové adresy a obsahují, mimo jiné, MAC adresu přepínače a uživatelem definovanou hodnotu priority. Kombinace těchto hodnot se nazývá ID mostu (bridge ID) a přepínač s nejnižším ID je zvolen jako kořenový most.

Po volbě kořenového mostu najde každý přepínač v síti rozhraní, které vede k nejlepší cestě ke kořenovému mostu a označí jej jako kořenový port (root port), zatímco přebytečné rozhraní jsou přepnuty do blokovacího režimu (blocked port). Všechna aktivní rozhraní na přepínači budou nakonec buď v režimu přesměrování(forwarding), nebo v režimu blokování. Tento proces se nazývá konvergence.

Změny topologie, jako například přidání nových přepínačů mohou způsobit, že bude zvolen nový kořenový most a doména STP bude znovu procházet konvergencí. Čas potřebný k dokončení procesu je výrazný a během této doby se nepředává žádný provoz.

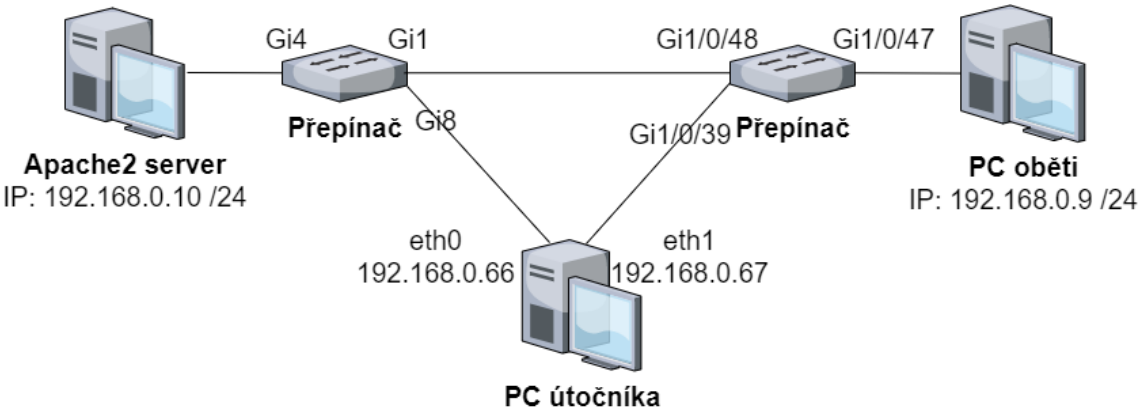
STP navíc sám o sobě nemá absolutně žádné zabezpečovací mechanismy. BPDU jsou vyměňovány v prostém textu (plain text) a neexistuje žádný mechanismus autentizace. Přepínač důvěřuje všem BPDU rámcům, které obdrží. Na základě těchto informací je snadné vydedukovat, že STP lze zneužít následujícími způsoby způsoby:

- **DoS útoky –** odesláním „ručně“ vytvořených BPDU není obtížné převzít roli kořenového mostu, což způsobí, že významná část provozu bude přesunuta na zařízení útočníka. I v případě nepřevzetí role kořenového mostu útočníkem, je možné (odesláním BPDU s oznámeními o změně topologie v krátkých intervalech) způsobit narušení provozu opakovaným vynucením konvergence.
- **MITM útoky** – v některých případech se může zařízení útočníka (pomocí propagace nízké priority mostu) stát kořenovým mostem. To způsobí, že přes něj projde významná část provozu, kterou lze zkopírovat, upravit a předat do skutečného cíle.

Potřebné nástroje

- **PC útočníka (Kali Linux ve VM VirtualBox)** se dvěma síťovými kartami
- **PC oběti (Win 10)**
- **PC cíle (Linux Mint)** se serverem Apache2
- **Přepínač (Cisco Catalyst 3650X)**
- **Přepínač (Cisco SG 250)**
- **Yersinia** (apt-get install yersinia) k vytvoření paketu na převzetí root bridge
- **Wireshark** (apt-get install wireshark) k odchytávání provozu na síti
- **Bridge utils** (apt-get install bridge-utils) k vytvoření síťového mostu na PC útočníka
- **Bittwist** (apt-get install bittwist) k poslání paketu zachyceného wiresharkem
- **PuTTY** (apt-get install putty) ke konfiguraci přepínačů

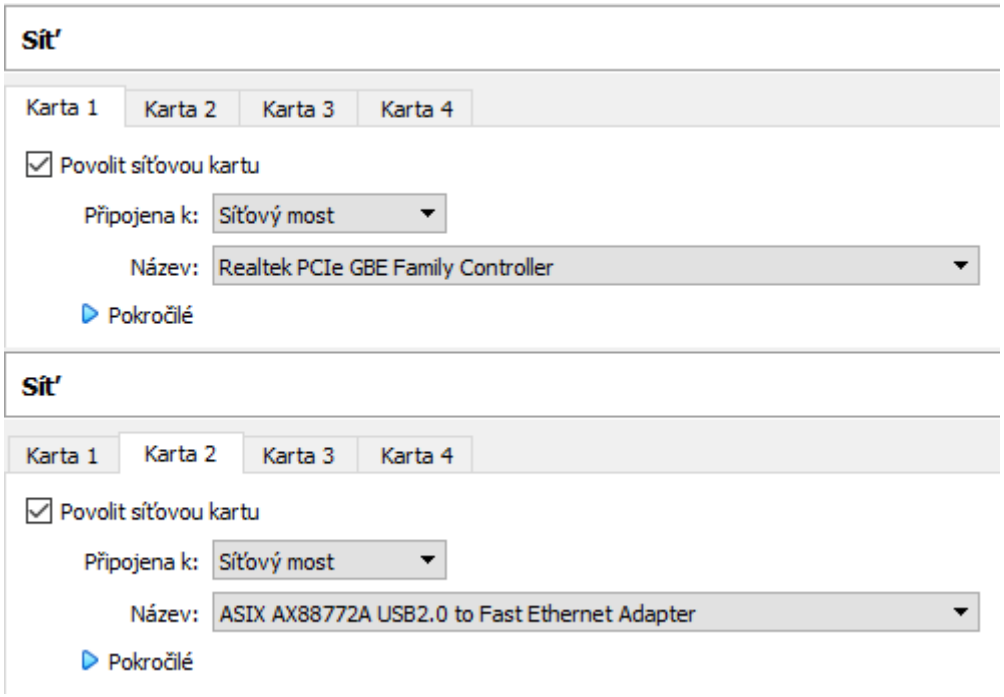
Topologie sítě



Obr. B.17: STP – Topologie sítě

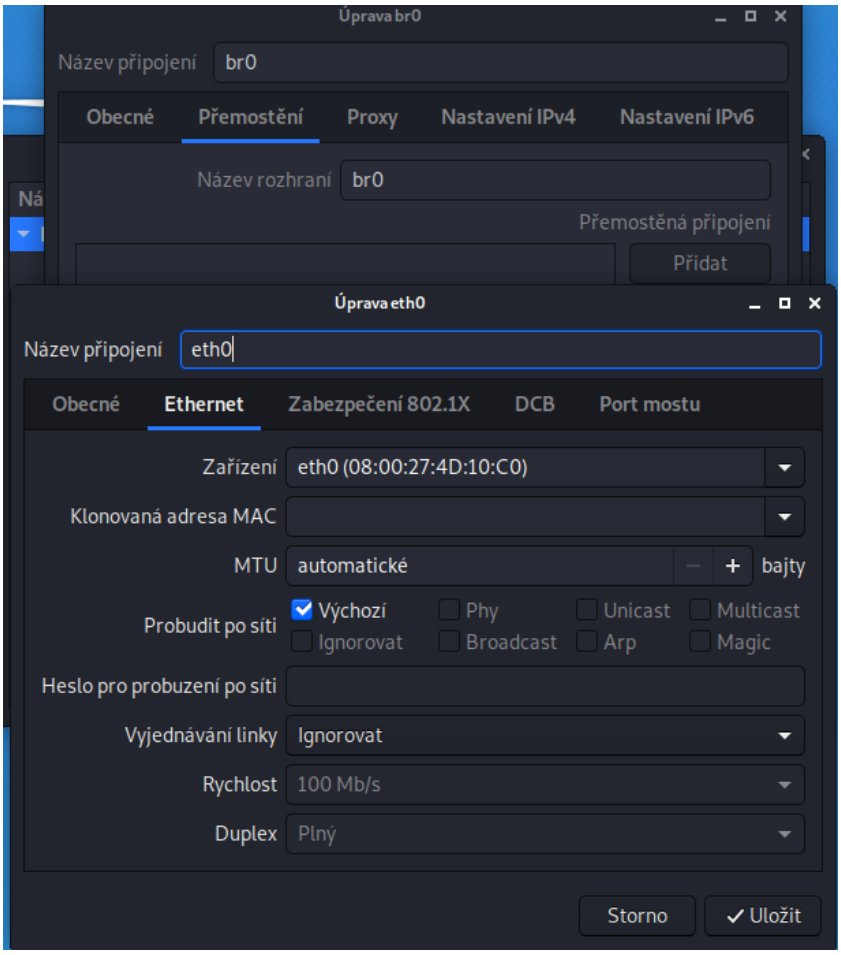
Konfigurace PC útočníka

Ještě před spuštěním virtuálního stroje je třeba nastavit síť onoho virtuálního PC pomocí „Nastavení –> Síť“ po zvolení Kali Linuxu ve VM VirtualBoX. V nastavení sítě povolíme dvě síťové karty, na kterých nastavíme „Síťový most“.



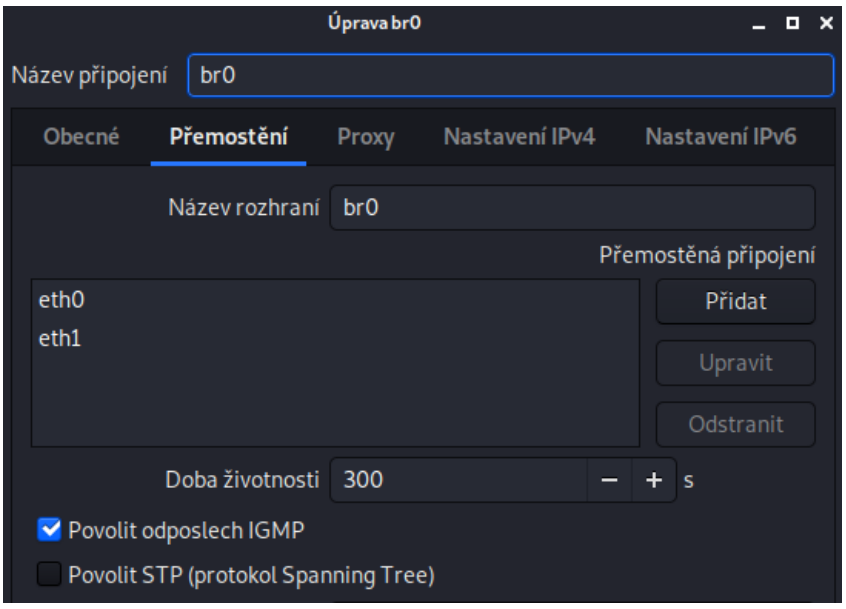
Obr. B.18: STP – Síťové nastavení PC útočníka

Na PC útočníka nainstalujeme pomocí konfiguračního terminálu nástroje: Wireshark, Yersinia, Bittwist a PuTTY. Dále je třeba nastavit přemostění sítě (aby se PC útočníka chovalo jako přepínač a aby přes něj mohl jít provoz, když se z něj stane root bridge). Přemostění se dá nastavit v „Síťová připojení“ tlačítkem se značkou „+“, kde vybereme typ připojení „Přemostění“ a dáme vytvořit. Přemostění pojmenujeme např. „br0“ a přidáme do něj síťová rozhraní (v tomto případě „eth0“ a „eth1“) pomocí „Přidat“ a vybráním typu připojení „Ethernet.



Obr. B.19: STP – Přidání rozhraní eth do přemostění

Síťové přemostění by mělo vypadat následovně:



Obr. B.20: STP – Nastavení přemostění sítě

Poté je nutné PC restartovat, aby byla konfigurace přemostění platná.

Konfigurace PC oběti

Na PC oběti stačí nakonfigurovat statickou IP adresu „192.168.0.9“.

Konfigurace PC cíle

Na PC cíle nainstalujeme pomocí konfiguračního terminálu server Apache2 příkazem „apt-get install apache2“ a nastavíme IP adresu na „192.168.0.10“. Po instalaci by měl být server přístupný z jakéhokoliv webového prohlížeče na URL „http://192.168.0.10“. Pro účel této laboratorní práce si na úvodní stránce serveru Apache2 nakonfigurujeme jednoduché přihlašovací rozhraní, na které se bude „přihlašovat“ PC oběti. Webový server můžeme upravit pomocí textového editoru „nano /var/www/html/index.html“.

```
  GNU nano 2.5.3         File: /var/www/html/index.html

<form method="POST" action="/dologin.html">
  Username: <input type="text" name="httpd_username" value="" />
  Password: <input type="password" name="httpd_password" value="" />
  <input type="submit" name="login" value="Login" />
</form>
```

Obr. B.21: STP – Konfigurace serveru Apache2

Dále server restartujeme pomocí příkazu „service apache2 restart“ a pomocí webového prohlížeče přejdeme na „http://10.20.10.55“. Měla by se zobrazit následující stránka:

Username: Password: Login

Obr. B.22: STP – Ukázka úvodní stránky serveru Apache2

Konfigurace přepínačů

Na obou přepínačích nastavíme spanning tree následovně:

```
Switch#conf t
Switch(config)#spanning tree mode rapid-pvst
Switch(config)#spanning tree vlan 1 priority 32768
Switch(config)#int g1/0/39
Switch(config-if)#spanning-tree cost 4
Switch(config)#int g1/0/47
Switch(config-if)#spanning-tree cost 4
Switch(config-if)#int g1/0/48
Switch(config-if)#spanning-tree cost 4
Switch(config-if)#end
Switch#show spanning-tree
```

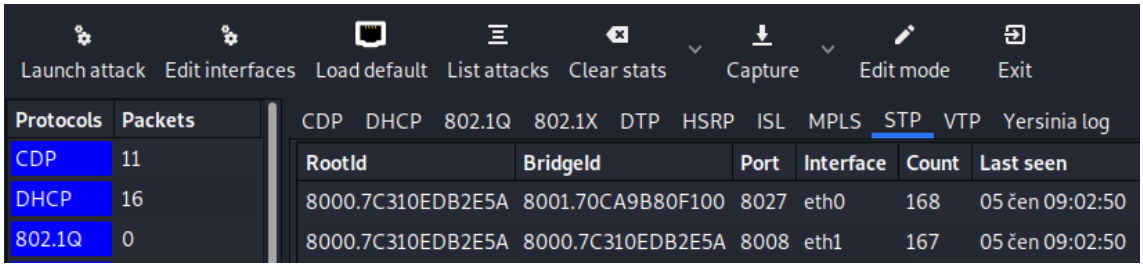
```
Switch(config-if)#do sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32768
              Address     7c31.0edb.2e5a
              Cost        4
              Port        39 (GigabitEthernet1/0/39)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     70ca.9b80.f100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/39            Root FWD 4         128.39   P2p
Gi1/0/47            Desg FWD 4         128.47   P2p
Gi1/0/48            Altn BLK 4         128.48   P2p
```

Obr. B.23: STP – Výpis spanning tree na přepínači

Nakonfigurovali jsme tedy mód spanning tree na PVST (per vlan spanning tree), path cost na „4“ a prioritu obou směrovačů na „32768“.

Provedení útoku

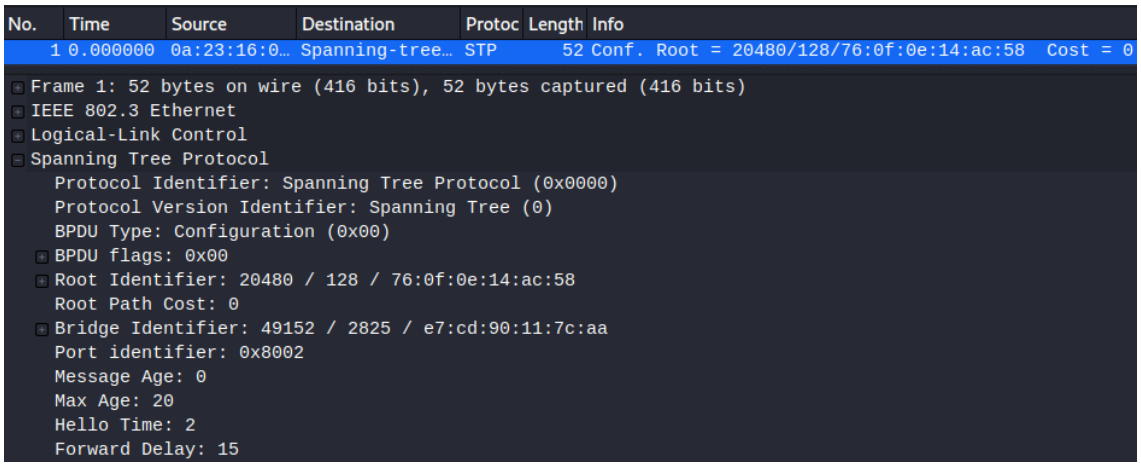
Na PC útočníka spustíme grafické rozhraní nástroje Yersinia příkazem „yersinia -G“. Přejdeme na záložku STP a měli bychom vidět oba přepínače v topologii spanning tree (musejí být povolena obě šíťová rozhraní eth0 i eth1“ pomocí „Edit interfaces“).



Obr. B.24: STP – Yersinia; zobrazení přepínačů

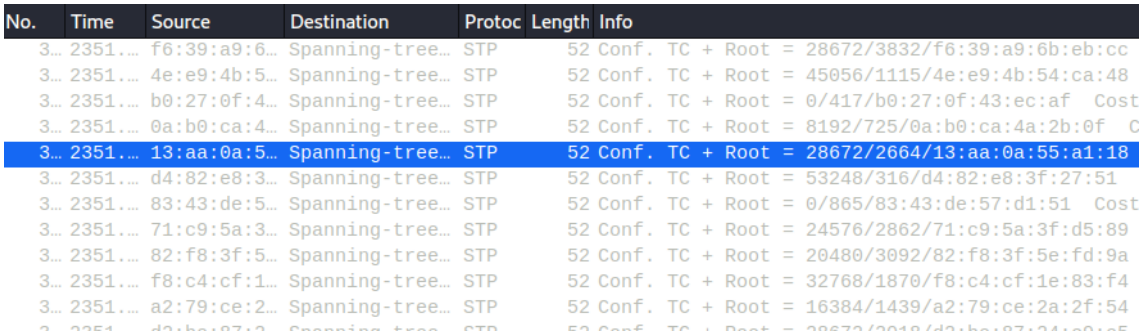
Nyní dáme „Launch attack“ a vybereme „Claiming Root Role With MiTM“ a následně se objeví tabulka, do které napíšeme rozhraní eth0 a eth1.

Nyní je v „List attacks“ útok ve frontě a je nutné jej spustit pomocí dalšího kliknutí na „Launch attack –> Sending conf BPDU“. Tímto vygenerujeme jeden STP paket, který zajistí naše vítězství ve volbě root bridge, protože priorita tohoto paketu bude menší, než 32768. Ovšem tím, že spanning tree posílá zprávy každé 2 sekundy, po uplynutí tohoto času se stane root bridgem opět předchozí přepínač. Tento paket můžeme sledovat pomocí nástroje Wireshark.



Obr. B.25: STP – Wireshark; paket na převzetí role root bridge

Zkusíme tedy možnost „Launch attack –> Sending conf BDPUs“, která zapříčiní neustálé odesílání útoku, dokud ho nepřerušíme. Tato volba je ovšem nestabilní, protože se pakety generují moc rychle a tím pádem se jedná spíše o DoS útok, než MiTM.

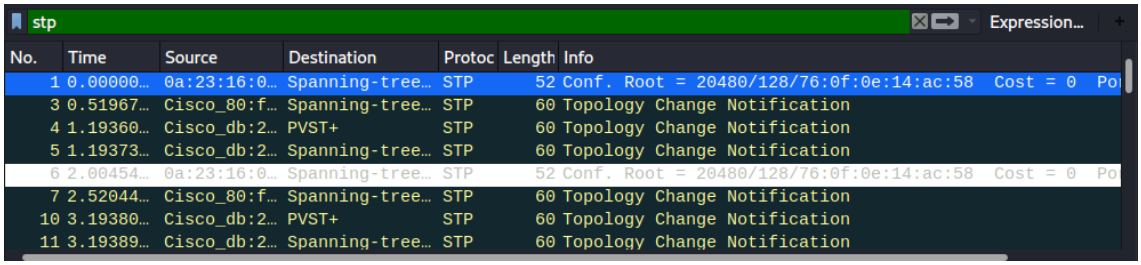


Obr. B.26: STP – Wireshark; generování STP BPDUs

Přistoupíme tedy k účinnější metodě MiTM útoku. Jeden z paketů vygenerovaných nástrojem Yersinia ve Wiresharku zvolíme a pomocí „File –> Extract Specified Packets…“ jej stáhneme do souboru např. „STPConfPacket.pcap“. Máme tedy jeden paket, který zaručí, že se PC útočníka stane root bridgem. Nyní k odesílání tohoto paketu v intervalu 2 sekund. Pro tento účel využijeme nástroj „Bittwist“ a funkci „watch“. Tohoto docílíme zadáním příkazu:

watch bittwist -i br0 /root/STPConfPacket.pcap

Obr. B.27: STP – Provedení útoku pomocí nástroje Bittwist



Obr. B.28: STP – Wireshark; sledování útoku

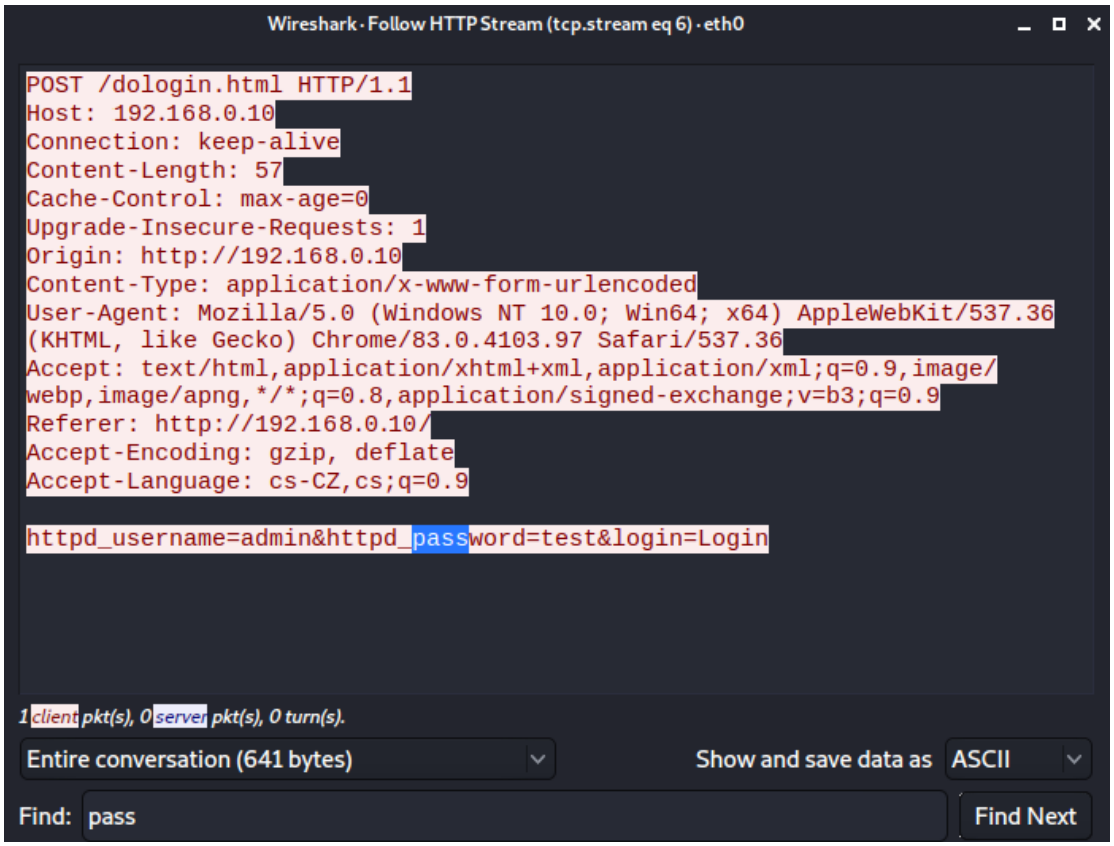
Nyní můžeme na jednom z přepínačů zadat příkaz „show spanning-tree“ pro kontrolu, zda útok funguje.

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    20608
              Address     760f.0e14.ac58
              Cost        4
              Port        39 (GigabitEthernet1/0/39)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     70ca.9b80.f100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/39            Root FWD 4         128.39   P2p Peer(STP)
Gi1/0/47            Desg FWD 4         128.47   P2p
Gi1/0/48            Altn BLK 4         128.48   P2p
```

Obr. B.29: STP – Výpis spanning tree

Jde vidět, že root bridge je nyní na portu „Gi1/0/39“ (tedy na portu, který vede k PC útočníka). Útok tedy funguje.

Nyní na PC oběti otevřeme webový prohlížeč a do vyhledávání zadáme adresu serveru Apache2 „http://192.168.0.10“ a zadáme náhodné přihlašovací údaje (např. username: „admin“ a password: „test“) . Paket s přihlašovacími údaji uvidíme ve Wiresharku a když na něm klikneme pravým tlačítkem myši a následovně „Follow –> HTTP Stream“, do vyhledávání napíšeme „pass“ pro najiří hesla a uvidíme zadané přihlašovací údaje, které byly odeslané přes PC oběti díky naší roli root bridge.



Obr. B.30: STP – Odchycení hesla

Obrana proti útoku

Jsou dva způsoby, kterými se dá bránit proti útoku převzetí root bridge, které následovně vyzkoušíme a budeme sledovat jejich efekt napsáním „show spanning-tree“ po jejich aktivaci:

- **BPDU Filter** – dá se nastavit na určitém portu příkazem „spanning-tree bpdufilter enable“. Plní funkci toho, že pokud na tento port přijde jakýkoliv BPDU paket, je zahozen. Tohle má bohužel za následek selhání topologie sítě STP a v síti se vytvoří smyčka (všechny porty přejdou do stavu forwarding).

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/39            Desg FWD 3         128.39   P2p
Gi1/0/47            Desg FWD 4         128.47   P2p
Gi1/0/48            Root FWD 4         128.48   P2p


Switch(config-if)#
*Jan  9 04:57:31.113: %SW_MATM-4-MACFLAP_NOTIF: Host 0021.cc67.bfaf in vlan 1 is
 flapping between port Gi1/0/48 and port Gi1/0/39
Switch(config-if)#
*Jan  9 04:57:33.378: %SW_MATM-4-MACFLAP_NOTIF: Host 0021.cc67.bfaf in vlan 1 is
 flapping between port Gi1/0/39 and port Gi1/0/48
*Jan  9 04:57:33.378: %SW_MATM-4-MACFLAP_NOTIF: Host 7c31.0edb.2e5a in vlan 1 is
 flapping between port Gi1/0/39 and port Gi1/0/48
```

Obr. B.31: STP – BPDU filtr (port Gi1/0/39)

- **BPDU Guard** – dá se na určitém portu nastavit pomocí „spanning-tree bpduguard enable“. Má za následek přepnutí portu do stavu blokování po přijetí paketu BPDU.

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     7c31.0edb.2e5a
             Cost        4
             Port        48 (GigabitEthernet1/0/48)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     70ca.9b80.f100
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/47            Desg BLK 4         128.47   P2p
Gi1/0/48            Root FWD 4         128.48   P2p
```

Obr. B.32: STP – BPDU guard (port Gi1/0/39)

Kontrolní otázky

Jakou funkci plní STP?

Jaké stálé stavy mohou mít porty v STP doméně a podle čeho se určují?

Jaký je rozdíl mezi BPDU guard a BPDU filter a jaký mají následek na STP doménu?

Podle jakého parametru se určí root bridge, pokud mají všechny přepínače stejnou prioritu a cenu cesty?