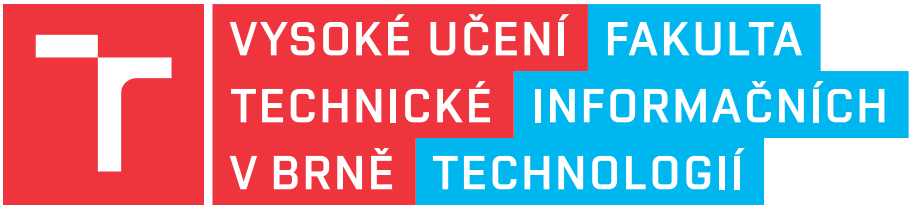


PDS 2016/2017: Projekt
L2 MitM

Dávid Mikuš
xmikus15@stud.fit.vutbr.cz

23. apríla 2017

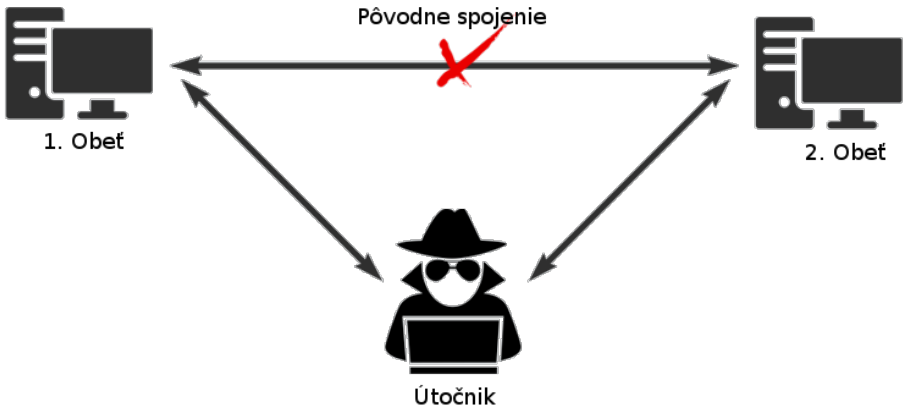
1 Man in the Middle

Man in the Middle *(človek medzi)* `MitM` je typ útoku kde sa útočnik do komunikácie medzi dvoma obetmi. Utočník sa javí pre prvú obeť ako druhá obeť a platí to aj naopak. Útočnik potom môže odpočúvat komunikáciu, alebo aj aktívne zasahovať a meniť zasielané dáta.

Pre dosiahnutie daného stavu sa používaju rôzne techniky:

1. ARP[1]/NDP[2] Spoofing - pomocou falošných správ sa podvrhne obeti útočnikova MAC adresa pre legitimnú IP adresu druhej obete
2. IP Spoofing - úťocnik sa maskuje ako aplikácia modikovaním hlavičiek paketu v IP adrese
3. DNS Spoofing - útočnik modifikuje DNS cache obete a mení záznamy o webovej adrese

[1] Address Resolution Protocol
[2] Neighbor Discovery Protocol



Obr. 1: Znázornenie komunikácie počas MitM útoku

2 Implementácia

Program bol implementovaný v jazyku C++ a je rozdelený do 3 častí:

1. Scanner - skenuje IP adresy v sieti a ich MAC adresy
2. Spoofer - mení obetiam MAC adresy ku IP adresám obete v cache
3. Intercept - vykonáva MitM útok

2.1 Scanner

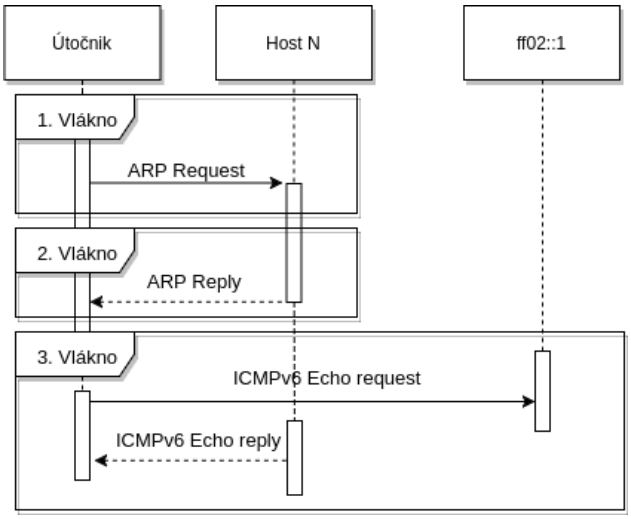
Scanner vyhľadáva IP adresy a priraďuje ich ku jednotlivým MAC adresám. Nezávisle sa skenujú `IPv4` a `IPv6` adresy. Ako vstup je meno rozhrania na ktorom sa bude vykonávať sken. Počas toho sa ukladáju adresy do tabuľky. Po skončení skenu je tabuľka uložena do XML súboru.

2.1.1 IPv4

Skenovanie `IPv4` adries je vykonané pomocou zasielaní `ARP` paketov. Z rozhrania sa získa IP adresa a adresa siete. Z ních sa získaju všetky IP adresy v sieti. V 1. vlákne je na každú túto adresu zaslaný `ARP Request`, medzi každým zaslaním je `10ms` rozostup. V 2. vlákne sa zachytáva každý `ARP Reply` paket, z ktorého sa získa `MAC` a `IPv4` adresa odosielateľa a uloži sa do tabuľky.

2.1.2 IPv6

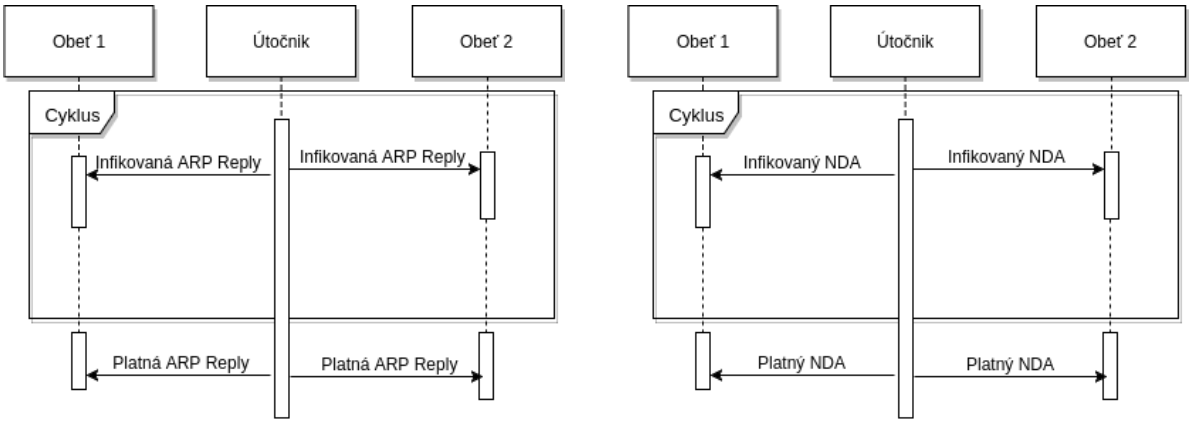
Pre skenovanie `IPv6` adries sa dá vykonať viacerými spôsobmi. Najjednoduchšie riešenie bolo zaslať `ICMPv6 Echo request` na adresu `ff02::1` kde sa nachádzaju všetky uzly v sieti. Na tento požiadavok môžu zariadenia odpovedať ale aj nemusia. Scanner zachytáva všetky `IPv6` pakety, najmä ale `ICMPv6 Echo reply` a `NDP` pakety. Údaje o odosielatelovi sa uložia do tabuľky.



Obr. 2: Zasielanie a príjimanie správ zo scannera

2.2 Spoofer

Úlohou tohto programu je infikovať cache pamäť obetiam na `L2` úrovni. V pravidelnom útočnikom zadanom intervale sa posielajú správy obetiam, ktoré prepíšu `MAC` adresu obete na adresu útočnika. Tieto správy sú zasielané až pokým neni program zastavený. Pred koncom programu sa pošle ešte jedna správa pre každú obeť ktorá obnoví cache pamäť do konzistneho stavu.



(a) IPv4 (b) IPv6

Obr. 3: Zasielanie správ pre infikovanie cache pamäte

2.2.1 IPv4

Pre preklad `IPv4` adresy na `MAC` adries sa používa `ARP`. Cache pamäť tohto protokulu sa infikuje pomocou opakovaného zasielania `ARP Reply` paketu. Do zdrojovej `IPv4` adresy sa priradí adresa 1.obete, do zdrojovej `MAC` adresy adresa útocnika. Paket sa zašle na `MAC` a `IPv4` adresu 2. obete.

2.2.2 IPv6

Pre `IPv6` sa pre preklad `MAC` adresy používa `NDP`. Pre infikovanie cache pamäte tohto protokolu sa využíva `Neighbor Advertisement` paket, ktorý obsahuje ako zdrojovú `MAC` adresu, adresu útočnika. Zdrojová `IPv6` adresa je adresa prvej obete a cieľova `MAC` aj `IPv6` adresa je adresa druhej obete.

2.3 Intercept

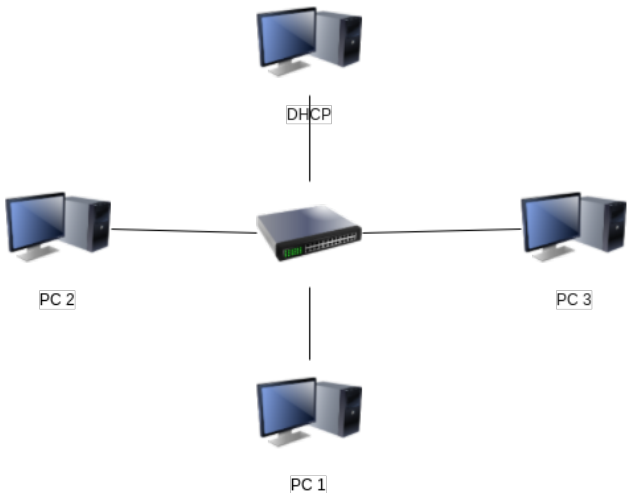
Tento program vytvára ilúziou že komunikáciu nikto nenarušuje. Zo vsupného XML súboru kde sa nachádzaju MAC a IP adresy sa zostrojí mapa v tvare `IP:MAC`. Následne príjima každý paket. Ak má paket v ethernet hlavičke typ `IPv4` alebo `IPv6` a súčasne cieľová `MAC` adresa je adresa útočnika tak sa vykonajú následujúce akcie:

1. Vyhľadá sa cieľová IP adresa paketu v mape, ak sa nenájde paket sa zahodí a čaká sa na ďalší
2. Zmení sa zdrojová MAC adresa paketu na adresu útočníka
3. Zmení sa cieľová MAC adresa paketu na adresu obete ktorá sa nachadza v mape
4. Paket sa odošle ďalej

Prebieha to do tej doby pokiaľ program neskončí.

3 Testovacia sieť

Ako testovacia sieť boli použité 3 virtuálne stroje pomocou nástroja VirtualBox v `NAT Network` s adresou `10.0.2.0/24`



Obr. 4: Topologia siete

MAC	08:00:27:cc:9d:5d
IPv4	10.0.2.7
IPv6	fe80::a00:27ff:fecc:9d5d
IPv6	fd17:625c:f037:2:64fc:1fe1:4f8b:f9ef
IPv6	fd17:625c:f037:2:a00:27ff:fecc:9d5d

Tabuľka 1: PC 1 - Útočník

MAC	08:00:27:4c:35:89
IPv4	10.0.2.8
IPv6	fe80::a00:27ff:fe4c:3589
IPv6	fd17:625c:f037:2:159c:2863:b5a7:427e
IPv6	fd17:625c:f037:2:a00:27ff:fe4c:3589

Tabuľka 2: PC 2 - Obeť 1

MAC	08:00:27:c4:54:81
IPv4	10.0.2.9
IPv6	fe80::a00:27ff:fec4:5481
IPv6	fd17:625c:f037:2:b580:53d2:47fb:2ae
IPv6	fd17:625c:f037:2:a00:27ff:fec4:5481

Tabuľka 3: PC 3 - Obeť 2

Najprv sme oskenovali sieť nástrojom `pds-scanner`

```
<devices>
    <host mac="0800.274c.3589">
        <ipv6>fd17:625c:f037:2:159c:2863:b5a7:427e</ipv6>
        <ipv6>fe80::a00:27ff:fe4c:3589</ipv6>
        <ipv4>10.0.2.8</ipv4>
    </host>
    <host mac="0800.2791.5ac8">
        <ipv4>10.0.2.3</ipv4>
    </host>
    <host mac="0800.27c4.5481">
        <ipv6>fd17:625c:f037:2:b580:53d2:47fb:2ae</ipv6>
        <ipv6>fe80::a00:27ff:fec4:5481</ipv6>
        <ipv4>10.0.2.9</ipv4>
    </host>
    <host mac="5254.0012.3500">
        <ipv4>10.0.2.1</ipv4>
        <ipv4>10.0.2.2</ipv4>
    </host>
</devices>
```

Listing 1: Výstup nástroja pds-scanner

Nastroj odhalil obe virtuálne stroje, u každej zistil IPv4 adresu a jednu link a jednu global IPv6 adresu.

Potom bol použitý nástroj `pds-chooser` pre zvolenie si párov a následne `pds-massspoof` pre infikovanie cache pamäti obeti.

Nakoniec nástroj `pds-intercept` ktorý preposielal pakety medzi obeťami a útočníkom.

Testovanie prebiehalo pri prenose 1GB sŭboru cez FTP.

```
1073741824 bytes received in 18.96 secs (55295.0 kB/s)
```

Listing 2: MitM prenos

```
1073741824 bytes received in 5.89 secs (177882.5 kB/s)
```

Listing 3: Neodpočúvany prenos

Priepustnosť siete počas MitM útoku bola 3.2x pomalšia.