Lab 2 - Arp Spoofing napad

Topologija

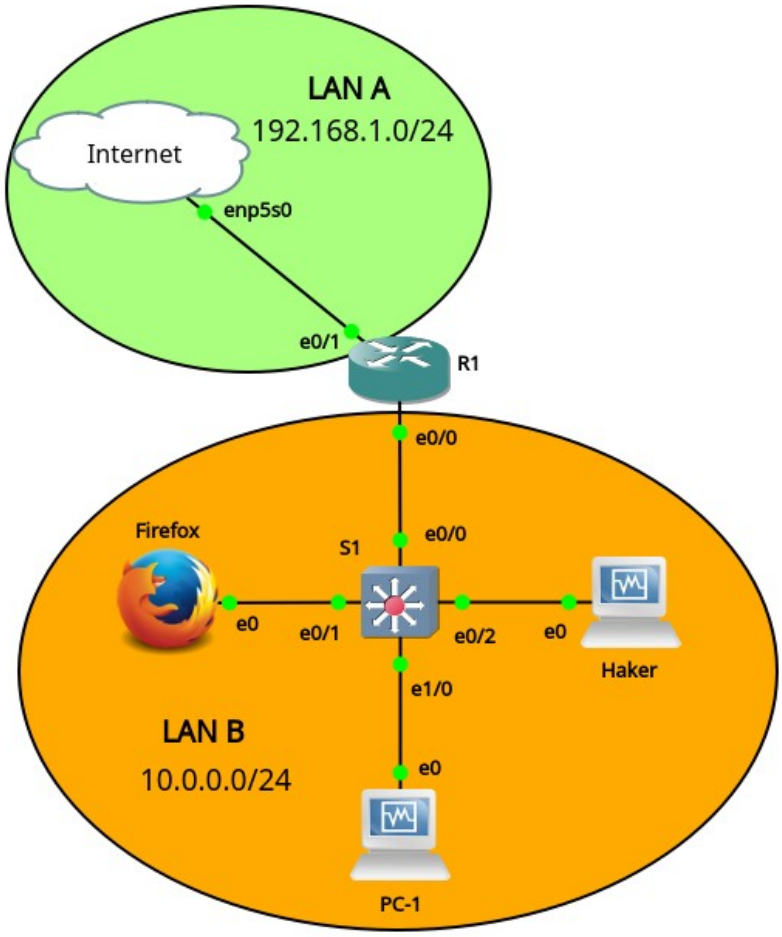


Tabela adresa

Uređaj	Interfejs	IP adresa	Mrežna maska	Default Gateway
R1	e0/1	DHCP	255.255.255.0	N/A
	e0/0	10.0.0.1	255.255.255.0	N/A
S1	VLAN 1	10.0.0.5	255.255.255.0	10.0.0.1
Haker	NIC	DHCP	DHCP	DHCP
PC-1	NIC	DHCP	DHCP	DHCP
Firefox	NIC	DHCP	DHCP	DHCP

Ciljevi

1. Postaviti topologiju i povezati uređaje
2. Konfigurisati uređaje i proveriti međusobne konekcije
3. Podesiti DHCP i HTTP server
4. Demonstrirati Arp Spoofing napad
5. Konfigurisati Dynamic ARP Inspection

Opis vežbe

MAC flooding napad se često se smatra „ključem“ za dalje napade na mrežu u cilju krađe podataka i poverljivih informacija, ili nadgledanje saobraćaja radi planiranja većih napada. Napad koji često sledi nakon MAC flooding napada jeste ARP spoofing.

Kako ARP radi po principu slanja *broadcast* zahteva sa pitanjem čija je određena IP adresa i čeka na ARP odgovor od vlasnika te IP adrese u vidu njegove MAC adrese, uz pomoć određenih alata, *black hat* haker može zloupotrebiti to i odgovoriti na tuđi ARP zahtev da je tražena IP adresa njegova i tako poslati svoju MAC adresu. Na primer, napadač se može nekom računaru predstavljati kao njegov *default gateway*, dok će se pravom *default gateway*-u predstavljati kao taj računar, tako da kad god računar inicira neku komunikaciju ka *default gateway*-u ili nekom van mreže, paket će prvo doći do napadača, a zatim će se proslediti ka destinaciji. Ova vežba demonstrira ovaj tip napada kao i kako ga uočiti pomoću Wireshark-a i sprečiti za u buduće, konfigurisanjem **Dynamic ARP Inspection** opcija na sviču kroz koji se odvija saobraćaj. Takođe je i opisan način povezivanja GNS3 programa sa internetom i fizičkom mrežnom karticom kako bi se i ostalim uređajima u mreži omogućio izlazak na internet.

Zahtevi

1. Cisco IOU L3 ruter
2. Cisco IOU L2 svič
3. Firefox
4. Kali Linux VM
5. Ubuntu/Windows VM

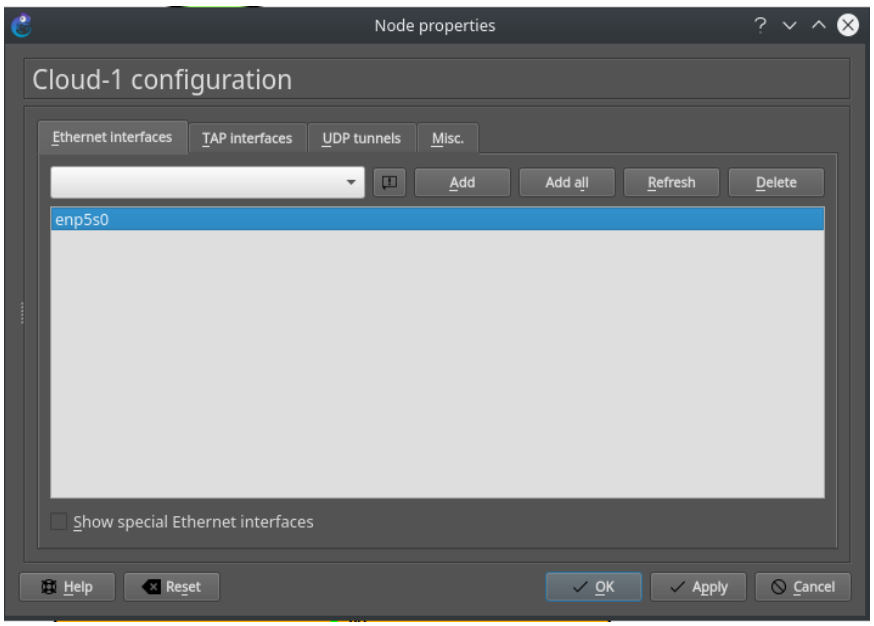
1. Osnovna podešavanja

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.

```
R1(config)# erase startup-config
R1(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/R1-confg (Socket error)
```

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

```
R1(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 0/1 koji je povezan na interfejs našeg fizičkog računara (na slici enp5s0)
2. Ethernet 0/0 koji je povezan sa LAN mrežom B 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.

```
R1(config)# interface Ethernet 0/1
R1(config-if)# description LINK TO INTERNET
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown
R1(config-if)# exit
```

Ubrzo nakon toga bi trebalo da vidite *syslog* poruku da je ruter na interfejsu Ethernet 0/1 dobio neku IP adresu.

```
*Jan 10 19:11:30.952: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/1 assigned
DHCP address 192.168.1.206, mask 255.255.255.0, hostname R1
```

Podesite podrazumevanu statičku rutu ka default gateway-u rutera na čiji ste se interfejs povezali putem interfejsa Ethernet 0/1 (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).

```
R1(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.

```
R1# 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
R1#
```

Podesite DNS server.

```
R1(config)# ip domain-lookup
R1(config)# ip name-server 8.8.8.8
```

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

```
R1# ping google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.58.212.46, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/20/21 ms
R1#
```

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 0/0 samo što ćete njemu dodeliti statičku adresu.

```
R1(config)# interface Ethernet 0/0
R1(config-if)# description LINK TO SWITCH S1
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

Da bi uređaji iz mreže LAN B mogli da izađu na internet, sama konfiguracija interfejsa Ethernet 0/0 nije dovoljna. Potrebno je i konfigurisati NAT koji će prevoditi adrese iz mreže 10.0.0.0/24 i omogućiti im prolaz ka internetu putem pristupne liste.

```
R1(config)# interface Ethernet 0/1
R1(config-if)# ip nat outside
R1(config-if)# exit
R1(config)# interface Ethernet 0/0
R1(config-if)# ip nat inside
R1(config-if)# exit
R1(config)# ip nat inside source list 1 interface Ethernet 0/1 overload
R1(config)# access-list 1 permit 10.0.0.0 0.0.0.255
R1(config)# end
```

Napomena: Ako vam se pojave neke greške nakon što konfigurišete interfejs Ethernet 0/1, ignorišite ih i slobodno nastavite vežbu.

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

```
R1# ping google.com source Ethernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.17.174, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/19/20 ms
```

2.2. Konfigurisanje sviča

```
S1(config)# interface Vlan 1
S1(config-if)# ip address 10.0.0.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
```

Konfigurišite default gateway na sviču

```
S1(config)# ip default-gateway 10.0.0.1
```

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

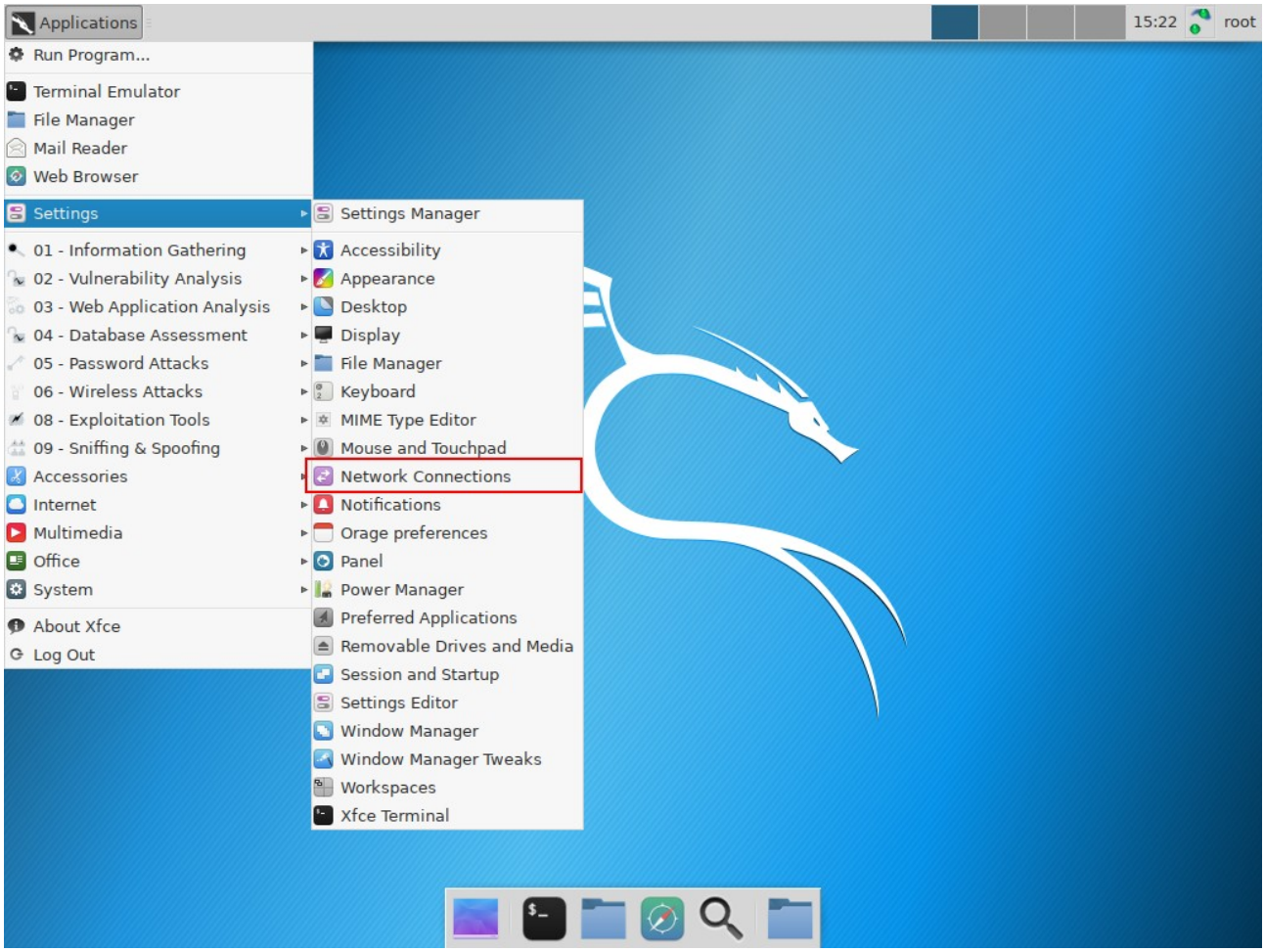
```
S1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1
S1(config)# exit
```

Pokušajte pingovati adresu Ethernet 0/1 interfejsa. Ping bi trebalo da bude uspešan.

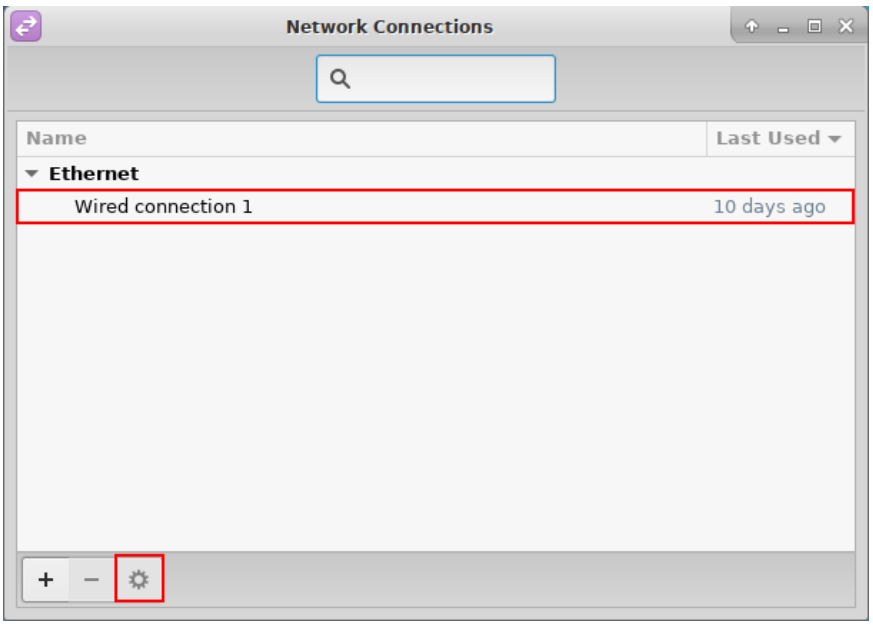
```
S1# ping 192.168.1.206
*Jan 10 20:35:17.053: %SYS-5-CONFIG_I: Configured from console by console
S1#ping 192.168.1.206
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.206, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
S1#
```

2.2. Kali Linux konfigurisanje

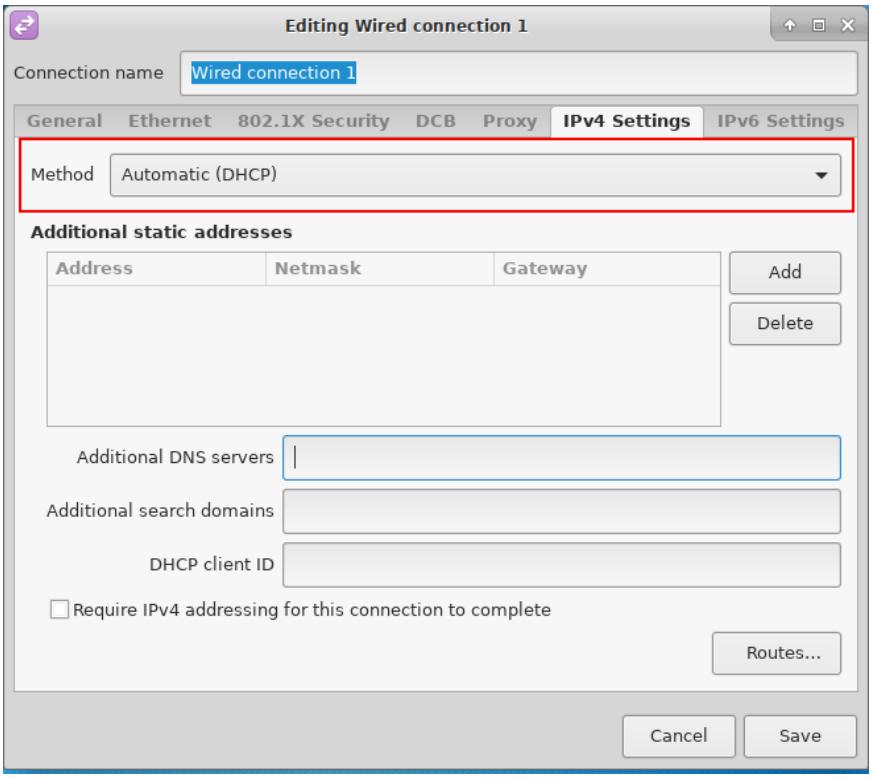
Potrebno je podesiti IP parametre na Kali Linux mašini da dobija adresu od DHCP servera. U gornjem levom uglu otvorite *Applications* meni, pa zatim *Setting*s i na kraju otvorite *Network Connections*.



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.

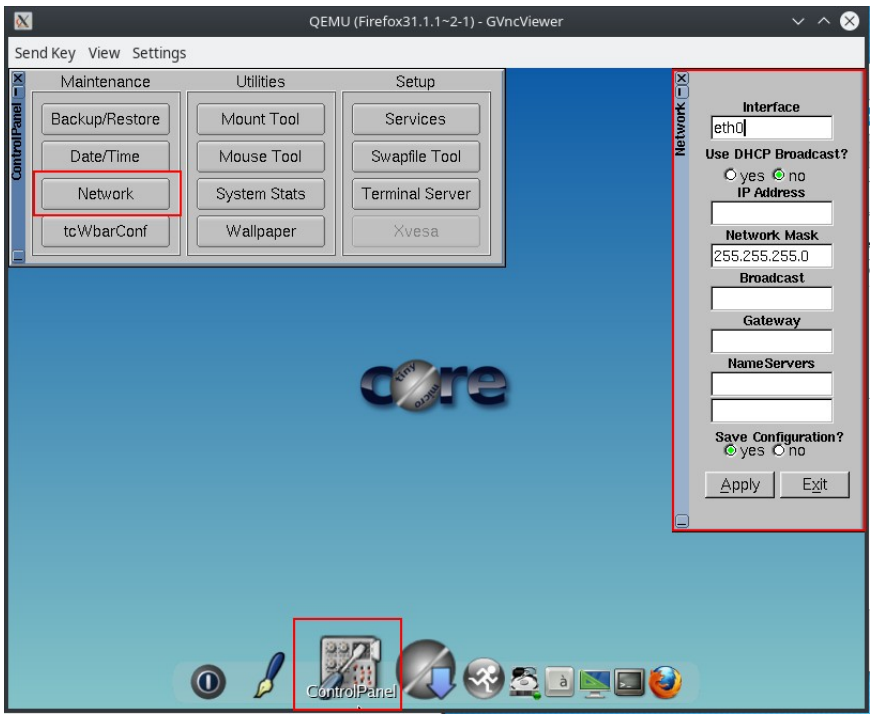


Kada se otvori prozor za podešavanje konekcije, otvorite tab *IPv4 Settings* i uverite se da pod polje *Method*, stoji *Automatic (DHCP)*.



1.6. Konfigurisanje Firefox uređaja

Pokrenite Firefox uređaj i otvorite njegovu konzolu desnim klikom na Firefox uređaj za zatim na *Console*. Kada vam se otvori Firefox uređaj, u donjem delu ekrana kliknite na *Control Panel* ikonicu, a zatim će se otvoriti prozor kao u gornjem levom uglu. Kliknite na *Network*, što će vam otvoriti novi prozorčić za podešavanje IP parametara. Pod poljem *Use DHCP Broadcast?* izaberite *yes* i kliknite na *Apply*.



1.7. Konfigurisanje PC-1 virtuelne mašine

Konfigurišite IP parametre na uređaju PC-1, u zavisnosti od toga da li vam je PC-1 Windows ili Ubuntu mašina, tako da koristi DHCP za dobijanje adrese.

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.

```
R1(config)# enable secret ciscopa55
R1(config) line console 0
R1(config-line)# password ciscoconpa55
R1(config-line)# login
R1(config-line)# exec-timeout 5 0
R1(config-line)# loggin synchronous
R1(config-line)# exit
R1(config) line vty 0 4
R1(config-line)# password ciscovtypa55
R1(config-line)# login
R1(config-line)# exec-timeout 5 0
R1(config-line)# loggin synchronous
R1(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:

```
R1(config)#service password-encryption

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

3.1. Postavljanje poruke upozorenja

Postavite poruku koja će se prikazivati prilikom pristupanja ruteru.

```
R1(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.

```
R1(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.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

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

```
R1(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.

```
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(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.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh telnet
R1(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.

```
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 90
R1(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 R1 na svič S1 i obrnuto. U slučaju da ne možete da se povežete proverite da li ste sve komande uneli tačno kao i lozinke.

```
R1# telnet 10.0.0.5
```

```
S1# telnet 10.0.0.1
```

4. Konfigurisanje DHCP servera

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 S1.

Prvo je potrebno rezervisati prvih 10 adresa kako ih ni jedan uređaj ne bi dobio.

```
S1(config)# ip dhcp excluded-address 10.0.0.0 10.0.0.10
```

Zatim konfigurišite DHCP pool sa sledećim parametrima:

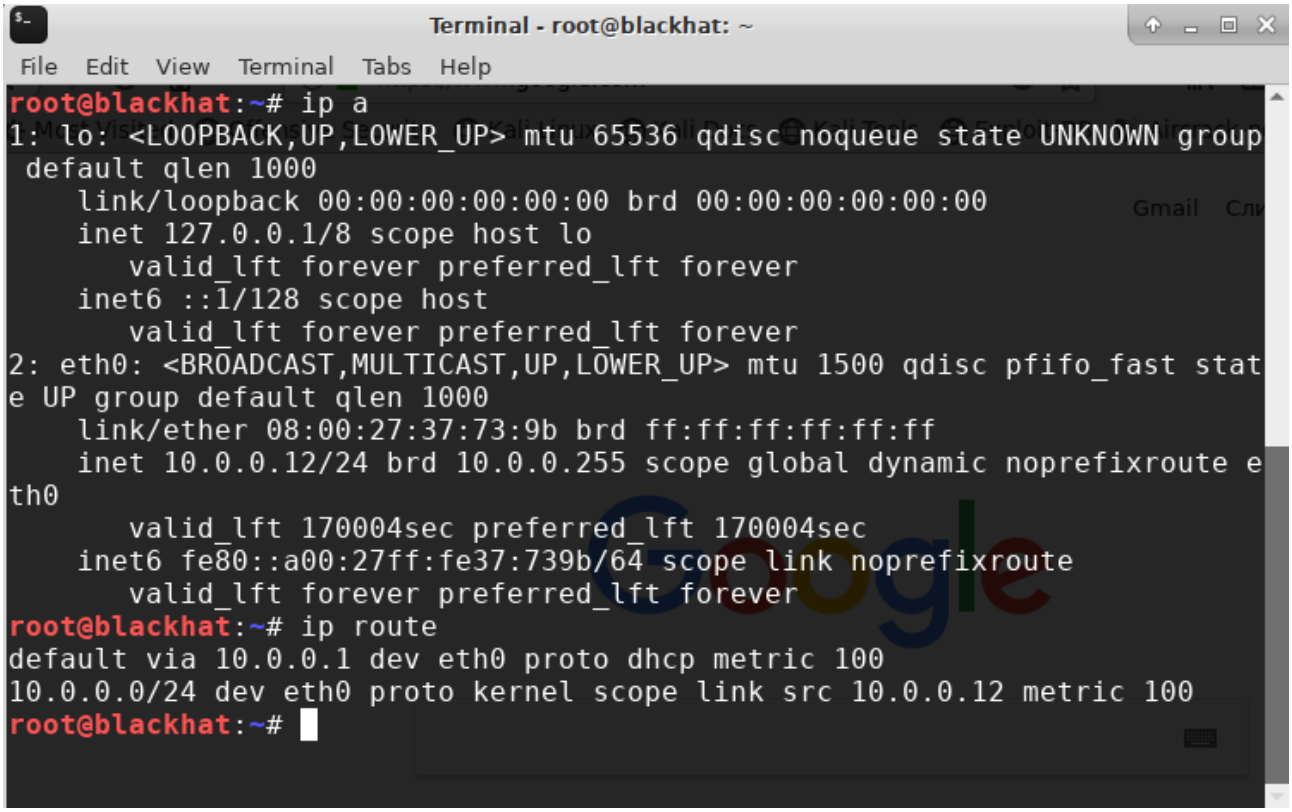
1. Kao ime pool-a stavite LAN_Network
2. Opseg adresa LAN B mreže
3. Domen bezbednost.com
4. DNS server 8.8.8.8
5. Default ruter 10.0.0.1
6. Iznajmljivanje adrese u trajanju od 2 dana

```
S1(config)# ip dhcp excluded-address 10.0.0.0 10.0.0.10
S1(dhcp-config)# ip dhcp pool LAN_Network
S1(dhcp-config)# network 10.0.0.0 255.255.255.0
S1(dhcp-config)# domain-name bezbednost.com
S1(dhcp-config)# dns-server 8.8.8.8
S1(dhcp-config)# default-router 10.0.0.1
S1(dhcp-config)# lease 2
S1(dhcp-config)# exit
```

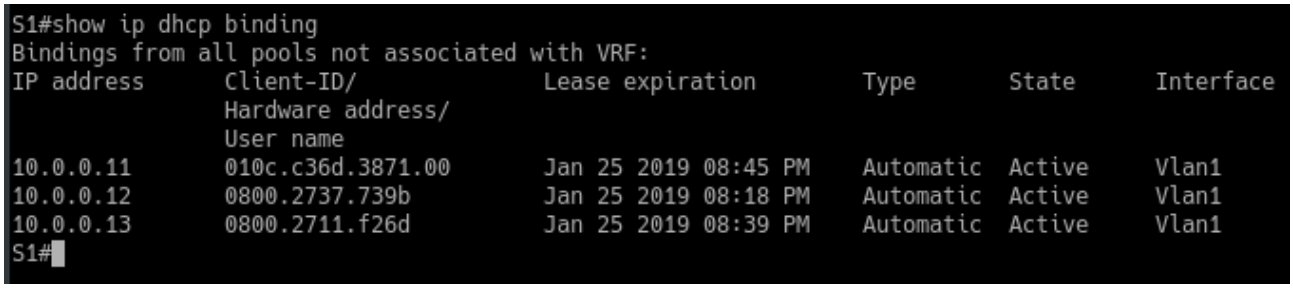
4.1. Provera DHCP podešavanja

Na Kali Linux i PC-1 mašinama restartujte mrežne interfejse (*disconnect* pa *connect*) kako biste dobili IP adrese i ostale podatke od DHCP servera.

Na Kali Linux mašini komandom **ip a** možete proveriti TCP parametre, dok komandom **ip route** možete proveriti ruting tabelu kao i *default gateway*.



Na sviču proverite komadnom `show ip dhcp binding` sve iznajmljene IP adrese.



4.2. Testiranje konekcije

Sa Kali Linux, PC-1 i Firefox mašina pokušajte pingovati:

1. VLAN 1 interfejs sviča S1
2. Ethernet 0/0 rutera R1
3. Ethernet 0/1 rutera R1
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 *default* 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:

```
R1(config)# ip http server
```

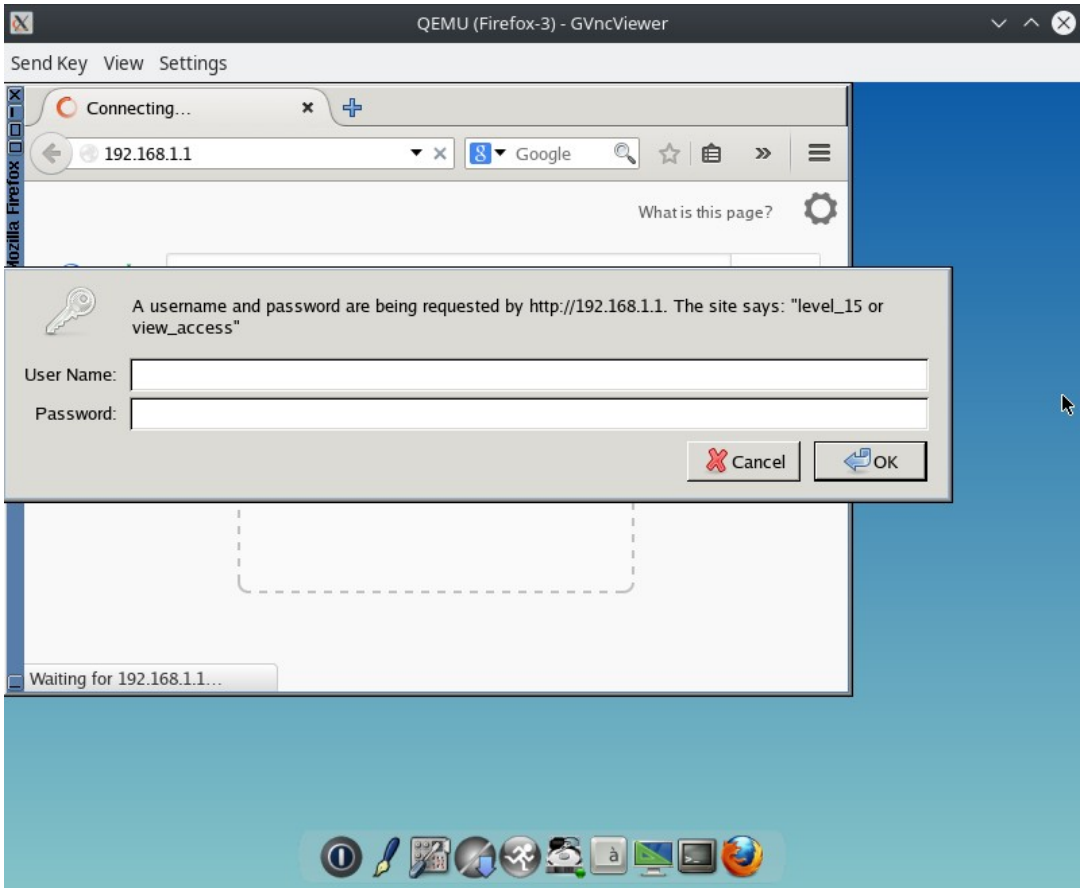
Da bismo bili sigurniji da niko ne može pristupiti ovom serveru bez dodatne zaštite, omogućićemo zahtevanje korisničkog imena i lozinke za pristup. Za to se koristi komanda **ip http authentication**. Izlistajte sve moguće metode autentifikacije komandom:

```
R1(config)# ip http authentication ?
 aaa     Use AAA access control methods
 enable  Use enable passwords
 local   Use local username and passwords
```

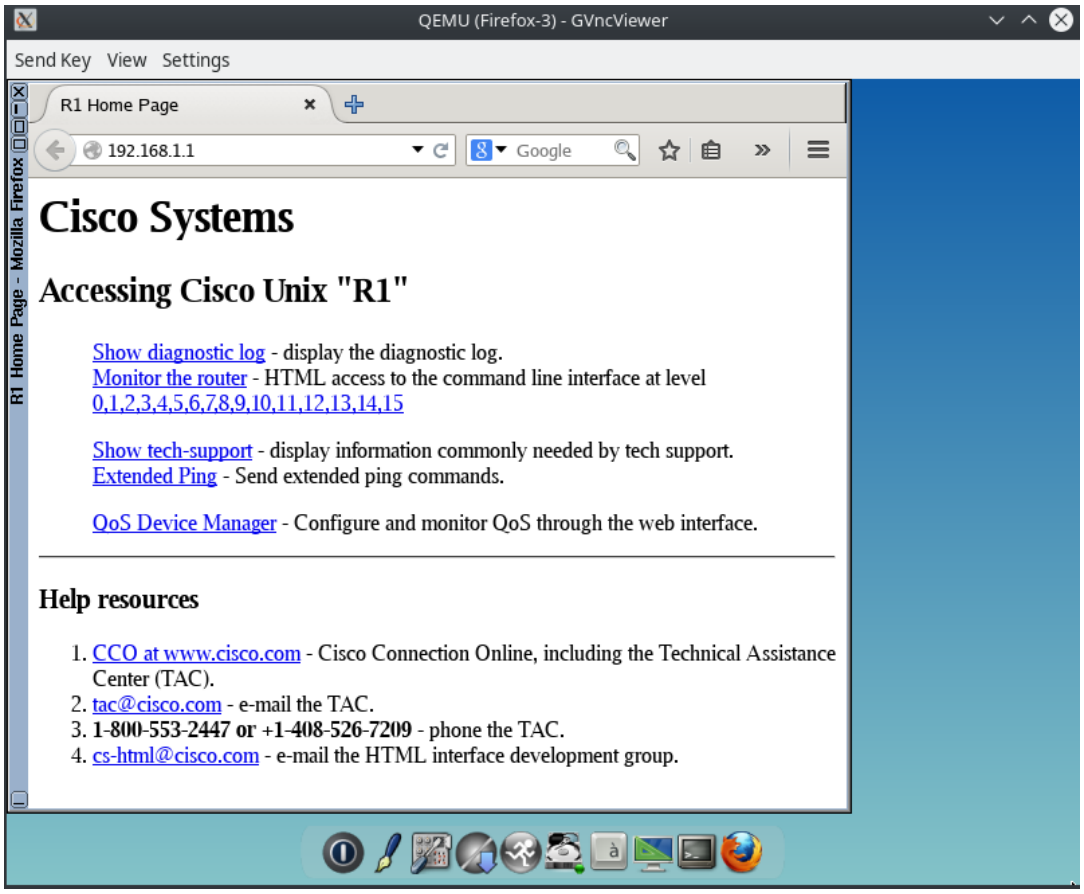
Mi ćemo koristiti opciju **local** što bi značilo da je za pristupanje našem HTTP serveru potreban lokalni nalog koji smo ranije kreirali.

```
R1(config)# ip http authentication local
```

Kada sa neke virtuelne mašine ili Firefox uređaja pokušate otvoriti R1 server (http://10.0.0.1), 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. Arp Spoofing napad

ARP Spoofing (poznat i kao ARP Poisoning) je tip napada u kojem napadač zloupotrebljava ARP protokol sa ciljem presretanja informacija ili onemogućavanjem resursa mreže. ARP protokol radi po principu pitanje-odgovor, tj. kada neki uređaj ne zna MAC adresu neke IP adrese, on šalje ARP pitanje svima u mreži (*broadcast*) i čeka ARP odgovor uređaja kome pripada ta IP adresa. Napadač može zloupotrebiti to i poslati ARP odgovor predstavljajući se kao uređaj sa tom IP adresom. Na taj način svi paketi namenjeni toj IP adresi biće prosleđeni napadaču čime će moći zabeležiti poverljive informacije i podatke.

Alat koji se koristi za ovaj napad se zove **arpspoof** koji omogućava napadaču da se lažno predstavlja drugim uređajima putem određenog mrežnog interfejsa i tako prima i preusmerava pakete koji se razmenjuju između dva ili više uređaja. U ovoj vežbi, glavna meta napada je ruter koji predstavlja *default gateway* u mreži. Forma komande za izvršenje napada je sledeća:

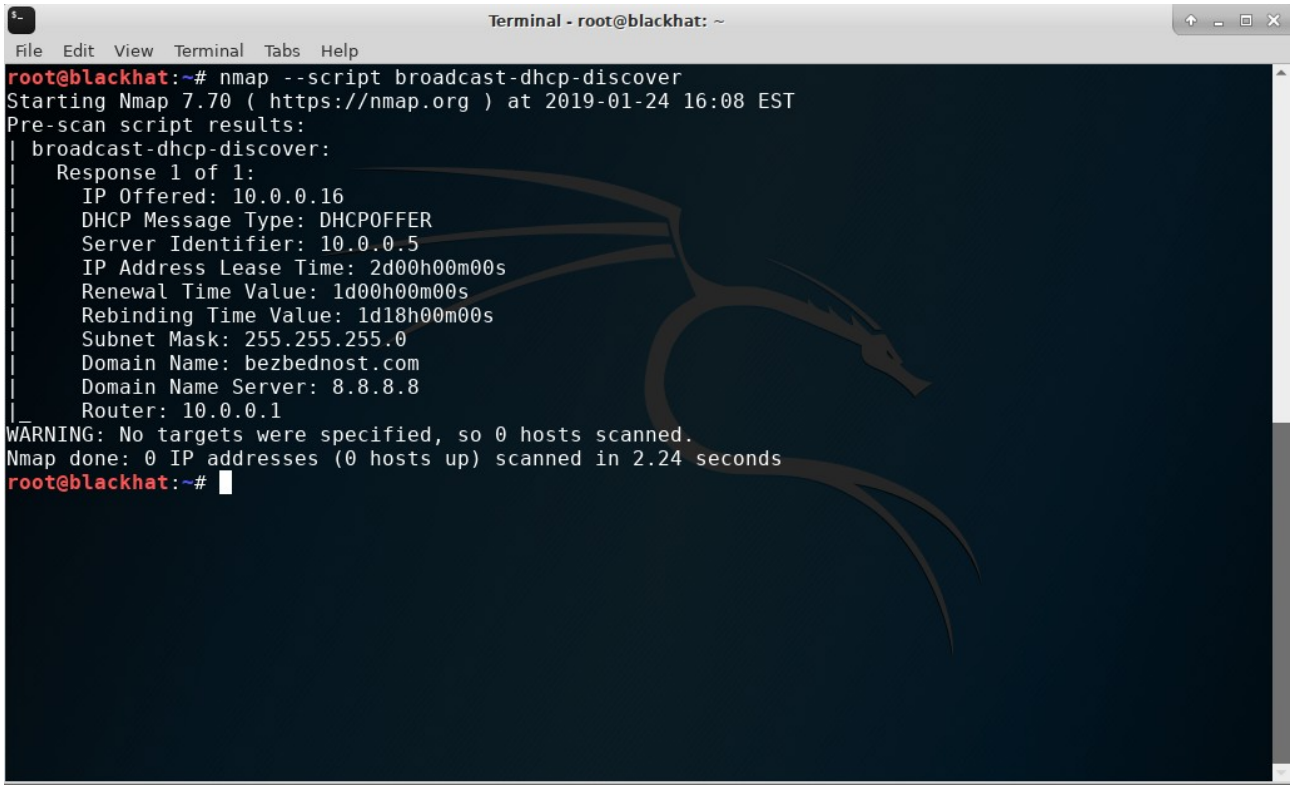
```
arpspoof -i [ interfejs ] -t [ IP adresa mete ] [ Lažna IP adresa ]
```

Napomena: U slučaju da nemate arpspoof, potrebno je instalirati paket **dsniff** u okviru kojeg se arpspoof i nalazi.

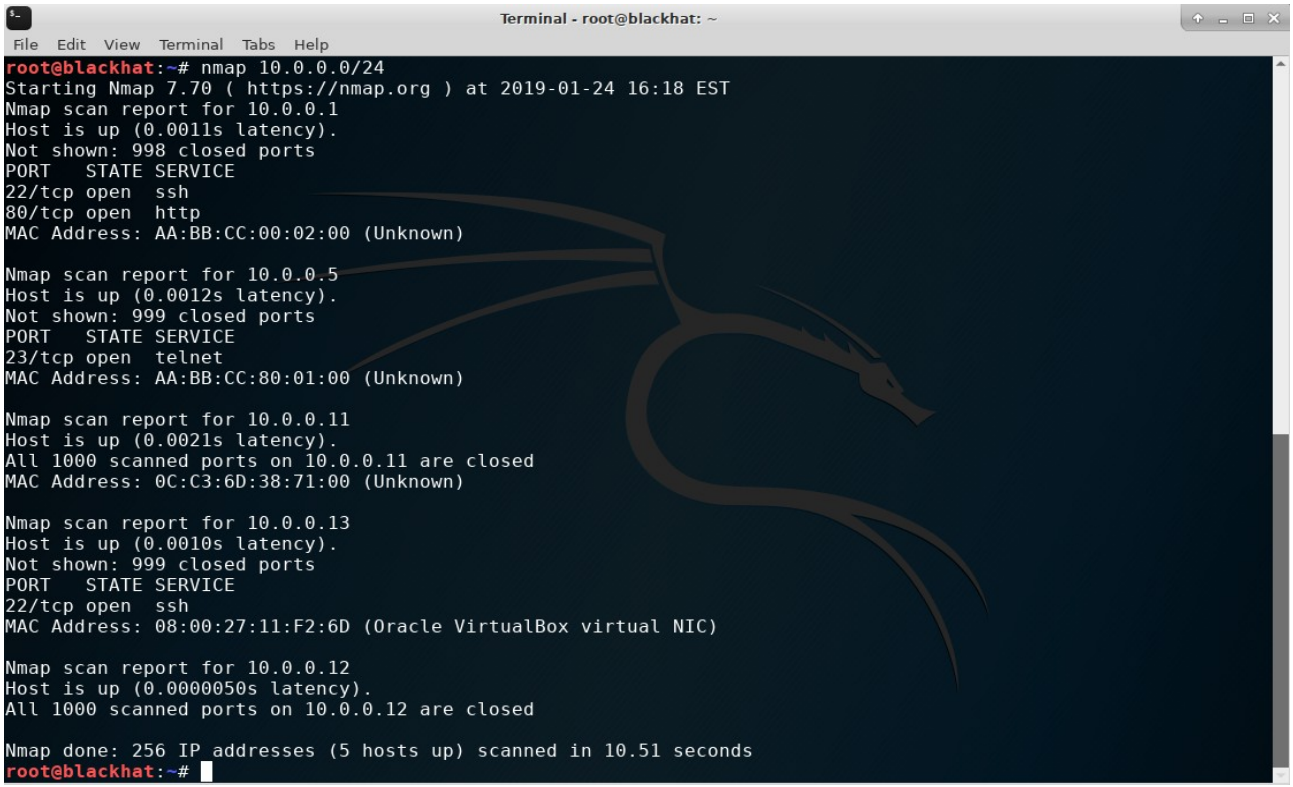
6.1. Prikupljanje informacija uz Nmap

Ali kako napadač zna koja je adresa rutera, koja DHCP servera ili nekog drugog uređaja u mreži? Za otkrivanje tih informacija se može koristiti alat **Nmap**. To je alat koji otkriva detalje zadate mreže kao što su koji su hostovi u mreži u *UP* stanju (odnosno uključeni), koje su im IP adrese, koji portovi na njima su otvoreni a koji zatvoreni, operativni sistem koji koriste i mnoge druge stvari. Da bi ste otkrili operativni sistem nekog uređaja potrebno je da određena pravila budu zadovoljena a to su da barem jedan port na hostu bude otvoren i barem jedan port zatvoren.

Prva stvar koju napadač radi jeste traženje DHCP servera i prikupljanja nekih osnovnih informacija. To postiže komandom **nmap --script broadcast-dhcp-discover**. Rezultat komande prikazan je na slici ispod, na kojoj se vidi adresa DHCP servera, IP adresa koju nudi kao i vreme trajanja iznajmljivanja adrese, adresa rutera itd.

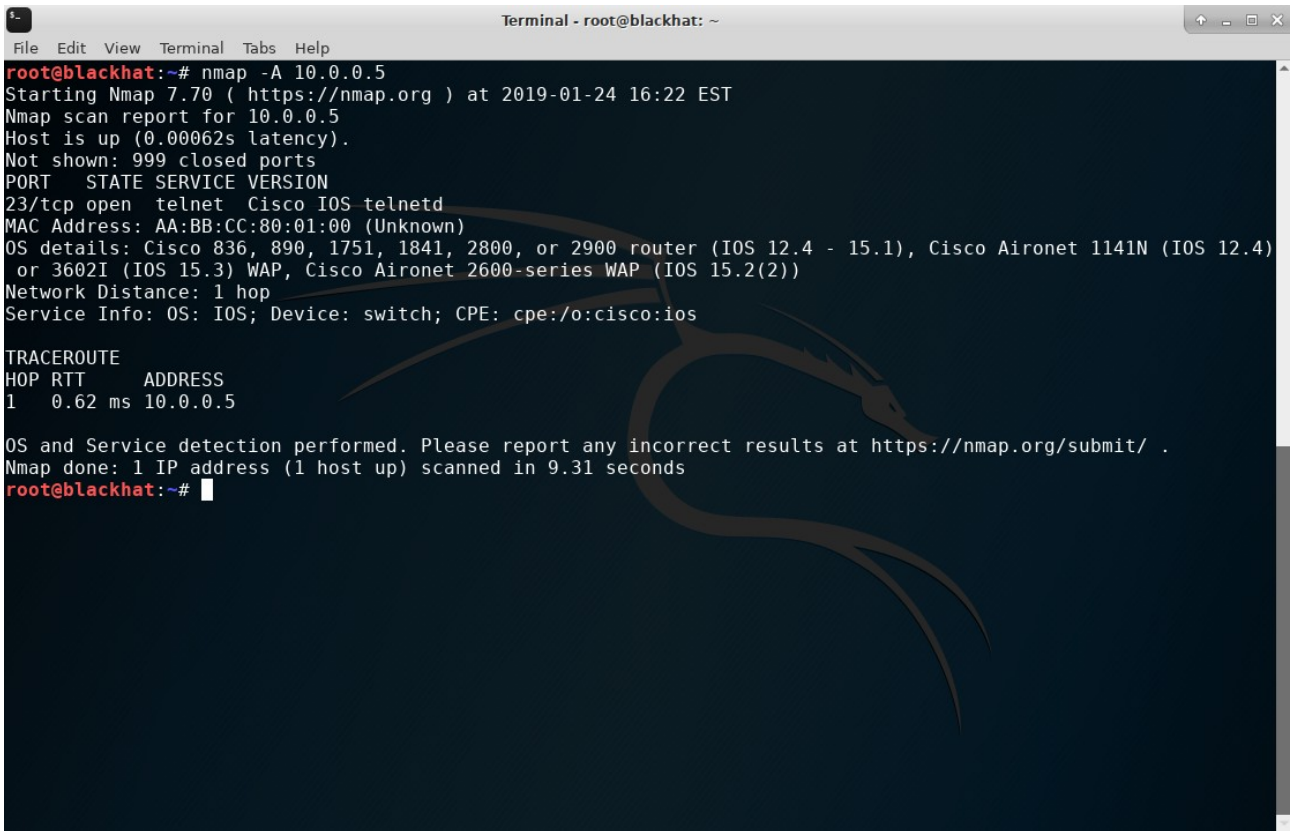


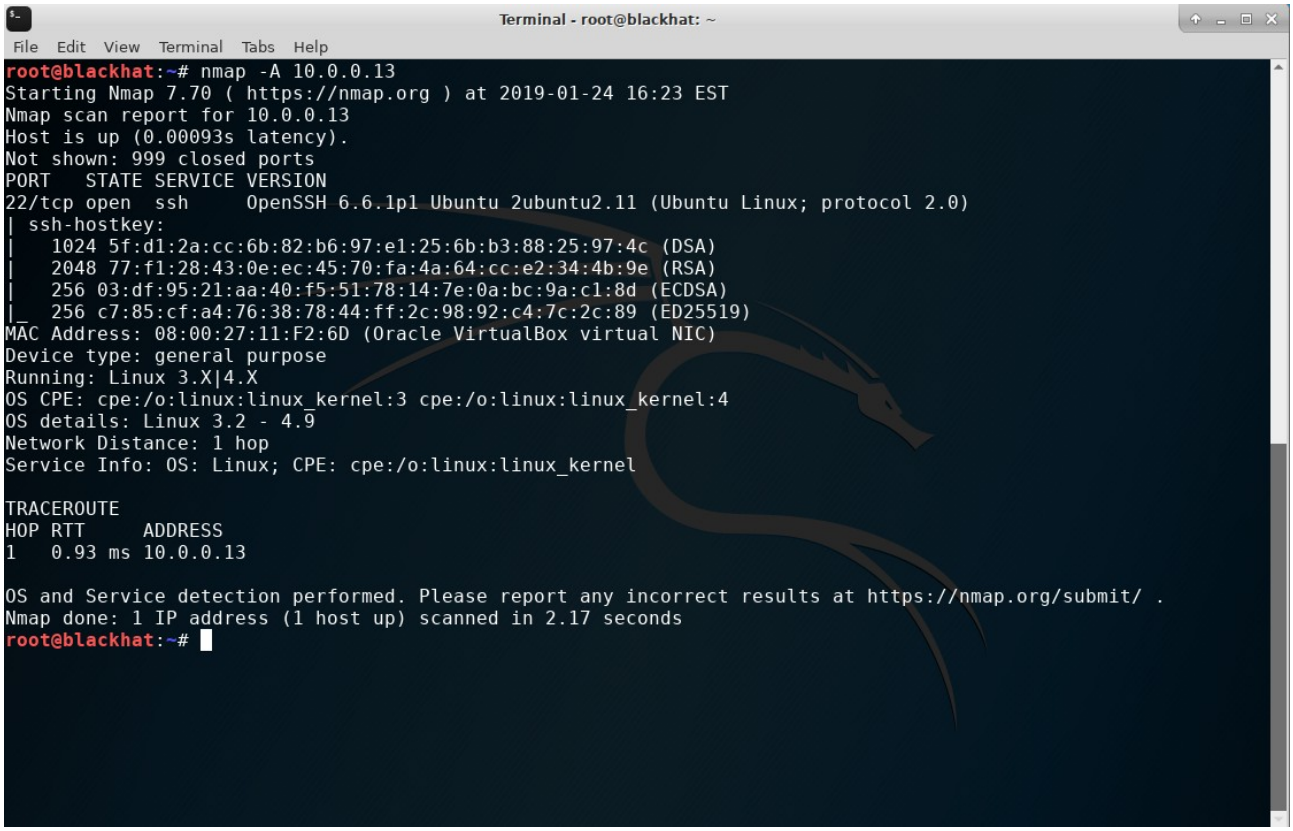
Sledeći cilj napadača je da pronađe sve hostove u mreži koji su u UP stanju, odnosno koji su dostupni, a to može učiniti komandom **nmap 10.0.0.0/24**. Kao rezultat se dobija lista svih hostova u mreži sa dodatnim informacijama o njima kao na primer da li su *UP* ili ne, koliko portova (i koji) su otvoreni ili zatvoreni na njima i slično, kao što je i prikazano na slici ispod.



Ako bi hteo samo spisak IP adresa hostova koji su UP, to može dobiti komandom
nmap -n -sn 10.0.0.0/24 -oG – | awk '/Up$/{print $2}'.

Ako napadač želi prikupiti neke dodatne informacije o uređajima, kao na primer saznati operativne sisteme DHCP servera ili nekog drugog uređaja u mreži, to može učiniti komandom
nmap -A [IP adresa uređaja].





6.2. Provera tabela pre napada

Proverite kako izgleda ARP tabela na ruteru R1 pre izvršenja napada.

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.1                -   aabb.cc00.0200  ARPA   Ethernet0/0
Internet  10.0.0.11               0   0cc3.6d38.7100  ARPA   Ethernet0/0
Internet  10.0.0.12               0   0800.2737.739b  ARPA   Ethernet0/0
Internet  10.0.0.13               8   0800.2711.f26d  ARPA   Ethernet0/0
Internet  192.168.1.1             1   38d5.4780.59b4  ARPA   Ethernet0/1
Internet  192.168.1.206           -   aabb.cc00.0210  ARPA   Ethernet0/1
R1#
```

6.3. Simulacija napada i beleženje paketa

U ovoj situaciji, napadač želi da se lažno predstavlja kao PC-1 u komunikaciji koja se odvija između uređaja PC-1 i rutera R1.

Ali pre nego što se započne sa napadom, važno je napomenuti da podrazumevano, Linux operativni sistemi ne prosleđuju IP pakete, što znači da paketi koji dolazi sa računara PC-1 neće se proslediti ruteru R1 i obrnuto.

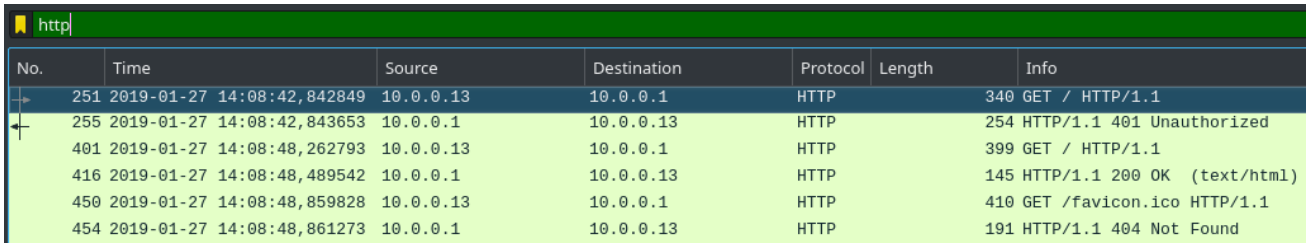
Da bismo to omogućili, potrebno je na Kali Linux mašini uneti komandu
sysctl -w net.ipv4.ip_forward=1 nakon čega ćemo privremeno omogućiti prosleđivanje IPv4 paketa.

Zatim je potrebno pokrenuti Wireshark na linku između sviča S1 i Kali Linux mašine.

Otvorite dva Terminal prozora: jedan za lažno predstavljanje ruteru, drugi za lažno predstavljanje uređaju PC-1. U prvom prozoru izvršite komandu **arpspoof -i eth0 -t 10.0.0.1 [PC-1 IP adresa]**, a u drugom **arpspoof -i eth0 -t [PC-1 IP adresa] 10.0.0.1** čime ćete započeti ARP Spoofing napad.

Sada napadač može da zabeleži svaki paket koji se kreće od uređaja PC-1 do rutera R1 i van njega, tj. ka internet mreži, i obrnuto.

U Wireshark-u postavite filter da se samo HTTP paketi beleže. Na uređaju PC-1 pokrenite veb pregledač (*browser*), otvorite HTTP stranicu rutera R1 (http://10.0.0.1) i unesite pristupne parametre koje smo ranije podesili. Sada se vratite na Wireshark i pogledajte sve HTTP pakete koje je zabeležio. Trebalo bi nešto slično slici ispod da dobijete (brojevi paketa će se razlikovati od računara do računara).



Svaki HTTP paket možete detaljno istražiti i pogledati koje sve informacije je zabeležio u tom trenutku. U primeru sa slike primećujemo da je paket 251 sa porukom **GET / HTTP/1.1** početak komunikacije između između uređaja sa adresom 10.0.0.0.13 i 10.0.0.1, dok bi sledeći paket sa porukom **HTTP/1.1 401 Unauthorized** mogao značiti ili da su uneti pogrešni pristupni podaci ili da je prekinut unos podataka, ili jednostavno kao upozorenje da se stranica nije odmah otvorila jer je pristup ograničen određenim pravima.

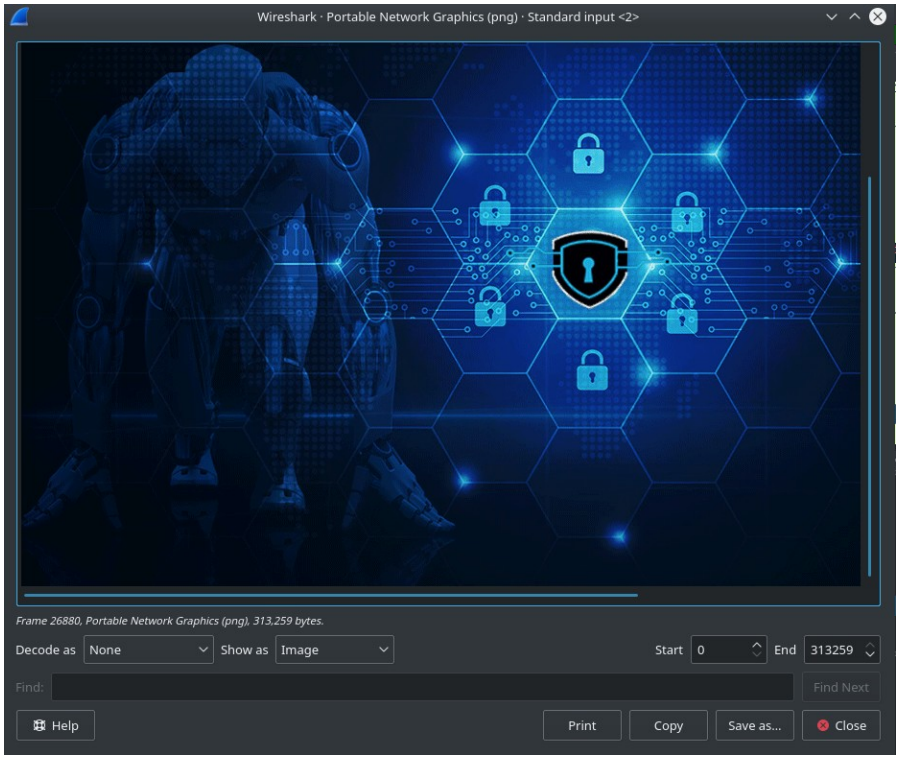
Nama su ovde najbitniji paketi 401 i 416 (zapravo paketi sa porukama *GET / HTTP/1.1* i *HTTP/1.1 200 OK (text/html)*) jer oni sadrže informacije koje napadač može ukrasti ili saznati nešto o samom uređaju. Otvorite *GET / HTTP/1.1* paket, proširite polje *Hypertext Transfer Protocol*, a zatim proširite polje *Authorization*. U tom polju se nalaze korisničko ime i lozinka za pristup HTTP serveru ruteru R1, u *clear-text* formatu. Takođe se može videti i polje *User-Agent* koji daje informacije putem kojeg veb pregledača je otvorena HTTP stranica.

Sada otvorite polje *HTTP/1.1 200 OK (text/html)*, a zatim proširite polje *Line-based text data*, videćete ceo HTML kod i sadržaj otvorene stranice. Naravno ovo je moguće videti jer stranica nema TLS/SSL zaštitu, jer u slučaju da ima, čitav sadržaj i komunikacija bi bila enkriptovana.

Pokušajte otvoriti sajt ICT škole (https://ict.edu.rs) i vratite se na Wireshark da istražite pakete koji su zabeleženi. Primetićete da su zabeleženi paketi OCSP protokola koji služi za dobijanje statusa digitalnih sertifikata. Iz njih se gotovo nikakve informacije ne mogu izvući. Ako biste otvorili neki javni sajt (http:sky-express.rs), umesto lokalnog HTTP servera koji ste sami podigli, koji nema TLS/SSL zaštitu, ceo sadržaj sajta i HTML kod se može videti kao i kod primera lokalnog HTTP servera. Ono što je zanimljivo jeste da će Wireshark prikazati i HTTP pakete koji beleže JavaScript skripte sa sajta, kao i CSS kodove, slike i drugi sadržaj, kao što je i prikazano na slici ispod.

23803	2019-01-27 15:47:31,420239	10.0.0.13	82.195.224.128	HTTP	358 GET / HTTP/1.1
23823	2019-01-27 15:47:31,620270	82.195.224.128	10.0.0.13	HTTP	848 HTTP/1.1 200 OK (text/html)
23837	2019-01-27 15:47:31,636779	10.0.0.13	82.195.224.128	HTTP	420 GET /dist/css/bootstrap.css HTTP/1.1
23853	2019-01-27 15:47:31,684924	10.0.0.13	82.195.224.128	HTTP	442 GET /vendor/font-awesome/css/font-awesome.min.css HTTP/1.1
23883	2019-01-27 15:47:31,695946	10.0.0.13	82.195.224.128	HTTP	420 GET /assets/css/animate.css HTTP/1.1
23885	2019-01-27 15:47:31,695984	10.0.0.13	82.195.224.128	HTTP	406 GET /assets/new-js/jquery.js HTTP/1.1
23899	2019-01-27 15:47:31,705194	10.0.0.13	82.195.224.128	HTTP	407 GET /assets/new-js/plugins.js HTTP/1.1
23904	2019-01-27 15:47:31,715354	10.0.0.13	82.195.224.128	HTTP	409 GET /assets/new-js/functions.js HTTP/1.1
23929	2019-01-27 15:47:31,742718	82.195.224.128	10.0.0.13	HTTP	797 HTTP/1.1 200 OK (text/css)
23962	2019-01-27 15:47:31,749246	10.0.0.13	82.195.224.128	HTTP	419 GET /assets/js/core/jquery.backstretch.js HTTP/1.1
24004	2019-01-27 15:47:31,803715	82.195.224.128	10.0.0.13	HTTP	775 HTTP/1.1 200 OK (text/css)
24006	2019-01-27 15:47:31,804700	82.195.224.128	10.0.0.13	HTTP	410 HTTP/1.1 200 OK (text/css)
24016	2019-01-27 15:47:31,809122	82.195.224.128	10.0.0.13	HTTP	1514 [TCP Previous segment not captured] Continuation
24018	2019-01-27 15:47:31,809555	82.195.224.128	10.0.0.13	HTTP	1514 Continuation
24019	2019-01-27 15:47:31,810200	82.195.224.128	10.0.0.13	HTTP	1514 Continuation
24020	2019-01-27 15:47:31,810839	82.195.224.128	10.0.0.13	HTTP	1412 [TCP Previous segment not captured] Continuation
24066	2019-01-27 15:47:31,827902	10.0.0.13	82.195.224.128	HTTP	456 GET /assets/images/favicon/android-icon-192x192.png HTTP/1.
24067	2019-01-27 15:47:31,828049	10.0.0.13	82.195.224.128	HTTP	449 GET /assets/images/favicon/favicon-32x32.png HTTP/1.1
24127	2019-01-27 15:47:31,924420	82.195.224.128	10.0.0.13	HTTP	401 HTTP/1.1 200 OK (PNG)

Kako Wireshark beleži pakete sa slikama, te pakete možete sačuvati na računar u formatu slika (jpeg, png...). Kliknite na neki paket sa opisom HTTP/1.1 200 OK (PNG) ili HTTP/1.1 200 OK (JPEG), a zatim u donjem panelu (panel u kome je prikazana hijerarhija protokola) pronađite polje Portable Network Graphics (ako ste izabrali PNG sliku) ili na JPEG (ako ste izavbrali JPEG sliku), obično je ono poslednje u protokol hijerarhiji. U tom polju se nalaze dodatne informacije o izabranoj slici. Kliknite desnim klikom na samo polje, a zatim kliknite na Show Packet Bytes. Otvoriće vam se novi prozor sa prikazom izabrane slike i mogućnostima da prikažete sliku u raznim formatima (HTML, ASCII, Hex Dump, itd.) odakle možete da je sačuvate na vaš računar.



Pokušajte pingovati ruter R1 sa računara PC-1 i obrnuto. Pingovi bi trebalo da budu uspešni a paketi bi trebalo biti zabeleženi u Wireshark-u.

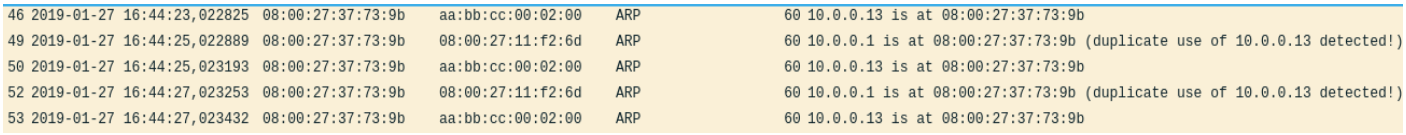
Sada proverite ARP tabelu na ruteru R1 i primetite da IP adrese 10.0.0.12 i 10.0.0.13 imaju istu MAC adresu, odnosno da svi paketi namenjeni ovim adresama zapravo završavaju na jednom uređaju.

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.1                -   aabb.cc00.0200  ARPA   Ethernet0/0
Internet  10.0.0.5               25   aabb.cc80.0100  ARPA   Ethernet0/0
Internet  10.0.0.11              16   0cc3.6d38.7100  ARPA   Ethernet0/0
Internet  10.0.0.12               2   0800.2737.739b  ARPA   Ethernet0/0
Internet  10.0.0.13               0   0800.2737.739b  ARPA   Ethernet0/0
Internet  192.168.1.206           -   aabb.cc00.0210  ARPA   Ethernet0/1
R1#
```

6.4. Detektovanje napada

Postoji nekoliko načina da se otkrije Arp Spoofing napad ili potencijalni napad. Otvorite ruter R1 i unesite komandu **debug arp table**. Ubrzo nakon toga ćete primećivati *syslog* poruke na ruteru koje ukazuju na to da se vrši neka izmena za adresu 10.0.0.13 (što je u ovom slučaju to adresa uređaja PC-1). Te poruke se konstanto prikazuju jer haker konstanto šalje lažne ARP pakete ruteru R1.

Drugi način jeste da se pokrene Wireshak na vezi između rutera R1 i sviča S1 i prate paketi kuda idu. Kada pokrente Wireshark, filtrirajte pakete da se samo ARP paketi prikazuju. Trebalo bi nešto slično slici ispod da dobijete.



Primetićete da gotovo svi paketi imaju istu izvornu MAC adresu a to je upravo MAC adresa hakera. Prvi paket nam govori da haker šalje ARP odgovor ruteru R1 (čija je mac adresa aa:bb:cc:00:02:00) da je MAC adresa uređaja 10.0.0.13 08:00:27:37:73:9b, dok nam drugi paket govori da haker šalje ARP odgovor uređaju PC-1 (čija je mac adresa 08:00:27:11:f2:6d) da je MAC adresa uređaja 10.0.0.1 zapravo njegova MAC adresa. Ali opis drugog paketa sadrži i dodatni tekst da je to zapravo duplikat MAC adresa, koju isto ima uređaj sa adresom 10.0.0.13.

Sada je potrebno proveriti kuda idu paketi zapravo kada kreću od adrese 10.0.0.1 do adrese 10.0.0.13. Prvo na ruteru unesite komandu **debug ip icmp**, zatim u Wireshark-u filtrirajte ICMP pakete i na kraju pingujte adresu 10.0.0.13 sa rutera R1. Rezultati pinga su prikazani ispod.

```
R1# ping 10.0.0.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Jan 27 16:59:56.359: ICMP: redirect rcvd from 10.0.0.12- for 10.0.0.13 use gw
10.0.0.13
*Jan 27 16:59:56.360: ICMP: echo reply rcvd, src 10.0.0.13, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Jan 27 16:59:56.361: ICMP: echo reply rcvd, src 10.0.0.13, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Jan 27 16:59:56.362: ICMP: echo reply rcvd, src 10.0.0.13, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Jan 27 16:59:56.363: ICMP: echo reply rcvd, src 10.0.0.13, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Jan 27 16:59:56.365: ICMP: echo reply rcvd, src 10.0.0.13, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
R1#
```

4233	2019-01-27 16:59:56,359602	10.0.0.12	10.0.0.1	ICMP	142	Redirect (Redirect for host)
4234	2019-01-27 16:59:56,359629	10.0.0.1	10.0.0.13	ICMP	114	Echo (ping) request id=0x0002, seq=0/0, ttl=254 (reply in 4235)
4235	2019-01-27 16:59:56,360274	10.0.0.13	10.0.0.1	ICMP	114	Echo (ping) reply id=0x0002, seq=0/0, ttl=63 (request in 4234)
4236	2019-01-27 16:59:56,360473	10.0.0.1	10.0.0.13	ICMP	114	Echo (ping) request id=0x0002, seq=1/256, ttl=255 (reply in 4237)
4237	2019-01-27 16:59:56,361426	10.0.0.13	10.0.0.1	ICMP	114	Echo (ping) reply id=0x0002, seq=1/256, ttl=63 (request in 4236)
4238	2019-01-27 16:59:56,361686	10.0.0.1	10.0.0.13	ICMP	114	Echo (ping) request id=0x0002, seq=2/512, ttl=255 (reply in 4239)
4239	2019-01-27 16:59:56,362635	10.0.0.13	10.0.0.1	ICMP	114	Echo (ping) reply id=0x0002, seq=2/512, ttl=63 (request in 4238)
4240	2019-01-27 16:59:56,362818	10.0.0.1	10.0.0.13	ICMP	114	Echo (ping) request id=0x0002, seq=3/768, ttl=255 (reply in 4241)
4241	2019-01-27 16:59:56,363775	10.0.0.13	10.0.0.1	ICMP	114	Echo (ping) reply id=0x0002, seq=3/768, ttl=63 (request in 4240)
4242	2019-01-27 16:59:56,363986	10.0.0.1	10.0.0.13	ICMP	114	Echo (ping) request id=0x0002, seq=4/1024, ttl=255 (reply in 4243)
4243	2019-01-27 16:59:56,364965	10.0.0.13	10.0.0.1	ICMP	114	Echo (ping) reply id=0x0002, seq=4/1024, ttl=63 (request in 4242)

I na ruteru i u Wireshark-u se može primetiti da paketi ne idu direktno ka 10.0.0.13, već da idu prvo ka 10.0.0.12 odakle se radi redirekcija ka 10.0.0.13 adresi.

Sada nam je sasvim jasno da je došlo do ARP Spoofing napada, odnosno da se neko lažno predstavlja kao uređaj sa adresom 10.0.0.13 i da prvi preuzima (dobija), a zatim preusmerava sve pakete.

7. Sprečavanje napada pomoću Dynamic ARP Inspection (DAI)

Sprečavanje Arp spoofing napada se vrši pomoću **Dynamic ARP Inspection (DAI)** mogućnosti koja se konfiguriše na sviču. Kada se DAI omogući na sviču, on proverava veze između IPv4 i MAC adresa pomoću DHCP snooping binding tabele. Kada dođe do nepoklapanja adresa na nepoverljivom portu (*untrusted port*), DAI će odbaciti lažni paket.

DAI proverava samo one pakete koji dolaze sa nepoverljivih portova, a može biti omogućen ili globalno po VLAN-u ili pojedinačno na određenom portu. Podrazumevano su svi portovi nepoverljivi.

Otvorite svič S1 i prvo omogućite globalno DAI.

```
S1(config)# ip arp inspection vlan 1
```

Zatim podesite interfejs na koji je povezan sa ruterom R1 da bude poverljiv.

```
S1(config)# interface Ethernet 0/0
S1(config-if)# ip arp inspection trust
S1(config-if)# end
S1#
```

Ubrzo nakon toga bi trebalo da primetite *syslog* poruke na sviču slične ovima ispod.

```
*Jan 27 17:22:38.880: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on
Et0/2, vlan 1.([0800.2737.739b/10.0.0.12/aabb.cc00.0200/10.0.0.1/18:22:38 CET
Sun Jan 27 2019])
*Jan 27 17:22:38.880: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on
Et0/1, vlan 1.([0cc3.6d38.7100/10.0.0.11/aabb.cc00.0200/10.0.0.1/18:22:38 CET
Sun Jan 27 2019])
```

Iz njih možemo zaključiti da neispravni ARP paketi stižu na interfejsima Ethernet 0/1 i 0/2 kao i koje adrese pokušavaju da ih pošalju i kome. S obzirom da je podešeno da se samo na Ethernet 0/0 interfejsu radi DAI provera, haker i dalje može da šalje lažne ARP pakete uređaju PC-1 s tim što uređaj PC-1 neće moći da izađe van mreže niti da pristupi ruteru jer je i njemu zabranjen prolaz van Ethernet 0/0 interfejsa.

S obzirom da smo utvrdili da je MAC adresa 0800.2737.739b, zapravo maliciozna adresa i da to nije MAC adresa uređaja sa IP adresom 10.0.0.13, pomoću komande **show mac address-table** možemo videti pravu MAC adresu tog uređaja kao i interfejs na koji je povezan.

```
S1# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  1    0800.2711.f26d    DYNAMIC     Et1/0
  1    0800.2737.739b    DYNAMIC     Et0/2
  1    0cc3.6d38.7100    DYNAMIC     Et0/1
  1    aabb.cc00.0200    DYNAMIC     Et0/0
Total Mac Addresses for this criterion: 4
S1#
```

Iz tabele vidimo da maliciozna MAC adresa dolazi sa porta Ethernet 0/2, te je prvo potrebno ugasiti taj port kako bi isključili hakera iz mreže.

```
S1(config)# interface Ethernet 0/2
S1(config-if)# shutdown
S1(config-if)# exit
```

Zatim iz DHCP binding tabele možemo pogledati MAC adresu uređaja 10.0.0.13 i videti u MAC tabeli na kojem je portu povezan i konfigurisati ga kao poverljivi port.

```
S1(config)# interface Ethernet 1/0
S1(config-if)# ip arp inspection trust
S1(config-if)# end
S1#
```

Očistite ARP tabelu na ruteru R1 i nakon nekog vremena će se ažurirati ponovo samo ovaj put sa pravim MAC adresama, a uređaj PC-1 će moći normalno da izlazi van mreže i da pristupa ruteru R1 bez redirekcije paketa što možete proveriti pingovanjem ili otvaranjem neke veb stranice.

```
R1# clear arp
```