Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Treća laboratorijska vežba -

ARP spoofing.

Za vežbu *ARP 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).
Uloge virtuelnih mašina će biti:

- VM1 – napadnuti uređaj koji će dobijati lažne *ARP* odgovore kada želi da komunicira sa VM3
- VM2 – napadač koji će *arpspoofing* napadom naterati VM1 da njegova komunikacija sa VM3 prođe kroz VM2
- VM3 – *web server* na koji se povezuje VM1

Programom *Putty* povezati se *SSH* protokolom na tri virtuelne mašine: jedna veza ka VM1, tri veze ka VM2 i jedna veza ka VM3. Na svim uređajima komandom *ifconfig* pronaći i zabeležiti *MAC* adrese na interfejsima *eth0* sve tri virtuelne mašine.

FAZA 1 – Nema *ARP spoofing* napada.

1. Pomoću *WinSCP* se povezati na VM3 (ista adresa i kredencijali kao i za *SSH* vezu) i postaviti fajl *SimpleAuthServer.py* u folder na putanji *home/student/Documents/web/*
2. Na VM3 podići prost *web* server sledećim komandama:
   `cd Documents/web`
   `sudo python SimpleAuthServer.py 80 username:password` (username i password su korisničko ime i lozinka koji se koriste na *web* serveru i mogu da se promene po želji).
3. Na VM2 u prozoru 1 instalirati potreban alat komandom
   `sudo apt install wireshark`
   a zatim pokrenuti snimanje paketa komandom:
   `sudo dumpcap -i eth0 -w /tmp/cap2.pcapng`
4. Na VM1 se povezati pomoću *VNC*. Po povezivanju pokrenuti *Firefox web browser* i otići na adresu 192.168.**x**.3. U prozor upisati kredencijale.
5. Po završetku uspešne komunikacije sa *web* serverom prekinuti snimanje paketa na VM2 u prozoru 1 (*CTRL+C*) i prebaciti fajl sa snimljenim paketima na VM2 i dati privilegije za čitanje fajla sledećim komandama:
   `sudo mv /tmp/cap2.pcapng /home/student/Documents/`
   `sudo chmod +rw cap2.pcapng`
6. Pomoću *WinSCP* se povezati na VM2 (ista adresa i kredencijali kao i za *SSH* vezu) i preuzeti fajl *cap2.pcapng*.
7. U *Wireshark* alatu analizirati preuzeti fajl. Da li se u njemu pojavljuje komunikacija između VM1 i VM3? Zašto?
8. Ugasiti *WinSCP* sesiju da u kasnijim fazama rada ova komunikacija ne bi nepotrebno povećala količinu snimljenih paketa.

FAZA 2 – *ARP spoofing*

1. Na VM2 u prozoru 1 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. Na VM2 u prozoru 2 instalirati potreban alat komandom
   `sudo apt install dsniff`
   a zatim pokrenuti *ARP spoofing* sledećom komandom
   `sudo arpspoof -i eth0 -t 192.168.x.1 192.168.x.3`
   (komanda se pokreće na interfejsu eth0, meta napada je VM1, a podmeće se lažna adresa za VM3)
3. Na VM2 u prozoru 3 pokrenuti *ARP spoofing* u drugom smeru sledećom komandom
   `sudo arpspoof -i eth0 -t 192.168.x.3 192.168.x.1`
4. Na VM2 u prozoru 1 pokrenuti snimanje paketa komandom:
   `sudo dumpcap -i eth0 -w /tmp/cap2.pcapng`
5. Na VM1 očistiti *ARP* ulaz za VM3 sledećom komandom
   `sudo arp -d 192.168.x.3`
6. Na VM1 pokrenuti snimanje paketa komandom:
   `sudo dumpcap -i eth0 -w /tmp/cap1.pcapng`
7. Na VM1 se povezati pomoću *VNC*. Po povezivanju pokrenuti *Firefox web browser* i otići na adresu 192.168.**x**.3. U prozor upisati kredencijale.
8. Po završetku uspešne komunikacije sa *web* serverom prekinuti snimanje paketa na VM1 i VM2 u prozoru 1 (*CTRL+C*) i prebaciti fajl sa snimljenim paketima na VM1 i VM2 i dati privilegije za čitanje fajla sledećim komandama (prve dve komande u prozoru 1 mašine VM2, druge dve komande na mašini VM1):
   ```
   sudo mv /tmp/cap2.pcapng /home/student/Documents/
   sudo chmod +rw cap2.pcapng
   sudo mv /tmp/cap1.pcapng /home/student/Documents/
   sudo chmod +rw cap1.pcapng
   ```
9. Pomoću *WinSCP* se povezati na VM1 i VM2 (ista adresa i kredencijali kao i za *SSH* vezu) i preuzeti fajlove *cap1.pcapng* i *cap2.pcapng*.
10. U *Wireshark* alatu analizirati preuzete fajlove.
    a. Da li se u fajlu *cap2.pcapng* pojavljuje komunikacija između VM1 i VM3?
    b. Koje su *MAC* adrese u paketima koji su namenjeni za VM3? Zašto postoje po dva ista paketa između VM1 i VM3? Koje su *MAC* adrese na njima?
    c. Da li se na VM2 vide *ARP* paketi kojima se VM1 vara tako što mu se podmeće lažna *MAC* adresa?
    d. Da li se u paketima koji prolaze kroz VM2 vide kredencijali koji su korišćeni za logovanje na *web* server? (po potrebi koristiti alat za konverziju *base64* u tekst, npr. *web* alat *base64decode.com*)
    e. Da li su u pitanju isti paketi kao oni koji su zabeleženi na VM1?