Adrian.Amarfii 28/10/2022

Report
Task

Per prima cosa

Nell'esercizio di oggi metteremo insieme le competenze acquisite finora. Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux IP 192.168.32.100
- Windows 7 IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

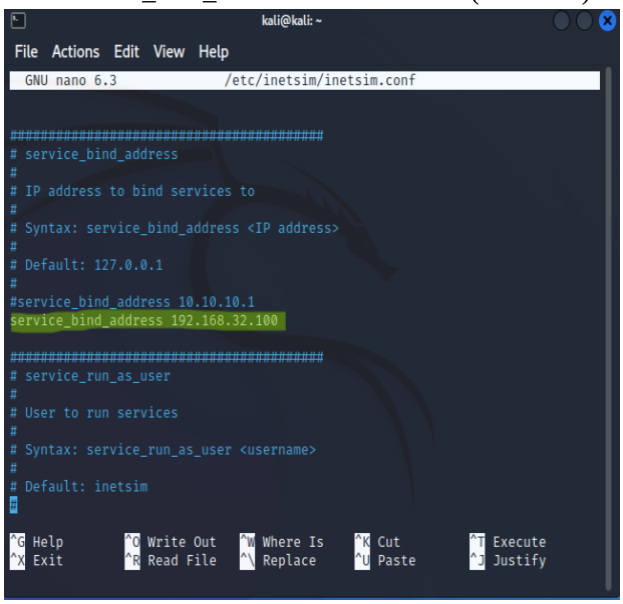
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100.

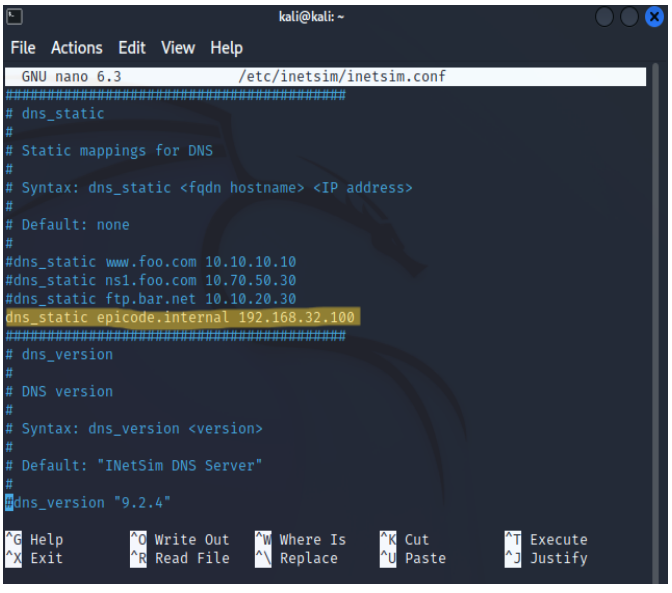
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze.

andiamo a cambiare IP dei 2 sistemi (Windows e Kali)
a)Kali → aprendo il Terminal emulator digitiamo ..sudo nano etc/network/interfaces dopo di che andiamo a modificare il IP inserendo quello che l'esercizio ci richiede (192.168.32.100)
b)su Windows 7 → apriamo il contro panel → network and internet→ change adapter settings → local area conection→ properties→ internet protocol verion 4 e andiamo a impostare l'IP chiesto nell'esercizio (192.168.32.101)

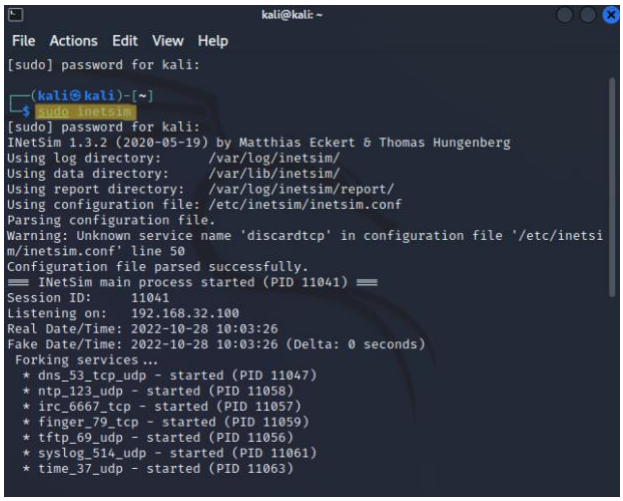
Configurazioni Kali: Dopo aver finito di impostare l'IP ai entrambi i sistemi (Kali,Windows 7)procediamo con la confugarzione del sinetsim → Aprimamo il Terminal Emulator e digitiamo _sudo nano / etc / inetsim /inetsim.conf
Adiamo a cercare la parte dove ci viene dato l'indirizzio Ip → la seguente foto mostra anche le modifiche che bisogna fare : service_bind_address 192.168.32.100(IP di Kali) :dns_static epicode.internal 192.168.32.100



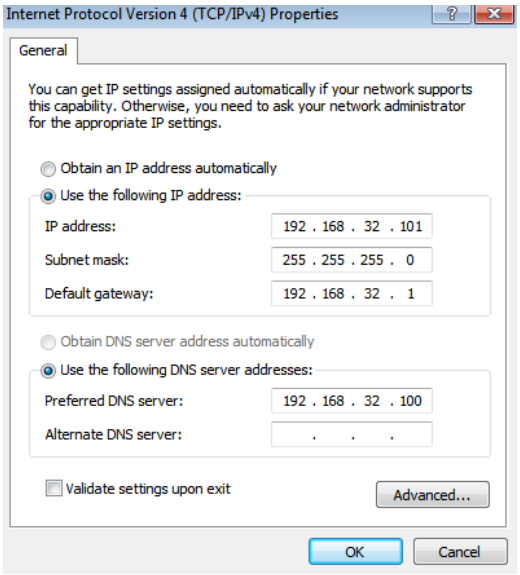


Configurazione Windows 7:

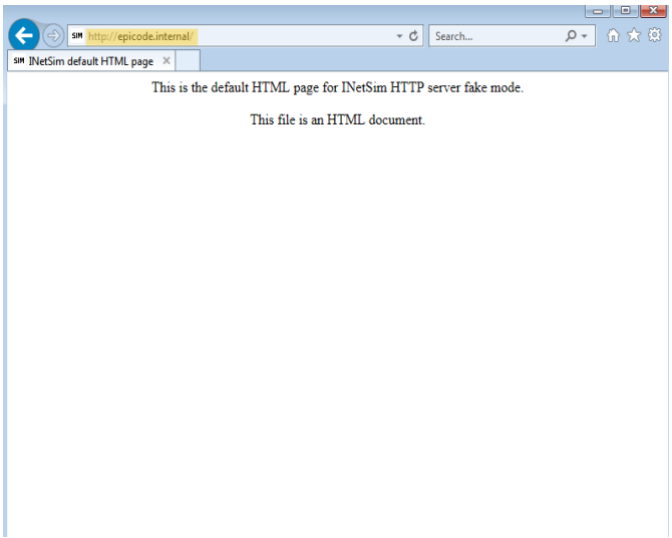
Apriamo Kali e andiamo su Terminal Emulator
e digitiamo: sudo inetsim e diamo avvia alla sessione
Apriamo anche Wireshark per riuscire a catturare i pacchetti

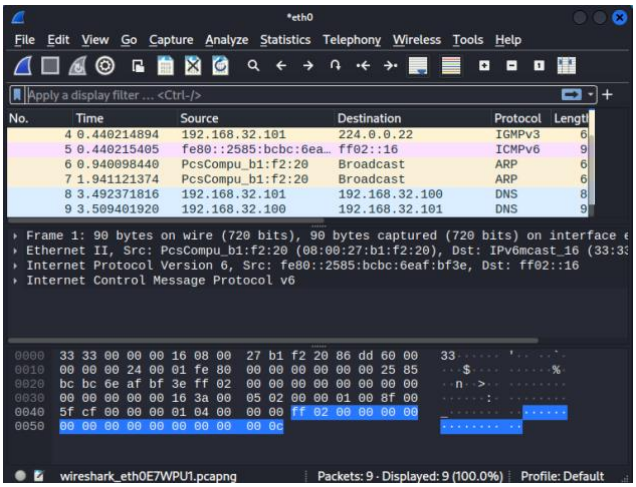


1Impostiamo il IP DNS server e il Default gateway.

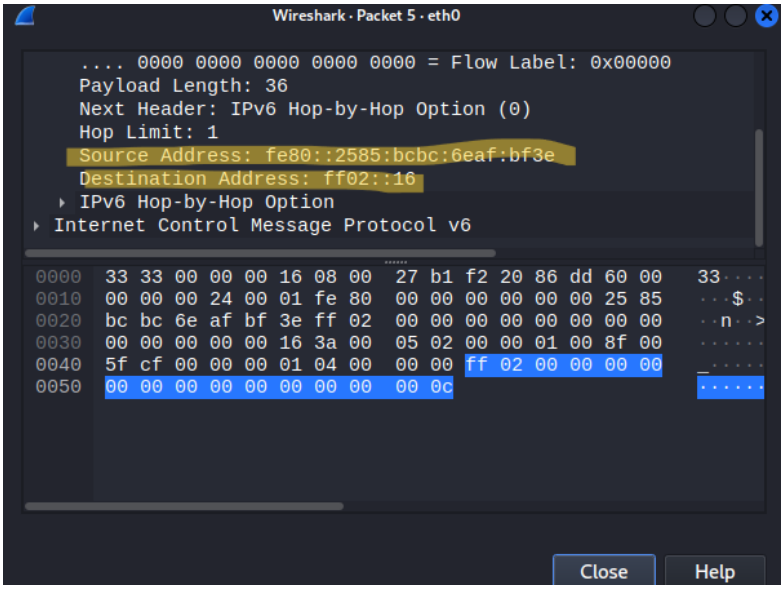


Avendo aperte intrambe le machine virtuali andiamo su internet explorer su Windows 7 e digitiamo nella bara di ricerca epicode.internal .Nello stesso momento andiamo su Kali con Wireshark attivo e clicanto su eth0 2 volte riusciamo a vedere i pacchetti .

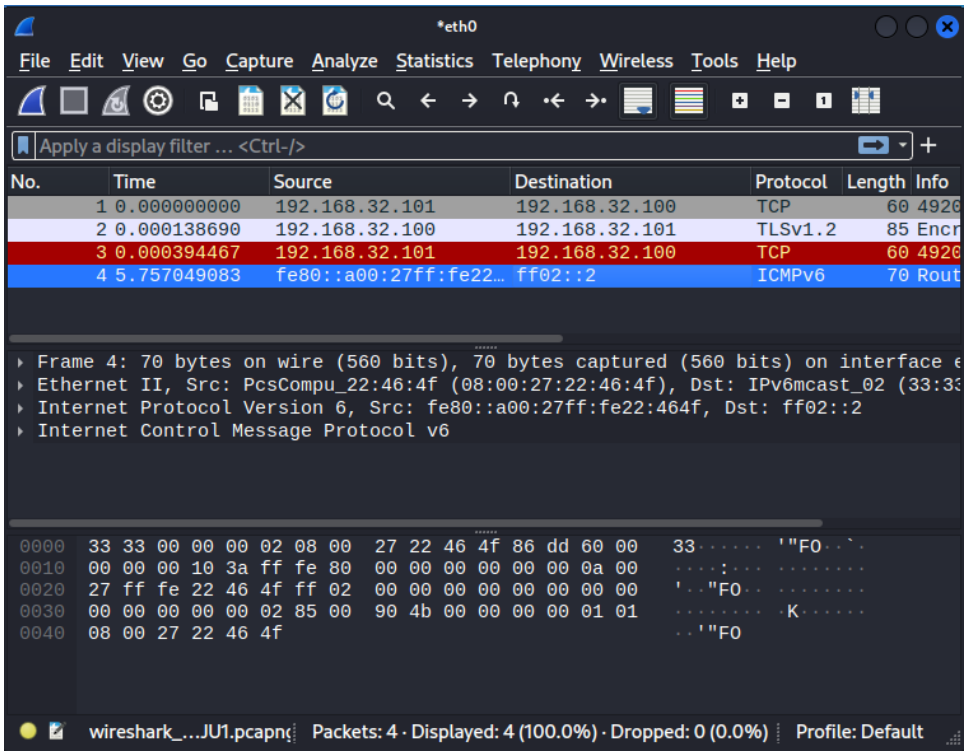




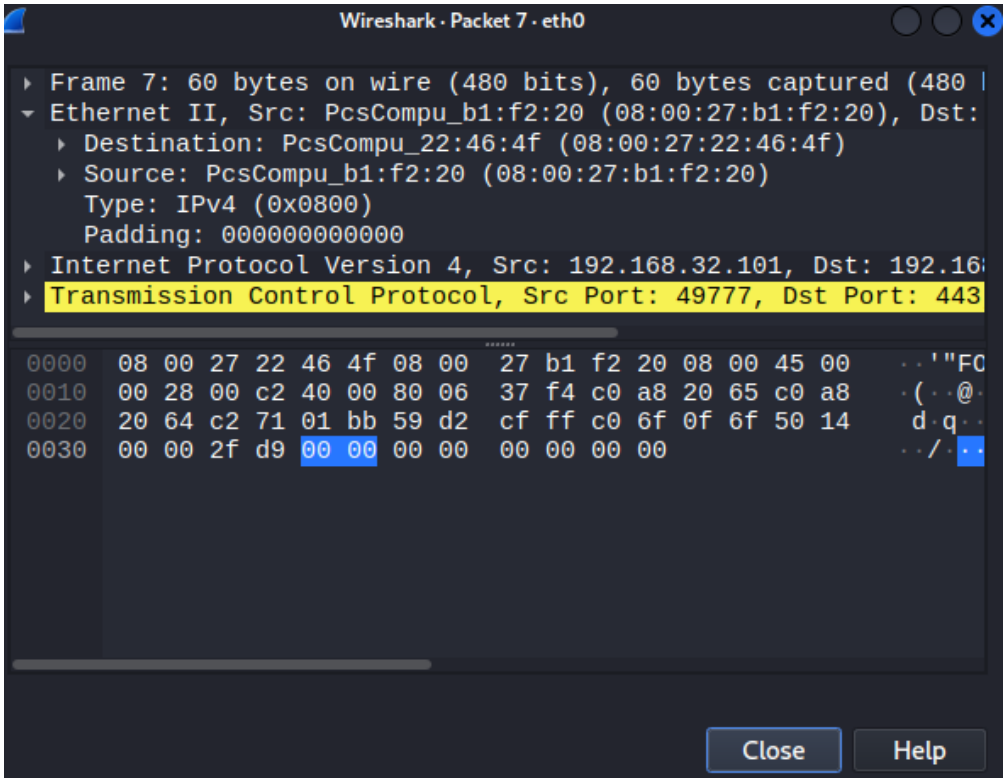
Selezionando un qualsiasi pacchetto e facendo doppio click riusciamo a vedere in modo accurato la MAC address della sorgente e della destinazione e il contenuto in se come nella seguente foto : (HTTP)



Nel seguente passaggio bisogna vedere cosa e come si cambia il MAC adress ,quando al posto di HTTP mettiamo HTTPS.Si va sulla bara di ricerca di Internet Explorer su Windows 7 e si aggiunge una S vicino al link di epicode.internal : ESEMPIO→ http://epicode.internal →https://epicode.internal . Fatto cio seguiamo i passaggi detti prima con wireshark.



Facciamo doppio clik sul pacchetto numero 3 ci viene fuori in rosso perche non riusciamo a guardare per esempio il contenuto .Poiché il HTTPS serve per verificare se il sito e falso o no.


Wireshark · Packet 7 · eth0
Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480
Ethernet II, Src: PcsCompu_b1:f2:20 (08:00:27:b1:f2:20), Dst:
Destination: PcsCompu_22:46:4f (08:00:27:22:46:4f)
Source: PcsCompu_b1:f2:20 (08:00:27:b1:f2:20)
Type: IPv4 (0x0800)
Padding: 000000000000
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.16
Transmission Control Protocol, Src Port: 49777, Dst Port: 443
0000 08 00 27 22 46 4f 08 00 27 b1 f2 20 08 00 45 00
0010 00 28 00 c2 40 00 80 06 37 f4 c0 a8 20 65 c0 a8
0020 20 64 c2 71 01 bb 59 d2 cf ff c0 6f 0f 6f 50 14
0030 00 00 2f d9 00 00 00 00 00 00 00 00
Close
Help