CS 02-23

05/2023

SIMULAZIONE RETE COMPLESSA

PREPARATO E PRESENTATO DA

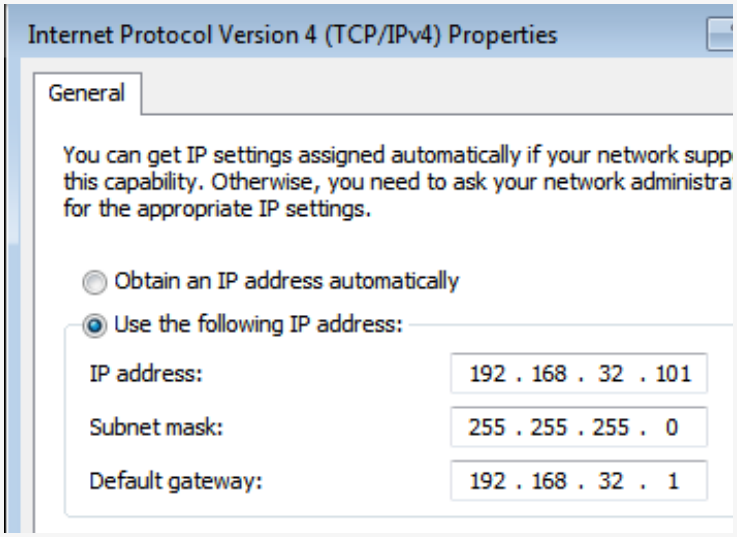
ALESSANDRO BOSSI

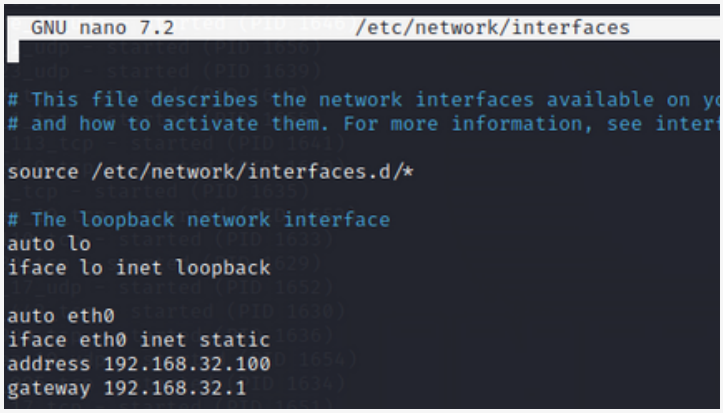
AMBIENTE DI DI RETE

FASE 01

SONO PARTITO INSTALLANDO LA ORACLE VIRTUAL BOX, L'AMBIENTE VIRTUALE PER L'ESERCIZIO SARÀ COSTITUITO DA UNA MACCHINA CON SO KALI LINUX (HOST) E UN'ALTRA CON WINDOWS 7 (GUEST) ENTRAMBI SONO SETTATI CON SCHEDA DI RETE INTERNA.

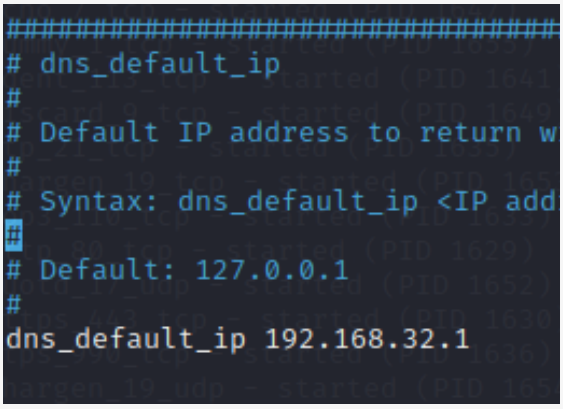
FASE 02

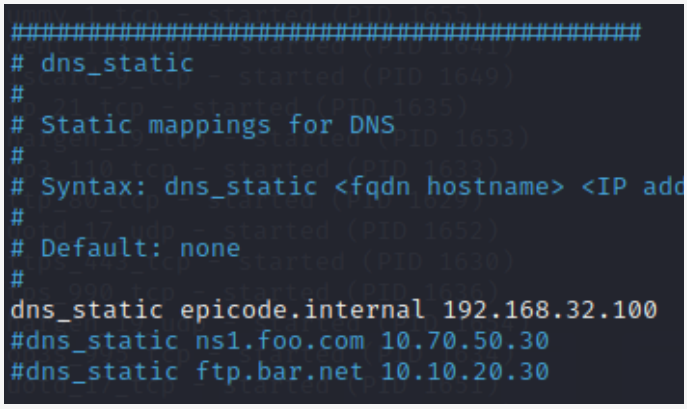


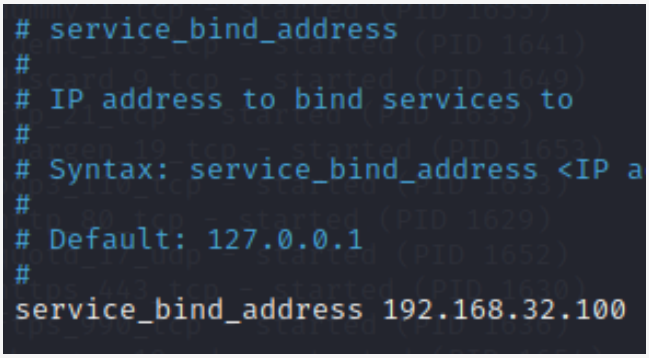


HO SUCCESSIVAMENTE SETTATO GLI IP SIA DI KALI CHE DI WINDOWS COME STATICI E LO STESSO GATEWAY PER IMPOSTARE UNA RETE TRA LE DUE MACCHINE

FASE 03

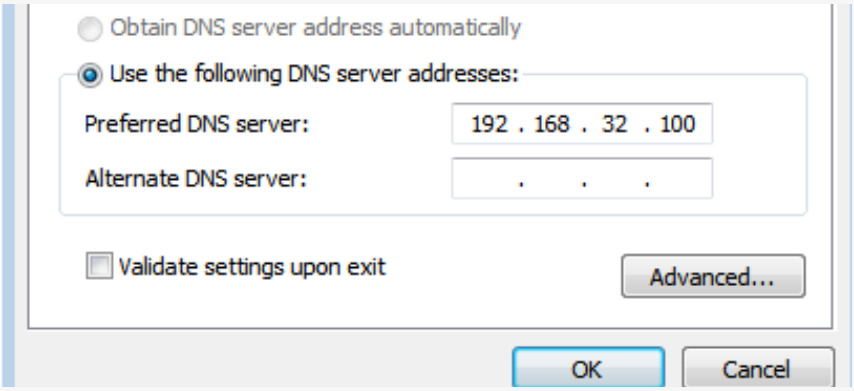






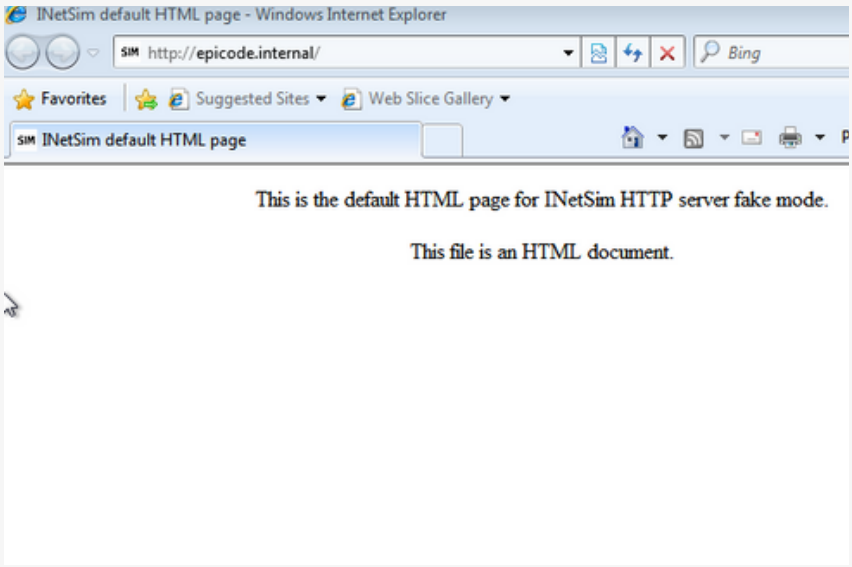
SUCCESSIVAMENTE HO VERIFICATO CHE SUL SISTEMA KALI FOSSE PRESENTE IL PROGRAMMA "INETSIM" PER SIMULARE UN SERVIZIO INTERNET CON DNS. COME SI VEDE DAGLI SCREENSHOT HO DOVUTO IMPOSTARE IL DNS DI INETSIM METTENDO COME INDIRIZZO IP STATICO QUELLO DELLA MACCHINA CON KALI, HO INOLTRE SETTATO UN HOSTNAME "EPICODE.INTERNAL" CHE RICHIAMI L'IP DEL DNS.

FASE 04



COME PASSO SUCCESSIVO HO INSERITO SU WINDOWS IL SERVER DNS CHE HO APPENA IMPOSTATO IN MANIERA TALE CHE MI RISPONDESSE ANCHE SU QUESTA MACCHINA.

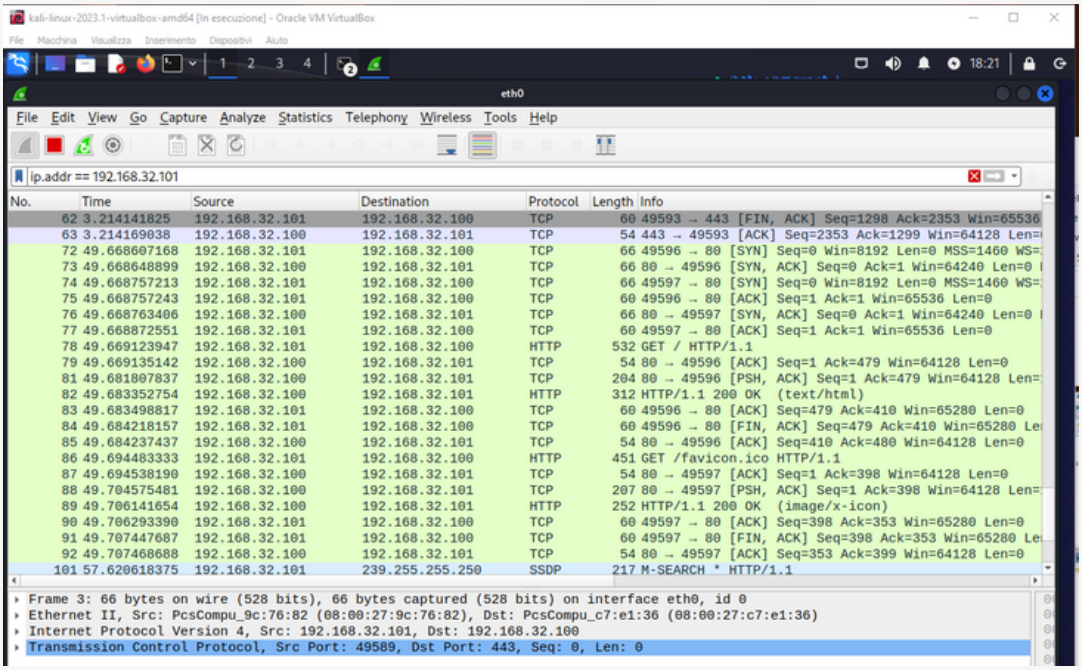
FASE 05



IN QUESTA MANIERA HO POTUTO TRAMITE BROWSER RICHIEDERE UNA RISORSA ALL'HOSTNAME EPICODE.INTERNAL APRENDO LA PAGINA DI INETSIM

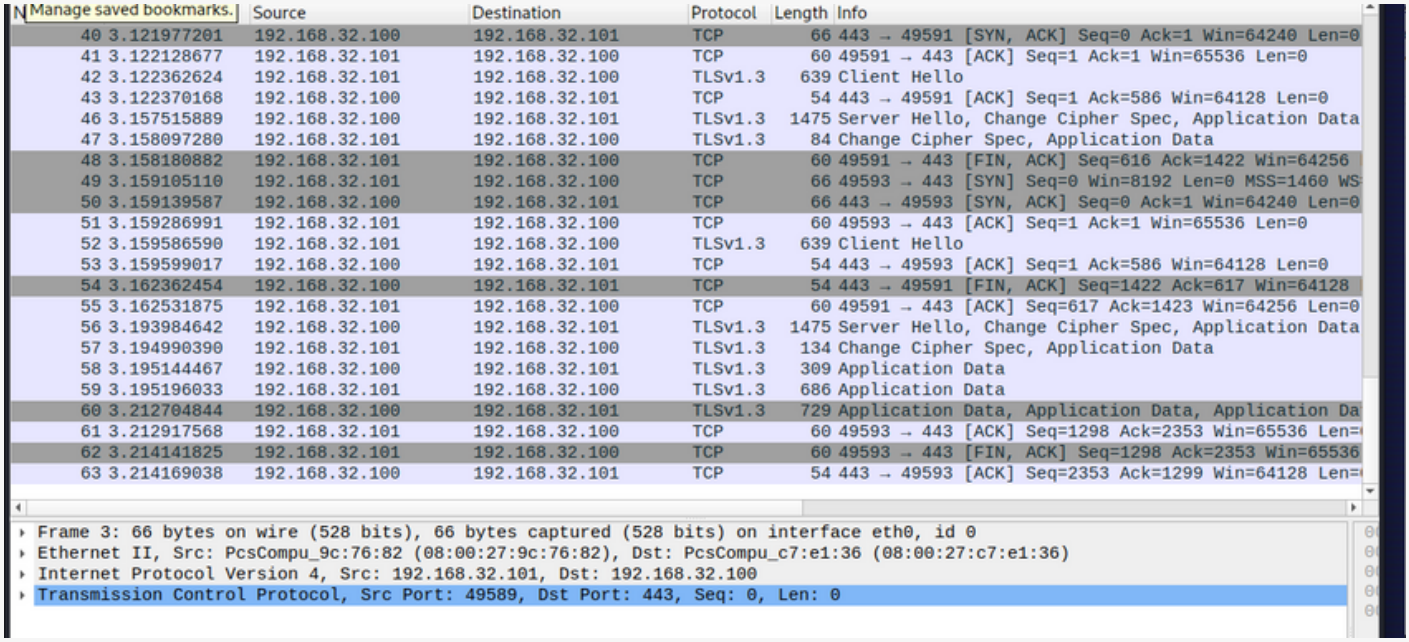
LETTURA PACCHETI CON WIRESHARK

FASE 06



LA FASE SUCCESSIVA È STATA QUELLA DI UTILIZZARE IL PROGRAMMA "WIRESHARK" PER ANALIZZARE I PACCHETTI CHE VENIVANO RICEVUTI TRA LE DUE MACCHINE, HO QUINDI RICHIESTO SIA TRAMITE PROTOCOLLO HTTP CHE HTTPS LA RISORSA EPICODE.INTERNAL

FASE 07



No.	Time	Source	Destination	Protocol	Length	Info
40	3.121977201	192.168.32.100	192.168.32.101	TCP	66	443 → 49591 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
41	3.122128677	192.168.32.101	192.168.32.100	TCP	60	49591 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
42	3.122362624	192.168.32.101	192.168.32.100	TLSv1.3	639	Client Hello
43	3.122370168	192.168.32.100	192.168.32.101	TCP	54	443 → 49591 [ACK] Seq=1 Ack=586 Win=64128 Len=0
46	3.157515889	192.168.32.100	192.168.32.101	TLSv1.3	1475	Server Hello, Change Cipher Spec, Application Data
47	3.158097280	192.168.32.101	192.168.32.100	TLSv1.3	84	Change Cipher Spec, Application Data
48	3.158180882	192.168.32.101	192.168.32.100	TCP	60	49591 → 443 [FIN, ACK] Seq=616 Ack=1422 Win=64256
49	3.159105110	192.168.32.101	192.168.32.100	TCP	66	49593 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS
50	3.159139587	192.168.32.100	192.168.32.101	TCP	66	443 → 49593 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
51	3.159286991	192.168.32.101	192.168.32.100	TCP	60	49593 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
52	3.159586590	192.168.32.101	192.168.32.100	TLSv1.3	639	Client Hello
53	3.159599017	192.168.32.100	192.168.32.101	TCP	54	443 → 49593 [ACK] Seq=1 Ack=586 Win=64128 Len=0
54	3.162362454	192.168.32.100	192.168.32.101	TCP	54	443 → 49591 [FIN, ACK] Seq=1422 Ack=617 Win=64128
55	3.162531875	192.168.32.101	192.168.32.100	TCP	60	49591 → 443 [ACK] Seq=617 Ack=1423 Win=64256 Len=0
56	3.193984642	192.168.32.100	192.168.32.101	TLSv1.3	1475	Server Hello, Change Cipher Spec, Application Data
57	3.194990390	192.168.32.101	192.168.32.100	TLSv1.3	134	Change Cipher Spec, Application Data
58	3.195144467	192.168.32.100	192.168.32.101	TLSv1.3	309	Application Data
59	3.195196033	192.168.32.101	192.168.32.100	TLSv1.3	686	Application Data
60	3.212704844	192.168.32.100	192.168.32.101	TLSv1.3	729	Application Data, Application Data, Application Da
61	3.212917568	192.168.32.101	192.168.32.100	TCP	60	49593 → 443 [ACK] Seq=1298 Ack=2353 Win=65536 Len=
62	3.214141825	192.168.32.101	192.168.32.100	TCP	60	49593 → 443 [FIN, ACK] Seq=1298 Ack=2353 Win=65536
63	3.214169038	192.168.32.100	192.168.32.101	TCP	54	443 → 49593 [ACK] Seq=2353 Ack=1299 Win=64128 Len=

```
▸ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_9c:76:82 (08:00:27:9c:76:82), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 49589, Dst Port: 443, Seq: 0, Len: 0
```

ANALIZZANDO LE IMMAGINI LE PRINCIPALI DIFFERENZE CHE HO NOTATO A PRIMA VISTA TRA LA CATTURA DI PACCHETTI CON HTTP (PRIMO SCREENSHOT) E HTTPS (SECONDO SCREENSHOT) È STATA SICURAMENTE LA PRESENZA IN HTTPS DEL PROTOCOLLO TLSV1.3 OLTRE A QUELLO TCP, QUESTO PROTOCOLLO VIENE USATO PER GARANTIRE UN LIVELLO DI SICUREZZA MAGGIORE AI PACCHETTI CHE RISULTANO ESSERE CIFRATI.
NELLO SCREEN SOTTOSTANTE INVECE POSSIAMO VEDERE COME ALL'INTERNO DEI PACCHETTI POSSIAMO TROVARE GLI INDIRIZZI MAC DI DESTINAZIONE (DESTINATION) E DI SORGENTE (SOURCE)

```
rame 60: 729 bytes on wire (5832 bits), 729 bytes captured (5832 bits) on interface eth0, id 0
thernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_9c:76:82 (08:00:27:9c:76:82)
 Destination: PcsCompu_9c:76:82 (08:00:27:9c:76:82)
    Address: PcsCompu_9c:76:82 (08:00:27:9c:76:82)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 Source: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
    Address: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 Type: IPv4 (0x0800)
nternet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
ransmission Control Protocol, Src Port: 443, Dst Port: 49593, Seq: 1677, Ack: 1298, Len: 675
ransport Layer Security
```

CONCLUSIONI

UTILIZZANDO UN SIMULATORE DI RETE SONO RIUSCITO AD APRIRE UNA FINTA PAGINA WEB SULLA RETE INTERNA CHE È STATA IMPOSTATA. CON WIRESHARK È STATO POSSIBILE INVECE VISUALIZZARE I PACCHETTI CHE VENGONO SCAMBIATI DAI DUE PC.
PER EFFETTUARE IL REPORT HO CERCATO DI ESSERE IL PIU' SINTETICO POSSIBILE ED HO IMPOSTATO LA COMUNICAZIONE COME SE DOVESSE ESSERE CONSEGNATO AD UN CLIENTE FINALE. GRAZIE.