Progetto Finale M1

Intercettare, mediante l'utilizzo di Wireshark, il traffico HTTPS tra Kali e Windows con l'URL epicode.internal.

Il fine del progetto è quello di intercettare, mediante Wireshark, il traffico criptato tra la VM Kali e Windows con la connessione all'URL epicode.internal.

Per prima cosa imposto un IPV4 statico ad entrambe le VM. Per la Kali viene impostato un IP 192.168.32.100, mentre per Windows IP 192.168.32.101

Se provo ad eseguire un ping tra le macchine vedo che funziona quindi riescono a comunicare. (Figura 1).

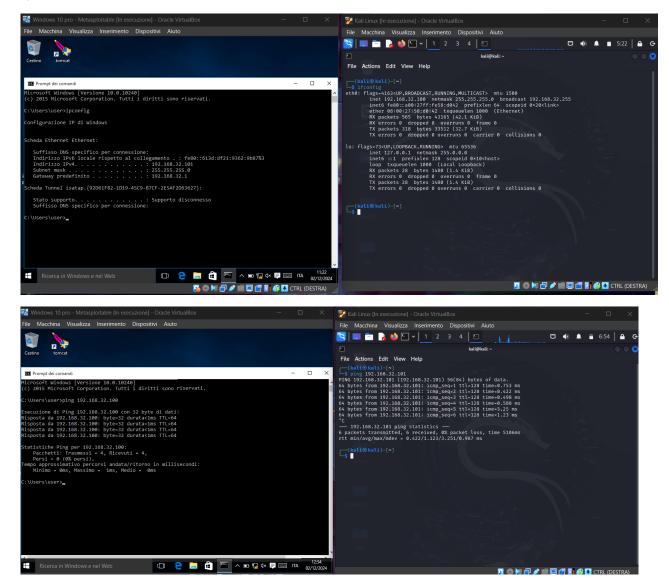


Figura 1

Dovrò simulare il traffico HTTPS quindi, sulla VM Kali avvio utilizzerò l'applicativo **inetsim.** Per usare tale applicativo devo prima modificare il file di configurazione per permettere al servizio di funzionare solamente con il traffico HTTPS. Per fare ciò, sulla VM Kali, userò il comando *sudo nano* /etc/inetsim/inetsim.conf. A questo file di configurazione andrò a disattivare i servizi che, al momento, non sono necessari per lo svolgimento della prova, mediante l'apposizione di un # prima del servizio (Figura 2).

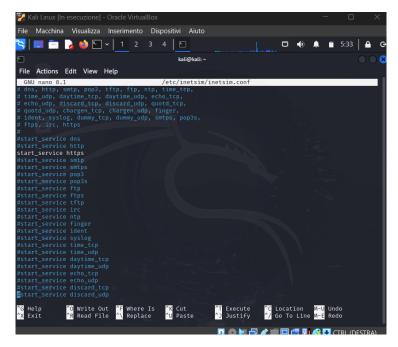


Figura 2

Una volta modificato il file di configurazione devo attivare il servizio mediante il comando sudo inetsim

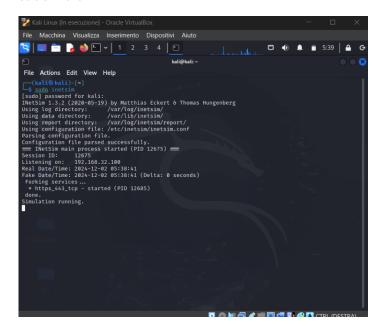


Figura 3

A questo punto devo attivare il servizio DNS per poter risolvere l'indirizzo **epicode.internal** in indirizzo IP 192.168.32.100. Per fare ciò utilizzo l'applicativo dnschef mediante il comando

dnschef ---fakedomains epicode.internal ---fakeip 192.168.32.100 -i 192.168.32.100

Adesso utilizzerò la VM Windows per poter verificare se il lavoro svolto funziona correttamente. Apro il browser Microsoft Edge ed inserisco l'indirizzo https://epicode.internal. Qui compare l'avviso di sicurezza relativo al certificato ssl (*Figura 4*), clicco su prosegui e vado avanti e mi viene mostrata la pagina HTML del server presente sulla kali (*Figura 5*).

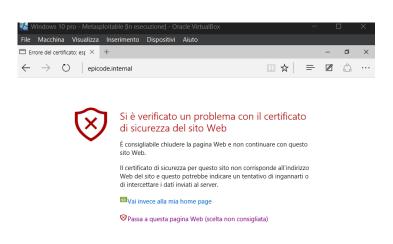




Figura 4

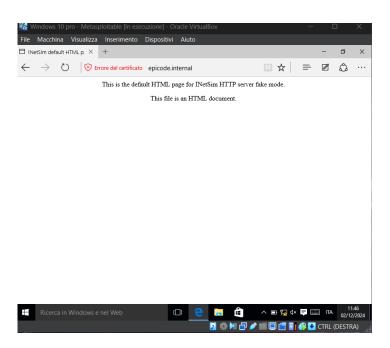


Figura 5

A questo punto chiudo il browser ed attivo Wireshark per poter catturare il traffico HTTPS che avviene tra le 2 VM. Appena attivato Wireshark e selezionato l'interfaccia eth0, viene mostrato lo scambio dati che avviene tra le macchine (*Figura 6*).

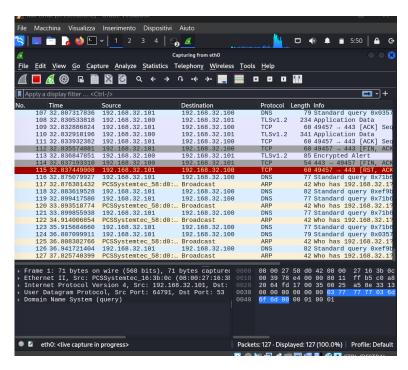


Figura 6

Dopo aver fatto comunicare le 2 macchine, ho impostato il filtro(tcp.port==443 per poter visualizzare solamente il traffico https. Selezionando un pacchetto tra quelli filtrati si viene a determinare l'indirizzo MAC sorgente e di destinazione, indirizzi IP sorgenti e destinazione insieme al contenuto della richiesta. (*Figura 7*)

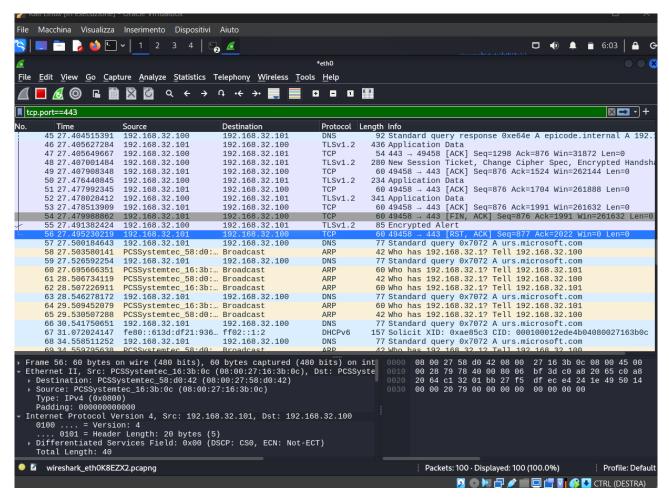


Figura 7

Intercettare, mediante l'utilizzo di Wireshark, il traffico HTTP tra Kali e Windows con l'URL epicode.internal.

Come per l'esercizio precedente dovrò catturare il traffico tra le 2 VM, tramite l'utilizzo di Wireshark, ma questa volta dovrò catturare il traffico HTTP.

Per fare ciò sulla VM Kali andrò ad aprire il file di configurazione del servizio inetsim ed andrò ad attivare il servizio http, disattivando il servizio https mediante l'apposizione di un # (Figura 8).

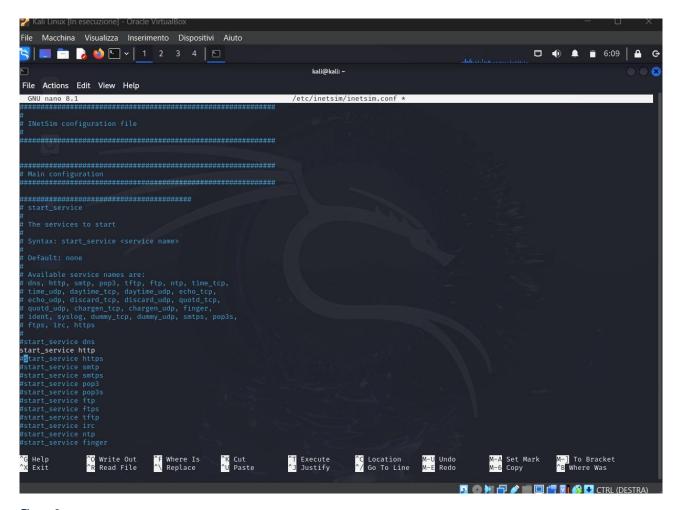


Figura 8

A questo punto avvio inetsim con il comando sudo inetsim ed attendo l'avvio del servizio. (Figura 9)

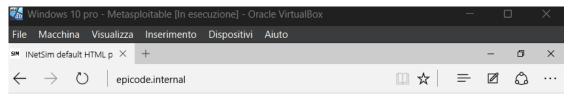
```
sudo inetsin
NetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
                          /var/log/inetsim/
Jsing log directory:
                          /var/lib/inetsim/
Jsing data directory:
Jsing report directory:
                          /var/log/inetsim/report/
Jsing configuration file: /etc/inetsim/inetsim.conf
arsing configuration file.
Configuration file parsed successfully.
≡ INetSim main process started (PID 29490) ==
               29490
Session ID:
Listening on: 192.168.32.100
Real Date/Time: 2024-12-02 06:11:30
ake Date/Time: 2024-12-02 06:11:30 (Delta: 0 seconds)
Forking services...
 * http_80_tcp - started (PID 29500)
done.
```

Figura 9

Adesso avvio nuovamente dnschef con il comando precedente

dnschef ---fakedomains epicode.internal ---fakeip 192.168.32.100 -i 192.168.32.100

ed attendo l'avvio del servizio. Una volta fatto ciò mi connetto sulla VM Windows e, sul browser Microsoft Edge, inserisco l'URL http://epicode.internal ottenendo la pagina http del server (*Figura 10*)



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.



Figura 10

Apro Wireshark e catturo il traffico sull'interfaccia eth0 tra le 2 VM. Una volta catturati i pacchetti, utilizzo il filtro tcp.port==80 per isolare il traffico HTTP (Figura 11).

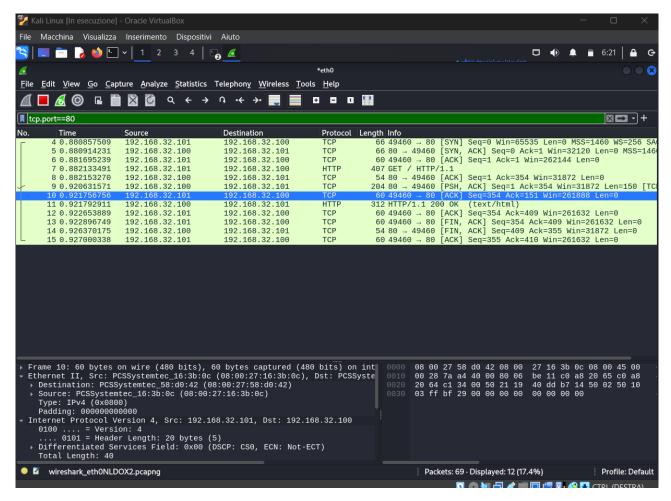


Figura 11

Anche in questo caso si riesce a determinare il MAC sorgente e di destinazione oltre agli indirizzi IP.

Le principali differenze rilevate innanzitutto il numero di porta in quanto http usa la porta 80 mentre il servizio HTTPS utilizza la porta 443. Altra differenza è come tutto sia in chiaro utilizzando il servizio http. Si riesce a rilevare la sequenza SYN, SYN ACK e ACK con le richieste GET (Figura 12 e 13).

Clicca sul tab del traffico GET si riesce a risalire alla richiesta della pagina web in chiaro.

Per quanto riguarda il servizio HTTPS anche qui è presente il 3 way handshake con le richieste SYN, SYN ACK e ACK ma abbiamo anche una richiesta TSL per la verifica del certificato di sicurezza per poter crittografare la connessione e renderla sicura (*Figura 14*).

4 0.880857509	192.168.32.101	192.168.32.100	TCP	66 49460 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SA
5 0.880914231	192.168.32.100	192.168.32.101	TCP	66 80 → 49460 [SYN, ACK] Seg=0 Ack=1 Win=32120 Len=0 MSS=140
6 0.881695239	192.168.32.101	192.168.32.100	TCP	60 49460 → 80 [ACK] Seg=1 Ack=1 Win=262144 Len=0
7 0.882133491	192.168.32.101	192.168.32.100	HTTP	407 GET / HTTP/1.1
8 0.882153270	192.168.32.100	192.168.32.101	TCP	54 80 → 49460 [ACK] Seg=1 Ack=354 Win=31872 Len=0
9 0.920631571	192.168.32.100	192.168.32.101	TCP	204 80 → 49460 [PSH, ACK] Seg=1 Ack=354 Win=31872 Len=150 [T
10 0.921756756	192.168.32.101	192.168.32.100	TCP	60 49460 → 80 [ACK] Seg=354 Ack=151 Win=261888 Len=0
11 0.921792911	192.168.32.100	192.168.32.101	HTTP	312 HTTP/1.1 200 OK (text/html)
12 0.922653889	192.168.32.101	192.168.32.100	TCP	60 49460 → 80 [ACK] Seg=354 Ack=409 Win=261632 Len=0
13 0.922896749	192.168.32.101	192.168.32.100	TCP	60 49460 → 80 [FIN, ACK] Seg=354 Ack=409 Win=261632 Len=0
14 0.926370175	192.168.32.100	192.168.32.101	TCP	54 80 → 49460 [FIN, ACK] Seg=409 Ack=355 Win=31872 Len=0
15 0 927000338	102 168 32 161	102 168 32 166	TCD	60 40460 80 [ACK] Seg-355 Ack-410 Win-261632 Len-0

Figura 12

```
66 49460 - 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 S
66 80 - 49460 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=14
60 49460 - 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
                                                              192.168.32.101
192.168.32.100
                                                                                                                            192.168.32.100
192.168.32.101
                5 0.880914231
                                                                                                                                                                                            TCP
                6 0.881695239
                                                               192.168.32.101
                                                                                                                              192.168.32.100
                                                                                                                                                                                            TCP
                                                                                                                                                                                                                        407 GET / HTTP/1.1

54 80 - 49460 [ACK] Seq=1 Ack=354 Win=31872 Len=0
204 80 - 49460 [PSH, ACK] Seq=1 Ack=354 Win=31872 Len=150 [1
60 49460 - 80 [ACK] Seq=354 Ack=151 Win=261888 Len=0
312 HTTP/1.1 200 OK (text/html)
60 49460 - 80 [ACK] Seq=354 Ack=409 Win=261632 Len=0
60 49460 - 80 [FIN, ACK] Seq=354 Ack=409 Win=261632 Len=0
54 80 - 49460 [FIN, ACK] Seq=409 Ack=355 Win=31872 Len=0
60 49460 - 80 [ACK] Seq=355 Ack=410 Win=261632 Len=0
77 Standard query 0x31a8 A urs.microsoft.com
77 Standard query 0x31a8 A urs.microsoft.com
72 Standard query 0x5100 A www.bing.com
                                                                                                                                                                                            HTT
TCP
                8 0.882153270
                                                               192.168.32.100
                                                                                                                             192.168.32.101
                 9 0.920631571
                                                               192.168.32.100
                                                                                                                              192.168.32.101
                                                                                                                                                                                            TCP
                                                                                                                                                                                            TCP
             10 0.921756756
                                                              192.168.32.101
                                                                                                                             192.168.32.100
              11 0.921792911
                                                              192.168.32.100
192.168.32.101
                                                                                                                             192.168.32.101
192.168.32.100
                                                                                                                                                                                           HTTP
TCP
             12 0.922653889
                                                              192.168.32.101
192.168.32.100
                                                                                                                             192.168.32.100
192.168.32.101
                                                                                                                                                                                           TCP
TCP
             13 0.922896749
              14 0.926370175
                                                              192.168.32.101
192.168.32.101
192.168.32.101
            15 0.927000338
16 0.953590662
                                                                                                                             192.168.32.100
192.168.32.100
                                                                                                                                                                                            TCP
                                                                                                                                                                                            DNS
             17 0.964641371
                                                                                                                             192.168.32.100
                                                                                                                                                                                           DNS
               18 1.026184840
                                                                                                                                                                                                                                                                                                        88 00 27 58 d0 42 08 00 61 89 7a a3 40 00 80 06 20 64 c1 34 00 50 21 19 04 00 17 35 00 00 47 45 2f 31 2e 31 0d 0a 41 63 78 74 2f 68 66 2c 74 69 6f 6e 2f 78 68 74 69 6f 6e 2f 78 68 74 69 66 6f 67 65 2f 6a 78 41 63 63 65 70 74 2d 4c 20 69 74 2d 49 54 2c 69 65 6e 2d 55 53 3b 71 3d 3d 30 2e 33 0d 0a 55 73 3a 20 4d 6f 7a 69 6c 6c 66 96 6e 4d 6f 77 73 20 4e 57 69 6e 36 34 3b 20 78 65 57 65 2e 4b 69 74 2f 4b 48 54 4d 4c 2c 20 6c 6f 29 20 43 68 72 6f 6d 33 31 31 2e 31 33 35 20 33 37 29 33 36 20 45 64 32 34 30 0d 0a 41 63 63
        [Checksum Status: Unverified]
Urgent Pointer: 0
                                                                                                                                                                                                                                                                                                                                                                                   27 16
bc b1
3f 7c
54 20
63 65
20 61
6d 6c
72 2c
61 6e
74 3b
30 2e
65 72
61 26
61 2f
54 20
36 34
35 33
665 2f
53 61
Urgent Pointer: 0
| [Timestamps]
| [SEQ/ACK analysis]
| [IRTI: 0.000837730 seconds]
| [Bytes in flight: 353]
| [Bytes sent since last PSH flag: 353]
| TOP payload (353 bytes)
| Hypertext Transfer Protocol
| GET / HTTP/1.1\r\n
       69
65
53
67
65
         [HTTP request 1/1]
```

Figura 13

	289 951.242247669 192.168.32.101	192.168.32.100	TCP	60 49462 → 443 [FIN, ACK] Seq=208 Ack=1298 Win=260608 Len=0
	290 951.242518998 192.168.32.100	192.168.32.101	TLSv1.2	61 Alert (Level: Fatal, Description: Decode Error)
	291 951.245989115 192.168.32.101	192.168.32.100	TCP	60 49462 → 443 [ACK] Seq=209 Ack=1305 Win=260608 Len=0
	292 951.245989334 192.168.32.101	192.168.32.100	TCP	60 49462 → 443 [RST, ACK] Seq=209 Ack=1305 Win=0 Len=0
- 1	_ 293 951.250935416 192.168.32.101	192.168.32.100	TCP	66 49463 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 \$
- 1	294 951.250966391 192.168.32.100	192.168.32.101	TCP	66 443 → 49463 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1
	295 951.252147827 192.168.32.101	192.168.32.100	TCP	60 49463 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
	296 951.252148055 192.168.32.101	192.168.32.100	TLSv1.2	261 Client Hello (SNI=epicode.internal)
	297 951.252195056 192.168.32.100	192.168.32.101	TCP	54 443 → 49463 [ACK] Seq=1 Ack=208 Win=32000 Len=0
	298 951.277534723 192.168.32.100	192.168.32.101	TLSv1.2	1351 Server Hello, Certificate, Server Key Exchange, Server He
	299 951.278226678 192.168.32.101	192.168.32.100	TCP	60 49463 → 443 [ACK] Seq=208 Ack=1298 Win=260608 Len=0
	300 951.294373453 192.168.32.101	192.168.32.100	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Hands
	301 951.294874371 192.168.32.101	192.168.32.100	TLSv1.2	436 Application Data
	302 951.295145201 192.168.32.100	192.168.32.101	TLSv1.2	280 New Session Ticket, Change Cipher Spec, Encrypted Handsh
	303 951.295501121 192.168.32.101	192.168.32.100	TCP	60 49463 → 443 [ACK] Seq=716 Ack=1524 Win=262144 Len=0
	304 951.314429817 192.168.32.100	192.168.32.101	TLSv1.2	234 Application Data
	305 951.315524880 192.168.32.101	192.168.32.100	TCP	60 49463 → 443 [ACK] Seq=716 Ack=1704 Win=261888 Len=0
	306 951.315546532 192.168.32.100	192.168.32.101	TLSv1.2	341 Application Data
	307 951.315843993 192.168.32.101	192.168.32.100	TCP	60 49463 → 443 [ACK] Seq=716 Ack=1991 Win=261632 Len=0

Figura 14

Progetto di Roberto Bella

2/12/2024

Progetto Finale M1 CSPT0524