

## W4D4

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

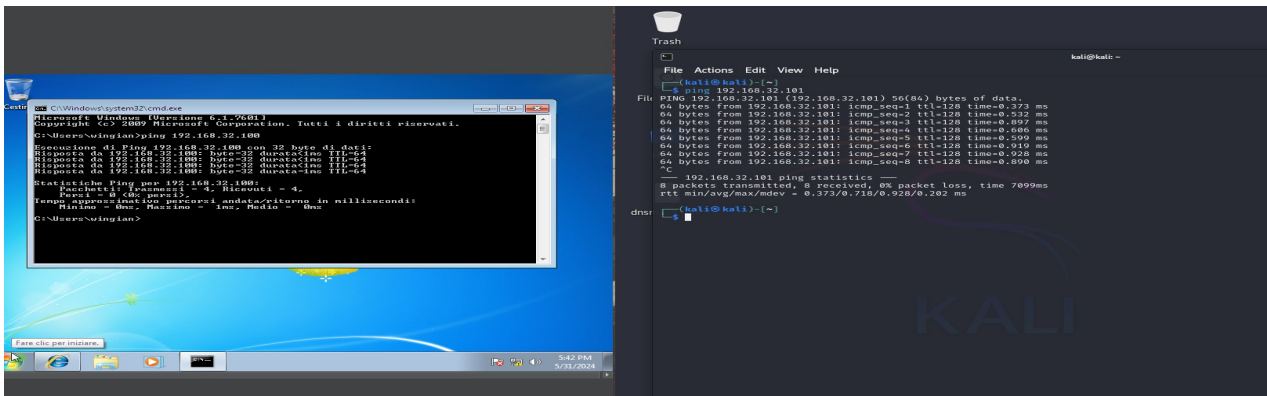
### Traccia:

Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname **epicode.internal** che risponde all'indirizzo 192.168.32.100 (Kali).

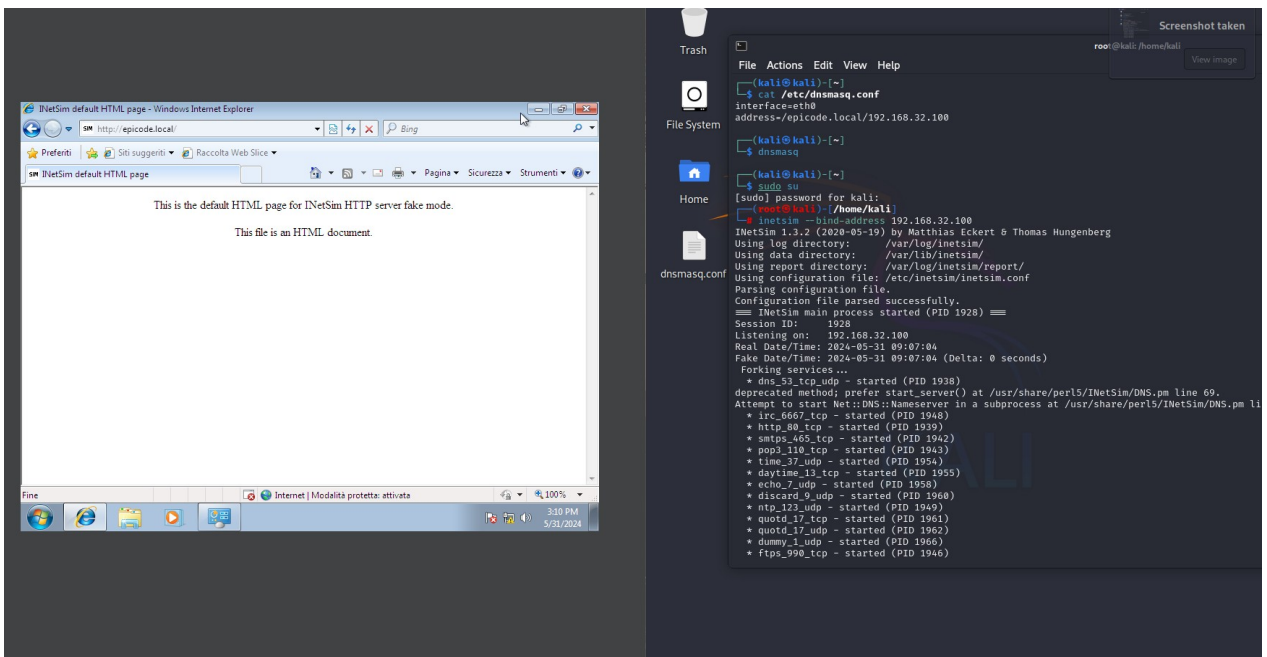
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

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

## COMUNICAZIONE FRA KALI E WINDOWS 7 (PING)



## EPICODE.LOCAL + INETSIM FUNZIONANTE



## MAC ADDRESS WIN ---> WIRESHARK

NetSim default HTML page - Windows Internet Explorer

http://epicode.local/

CA:\Windows\system32\cmd.exe

```
Suffisso DNS specifico per connessione: Scheda desktop Intel(R) PRO/1000 MT
Descrizione: . . . . . : 08-00-27-62-CB-01
Indirizzo fisico: . . . . . : 08-00-27-62-CB-01
DHCP abilitato: . . . . . : No
Configurazione automatica abilitata: S1
Indirizzo IPv6 locale rispetto al collegamento: fe80::51a9:54fc:bbaa::1
11(Preferenziale)
Indirizzo IPv4: . . . . . : 192.168.32.101(Preferenziale)
Subnet mask: . . . . . : 255.255.255.0
Gateway predefinito: . . . . . : 192.168.32.100
IDID DHCPv6: . . . . . : 235405351
DUID Client DHCPv6: . . . . . : 00-01-00-01-2D-D0-7A-7E-08-00-27-62-CB-01

Server DNS: . . . . . : 192.168.32.100
NetBIOS su TCP/IP: . . . . . : Attivato

Scheda Tunnel isatap.{FAED920E-6D50-4810-BAD1-B0F67CA10DBA}:
Stato supporto: . . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione: . . . . . : Microsoft ISA/AT Adapter
Indirizzo fisico: . . . . . : 00-00-00-00-00-00-E0
DHCP abilitato: . . . . . : No
Configurazione automatica abilitata: S1

C:\Users\wingian>
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
10	6.002816652	192.168.32.101	192.168.32.100	DNS	85	Standard query 0xa6
11	6.003027429	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.
12	7.005577256	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.
13	8.029981446	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.
14	33.261343401	fe80::51a9:54fc:bbaa::	ff02::1:2	DHCPv6	152	Solicit XID: 0xc18
15	34.251037583	fe80::51a9:54fc:bbaa::	ff02::1:2	DHCPv6	152	Solicit XID: 0xc18
16	34.999582133	192.168.32.101	192.168.32.100	TCP	66	49166 -> 80 [SYN] Se
17	34.999531195	192.168.32.100	192.168.32.101	TCP	66	80 -> 49166 [SYN, AC
18	35.000226756	192.168.32.101	192.168.32.100	TCP	60	49166 -> 80 [ACK] Se
19	35.001225317	192.168.32.101	192.168.32.100	HTTP	351	GET / HTTP/1.1
20	35.001246955	192.168.32.100	192.168.32.101	TCP	54	80 -> 49166 [ACK] Se
21	35.019571181	192.168.32.100	192.168.32.101	TCP	204	80 -> 49166 [PSH, AC
22	35.021844844	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (t
23	35.022957721	192.168.32.101	192.168.32.100	TCP	60	49166 -> 80 [FIN, AC
24	35.022957985	192.168.32.100	192.168.32.100	TCP	60	49166 -> 80 [ACK] Se
25	35.023007861	192.168.32.100	192.168.32.101	TCP	54	80 -> 49166 [ACK] Se
26	35.035926912	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x96
27	35.036919226	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.
28	36.033732224	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x96
29	36.063501446	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.
30	36.251037583	fe80::51a9:54fc:bbaa::	ff02::1:2	DHCPv6	152	Solicit XID: 0xc18

Frame 5: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec\_07:cb:01 (08:00:27:62:cb:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

NetBIOS Datagram Service

SMB (Server Message Block Protocol)

SMB MailSlot Protocol

Microsoft Windows Browser Protocol

Ethernet (eth), 14 bytes

Packets: 72 - Displayed: 72 (100.0%) - Dropped: 0 (0.0%)

## ANALISI PACHETTI HTTP

root@kali: /home/kali

```
File Actions Edit View Help
(kali@kali)~$ cat /etc/dnsmasq.conf
interface=eth0
address=/epicode.local/192.168.32.100

(kali@kali)~$ dnsmasq
[sudo] password for kali:
(kali@kali)~$ sudo su
[sudo] password for kali:
root@kali: /home/kali#
root@kali: /home/kali# inetsim --bind-address 192.168.32.100
InetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
InetSim main process started (PID 1928)
Session ID: 1928
Listening on: 192.168.32.100
Real Date/Time: 2024-05-31 09:07:04
Fake Date/Time: 2024-05-31 09:07:04 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1938)
  deprecated method; prefer start_server() at /usr/share/perl5/InetSim
  Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/
  * trc_660_tcp - started (PID 1948)
  * http_80_tcp - started (PID 1958)
  * smtps_465_tcp - started (PID 1942)
  * pop3_110_tcp - started (PID 1943)
  * line_37_udp - started (PID 1954)
  * daytime_13_tcp - started (PID 1955)
  * echo_7_udp - started (PID 1958)
  * discard_9_udp - started (PID 1960)
  * ntp_123_udp - started (PID 1949)
  * quotd_17_tcp - started (PID 1961)
  * quotd_17_udp - started (PID 1962)
  * dummy_1_udp - started (PID 1966)
  * ftps_990_tcp - started (PID 1946)
  * chargen_19_tcp - started (PID 1963)
  * https_443_tcp - started (PID 1940)
  * echo_7_tcp - started (PID 1957)
  * ident_112_tcp - started (PID 1951)
  * ftpp_69_udp - started (PID 1947)
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::51a9:54fc:bbaa::	ff02::1:2	DHCPv6	152	Solicit XID: 0xb9008c CID: 00010001
2	11.675848511	192.168.32.101	192.168.32.100	TCP	66	49165 -> 80 [SYN] Seq=0 Win=8192 Len=0
3	11.675875347	192.168.32.100	192.168.32.101	TCP	66	80 -> 49165 [SYN, ACK] Seq=0 Ack=1 W
4	11.676298915	192.168.32.101	192.168.32.100	TCP	60	49165 -> 80 [ACK] Seq=1 Ack=1 Win=65
5	11.676421770	192.168.32.101	192.168.32.100	HTTP	351	GET / HTTP/1.1
6	11.676429513	192.168.32.100	192.168.32.101	TCP	54	80 -> 49165 [ACK] Seq=1 Ack=298 Win=
7	11.691669061	192.168.32.100	192.168.32.101	TCP	204	80 -> 49165 [PSH, ACK] Seq=1 Ack=298
8	11.694491763	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
9	11.694919933	192.168.32.101	192.168.32.100	TCP	60	49165 -> 80 [ACK] Seq=298 Ack=410 W
10	11.695110174	192.168.32.101	192.168.32.100	TCP	60	49165 -> 80 [FIN, ACK] Seq=298 Ack=4
11	11.695124091	192.168.32.100	192.168.32.101	TCP	54	80 -> 49165 [ACK] Seq=410 Ack=299 W
12	11.706570169	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x4b7d A urs.microso
13	11.706705422	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.17 Tell 192.168.
14	12.694412323	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x4b7d A urs.microso
15	12.734473854	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.17 Tell 192.168.
16	13.695748327	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x4b7d A urs.microso
17	13.758351066	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.17 Tell 192.168.
18	15.695466263	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x4b7d A urs.microso
19	15.695857642	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.17 Tell 192.168.
20	16.762362502	PCSSystemtec_1e:36:...	Broadcast	ARP	42	Who has 192.168.32.17 Tell 192.168.

Frame 8: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec\_1e:36:4a (08:00:27:1e:36:4a), Dst: PCSSystemtec\_07:cb:01 (08:00:27:62:cb:01)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

Transmission Control Protocol, Src Port: 80, Dst Port: 49165, Seq: 151, Ack: 298, Len: 258

[2 Reassembled TCP Segments (408 bytes): #7(150), #8(258)]

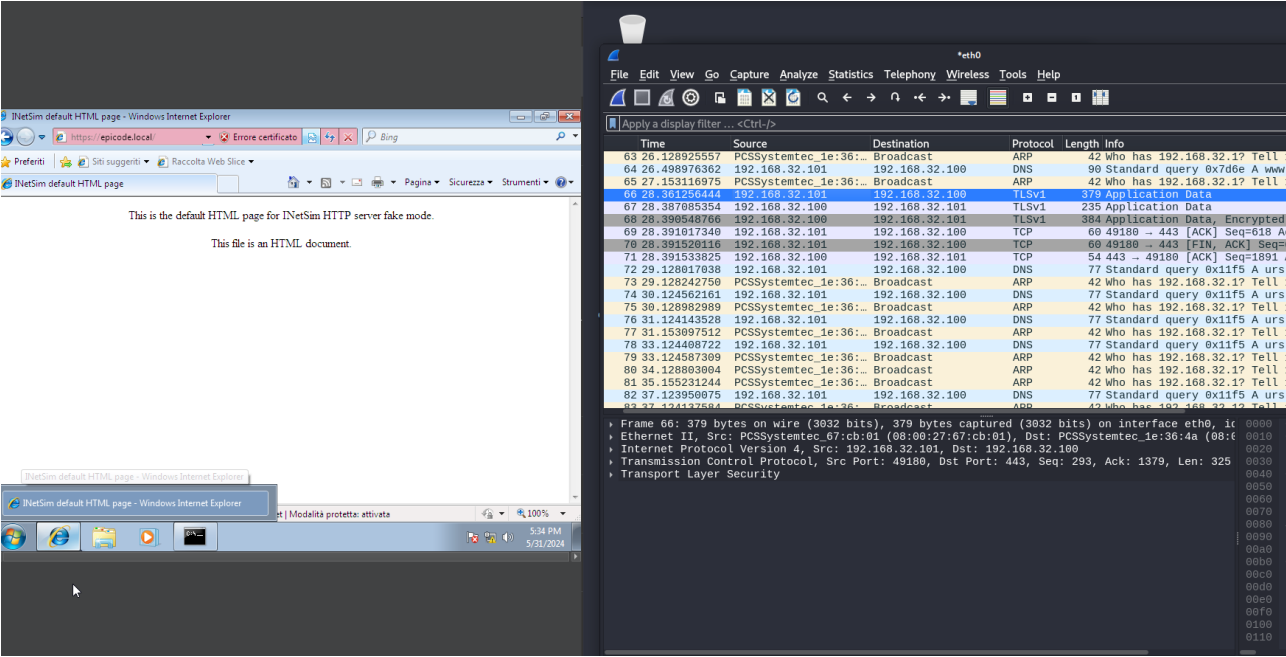
HyperText Transfer Protocol

Line-based text data: text/html (10 lines)

eth0: <live capture in progress>

Packets: 83 - Displayed: 83 (100.0%) Profile: Default

# ANALISI HTTPS



La differenza sostanziale fra la scansione HTTP e HTTPS è che i pacchetti sono criptati con HTTPS.

