

## REPORT 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

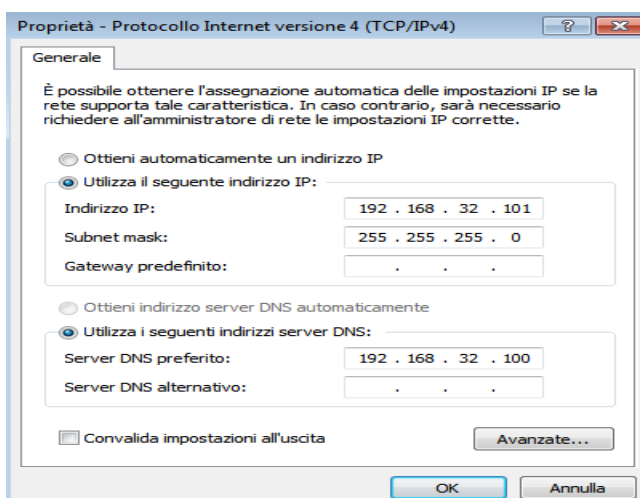
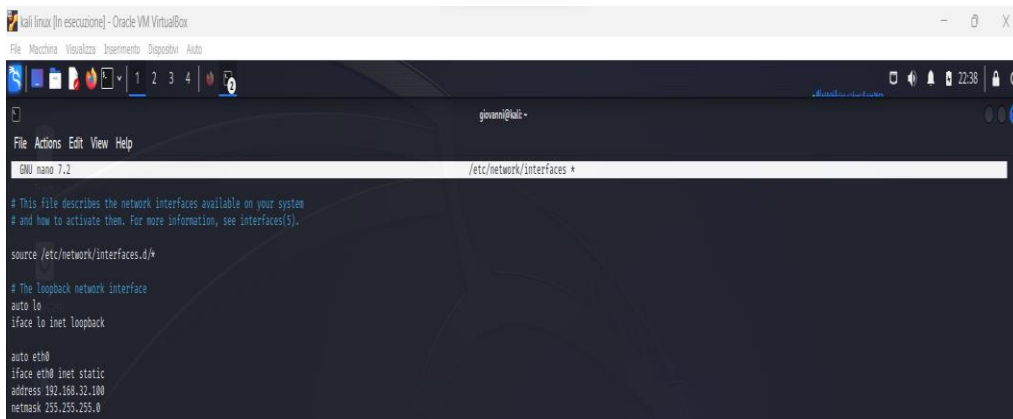
### Traccia:

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.

## Configurazione Ip windows e Kali



## Configurazione DNS su Inetsim

```
# time_udp, daytime_tcp, daytime_udp, echo_t
# echo_udp, discard_tcp, discard_udp, quotd_
# quotd_udp, chargen_tcp, chargen_udp, finge
# ident, syslog, dummy
# ftps, irc, https
#
start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s

#####
# service_bind_address
#
# IP address to bind services to
# Syntax: service_bind_address <IP address>
# Default: 127.0.0.1
service_bind_address 192.168.32.100

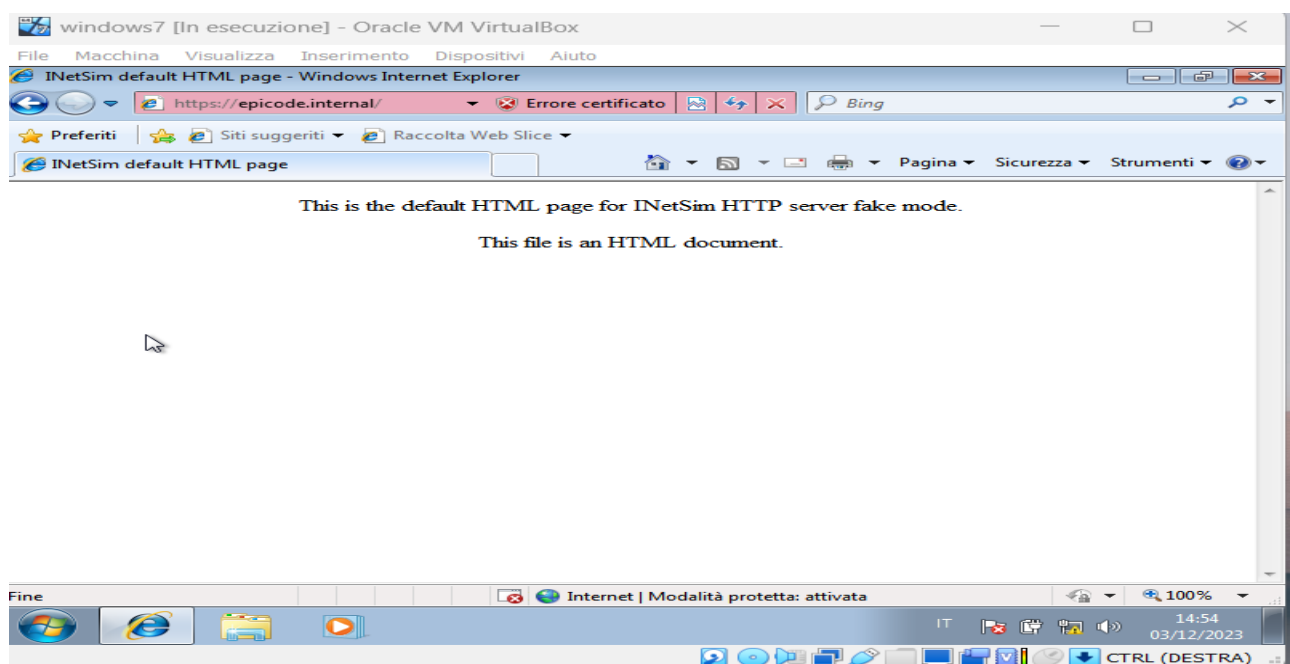
#####
# dns_default_ip
#
# Default IP address to return with DNS repl
# Syntax: dns_default_ip <IP address>
# Default: 127.0.0.1
dns_default_ip 192.168.32.100

#####
# dns_default_domainname
#
# Default domain name to return with DNS
# Syntax: dns_default_domainname <domain>
# Default: inetsim.org
dns_default_domainname epicode.internal

#####
# dns_static
#
# Static mappings for DNS
# Syntax: dns_static <fqdn hostname> <IP address>
# Default: none
dns_static epicode.internal 192.168.32.100
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30

#####
# https_default_fakefile
#
# Syntax: https_default_fakefile <filename> <mime-type>
# Default: none
https_default_fakefile sample.html text/html
```

Dopo aver caricato la pagina <https://epicode.internal> su windows, catturo i pacchetti con wireshark in HTTPS e http



## HTTPS

Wireshark capture of an HTTPS session. The packet list shows a series of TLS messages: Client Hello, Server Hello, Certificate, Server Key Exchange, Encrypted Handshake Message, Change Cipher Spec, and another Encrypted Handshake Message. The packet details pane for packet 43 shows the TLS structure with fields like Version, Length, Sequence Number, and Window. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_dc:d3:4b	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000041500	PcsCompu_dc:d3:4b	PcsCompu_dc:d3:4b	ARP	42	192.168.32.100 is at 08:00:27:13:df:3e
3	0.000715620	192.168.32.101	192.168.32.100	TCP	66	49223 → 443 [SYN] Seq=0 Win=6192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000715620	192.168.32.100	192.168.32.101	TCP	66	49223 → 443 [ACK] Seq=1 Ack=1 Win=65760 Len=0
5	0.001211549	192.168.32.101	192.168.32.100	TCP	66	49223 → 443 [ACK] Seq=1 Ack=1 Win=65760 Len=0
6	0.001714561	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
7	0.001784438	192.168.32.100	192.168.32.101	TLSv1	54	443 → 49223 [ACK] Seq=1 Ack=102 Win=64128 Len=0
8	0.102160522	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9	0.115973942	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.116070546	192.168.32.100	192.168.32.101	TCP	54	443 → 49223 [ACK] Seq=1320 Ack=296 Win=64128 Len=0
11	0.117641584	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.142010807	fe80::0110:9f04:aa2...	ff02::1:3	LLMNR	84	Standard query 0x8a27 A wpad
13	0.142231495	192.168.32.101	224.0.0.252	LLMNR	84	Standard query 0x8a27 A wpad
14	0.240390463	fe80::0110:9f04:aa2...	ff02::1:3	LLMNR	84	Standard query 0x8a27 A wpad
15	0.242393254	192.168.32.101	224.0.0.252	LLMNR	84	Standard query 0x8a27 A wpad
16	0.316391934	192.168.32.101	192.168.32.100	TCP	60	49223 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
17	0.442404734	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPA0<0>
18	1.191750000	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPA0<0>
19	1.942690815	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPA0<0>

Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0  
Ethernet II, Src: PcsCompu\_13:df:3e (08:00:27:13:df:3e), Dst: PcsCompu\_dc:d3:4b (08:00:27:dc:d3:4b)  
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101  
Transmission Control Protocol, Src Port: 443, Dst Port: 49223, Seq: 0, Ack: 1, Len: 0  
Source Port: 443  
Destination Port: 49223  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 3441821748  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 1078502991  
1000 ... = Header Length: 32 bytes (8)  
Flags: 0x012 [SYN, ACK]  
Window: 64240  
[calculated window size: 64240]  
Checksum: 0xc240 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Transmission Control Protocol (tcp), 32 byte(s)

Packets: 93 · Displayed: 93 (100.0%) Profile: Default

## HTTP

Wireshark capture of an HTTP session. The packet list shows a GET request and its corresponding 200 OK response. The packet details pane for packet 12 shows the HTTP structure with fields like Version, Method, URI, Status, and Content-Type.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_dc:d3:4b	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000049902	PcsCompu_13:df:3e	PcsCompu_dc:d3:4b	ARP	42	192.168.32.100 is at 08:00:27:13:df:3e
3	0.000545147	192.168.32.101	192.168.32.100	TCP	66	49264 → 80 [SYN] Seq=0 Win=6192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000599306	192.168.32.100	192.168.32.101	TCP	66	80 → 49264 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.001090690	192.168.32.101	192.168.32.100	TCP	66	49264 → 80 [ACK] Seq=1 Ack=1 Win=65760 Len=0
6	0.001541810	192.168.32.101	192.168.32.100	HTTP	361	GET / HTTP/1.1
7	0.001567380	192.168.32.100	192.168.32.101	TCP	54	80 → 49264 [ACK] Seq=1 Ack=308 Win=64128 Len=0
8	0.045623657	192.168.32.100	192.168.32.101	TCP	204	80 → 49264 [PSH, ACK] Seq=1 Ack=308 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.053242184	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	0.055240344	192.168.32.101	192.168.32.100	TCP	60	49264 → 80 [ACK] Seq=308 Ack=410 Win=65292 Len=0
11	0.055241319	192.168.32.101	192.168.32.100	TCP	60	49264 → 80 [FIN, ACK] Seq=308 Ack=410 Win=65292 Len=0
12	0.055335638	192.168.32.100	192.168.32.101	TCP	54	80 → 49264 [ACK] Seq=410 Ack=309 Win=64128 Len=0