

# PROGETTO GIORNO 5

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:

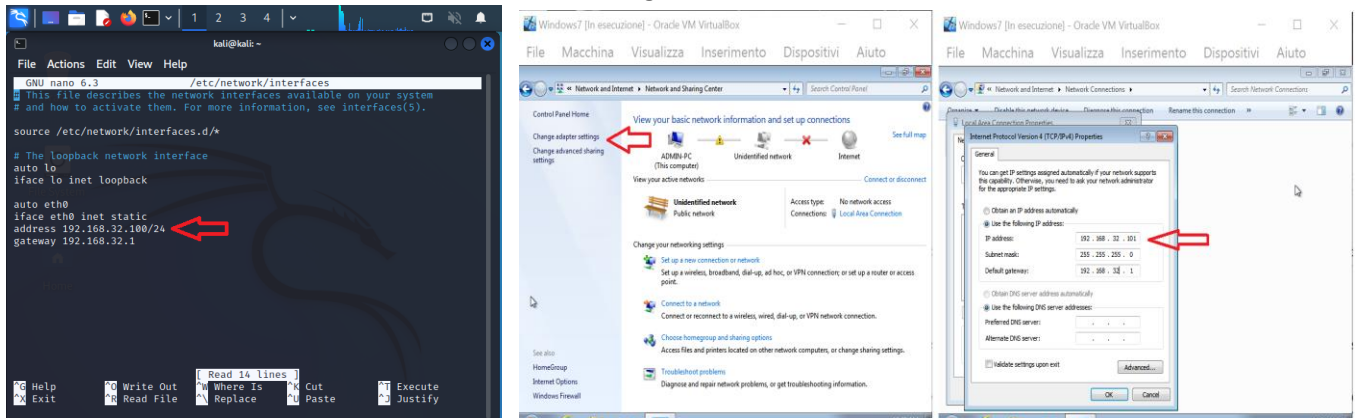
Simulare su VirtualBox un'architettura client-server in cui un client (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'IP di Kali Linux

Intercettare poi la comunicazione con Wireshark evidenziando i MAC address di source e dest. ed il contenuto della richiesta HTTPS

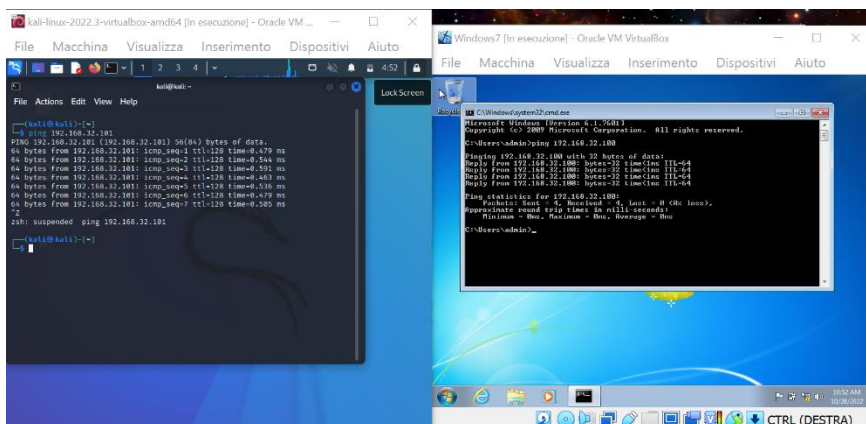
Ripetere sostituendo al server HTTPS il server http, intercettando nuovamente ed evidenziando le eventuali differenze tra i traffici catturati con HTTP e HTTPS.

Svolgimento:

Cambiare IP di Kali e Windows come mostrato nelle figure



Verificare la connessione facendo fare il ping tra le due macchine



Attraverso il Terminal di Kali mettere il comando ping 192.168.32.101 (IP Windows 7).

Attraverso il cmd di Windows 7 inserire il comando ping 192.168.32.100 (IP Kali).

Tramite il Terminal di Kali inserire il comando `sudo nano /etc/inetsim/inetsim.conf` e cambiare il bind address con IP 192.168.32.100 ed il DNS static con `epicode.internal`

```

GNU nano 6.3 /etc/inetsim/inetsim.conf
start_service dummy_tcp
start_service dummy_udp

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 10.10.10.1
service_bind_address 192.168.32.100

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
#service_run_as_user nobody

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

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100

#####
# dns_version

```

Tramite Terminal Kali avviare inetsim e verificare che le modifiche siano state fatte con successo

```

File Actions Edit View Help
Forking services...
* dns_33_tcp_udp - started (PID 6526)
* irc_6667_tcp - started (PID 6536)
* ident_113_tcp - started (PID 6539)
* time_37_udp - started (PID 6542)
* ntp_123_udp - started (PID 6537)
* time_37_tcp - started (PID 6544)
* echo_7_udp - started (PID 6546)
* tftp_69_udp - started (PID 6535)
* daytime_13_tcp - started (PID 6543)
* syslog_514_udp - started (PID 6540)
* daytime_13_udp - started (PID 6544)
* finger_79_tcp - started (PID 6538)
* echo_7_tcp - started (PID 6545)
* chargen_19_tcp - started (PID 6551)
* discard_9_tcp - started (PID 6547)
* discard_9_udp - started (PID 6548)
* dummy_1_udp - started (PID 6554)
* quotd_17_tcp - started (PID 6549)
* dummy_1_tcp - started (PID 6553)
* quotd_17_udp - started (PID 6550)
* chargen_19_udp - started (PID 6552)
* smtps_465_tcp - started (PID 6530)
* smtp_25_tcp - started (PID 6529)
* pop3s_995_tcp - started (PID 6532)
* pop3_110_tcp - started (PID 6531)
* ftp_21_tcp - started (PID 6533)
* https_443_tcp - started (PID 6528)
* http_80_tcp - started (PID 6527)
* ftps_990_tcp - started (PID 6534)
done.
Simulation running.

```

Ora verificare se Windows 7 riesce a fare il ping per il percorso `epicode.internal`:

```

C:\Users\Admin>ping epicode.internal

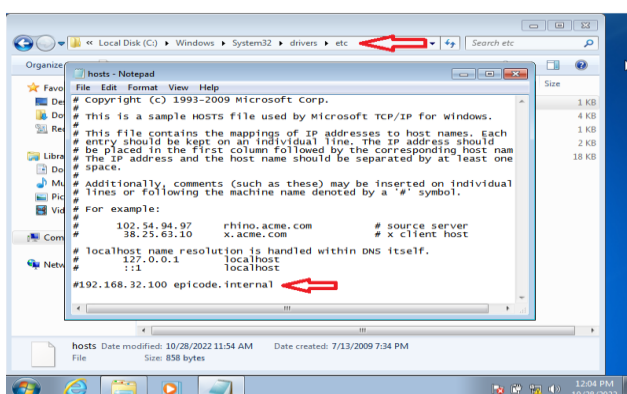
Pinging epicode.internal [192.168.32.100] with 32 bytes of data:
Reply from 192.168.32.100: bytes=32 time=1ms TTL=64
Reply from 192.168.32.100: bytes=32 time=1ms TTL=64
Reply from 192.168.32.100: bytes=32 time=1ms TTL=64
Reply from 192.168.32.100: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>

```

Tramite i driver del System32 di Windows andare a modificare il file hosts e su Terminal Kali tramite `sudo /etc/hosts` inserendo `#192.168.32.100 epicode.internal`



```

GNU nano 6.3 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

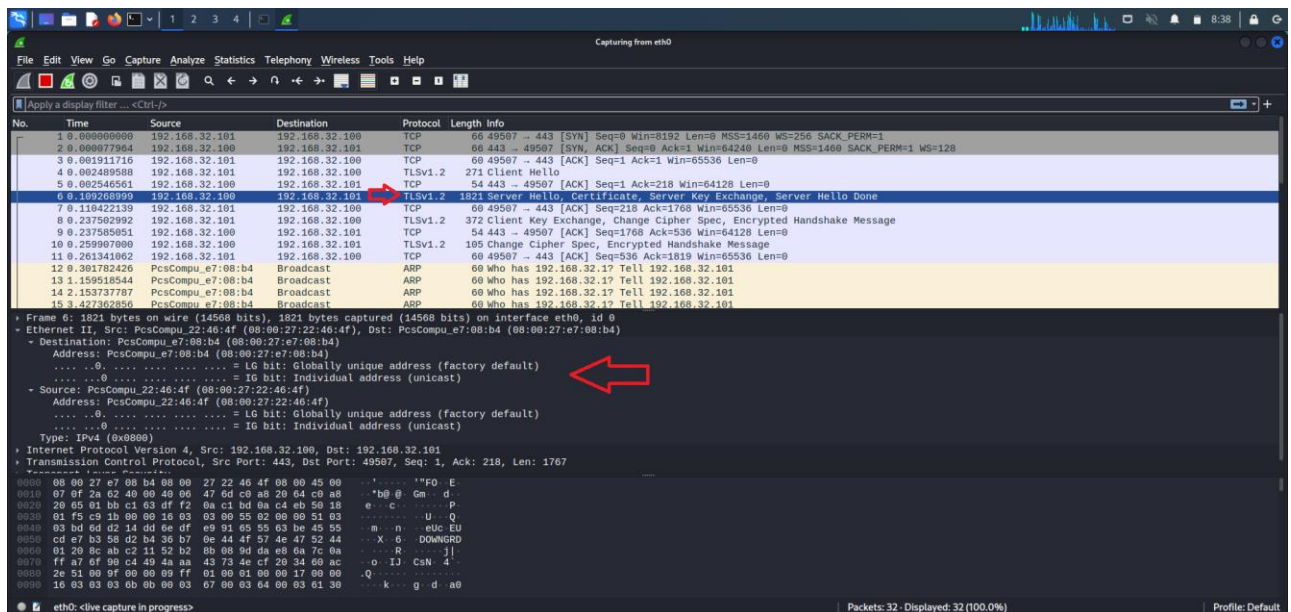
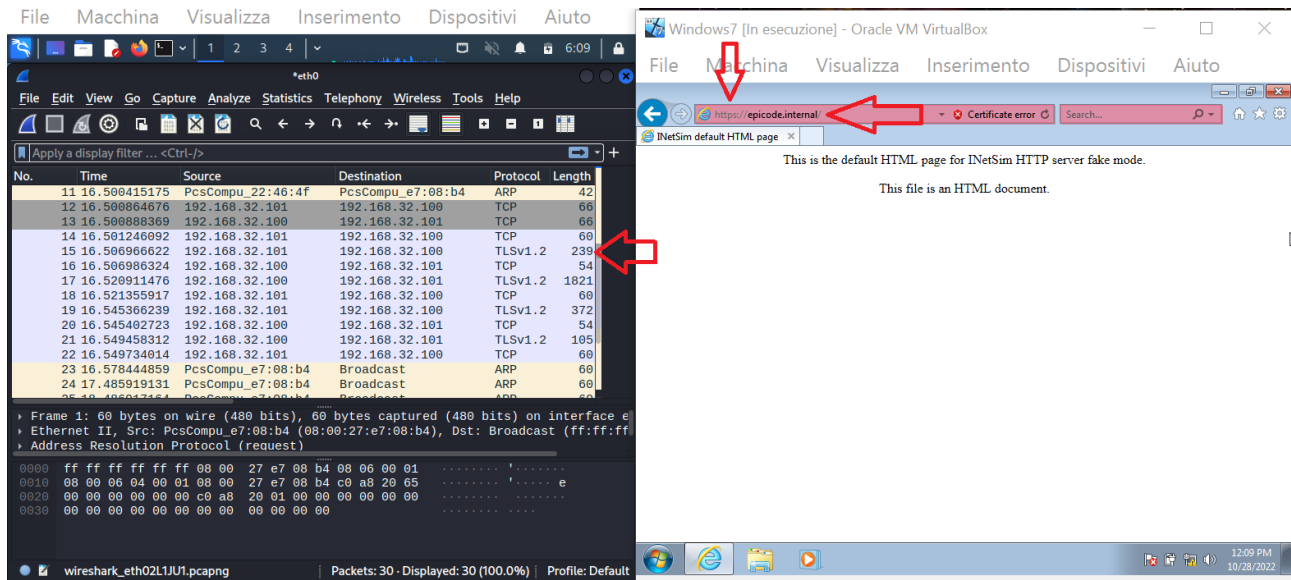
#192.168.32.100 epicode.internal

```

Così facendo il DNS convertirà epicode.internal nell'indirizzo IP specificato; Windows 7 si è collegato al DNS di Kali.

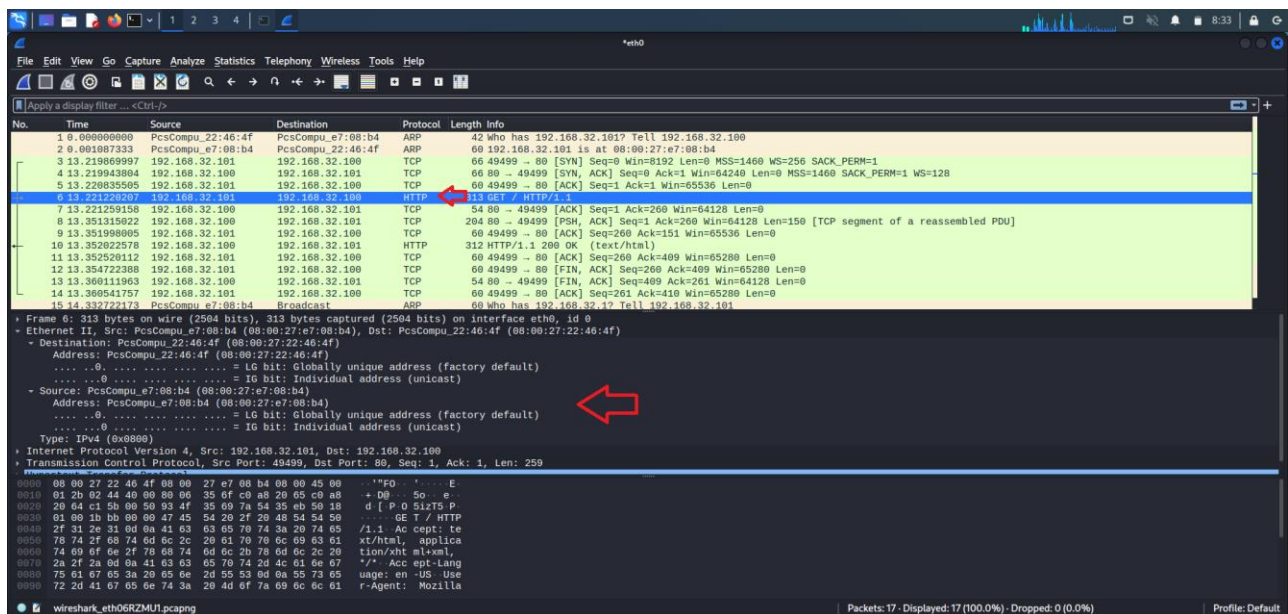
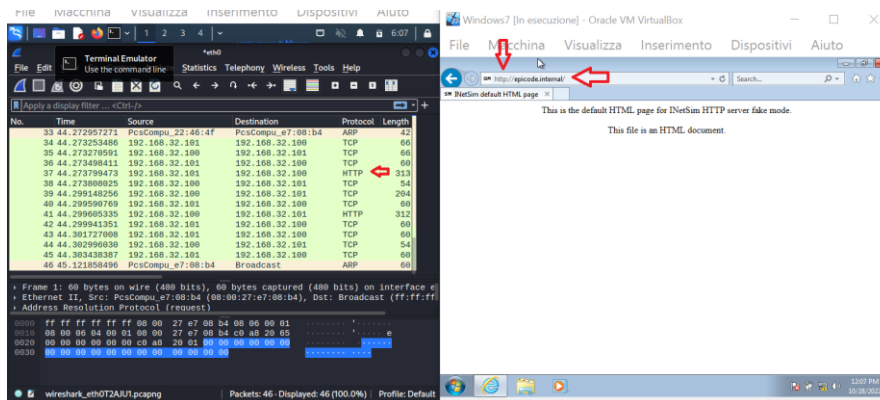
Mantenere aperta la finestra del terminal Kali di inetsim:

Aprire Internet Explorer su Windows 7 iniziando la ricerca HTTPS di "epicode.internal" e nello stesso tempo avviare la cattura dati di Wireshark su Kali



Durante la ricerca internet verificare il passaggio di pacchetti TLS con la cattura Wireshark ed evidenziare gli indirizzi MAC source e dest. come evidenziato in figura.

## Ripetere lo stesso procedimento per HTTP



Come evidenziato nelle foto ci sono delle differenze negli indirizzi MAC lato client e server nei traffici HTTPS e HTTP.

HTTPS è un metodo per eseguire HTTP su un protocollo cifrato, come TLS (si può vedere in figura).

Le differenze del traffico catturato da Wireshark sarà quindi evidente dal tipo di messaggio catturato,

nel primo caso (HTTPS) sarà un TLS, mentre nel caso di HTTP sarà un TCP e saranno visibili le risposte di SYN e ACK.