

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

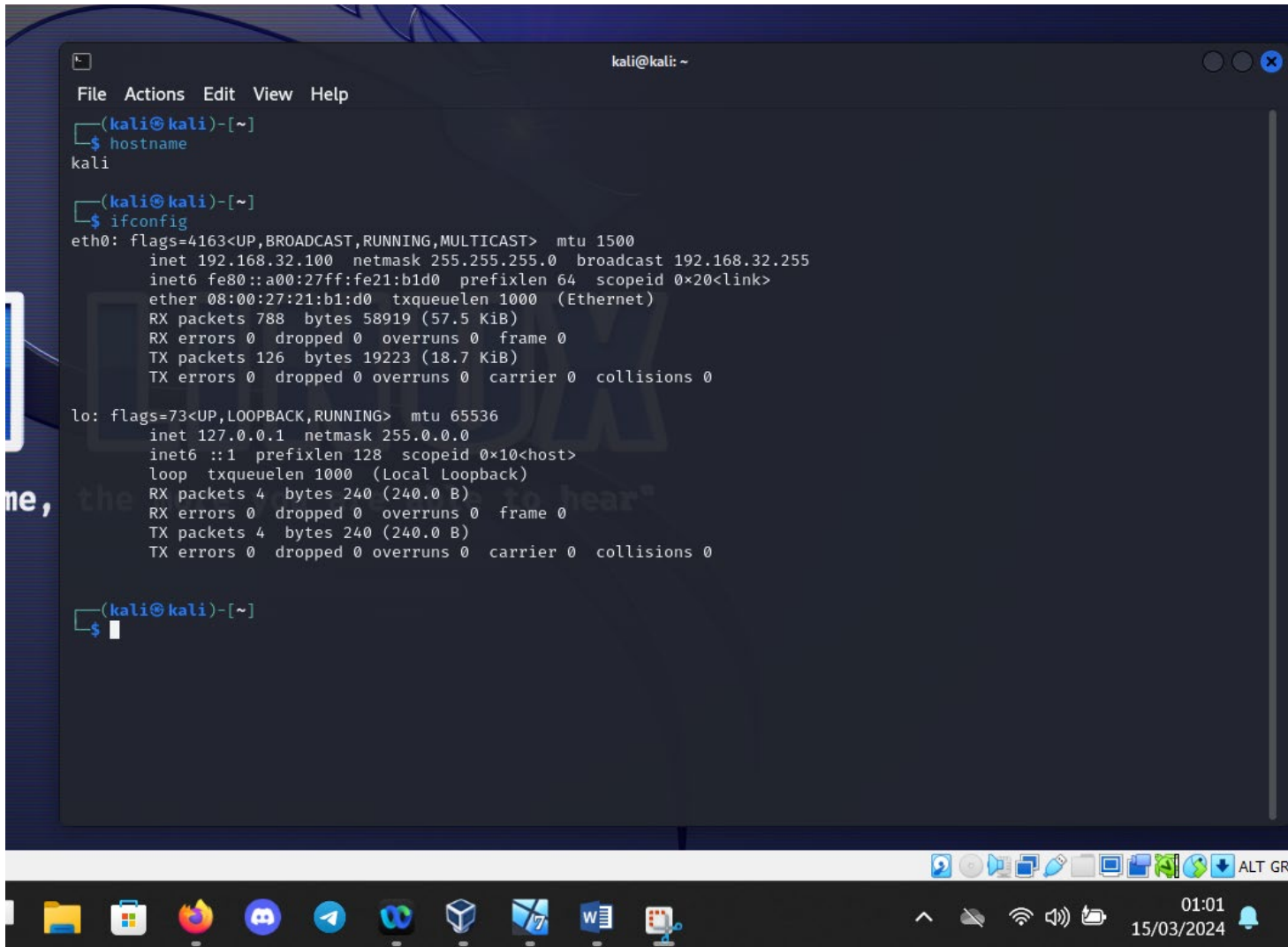
**Traccia:**

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 192.168.32.100 della macchina Kali come indicato nell'esercizio



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hostname  
kali  
  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
    RX packets 788 bytes 58919 (57.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 126 bytes 19223 (18.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

Configurazione dell'indirizzo IP 192.168.32.100 della macchina Windows, come gateway e come DNS punto alla macchina KALI dove ho provveduto a configurare ed avviare INETSIM.

```
C:\Windows\system32\cmd.exe
C:\Users\vboxuser>ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : Windows-7
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato . . . . . : No
Proxy WINS abilitato . . . . . : No

Scheda Ethernet Connessione alla rete locale (LAN):

Suffisso DNS specifico per connessione:
Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
Indirizzo fisico. . . . . : 08-00-27-FE-D6-96
DHCP abilitato . . . . . : No
Configurazione automatica abilitata . . . . . : Sì
Indirizzo IPv6 locale rispetto al collegamento . . . . . : fe80::f836:dbfa:340c:3cd9%11(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.32.101(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.100
IAD DHCPv6 . . . . . : 235405351
DUID Client DHCPv6. . . . . : 00-01-00-01-2D-6A-B2-47-08-00-27-FE-D6-96

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

Scheda Tunnel isatap.<907CE123-ADD4-41E9-9189-F7580783BD7E>:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Microsoft ISATAP Adapter
Indirizzo fisico. . . . . : 00-00-00-00-00-00-E0
DHCP abilitato . . . . . : No
Configurazione automatica abilitata . . . . . : Sì

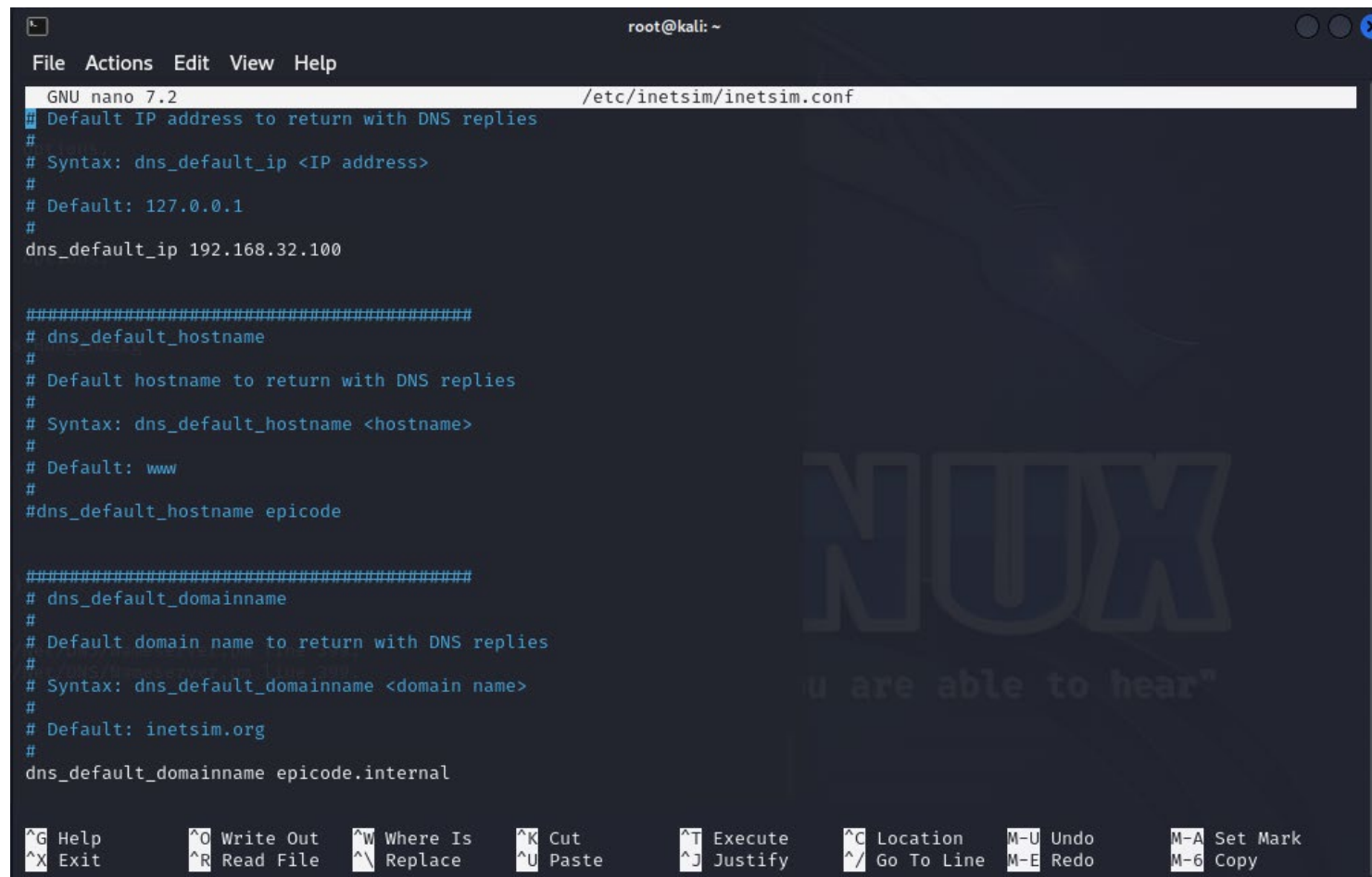
C:\Users\vboxuser>
```

Sulla macchina Kali avvio INETSIM provvedendo a configurare i servizi DNS, HTTP e HTTPS uno alla volta prima l'uno e poi l'altro, mentre ho disabilitato tutti gli altri servizi.

Nel servizio DNS provvedo a configurare le seguenti variabili al fine di far risolvere il dominio "epicode.internal" e poterci puntare tramite il browser:

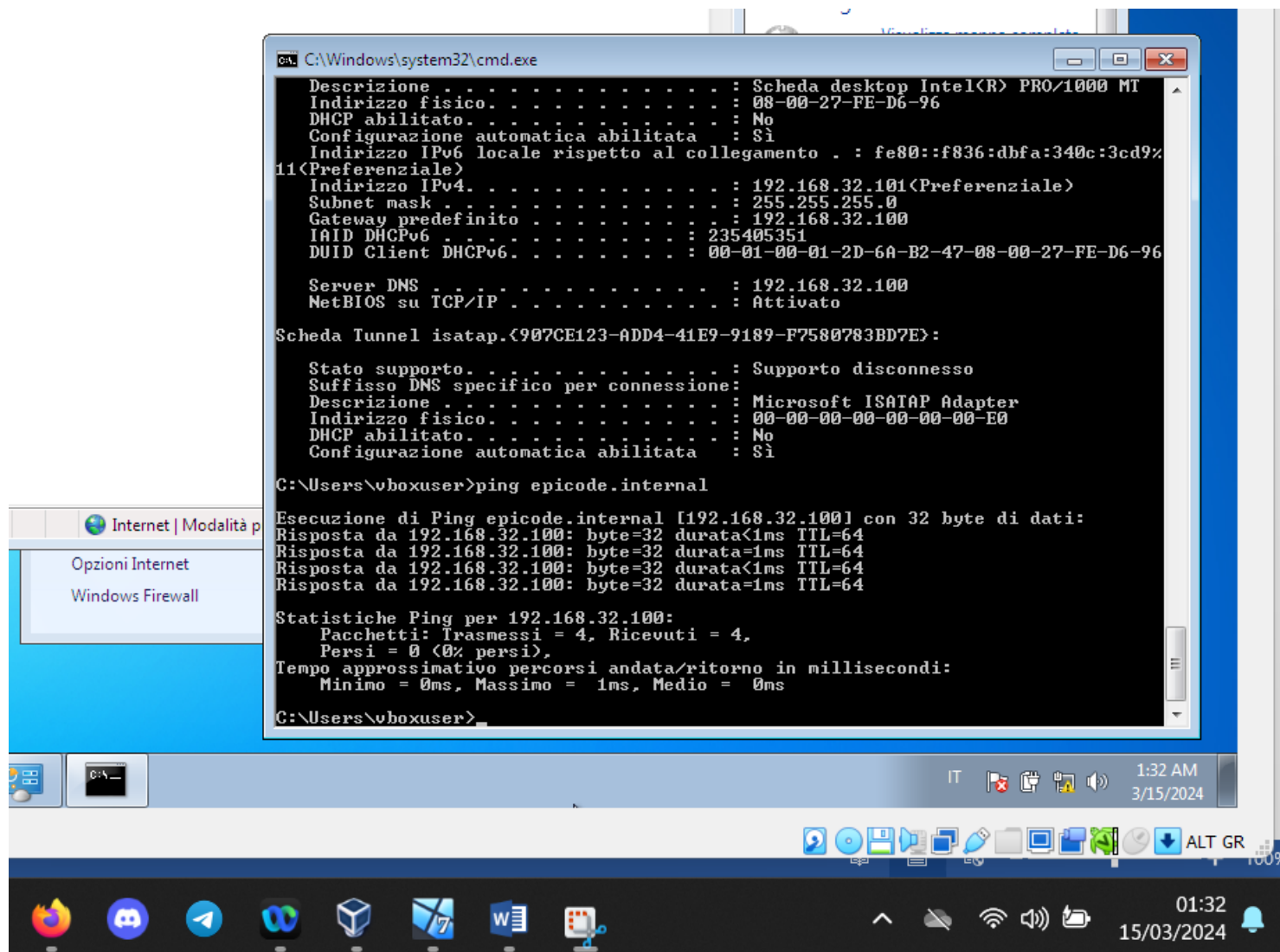
**dns\_default\_ip 192.168.32.100**

**dns\_default\_domainname epicode.internal 192.168.32.100**



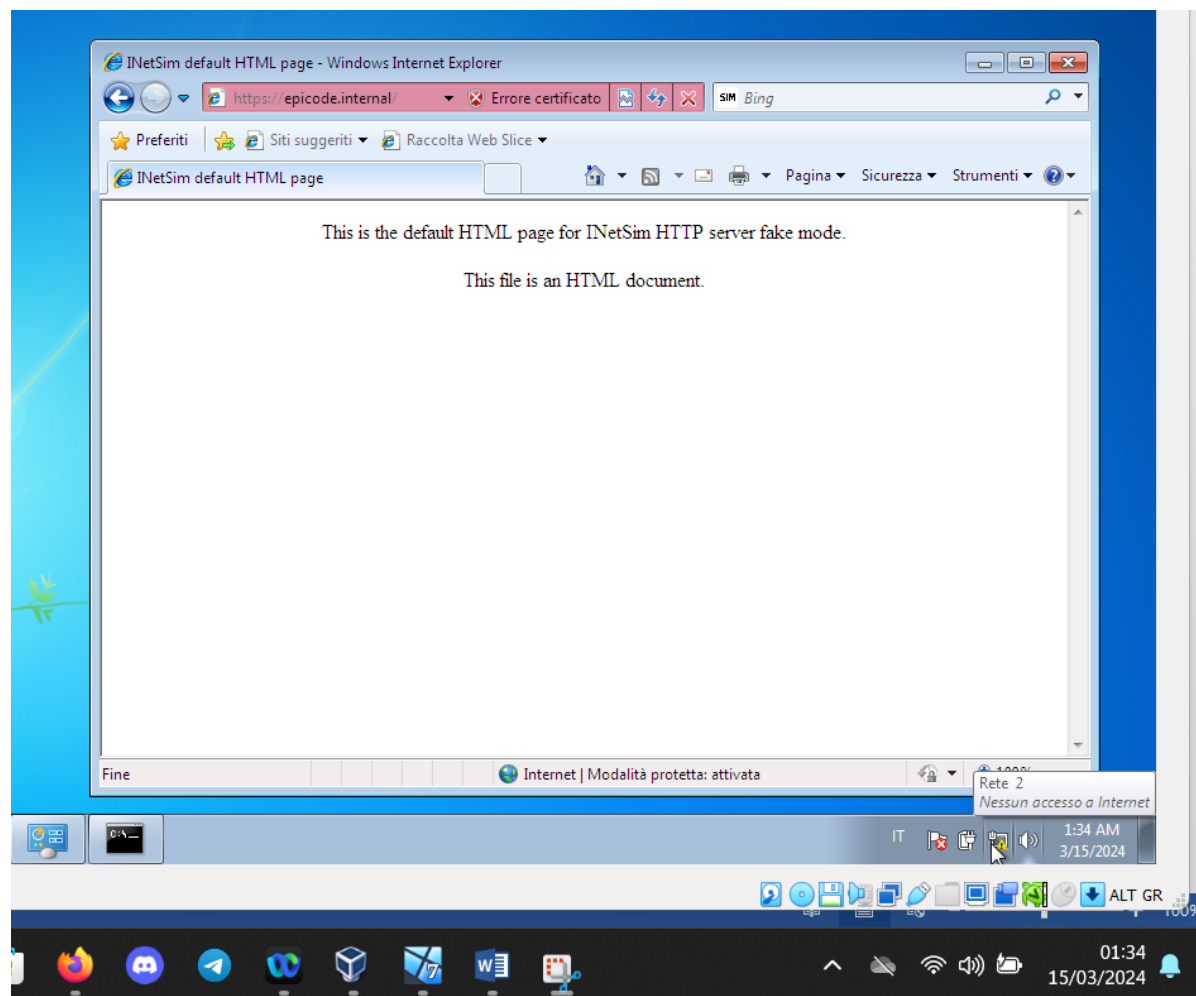
```
root@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf  
# Default IP address to return with DNS replies  
#  
# Syntax: dns_default_ip <IP address>  
#  
# Default: 127.0.0.1  
#  
dns_default_ip 192.168.32.100  
  
#####  
# dns_default_hostname  
#  
# Default hostname to return with DNS replies  
#  
# Syntax: dns_default_hostname <hostname>  
#  
# Default: www  
#  
#dns_default_hostname epicode  
  
#####  
# dns_default_domainname  
#  
# Default domain name to return with DNS replies  
#  
# Syntax: dns_default_domainname <domain name>  
#  
# Default: inetsim.org  
#  
dns_default_domainname epicode.internal  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_/ Go To Line  M-E Redo      M-6 Copy
```

Successivamente ho effettuato un ping al dominio "epicode.internal" per testare il funzionamento del DNS e la corretta configurazione del record



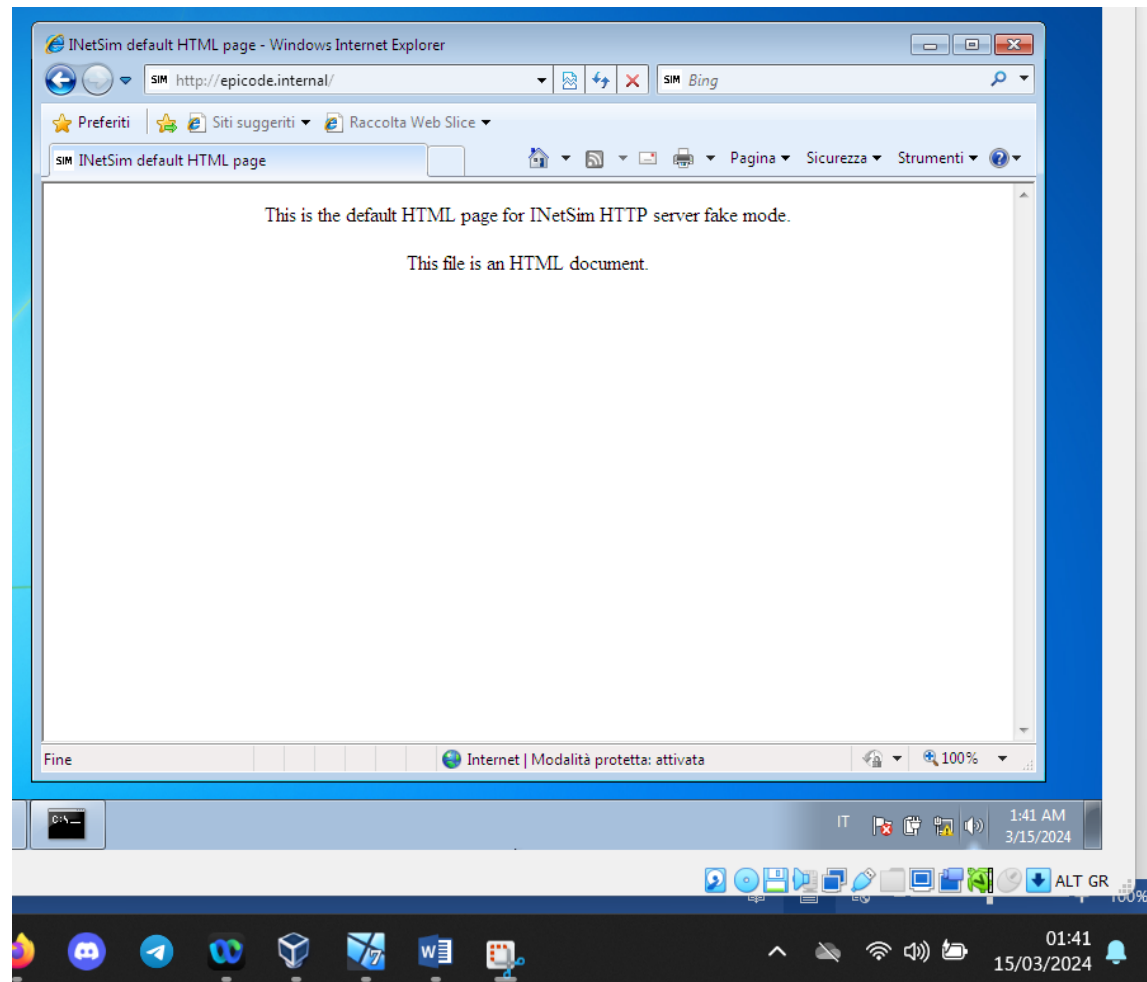
Nel seguente print screen ho riportato il funzionamento della risoluzione del servizio e del record DNS tramite protocollo HTTPS puntando a <https://epicode.internal> con il risultato di raggiungere il sito creato da INETSIM.

Ovviamente non essendoci installato sul server web di INETSIM un certificato SSL valido, il canale di comunicazione non è cifrato e la trasmissione dei pacchetti o frame avviene in chiaro e quindi non è sicura, pur utilizzando il protocollo HTTPS il browser si accorge della mancanza del certificato e segnala un errore.



Nel seguente print screen ho riportato il funzionamento della risoluzione del servizio e del record DNS tramite protocollo HTTP puntando a <http://epicode.internal> con il risultato di raggiungere il sito creato da INETSIM.

In questo caso viene utilizzato il protocollo HTTP che trasmette i dati in chiaro e non utilizza quindi di certificato SSL, la connessione non è sicura ed è possibile intercettare il traffico dati qualora mi mettessi in ascolto nel canale comunicativo tra il client e il server (Man In The Middle)





## CATTURA PACCHETTI UTILIZZANDO IL PROTOCOLLO HTTPS

Di seguito sono ripostati i print screen della cattura dei pacchetti o frame tra il pc windows e il server web creato con INETSIM, il protocollo utilizzato è HTTPS ma non essendoci un certificato valido si nota come la porta utilizzata è la 443, inizia e prova ad utilizzare la cifratura con il protocollo TLSv1, ma poi non avviene la cifratura dei pacchetti mancando il certificato e alla riga 11 viene cambiata la porta passando dalla 443 alla porta 80, quella utilizzata dal protocollo HTTP, alla prima riga viene individuato il sistema operativo e alla riga 19 viene evidenziato un alert sulla cifratura, nei record si evince anche il Three-way handshake (SYN-ACK)

kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.255	BROWSER	245	Host Announcement WINDOWS-7, Workstation, Server, NT Workstation
2	5.344393524	192.168.32.101	192.168.32.100	TCP	68	49232 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
3	5.344430643	192.168.32.100	192.168.32.101	TCP	68	443 → 49232 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
4	5.345197011	192.168.32.101	192.168.32.100	TCP	62	49232 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
5	5.345475388	192.168.32.101	192.168.32.100	TLSv1	217	Client Hello (SNI=epicode.internal)
6	5.345484179	192.168.32.100	192.168.32.101	TCP	56	443 → 49232 [ACK] Seq=1 Ack=162 Win=64128 Len=0
7	5.375378039	192.168.32.100	192.168.32.101	TLSv1	1375	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8	5.384796402	192.168.32.101	192.168.32.100	TLSv1	190	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	5.385625672	192.168.32.100	192.168.32.101	TLSv1	115	Change Cipher Spec, Encrypted Handshake Message
10	5.396722088	192.168.32.101	192.168.32.100	TCP	68	49233 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
11	5.396748441	192.168.32.100	192.168.32.101	TCP	56	80 → 49233 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	5.587102679	192.168.32.101	192.168.32.100	TCP	62	49232 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
13	5.897313284	192.168.32.101	192.168.32.100	TCP	68	[TCP Port numbers reused] 49233 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
14	5.897350935	192.168.32.100	192.168.32.101	TCP	56	80 → 49233 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	6.408926034	192.168.32.101	192.168.32.100	TCP	64	[TCP Port numbers reused] 49233 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
16	6.408953079	192.168.32.100	192.168.32.101	TCP	56	80 → 49233 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	6.415500239	192.168.32.101	192.168.32.100	TLSv1	365	Application Data
18	6.427664919	192.168.32.100	192.168.32.101	TLSv1	237	Application Data
19	6.429667180	192.168.32.100	192.168.32.101	TLSv1	386	Application Data, Encrypted Alert
20	6.430355970	192.168.32.101	192.168.32.100	TCP	62	49232 → 443 [ACK] Seq=605 Ack=1891 Win=65700 Len=0
21	6.430581961	192.168.32.101	192.168.32.100	TCP	62	49232 → 443 [FIN, ACK] Seq=605 Ack=1891 Win=65700 Len=0
22	6.430595062	192.168.32.100	192.168.32.101	TCP	56	443 → 49232 [ACK] Seq=1891 Ack=606 Win=64128 Len=0

▼ Frame 1: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) on interface a  
Section number: 1  
Interface id: 0 (any)  
Encapsulation type: Linux cooked-mode capture v1 (25)  
Arrival Time: Mar 14, 2024 21:35:35.556624786 EDT  
UTC Arrival Time: Mar 15, 2024 01:35:35.556624786 UTC  
Epoch Arrival Time: 1710466535.556624786  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.000000000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.000000000 seconds]  
Frame Number: 1  
Frame Length: 245 bytes (1960 bits)  
Capture Length: 245 bytes (1960 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: sll:ethertype:ip:udp:nbdgm:smb:browser]  
[Coloring Rule Name: SMB]  
[Coloring Rule String: smb || http || https || ftp || nbdgm || smb || browser]

Frame is marked in the GUI (frame.marked)

Packets: 22 · Displayed: 22 (100.0%)

Profile: Default

Via Casilina  
Strada chiusa

Cerca

02:37  
15/03/2024



Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.255	BROWSER	245	Host Announcement WINDOWS-7, Workstation, Server, NT Workstation

▼ Frame 1: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) on interface a

- Section number: 1
- Interface id: 0 (any)
- Encapsulation type: Linux cooked-mode capture v1 (25)
- Arrival Time: Mar 14, 2024 21:35:35.556624786 EDT
- UTC Arrival Time: Mar 15, 2024 01:35:35.556624786 UTC
- Epoch Arrival Time: 1710466535.556624786
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1
- Frame Length: 245 bytes (1960 bits)
- Capture Length: 245 bytes (1960 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: sll:ethertype:ip:udp:nbdgm:smb:browser]
- [Coloring Rule Name: SMB]
- [Coloring Rule String: smb || nbss || nbns || netbios]
- ▼ Linux cooked capture v1
  - Packet type: Broadcast (1)
  - Link-layer address type: Ethernet (1)
  - Link-layer address length: 6
  - Source: PCSSystemtec\_fe:d6:96 (08:00:27:fe:d6:96)
  - Unused: 0000
  - Protocol: IPv4 (0x0800)
- ▼ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.255
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 229
  - Identification: 0x066e (1646)
  - 0000. .... = Flags: 0x0
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 128
  - Protocol: UDP (17)
  - Header Checksum: 0x70e5 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 192.168.32.101
  - Destination Address: 192.168.32.255
- ▼ User Datagram Protocol, Src Port: 138, Dst Port: 138

Frame is marked in the GUI (frame.marked)

Packets: 23 · Displayed: 23 (100.0%) Profile: Default

7°C Nuvoloso

Cerca

02:41 15/03/2024

## CATTURA PACCHETTI UTILIZZANDO IL PROTOCOLLO HTTP

In questa schermata sono elencati i pacchetti scambiati tra il pc windows e il server web INETSIM, in questo caso il protocollo utilizzato è HTTP, il traffico è in chiaro e i pacchetti trasmessi sono molti di meno rispetto alla trasmissione HTTPS. La porta utilizzata è sin da subito la porta 80 . Alla seconda riga si può vedere il MAC address del pc windows, inoltre si può notare che i protocollo utilizzati sono ARP, TCP, http e il Three-way handshake (SYN-ACK), mentre in basso a sinistra alla voce "Source" è riportato il MAC Address del PC Linux.

The screenshot shows a Wireshark capture of network traffic between a Kali Linux virtual machine and a Windows PC. The interface includes a menu bar, toolbar, packet list, packet details, and packet bytes panes.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_fe:d6:96		ARP	62	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000023954	PCSSystemtec_21:b1:d0		ARP	44	192.168.32.101 is at 08:00:27:21:b1:d0
3	0.000893360	192.168.32.101	192.168.32.100	TCP	68	49221 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000927528	192.168.32.100	192.168.32.101	TCP	68	80 → 49221 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.001706169	192.168.32.101	192.168.32.100	TCP	62	49221 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.002008541	192.168.32.101	192.168.32.100	HTTP	335	GET / HTTP/1.1
7	0.002018386	192.168.32.100	192.168.32.101	TCP	56	80 → 49221 [ACK] Seq=1 Ack=280 Win=64128 Len=0
8	0.018086227	192.168.32.100	192.168.32.101	TCP	206	80 → 49221 [PSH, ACK] Seq=1 Ack=280 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.020709839	192.168.32.100	192.168.32.101	HTTP	314	HTTP/1.1 200 OK (text/html)
10	0.021480326	192.168.32.101	192.168.32.100	TCP	62	49221 → 80 [ACK] Seq=280 Ack=410 Win=65292 Len=0
11	0.021818877	192.168.32.101	192.168.32.100	TCP	62	49221 → 80 [FIN, ACK] Seq=280 Ack=410 Win=65292 Len=0
12	0.021838273	192.168.32.100	192.168.32.101	TCP	56	80 → 49221 [ACK] Seq=410 Ack=281 Win=64128 Len=0

**Packet Details (Section number: 1):**

- Interface id: 0 (any)
- Encapsulation type: Linux cooked-mode capture v1 (25)
- Arrival Time: Mar 14, 2024 21:16:24.026090199 EDT
- UTC Arrival Time: Mar 15, 2024 01:16:24.026090199 UTC
- Epoch Arrival Time: 1710465384.026090199
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1
- Frame Length: 62 bytes (496 bits)
- Capture Length: 62 bytes (496 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: sll:ethertype:arp]
- [Coloring Rule Name: ARP]
- [Coloring Rule String: arp]
- Linux cooked capture v1
  - Packet type: Broadcast (1)
  - Link-layer address type: Ethernet (1)
  - Link-layer address length: 6
  - Source: PCSSystemtec\_fe:d6:96 (08:00:27:fe:d6:96)
  - Unused: 0000
  - Protocol: ARP (0x0806)
  - Padding: 00000000000000000000000000000000
  - Trailer: 0000
- Address Resolution Protocol (request)
  - Hardware type: Ethernet (1)

**Packet Bytes:**

```
0000  00 01 00 01 00 06 08 00 27 fe d6 96 00 00 08 06  .....f.....
0010  00 01 08 00 06 04 00 01 08 00 27 fe d6 96 c0 a8  .....d....
0020  20 65 00 00 00 00 00 00 c0 a8 20 64 00 00 00 00  e.....d...
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

At the bottom of the packet details pane, the source MAC address **08:00:27:fe:d6:96** is circled in red.

The status bar at the bottom indicates: **Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (0.0%)** and **Profile: Default**.