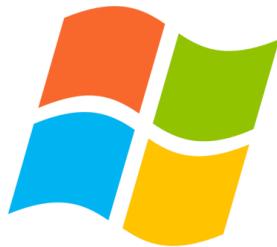


# Laboratorio Virtuale

## CSPT0324 Modulo 1



Windows 7

1

Yilei Wu

19 Luglio 2024

# Indice

Consegna dell'esercizio.....	3
Architettura del laboratorio virtuale e della rete interna.....	3
Requisiti.....	4
Configurazione di Kali Linux.....	4
Controlli preliminari su Virtual Box e avvio.....	4
Impostare l'indirizzo IP statico a 192.168.32.100 .....	6
Configurazione di Windows 7.....	8
Controlli preliminari su Virtual Box .....	8
Impostare l'indirizzo IP statico a 192.168.32.101 .....	9
Configurazione firewall di Windows 7 .....	12
Verifica e test sulla rete del laboratorio virtuale.....	13
Configurazione Client, HTTPS Server & DNS Server .....	14
Configurazione DNS di Windows 7 (Client).....	14
Configurazione Inetsim su Kali Linux (Server HTTPS & DNS).....	14
Test sulla configurazione di INetSim .....	16
Analisi e risoluzione del mancato funzionamento del server DNS.....	17
Test sulla risoluzione DNS del dominio epicode.internal .....	19
Ulteriori verifiche sulla risoluzione dei domini personalizzati.....	20
Wireshark .....	21
Analisi con protocollo HTTPS.....	21
MAC Address .....	22
Analisi contenuto richiesta HTTPS .....	23
Analisi con protocollo HTTP .....	24
Configurazione in HTTP .....	24
Analisi contenuto richiesta HTTP .....	25
Conclusione .....	25

## Consegna dell'esercizio

### 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

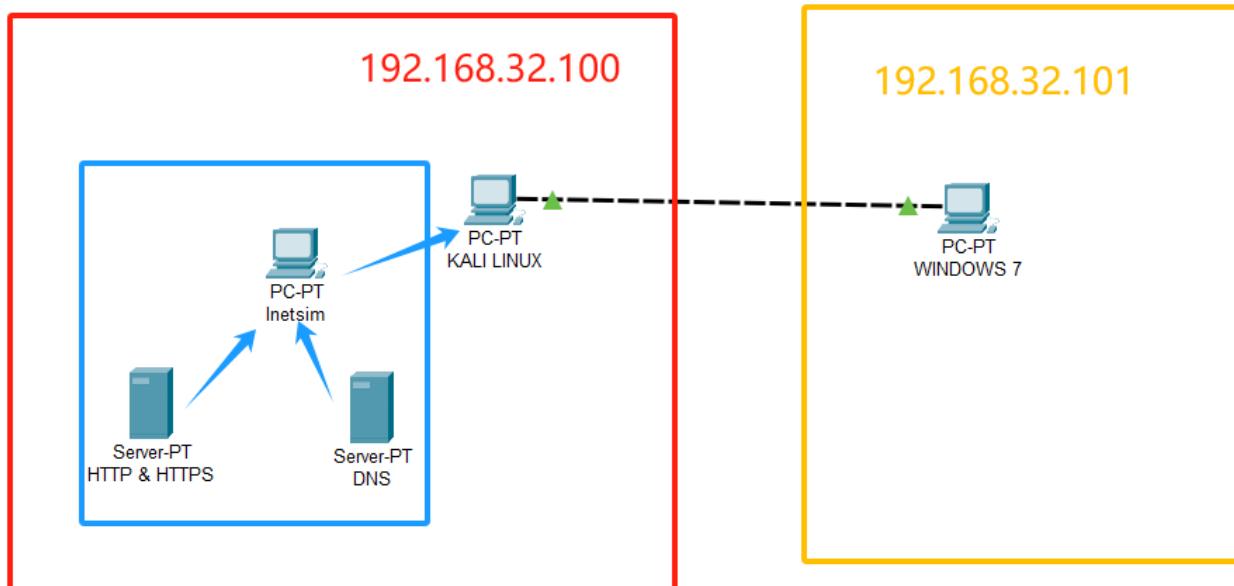
### Traccia:

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

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.

### Architettura del laboratorio virtuale e della rete interna



Kali Linux, che ospita il programma Inetsim, avrà diversi ruoli chiave nella rete: server HTTP e HTTPS per il caricamento delle pagine web e servizio DNS per la risoluzione del dominio. Windows 7 sarà il nostro client, da cui partiranno tutte le richieste al server.

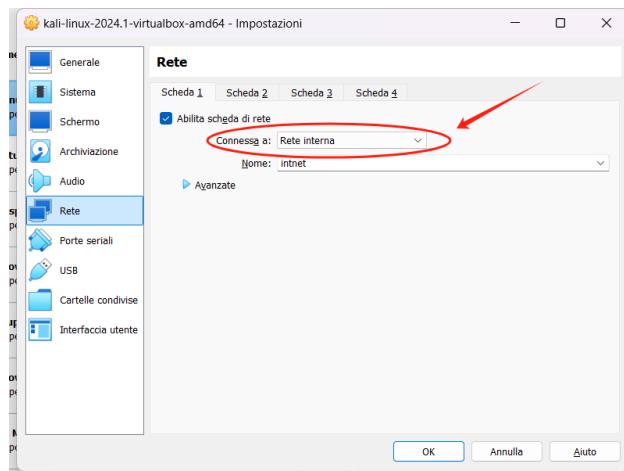
# Requisiti

## Configurazione di Kali Linux

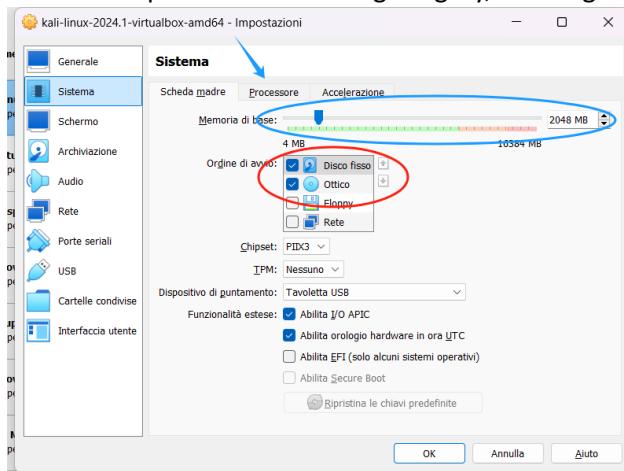
### Controlli preliminari su Virtual Box e avvio

Fondamentali sono i controlli prima di avviare la macchina virtuale:

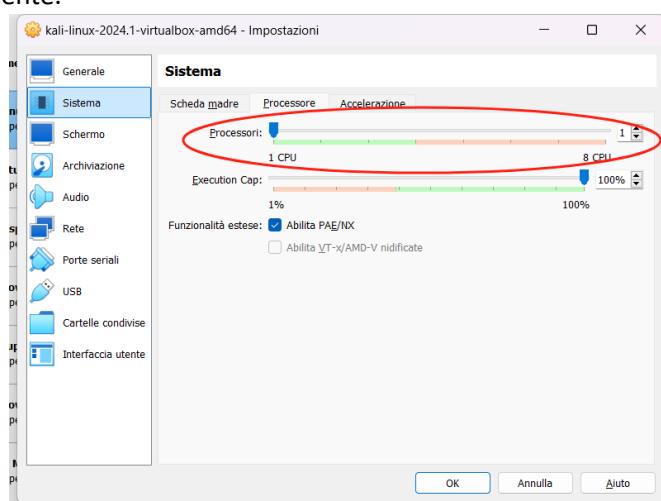
1. la rete deve essere impostata su interna, come in figura, e da consegna si deduce che l'ip del gateway sarà 192.168.32.1;



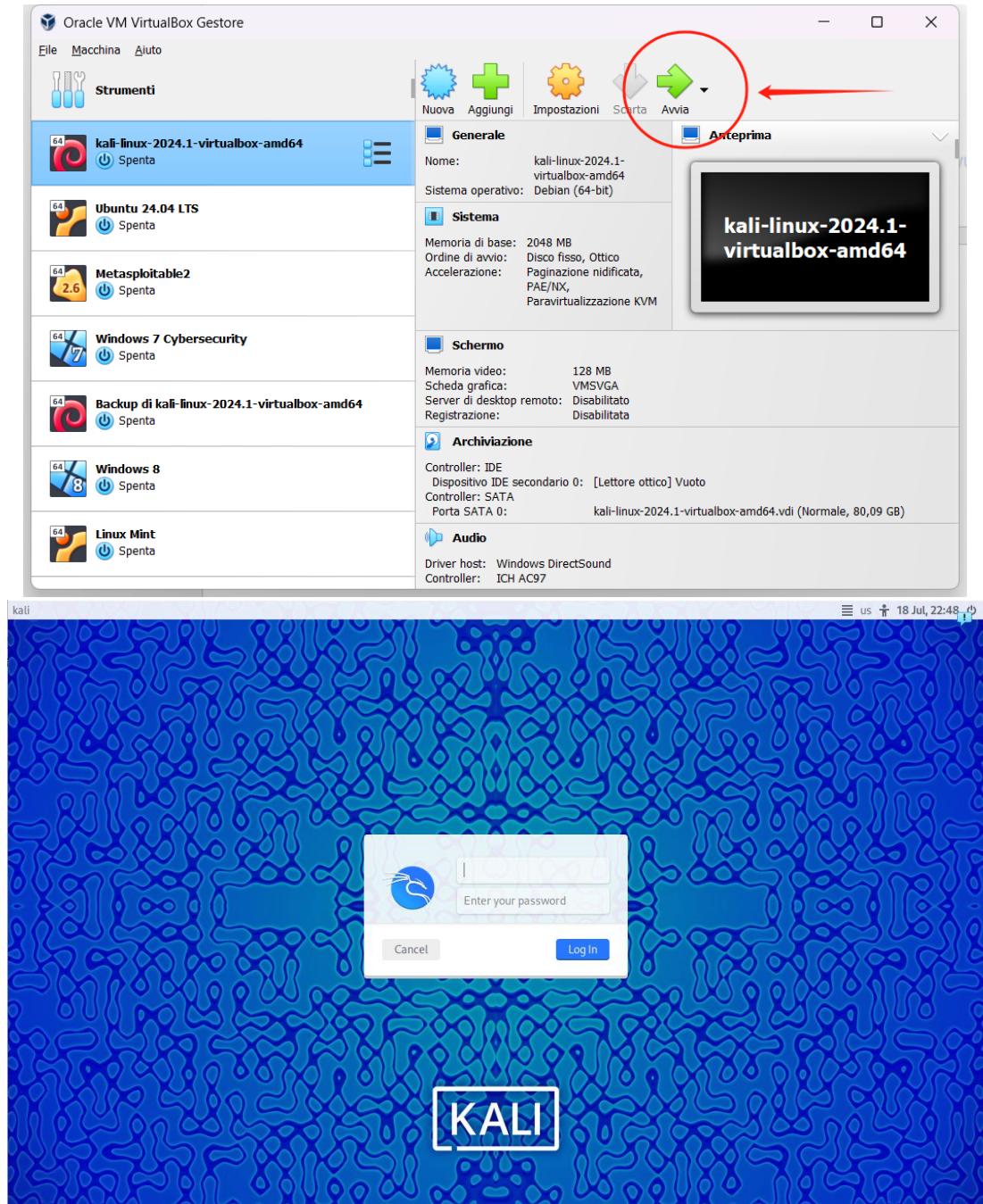
2. evitare eventuali problemi di incompatibilità di tecnologie legacy, si consiglia di deselezionare "floppy"



3. concedere i requisiti minimi o consigliati per la macchina virtuale, in questo caso, la configurazione da immagine è sufficiente.



4. Avvio di Kali Linux e inserimento delle credenziali di default. User e Password: kali



## Impostare l'indirizzo IP statico a 192.168.32.100

- 11 Check dell'indirizzo IP corrente attraverso il comando "ifconfig".

The screenshot shows a Kali Linux desktop environment. A terminal window titled 'kali@kali: ~' is open, displaying the output of the 'ifconfig' command. The output shows two interfaces: 'eth0' and 'lo'. 'eth0' has an IP of 192.168.50.100 and a netmask of 255.255.255.0. 'lo' has an IP of 127.0.0.1 and a netmask of 255.0.0.0. Below the terminal, a file manager window is visible with icons for Trash, File System, and Home. A green arrow points from the terminal's 'ifconfig' command to the terminal's prompt. Another green arrow points from the terminal's 'sudo nano /etc/network/interfaces' command to the password entry field.

- 12 L'indirizzo IP attuale è 192.168.50.100 e quindi per la modifica lanciare il comando "sudo nano /etc/network/interfaces", la password se necessaria è "kali" (quella di login) e si preme invio.
- 13 Utilizzando l'editor di testo nano, modificare come da immagine: l'address 192.168.32.100 con lo slash /24 indica la subnet 255.255.255.0, il gateway ai fini dell'esercizio non è necessario, ma è impostato in questo caso per coerenza con la configurazione della rete.

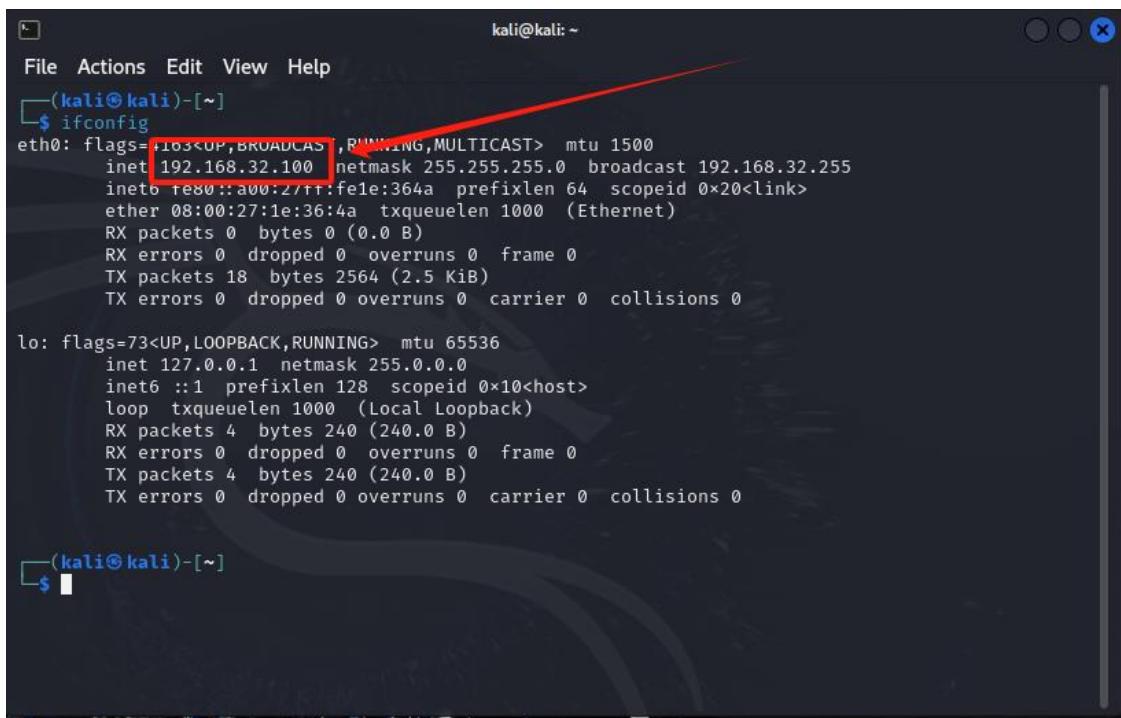
The screenshot shows a terminal window with the title 'GNU nano 8.0 /etc/network'. The file contains the configuration for network interfaces. A red box highlights the section for 'iface eth0'. Inside this box, a red arrow points to the 'static' keyword. The highlighted section is as follows:

```
# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 192.168.32.100/24
    gateway 192.168.32.1
```

- 14 Per salvare le modifiche dell'editor CTRL+O e Invio, poi per uscire CTRL+X.
- 15 Lanciare il comando "sudo reboot" per riavviare il sistema e quindi far sì che si applichino le modifiche.

The screenshot shows a terminal window with the title '(kali㉿kali)-[~]'. The user has typed '\$ sudo reboot' and is awaiting confirmation.

16 lancia nuovamente il comando "ifconfig" per verificare che sia stata impostata il nuovo indirizzo IP.



```
kali㉿kali: ~
File Actions Edit View Help
[(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
        inetb fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 18 bytes 2564 (2.5 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)-[~]
$
```

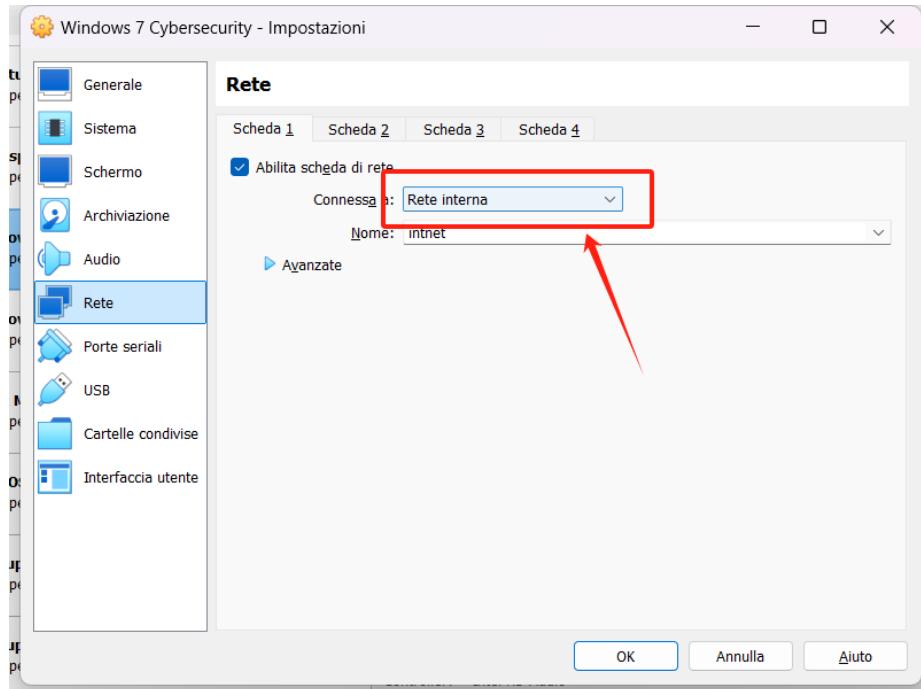
Indirizzo IP statico di Kali Linux modificato con successo.

# Configurazione di Windows 7

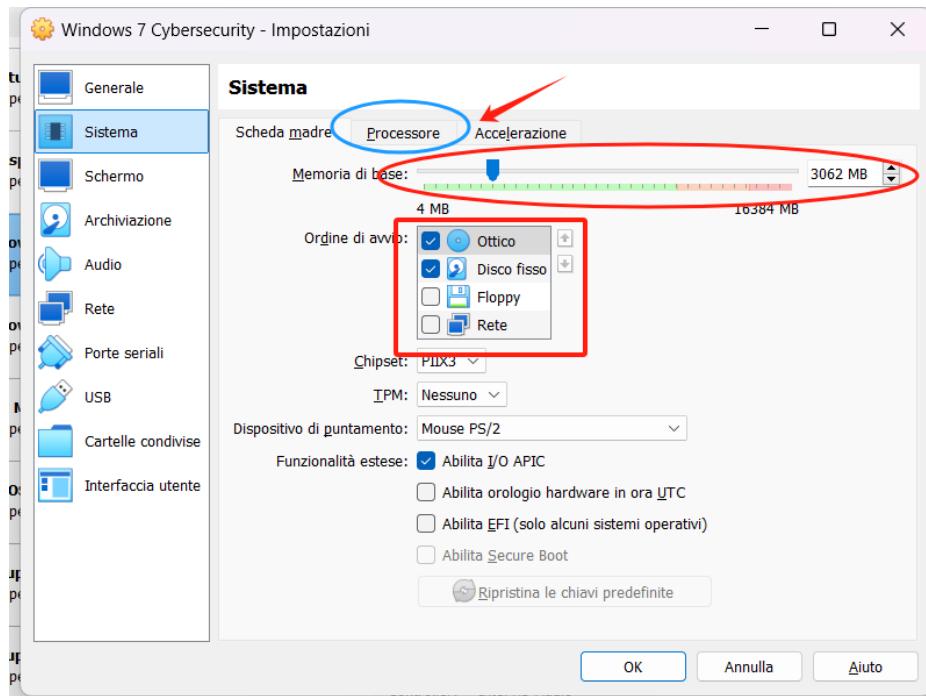
## Controlli preliminari su Virtual Box

I controlli preliminari consistono in

1. impostazione in rete interna sulla scheda di rete;

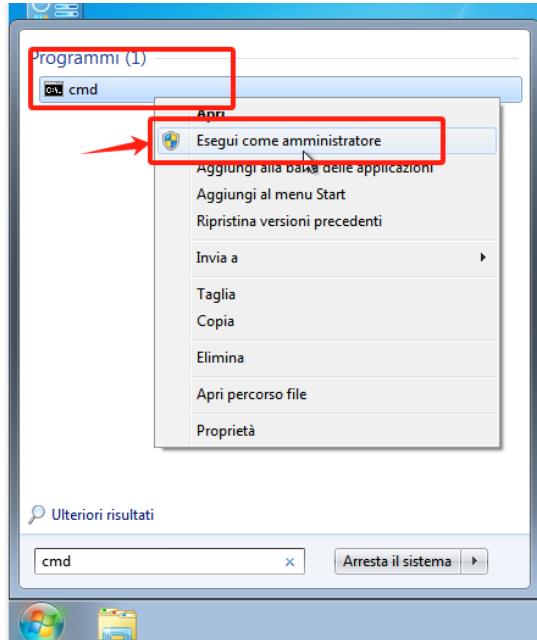


2. per evitare eventuali problemi di compatibilità, deselectare "floppy"
3. assegnare almeno 2 CPU e 2 GB ram alla macchina virtuale.



## Impostare l'indirizzo IP statico a 192.168.32.101

1. Avviare la macchina virtuale di Windows 7 e in basso a sinistra, sul simbolo di Windows, cercare "cmd", il terminale, e per evitare possibili limitazioni, aviarlo con i privilegi di amministratore (click destro mouse su cmd)



2. Dal terminale cmd lanciare il comando "ip config/all" per ottenere le informazioni più complete relativo all'indirizzo IP. IP statico attualmente configurato è 192.168.50.102, quindi bisogna procedere alla modifica al nuovo indirizzo IP statito 192.168.32.101

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Windows\system32>ipconfig /all

Configurazione IP di Windows

    Nome host . . . . . : Corso-PC
    Suffixo DNS primario . . . . . :
    Tipo nodo . . . . . : Ibrido
    Routing IP abilitato . . . . . : No
    Proxy WINS abilitato . . . . . : No

Scheda Ethernet Connessione alla rete locale <LAN>:

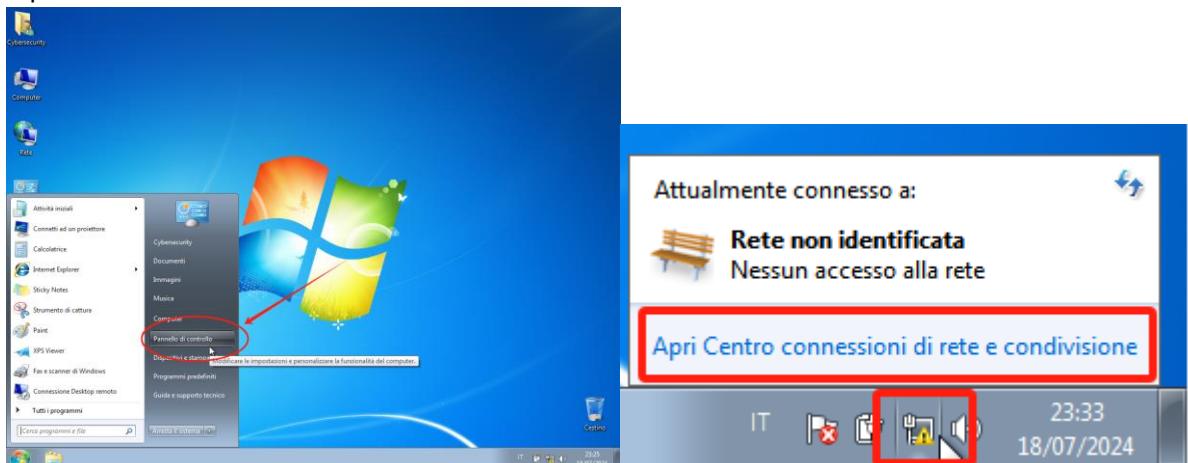
    Suffixo DNS specifico per connessione: Scheda desktop Intel(R) PRO/1000 MT
    Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
    Indirizzo fisico . . . . . : 08-00-27-37-B4-EB
    DHCP abilitato . . . . . : No
    Configurazione automatica abilitata . . . . . : Sì
    Indirizzo IPv6 locale rispetto al collegamento . . . . . : fe80::385a:72eb:edd3:b128%11<referenziale>
    Indirizzo IPv4 . . . . . : 192.168.50.102<referenziale>
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.50.1
    ILID DHCPv6 . . . . . : 235405381
    DUID Client DHCPv6 . . . . . : 00-01-00-01-2E-0B-95-A6-00-00-27-37-B4-EB
    Server DNS . . . . . : 1.1.1.1
    1.0.0.1
    NetBIOS su TCP/IP . . . . . : Attivato

Scheda Tunnel isatap.<D14DF312-15C0-4370-9966-C43F9621BD3C>:

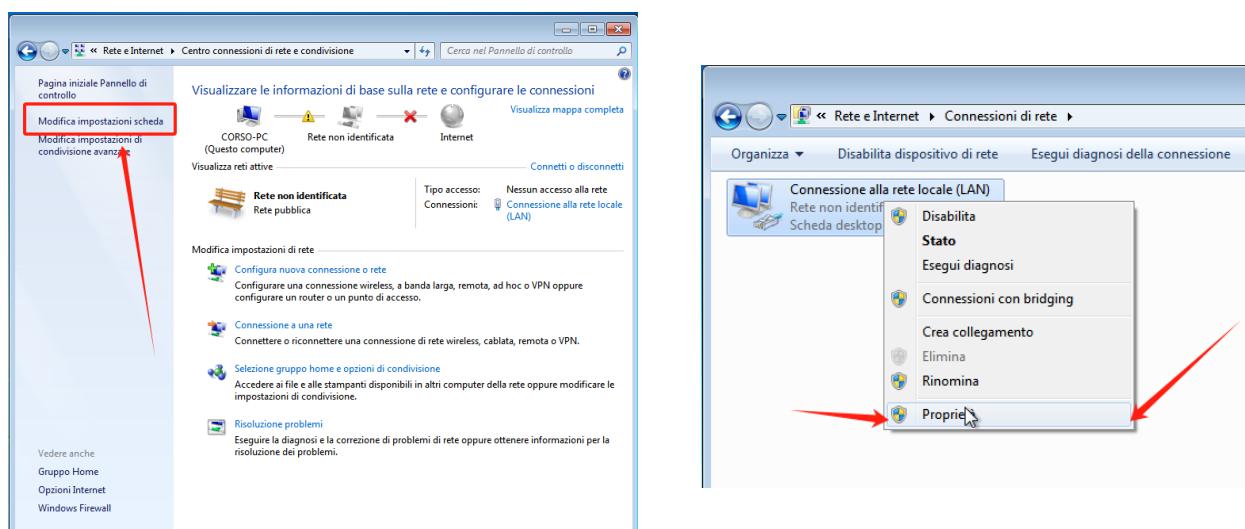
    Stato supporto. . . . . : Supporto disconnesso
    Suffixo DNS specifico per connessione: Microsoft ISATAP Adapter
    Descrizione . . . . . : Microsoft ISATAP Adapter
    Indirizzo fisico . . . . . : 00-00-00-00-00-00-E0
    DHCP abilitato . . . . . : No
    Configurazione automatica abilitata . . .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

C:\Windows\system32>
```

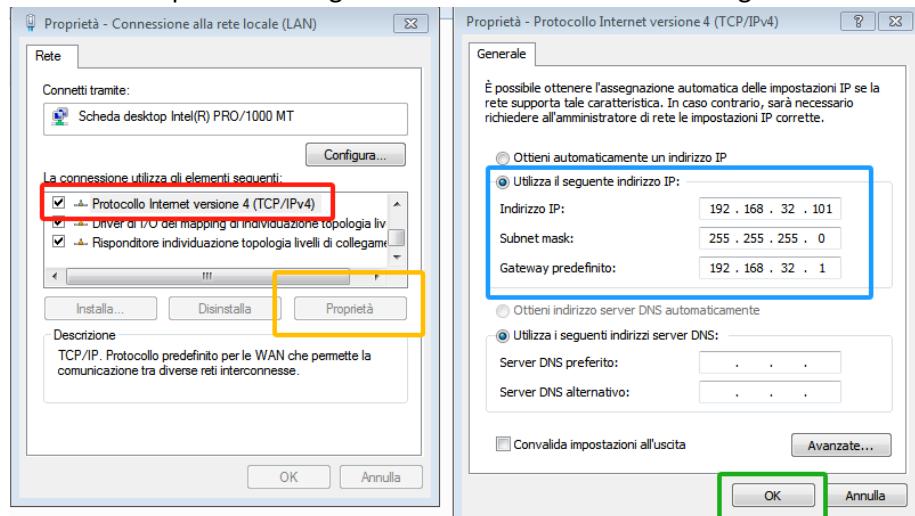
3. Per impostare l'indirizzo IP statico in Windows 7 aprire l'icona Windows in basso a sinistra e recarsi su Pannello di Controllo > Rete e Internet > Centro connessioni di rete e condivisione oppure un altro modo più veloce è cliccare l'icona di rete in basso a destra col tasto destro del mouse e cliccare su "Apri Centro connessioni di rete e condivisione".



4. Andare su modifica impostazioni scheda e poi tasto destro del mouse sulla scheda di rete e poi proprietà.



5. Scorrere fino a IPv4 > Proprietà e configurare l'indirizzo IP come da immagine.



6. Indirizzo IP 192.168.32.101, subnet mask 255.255.255.0 e Gateway predefinito 192.168.32.1 poi cliccare “OK” per salvare.
7. Riavviare Windows, consigliato il metodo classico tramite l’icona o ALT+F4 da desktop.
8. Dopo aver riavviato, avviare il terminale cmd e lanciare il comando “ipconfig /all” per accertarsi dell’avvenuta modifica al nuovo indirizzo IP.

```
C:\Users\Cybersecurity>ipconfig /all
Configurazione IP di Windows

Nome host . . . . . : Corso-PC
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 . . . . . : 08-00-27-37-B4-EB
DHCP abilitato . . . . . : No
Configurazione automatica abilitata . . . . . : Si
Indirizzo IPv6 locale rispetto al collegamento . . . : fe80::385a:72eb:edd3:b128%11<Preferenziale>
Indirizzo IPv4 . . . . . : 192.168.32.101<Preferenziale>
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.1
IAID DHCPv6 . . . . . : 235405351
DUID Client DHCPv6 . . . . . : 00-01-00-01-2E-0B-95-A6-08-00-27-37-B4-EB
Server DNS . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS su TCP/IP . . . . . : Attivato

Scheda Tunnel isatap.<D14DF312-15C0-4370-9966-C43F9621BD3C>:

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 . . . . . : Si

C:\Users\Cybersecurity>
```

Configurazione effettuata con successo.

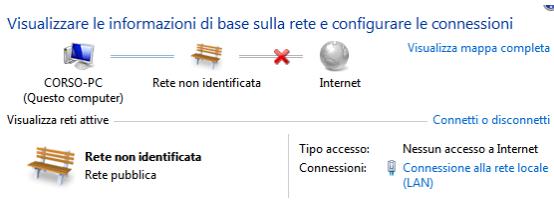
11

#### **NOTA BENE**

Si è utilizzato il comando “ipconfig /all” per avere più informazioni, ma per questi passaggi si poteva usare anche il comando semplice “ipconfig”.

## Configurazione firewall di Windows 7

Di default in Windows 7 la rete interna è considerata dal sistema operativo come una rete pubblica e in questo caso specifico non è possibile la modifica, questo implica delle restrizioni, ovvero Windows blocca tutti i tentativi di connessione in entrata, compreso Kali Linux e per quest'ultima risulterà sempre non raggiungibile.

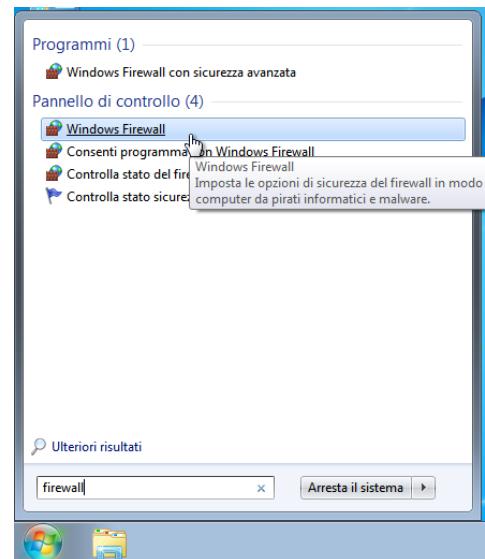
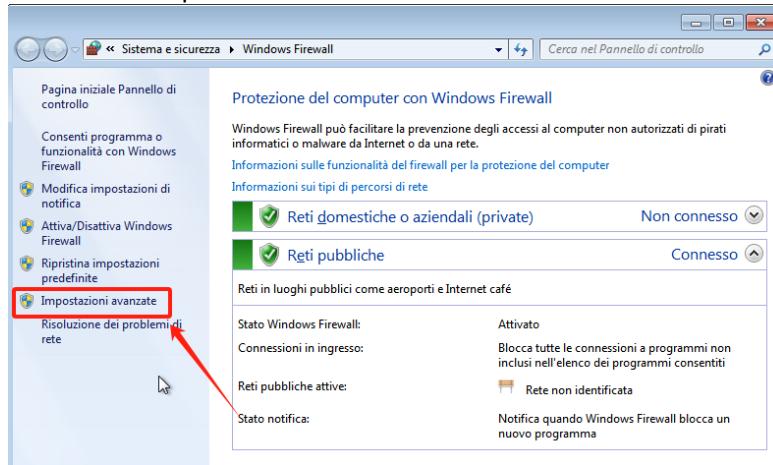


Per superare questa restrizione bisogna configurare il firewall di Windows 7.

1. Aprire il Windows Firewall cercandolo dalla barra di ricerca sull'icona Windows in basso a sinistra

oppure cercarlo sul pannello di controllo.

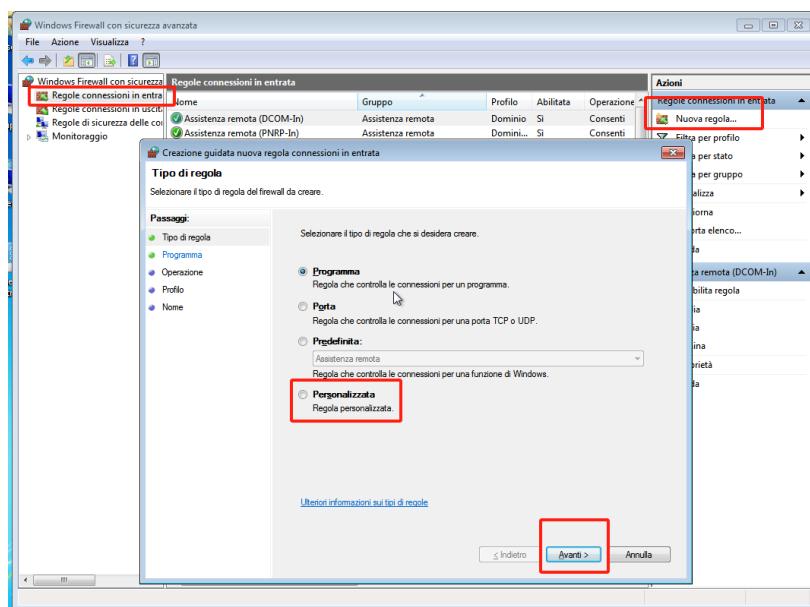
Su "Impostazioni Avanzate"



2. Creare una nuova regola di connessione in entrata. Come

da figura "Nuova regola..." > Tipo di regola

"Personalizzata" > tutti i programmi e lasciare invariato il resto. Poi salvarlo con un nome a discrezione.

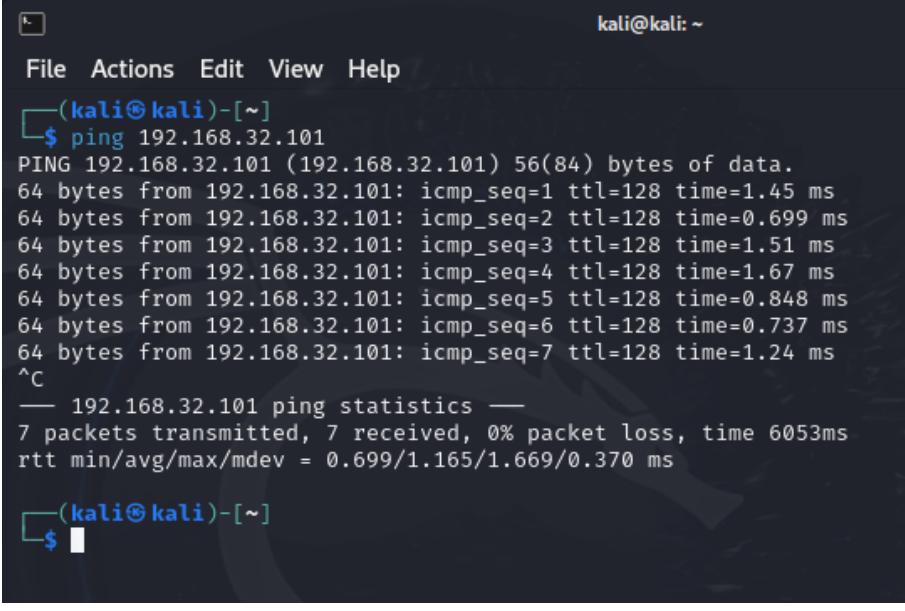


Non è stato creato una regola più stringente sul firewall per agevolare futuri utilizzi e/o implementazione della macchina virtuale con altre macchine del laboratorio virtuale.

## Verifica e test sulla rete del laboratorio virtuale

Per verificare che le due macchine virtuali siano correttamente configurate e comunichino tra di loro utilizzare il comando PING da terminale.

Da Kali a Windows “ping 192.168.32.101”

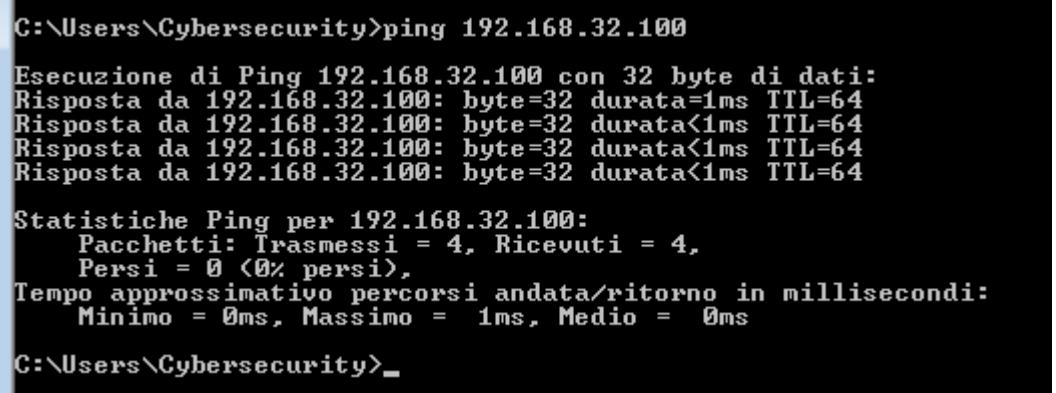


```
kali@kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ ping 192.168.32.101
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data.
64 bytes from 192.168.32.101: icmp_seq=1 ttl=128 time=1.45 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.699 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=1.51 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=1.67 ms
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=0.848 ms
64 bytes from 192.168.32.101: icmp_seq=6 ttl=128 time=0.737 ms
64 bytes from 192.168.32.101: icmp_seq=7 ttl=128 time=1.24 ms
^C
--- 192.168.32.101 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6053ms
rtt min/avg/max/mdev = 0.699/1.165/1.669/0.370 ms

└─(kali㉿kali)-[~]
$
```

Collegamento effettuato con successo, il pacchetto è stato correttamente inviato a Windows 7 e quindi ha confermato l'avvenuta ricezione del pacchetto.

Da Windows a Kali “ping 192.168.32.100”



```
C:\Users\Cybersecurity>ping 192.168.32.100

Esecuzione di Ping 192.168.32.100 con 32 byte di dati:
Risposta da 192.168.32.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.32.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 <0% persi>,
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 1ms, Medio = 0ms

C:\Users\Cybersecurity>
```

Collegamento effettuato con successo, il pacchetto è stato correttamente inviato a Kali Linux e quindi ha confermato l'avvenuta ricezione del pacchetto.

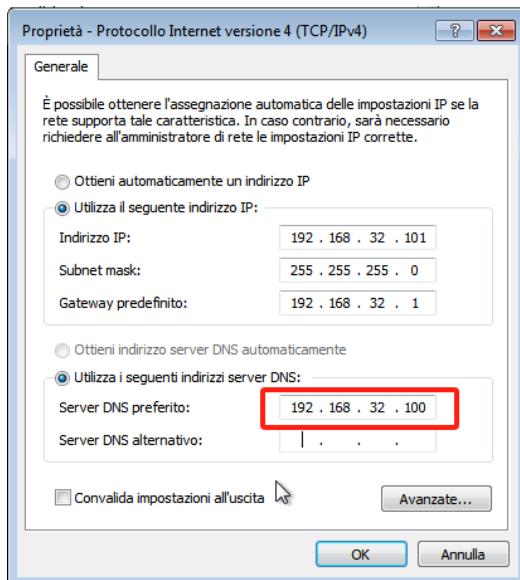
## Configurazione Client, HTTPS Server & DNS Server

Sono necessari attivare il servizio di HTTPS come server per caricare la pagina web e il servizio DNS per tradurre il dominio `epicode.internal` all'indirizzo IP statico 192.168.32.100 (corrispondente a Kali)

Come da traccia consegna, quando si digita sul browser di Windows 7 `epicode.internal` deve attivarsi il servizio DNS impostato su Inetsim all'interno di Kali Linux e reindirizzarà la richiesta all'indirizzo IP 192.168.32.100.

### Configurazione DNS di Windows 7 (Client)

Per impostare l'indirizzo IP del server DNS dal client Windows 7 si torna sulla stessa finestra per configurare l'indirizzo IP statico (vedi sezione precedente “Impostare l'indirizzo IP statico a 192.168.32.101”), su “Server DNS preferito”, immettere l'indirizzo IP 192.168.32.100.



14

### Configurazione Inetsim su Kali Linux (Server HTTPS & DNS)

Aprire il terminale in Kali Linux e avviare la configurazione di Inetsim: comando `sudo nano /etc/inetsim/inetsim.conf`

Attivare i servizi di https e dns togliendo il commento # e impostare l'indirizzo IP del service\_bind\_address su 192.168.32.100 poiché è l'indirizzo IP locale su cui il servizio simulato sarà in ascolto. Lo stesso indirizzo IP lo si attribuisce anche a dns\_default per attivare il servizio di DNS e “dns\_static episode.internal 192.168.32.100” affinché traduca solo il dominio `episode.internal`

```
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quodt_tcp,
# quodt_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3
# ftps, irc, https
#
#start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
```

The screenshot shows a terminal window with the command `sudo nano /etc/inetsim/inetsim.conf`. The file contains configuration for various services. The line `start_service https` and the line `service_bind_address 192.168.32.100` are highlighted with red boxes. The nano editor interface is visible at the bottom.

```

GNU nano 8.0          /etc/inetsim/
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
#dns_bind_port 53

#####
# dns_default_ip
#
# 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

^G Help      ^O Write Out    ^F Where Is      ^K Cut
^X Exit      ^R Read File    ^W Replace     ^U Paste

```

```

GNU nano 8.0          /etc/inetsim/inetsim
#dns_default_domainname epicode.internal

#####
# 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
#
# DNS version
#
# Syntax: dns_version <version>

^G Help      ^O Write Out    ^F Where Is      ^K Cut
^X Exit      ^R Read File    ^W Replace     ^U Paste

```

Non è necessario configurare “dns\_default\_domainname epicode.internal” perché quanto configurato in figura, è sufficiente per la richiesta dell'esercizio. Se si configurasse il dns\_default\_domainname od entrambi, qualsiasi dominio sarebbe stato reindirizzato a 192.168.32.100, invece in questo caso specifico è solo il dominio della consegna **epicode.internal** che andrà a reindirizzare.

Per quanto riguarda il caricamento della pagina di inetsim in html in entrambi i protocoli http e https, sulla versione di inetsim attualmente in utilizzo, sono attivi di default.

#  
https\_default\_fakefile sample.html text/html

15

Premere CTRL+O e invio per salvare e CTRL+X per tornare al terminale, dove si può subito avviare inetsim con il comando “sudo inetsim”.

```

File Actions View Help
File Actions View Help
GNU nano 8.0          /usr/share/perl5/INetSim/DNS.pm *
my $uid = getpwnam($runasuser); ... no servers could be reached
my $gid = getgrnam($runasgroup);
POSIX::setgid($gid); ... up to setup with fd00::feed:ffff:fe42:3b53
my $newgid = POSIX::getegid(); ... no servers could be reached
if ($newgid != $gid) { ... failed! (Cannot switch group)", INetSim::Conf
    exit 0;
}

POSIX::setuid($uid);
if ($< != $uid || $> != $uid) {
    $< = $> = $uid; # try again - reportedly needed by some Perl 5.8.0 L
    if ($< != $uid) {
        INetSim::Log::MainLog("failed! (Cannot switch user)", INetSim::Conf
        exit 0;
    }
}

$0 = 'inetsim_'.INetSim::Config::getConfigParameter("DNS_ServiceName");
INetSim::Log::MainLog("started (PID $CPID)", INetSim::Config::getConfigP
$server->start_server();
INetSim::Log::MainLog("stopped (PID $CPID)", INetSim::Config::getConfigP
exit 0;
}

```

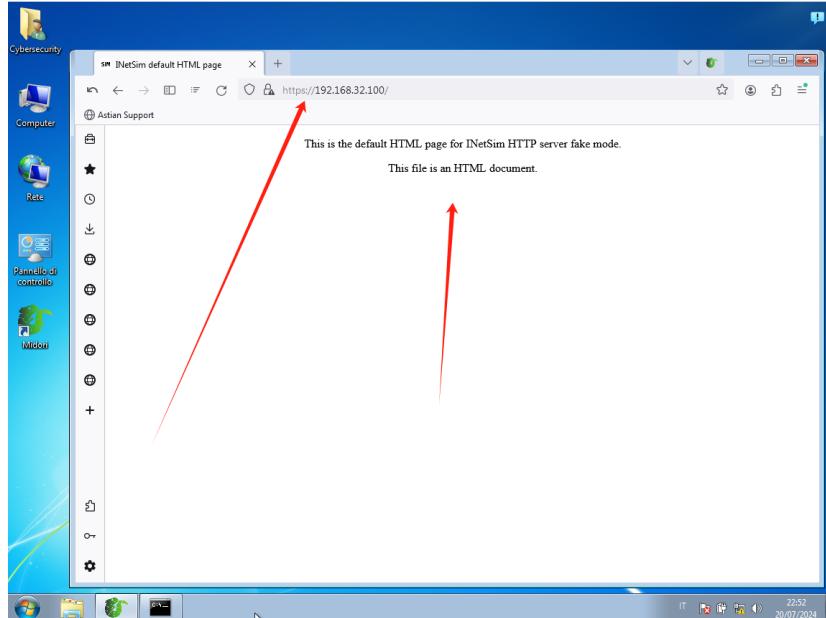
Dopo l'avvio c'è un suggerimento che consiglia di aggiornare il metodo obsoleto con quello preferenziale “start\_server()”. Come suggerito aprire il file di configurazione “sudo nano /usr/share/perl5/INetSim/DNS.pm” (fare attenzione alle maiuscole e minuscole) e modificare come da immagine. Salvare con CTRL+O e invio. Si fa questa operazione anche per non avere problemi con eventuali futuri aggiornamenti, se previsti, in quanto è stato dichiarato “deprecated method” dal programma stesso.

## Test sulla configurazione di INetSim

Andare su Windows 7 e avviare il browser.

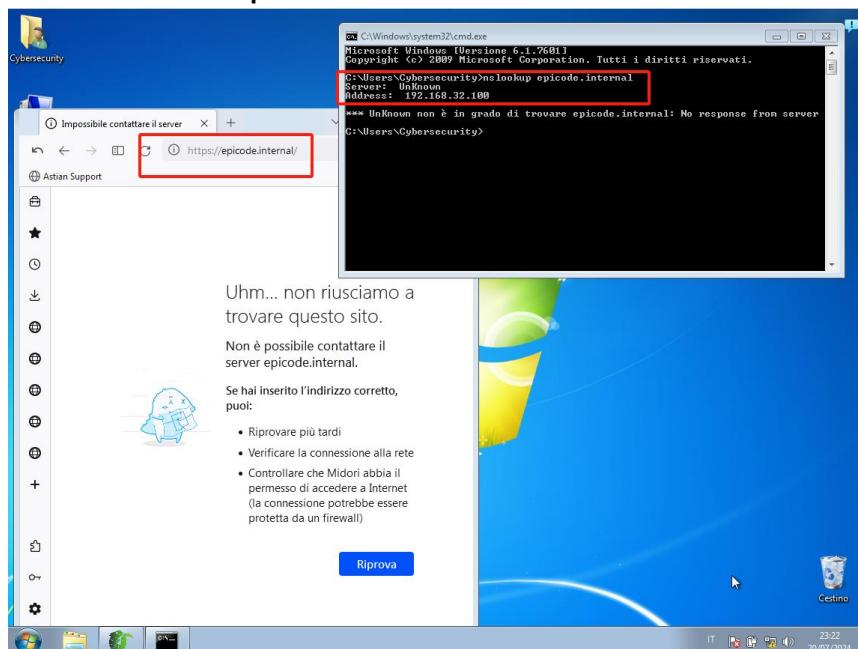
In questo caso specifico è stato aggiornato manualmente Windows 7 scaricando alcuni aggiornamenti ufficiali, non essendo possibile scaricarli in automatico con Windows Update per il termine del supporto ufficiale avvenuto il 14 gennaio 2020. Gli aggiornamenti sono stati necessari affinché possa supportare un browser veloce, sicuro e leggero, in sostituzione del browser di default Internet Explorer, molto lento e legacy, Midori.

Inserire nell'url l'indirizzo ip **192.168.32.100**



Il collegamento e il caricamento della pagina fake HTML di Inetsim avviene con successo quindi il server HTTP funziona perfettamente.

Inserire nell'url l'indirizzo il dominio **epicode.internal**



Purtroppo la pagina non carica. Interrogando il server DNS con il comando sul terminale "*nslookup epicode.internal*" si scopre che il DNS è configurato correttamente (vedi riferimento sezione "Configurazione DNS di Windows 7) tuttavia il server è "Unkown" il ché vuol dire che il server non viene carica. C'è un probabile errore di collegamento/ configurazione DNS lato Kali Linux/ Inetsim si verificherà e si analizzerà nel prossimo paragrafo. Attualmente il server DNS non funziona.

## Analisi e risoluzione del mancato funzionamento del server DNS

Una volta accertato che il problema non dipende da Windows 7, verificare Kali Linux ed Inetsim.

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-~]
$ sudo inetsim
[sudo] password for kali:
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 1541) ==
Session ID: 1541
Listening on: 192.168.32.100
Real Date/Time: 2024-07-20 17:20:49
Fake Date/Time: 2024-07-20 17:20:49 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1543)
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INETSim/DNS.pm line 69.
* https_443_tcp - started (PID 1544)
done.
Simulation running.
```

Avviato nuovamente Inetsim, si nota subito che c'è stato un tentativo di aprire la porta 53 relativo al server DNS. Approfondendo che il comando “nslookup episode.internal 192.168.32.100” la porta 53, necessaria per il funzionamento del server DNS, non risulta aperta perché rifiuta la connessione.

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]
$ nslookup episode.internal
;; UDP setup with fd00::1eed:6fff:fe42:3b53#53(fd00::1eed:6fff:fe42:3b53) for
episode.internal failed: network unreachable.
;; no servers could be reached

;; UDP setup with fd00::1eed:6fff:fe42:3b53#53(fd00::1eed:6fff:fe42:3b53) for
episode.internal failed: network unreachable.
;; no servers could be reached

;; UDP setup with fd00::1eed:6fff:fe42:3b53#53(fd00::1eed:6fff:fe42:3b53) for
episode.internal failed: network unreachable.
;; no servers could be reached

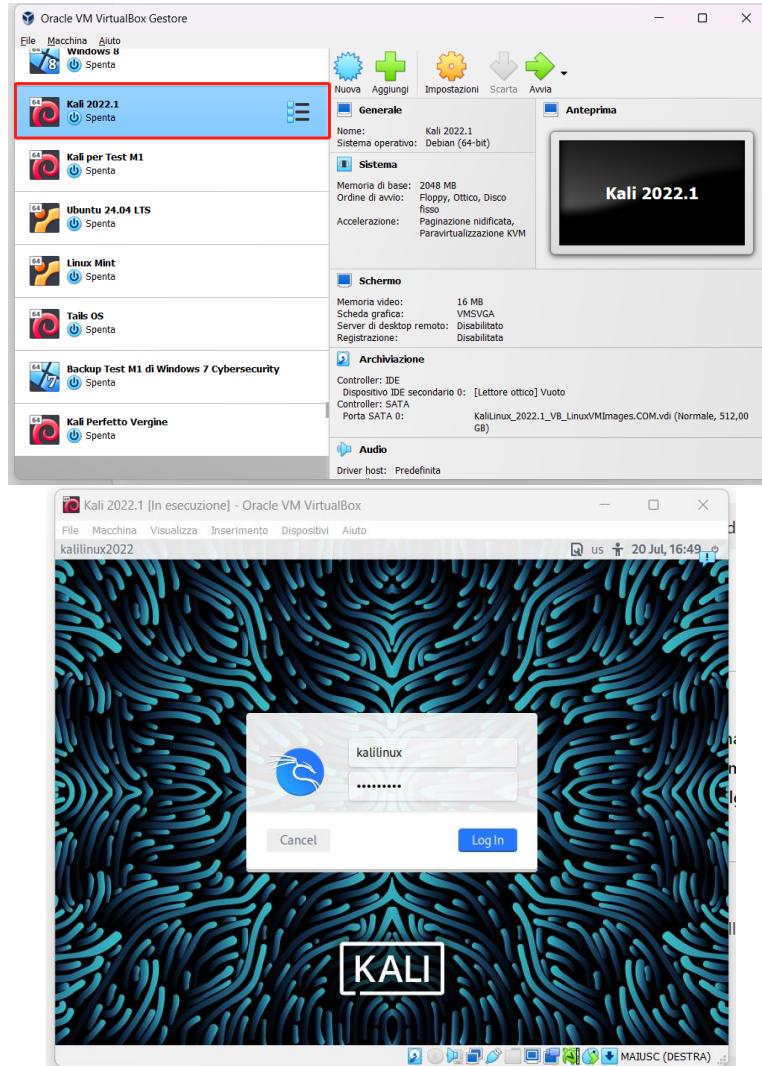
9 (Delta: 0 seconds)
[(kali㉿kali)-~]
$ nslookup episode.internal 192.168.32.100
;; communications error to 192.168.32.100#53: connection refused
;; communications error to 192.168.32.100#53: connection refused
;; communications error to 192.168.32.100#53: connection refused
;; no servers could be reached

[(kali㉿kali)-~]
$
```

Trovato il motivo della mancata traduzione del dominio episode.internal si tenta con l'aggiornamento di sistema e inetsim: il problema rimane ugualmente.

Ricontrollando tutte le configurazioni, facendo varie ricerche, consultazioni e ragionamenti si conclude che è molto probabile un problema di compatibilità: Kali Linux è alla versione 2024.2 mentre Inetsim è alla versione 1.3.2 che è stata rilasciata il 19 maggio 2020, quindi ormai 4 anni che non è stato aggiornato (fonti <https://www.inetsim.org/>). A conferma di questo sospetto, si è trovato prove che INetSim funzionava correttamente con una configurazione simile, in cui il server DNS operava perfettamente e il dominio veniva interpretato in modo corretto. Tuttavia, i test che sono stati consultati risalgono a sei anni fa. (Fonte <https://www.youtube.com/watch?v=72YXELAZK2Q>) Quindi il forte sospetto per l'incompatibilità tra Kali Linux (aggiornato di recente) e Inetsim (non aggiornato dal 2020) è più che fondato.

Per dimostrare che questa tesi sia corretta, si prosegue con l'installazione e configurazione identica al paragrafo "Configurazione di Kali Linux" di una nuova macchina virtuale Kali Linux ma versione 2022.1. L'unica differenza è che le credenziali di accesso sono "kalilinux" sia per nome utente che password.



Una volta avviato inetsim si contraddistingue che la porta 53 è correttamente avviata.

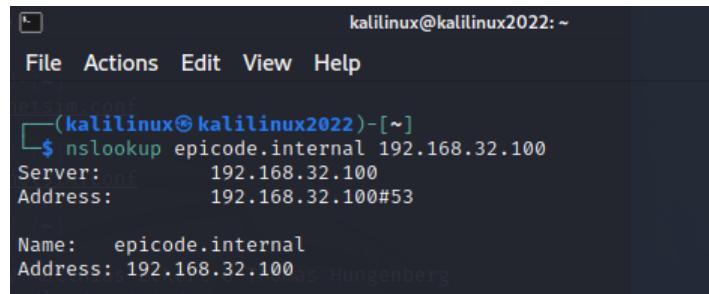
```

kalilinux@kalilinux2022: ~
File Actions View Help
[(kalilinux@kalilinux2022)-[~]
$ sudo inetsim
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 1237) ==
Session ID: 1237
Listening on: 192.168.32.100
Real Date/Time: 2024-07-20 16:50:43
Fake Date/Time: 2024-07-20 16:50:43 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 1239)
* https_443_tcp - started (PID 1240)
done.
Simulation running.

```

## Test sulla risoluzione DNS del dominio epicode.internal

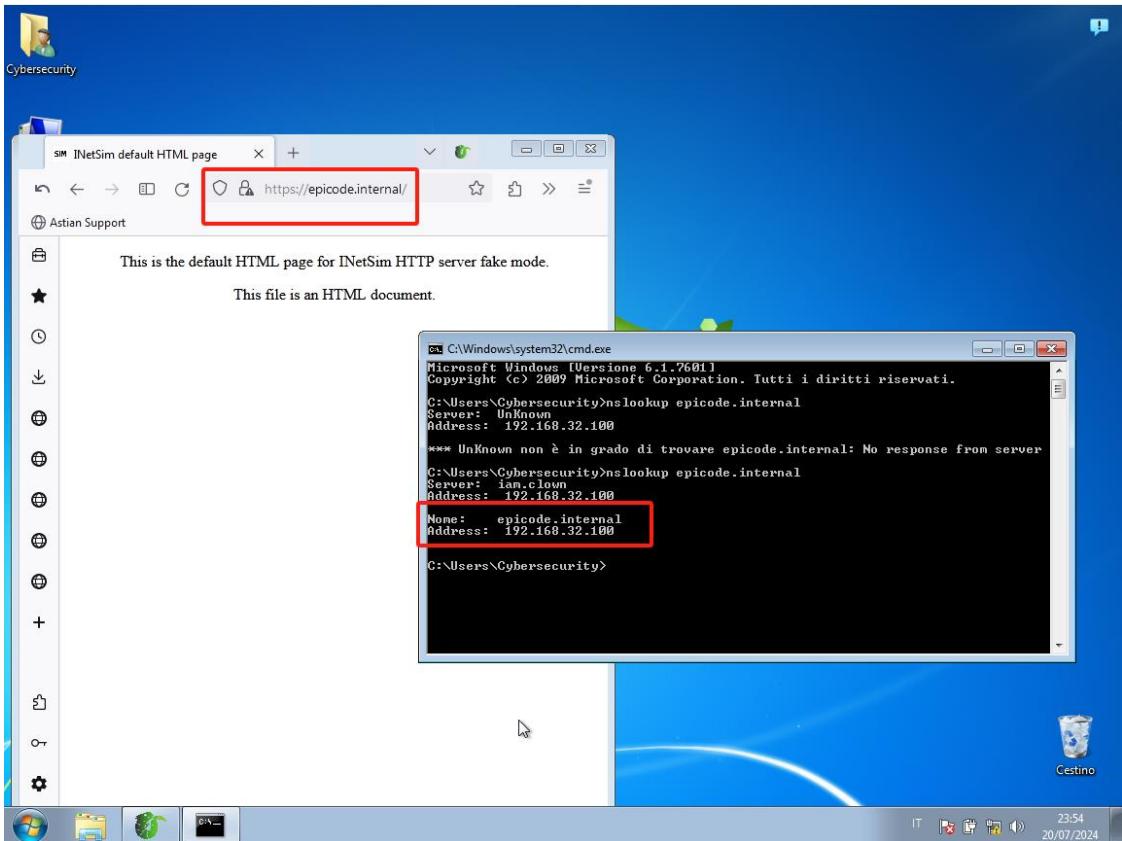
Testare con il comando “nslookup epicode.internal 192.168.32.100” sul terminale del Kali Linux 2022.1 la risoluzione del dominio.



```
kalilinux@kalilinux2022:~  
File Actions Edit View Help  
Inetsim.conf  
(kalilinux@kalilinux2022)-[~]  
$ nslookup epicode.internal 192.168.32.100  
Server: [omitted] 192.168.32.100  
Address: 192.168.32.100#53  
  
Name: epicode.internal  
Address: 192.168.32.100
```

Tutto corretto, quindi test eseguito con successo.

Si ripete sul browser di Windows 7 con il link <https://epicode.internal/> e lo stesso comando sul terminale.



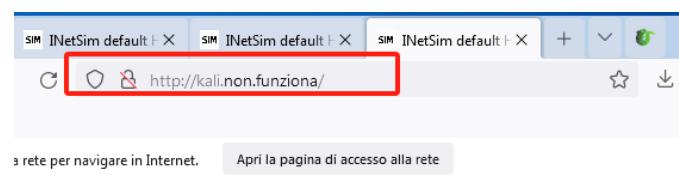
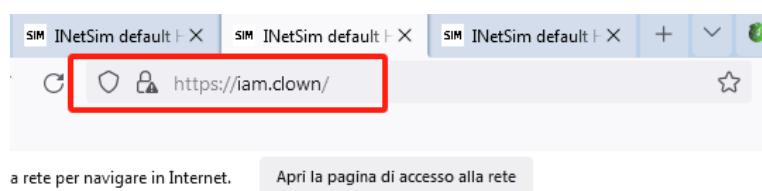
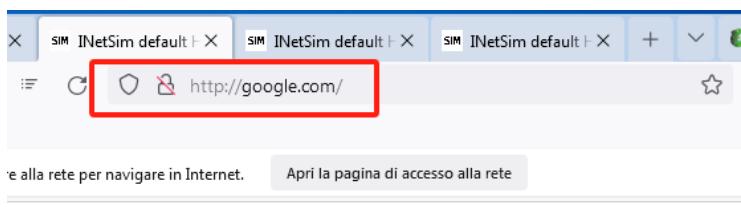
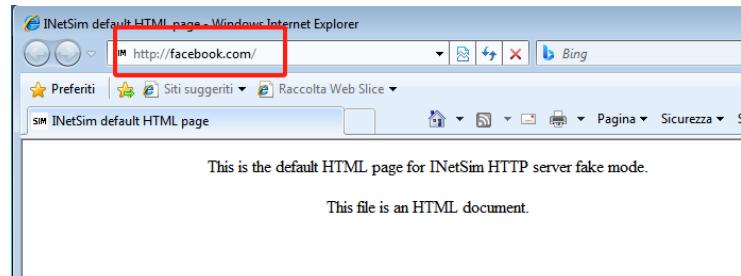
Test eseguito con successo.

Si può concludere che effettivamente il problema è legato alla compatibilità tra Kali Linux aggiornato e Inetsim, privo di aggiornamenti dal 2020.

## Ulteriori verifiche sulla risoluzione dei domini personalizzati

Si prosegue con ulteriori verifiche di domini personalizzati che risolvono sul server di inetsim per confermare che ora, con una versione meno recente di Kali Linux, il tutto funziona correttamente.

```
root@kali:~# nslookup -query=txt http://facebook.com/ 10.10.20.50
dns_static epicode.internal 192.168.32.100
dns_static facebook.com 192.168.32.100
dns_static google.com 192.168.32.100
dns_static iam.clown 192.168.32.100
dns_static kali.non.funziona 192.168.32.100
```

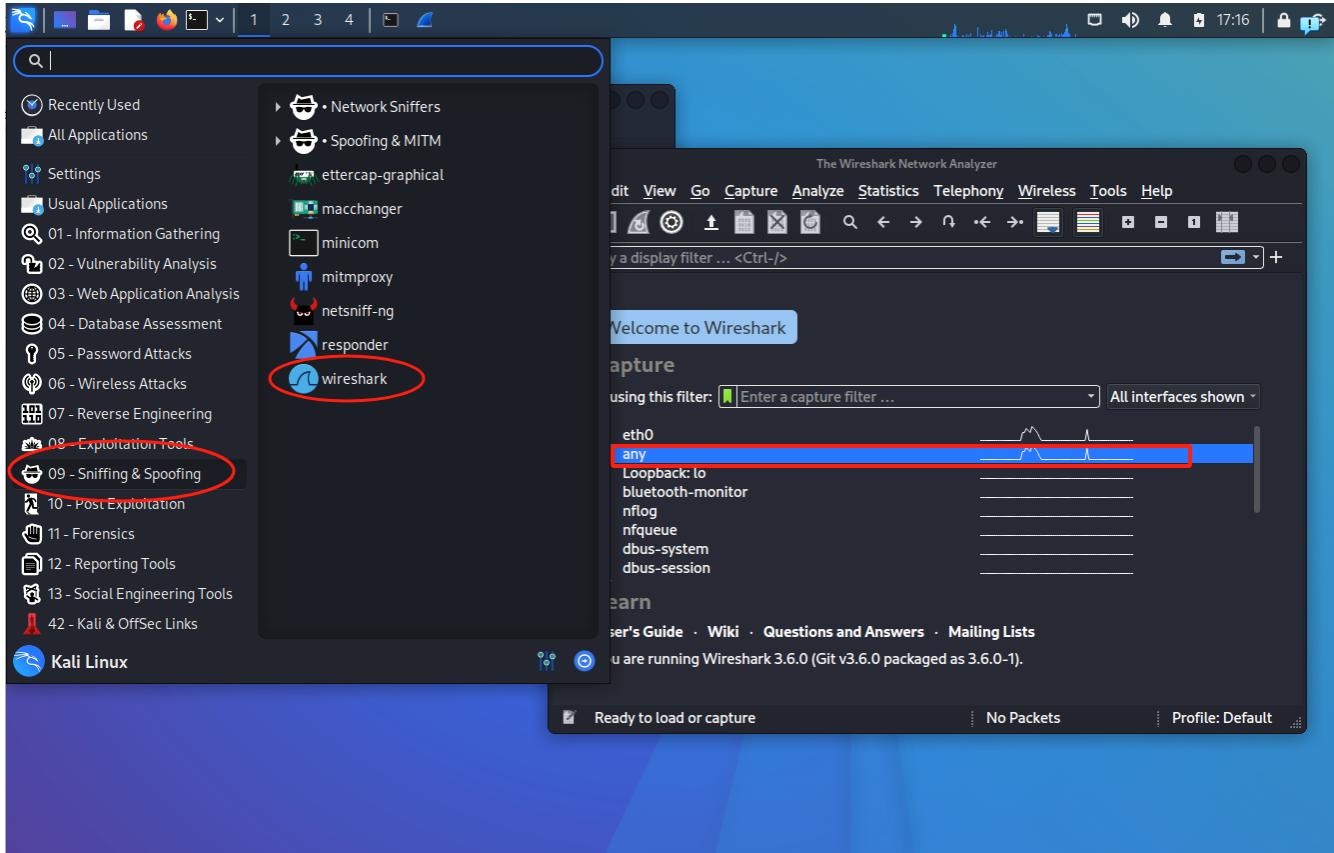


Tutti i test hanno avuto esito positivo.

# Wireshark

## Analisi con protocollo HTTPS

Tenendo attivo inetsim come configurato precedentemente, aprire Wireshark su Kali Linux e selezionare "Any".

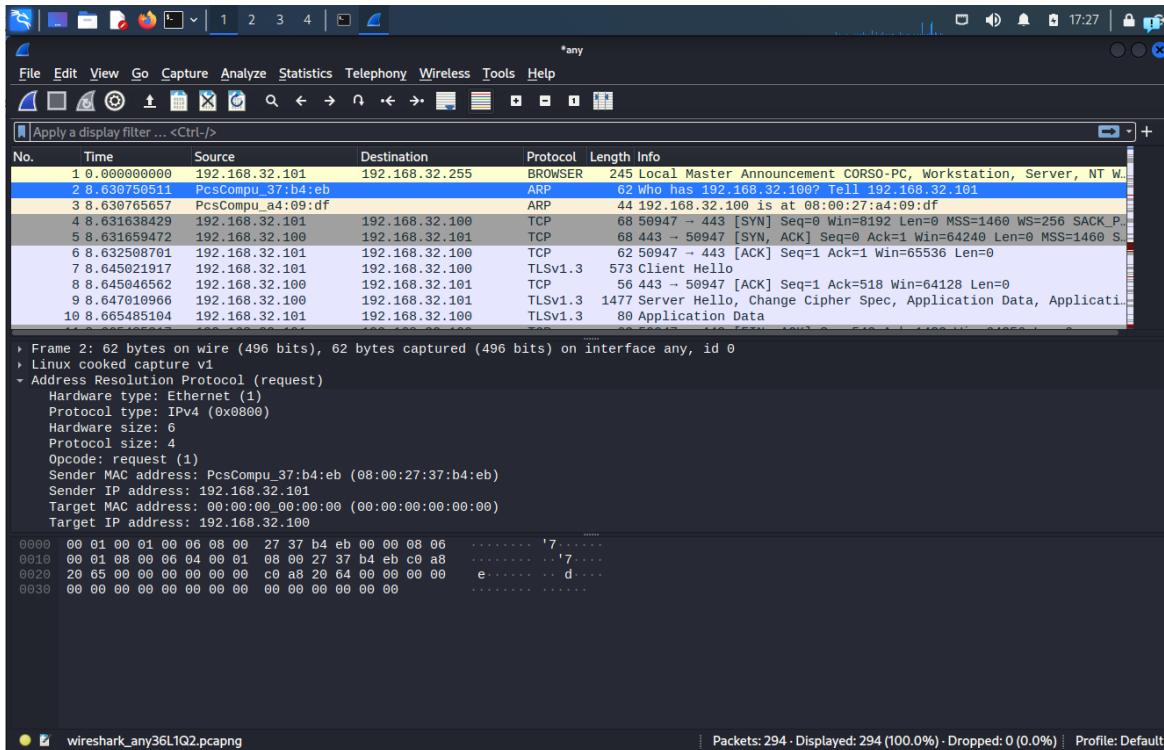


Premere la pinna blu e su Windows 7, dal browser, ricaricare la pagina web <https://epicode.internal/> e da Wireshark fermare con il quadrato rosso al termine della cattura.

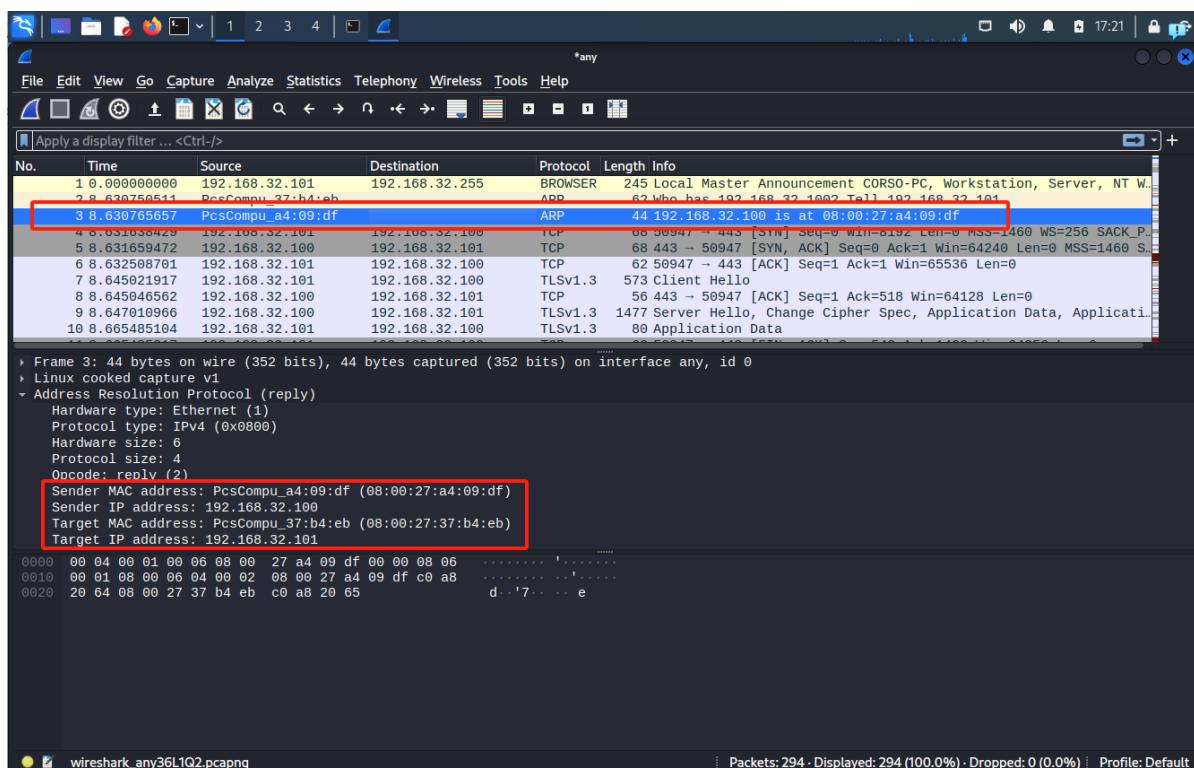
Wireshark, in questo modo, cattura tutti i pacchetti che parte dalla richiesta del browser di Windows 7 al server https e tradotto dal server DNS di Inetsim, presente all'interno di Kali, come da architettura presente in pagina 3.

## MAC Address

Il primo pacchetto è in protocollo ARP perché il mittente Windows 7 192.168.32.101 inizia con una richiesta broadcast alla rete, domandando a chi appartenga l'indirizzo IP 192.168.32.100 ( risultato della risoluzione del dominio dal server DNS).

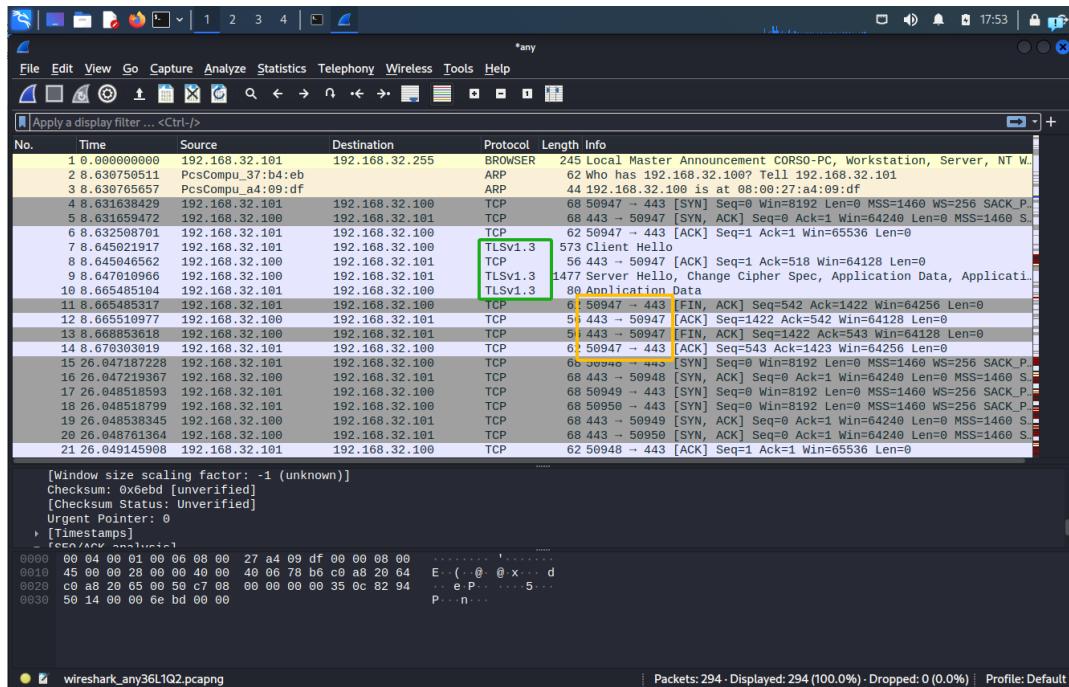


In risposta il server HTTPS 192.168.32.100 inoltra il proprio indirizzo MAC. A partire da questo punto avviene l'associazione IP | MAC ADDRESS che verrà salvata in un'apposita lista per agevolare la comunicazione senza dover ripetere la richiesta ARP. Appunto da questo pacchetto di ritorno si può, come evidenziato, trovare gli indirizzi MAC di Windows 7 e Kali Linux



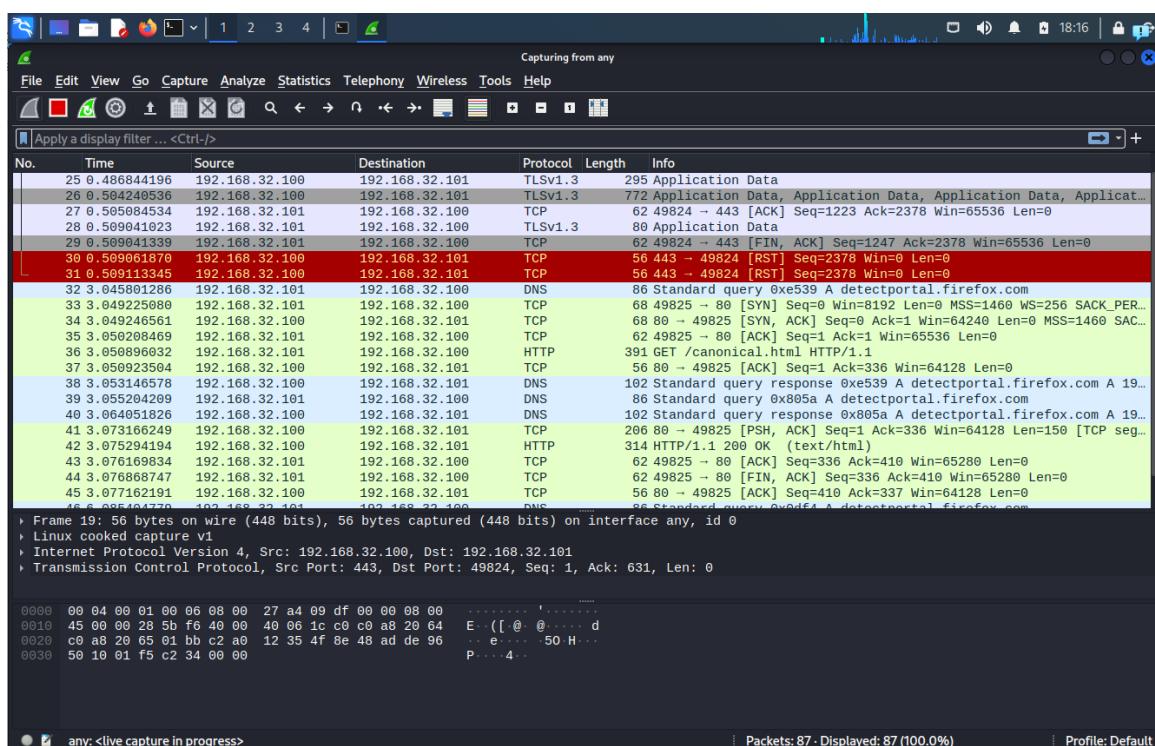
## Analisi contenuto richiesta HTTPS

Una volta trovati mittente e destinatario si nota che il collegamento attraverso il protocollo TCP è avvenuto con successo.



È presente il protocollo di crittografia TLS (rettangolo verde) e la porta 443 (rettangolo giallo) convenzionalmente impostata per HTTPS, appunto, conferma che il protocollo utilizzato è in HTTPS.

Per quanto riguarda il protocollo TCP ci sono prove dell'utilizzo del principio del "three-way handshake" perché sono presenti SIN, SIN-ACK e ACK. Questo processo garantisce che sia il client che il server siano sincronizzati e pronti a trasmettere dati in modo affidabile.



## Analisi con protocollo HTTP

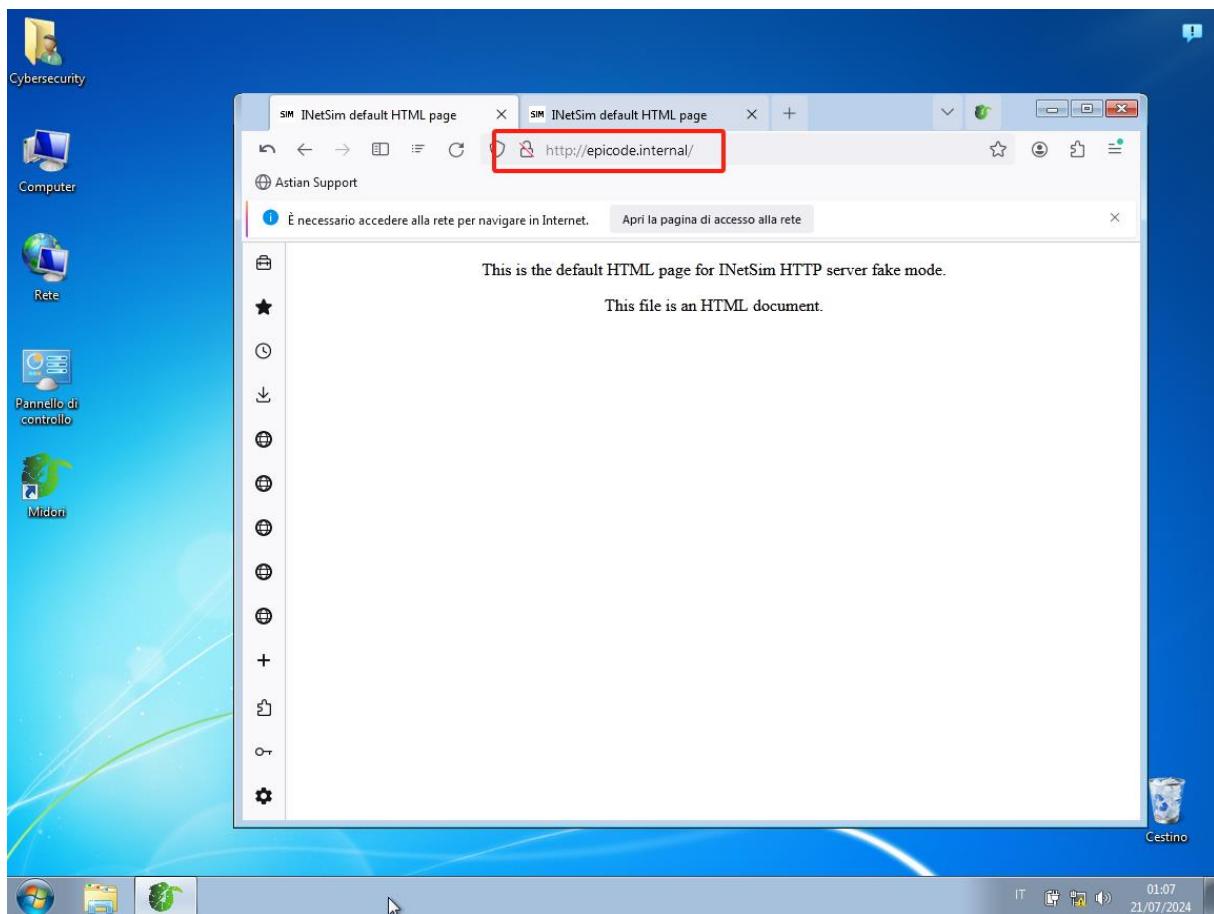
### Configurazione in HTTP

Per analizzare il tutto attraverso il protocollo HTTP. Riconfigurare Inetsim attivando il servizio http e, a discrezione, disattivare o meno, il servizio https.



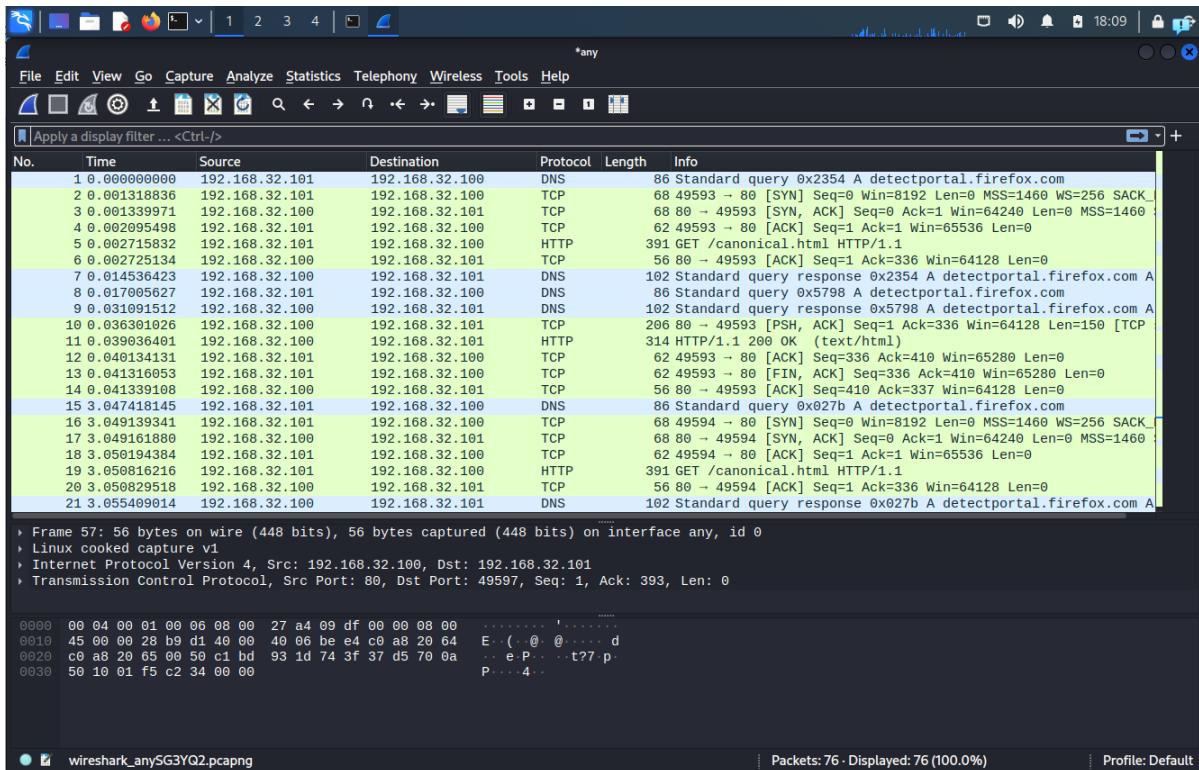
```
GNU nano 6.0          /etc/inetsim/inetsim.conf *
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
#start_service https
#start_service smtp
#start_service smtps
```

Ripetere quanto fatto precedente per l'analisi con Wireshark, aprendo tuttavia il link senza la "s" finale, quindi <http://epicode.internal/>



## Analisi contenuto richiesta HTTP

Come precedentemente effettuato ricaricare la pagina **epicode.internal** con Wireshark attivo.



Le principali differenze:

- l'assenza del protocollo di crittografia TLS perché il protocollo HTTP è privo di crittografia;
- la porta 80, convenzionalmente utilizzato per il protocollo HTTP e assenza della porta 443 riservata al protocollo HTTPS;
- non c'è nessuna richiesta ARP in quanto, non avendo spento le macchine, l'associazione indirizzi IP MAC è ancora salvata nella lista, sarebbe presente se si avesse riavviato anche una sola macchina.

25

Si conferma l'utilizzo del protocollo TCP e dell'utilizzo del principio del “three-way handshake” perché sono nuovamente presenti SIN, SIN-ACK e ACK.

## Conclusioni

La tecnologia evolve a una velocità impressionante, e parlare di anni in questo contesto può sembrare un'eternità. INetSim, non è stato aggiornato dal 2020, come indicato sul sito ufficiale [INetSim](#). Questa mancanza di aggiornamenti rischia di far diventare INetSim obsoleto e creare problemi di compatibilità, come in questo caso specifico, nonostante la sua grandissima utilità anche ai fini didattici.

Durante l'esercizio, la capacità di ricercare informazioni e risolvere problemi è stata fondamentale. È essenziale non solo sapere come eseguire le operazioni, ma anche comprendere il perché, adottando un approccio analitico per affrontare le difficoltà. Questo progetto ha messo in luce l'importanza di mantenersi costantemente aggiornati con le ultime tecnologie e pratiche per prevenire problemi di compatibilità e sfruttare al meglio le nuove funzionalità. Ad esempio, è stato aggiornato, come suggerito, la modalità di avvio del server di INetSim ed è stato necessario sostituire Internet Explorer, un browser legacy e non sicuro nel 2024, con una soluzione più moderna come Midori.

Le competenze acquisite dimostrano che l'aggiornamento continuo, il pensiero critico e la ricerca proattiva sono elementi chiave per mantenere la competenza in questo campo che è in continua evoluzione.