

TEST 28/10/2022

FACCILONGO DOMENICO

REQUISITI E SERVIZI

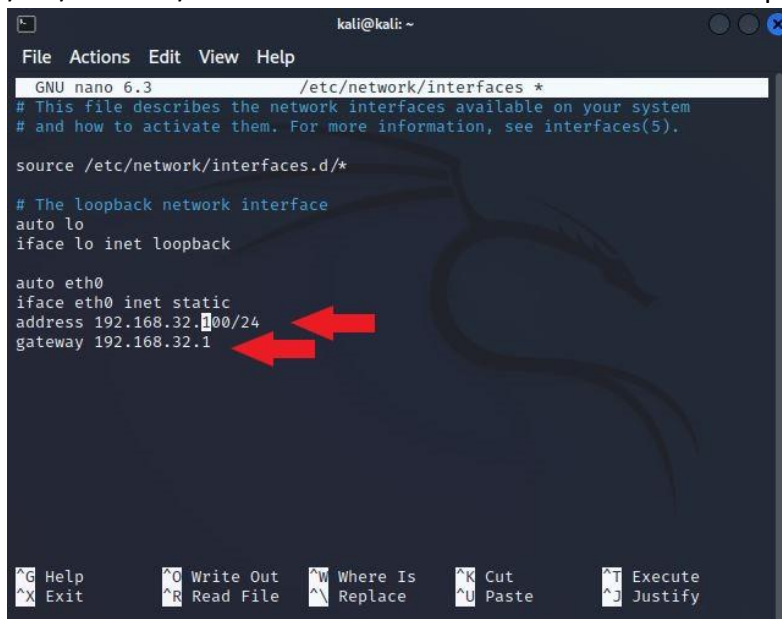
- Kali Linux IP 192.168.32.100
- Windows 7 IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

TRACCIA

1. Simulare in ambiente di laboratorio virtuale, un architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all'hostname <<epicode.internal>> che risponde all'indirizzo 192.168.32.100
2. Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS
3. Ripetere l'esercizio sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole le principali differenze.

ANALISI E VALUTAZIONI

1. Innanzitutto dobbiamo andare a modificare le configurazioni delle nostre macchine come richiesto dai requisiti.
 - Per Kali basterà andare nel prompt dei comandi e digitare <<sudo nano /etc/network/interfaces>> ed andiamo a modificare i campi come indicati in figura:



```
kali@kali: ~
File Actions Edit View Help
GNU nano 6.3 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

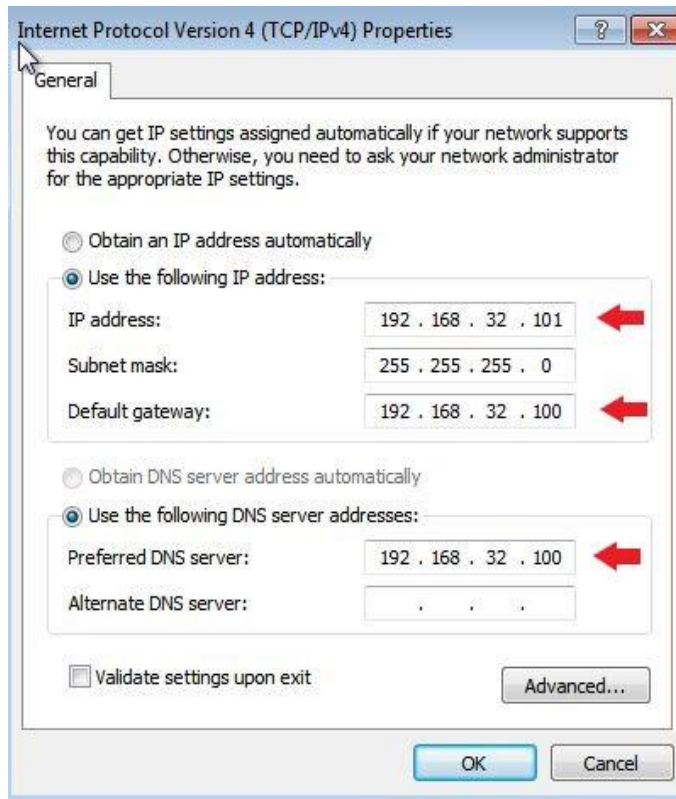
source /etc/network/interfaces.d/*

# 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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

- Per Windows i passaggi sono questi Control Panel → Network and Settings → Change Settings → Properties → IPv4 → Properties:



Non basterà altro che andare a Modificare i campi evidenziati dalle Freccette in rosso, inserendo come Default Gateway l'IP della macchina da cui dobbiamo permettere il collegamento per il Browser, stessa cosa faremo per il DNS. Mentre per l'IP address inseriremo l'IP come richiesto dai requisiti.

FACOLTATIVO: Per fare un test possiamo pingare le due macchine sempre con il comando, dal prompt dei comandi, "ping (IP della macchina opposta)" e il risultato sarà questo:

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.32.100
PING 192.168.32.100 (192.168.32.100) 56(84) bytes of data:
64 bytes from 192.168.32.100: icmp_seq=1 ttl=64 time=0.036 ms
64 bytes from 192.168.32.100: icmp_seq=2 ttl=64 time=0.068 ms
64 bytes from 192.168.32.100: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 192.168.32.100: icmp_seq=4 ttl=64 time=0.039 ms
64 bytes from 192.168.32.100: icmp_seq=5 ttl=64 time=0.047 ms
^Z
zsh: suspended ping 192.168.32.100
```

[Ping di Kali per Windows]

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Domenico>ping 192.168.32.101

Pinging 192.168.32.101 with 32 bytes of data:
Reply from 192.168.32.101: bytes=32 time<1ms TTL=128
Reply from 192.168.32.101: bytes=32 time<1ms TTL=128
Reply from 192.168.32.101: bytes=32 time<1ms TTL=128
Reply from 192.168.32.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.32.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Domenico>
```

[Ping di Windows per Kali]

2. Come passaggio successivo dobbiamo andare a configurare il DNS su Kali, per farlo abbiamo bisogno di entrare nella configurazione di InetSim, per farlo basterà andare sempre nel prompt dei comandi di Kali e digitare `<<sudo /etc/inetsim/inetsim.conf>>`

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 6.3 /etc/inetsim/inetsim.conf  
# 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  
start_service pop3  
start_service pop3s  
start_service ftp  
start_service ftps  
start_service tftp  
start_service irc  
start_service ntp  
start_service finger  
start_service ident  
start_service syslog  
start_service time_tcp  
start_service time_udp  
start_service daytime_tcp  
start_service daytime_udp
```

[pagina di avvio successivamente al comando]

```

kali@kali: ~
File Actions Edit View Help
GNU nano 6.3 /etc/inetsim/inetsim.conf
# Default: inetsim.org
#
# dns_default_domainname some.domain as Ickert & Thomas Mueggens
#
#####
# dns_static 
```

Bisognerà ora andare ad impostare il DNS statico andando ad inserire la nomenclatura come indicata in figura in modo tale da dare l'input alla macchina di Windows di cercare dal Browser il sito "epicode.intel" inserendo anche l'indirizzo IP della macchina che hosterà.

3. Subito dopo possiamo avviare inetsim dal prompt dei comandi di Kali inserendo la dicitura `<<sudo inetsim>>`:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ 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.  
Warning: Unknown option 'dns_satic' in configuration file '/etc/inetsim/inetsim.conf' line 246  
Configuration file parsed successfully.  
== InetSim main process started (PID 12119) ==  
Session ID: 12119  
Listening on: 192.168.32.100  
Real Date/Time: 2022-10-28 05:39:51  
Fake Date/Time: 2022-10-28 05:39:51 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 12137)  
* irc_6667_tcp - started (PID 12147)  
* ident_113_tcp - started (PID 12150)  
* time_37_udp - started (PID 12153)  
* ntp_123_udp - started (PID 12148)  
* daytime_13_tcp - started (PID 12154)  
* echo_7_tcp - started (PID 12157)  
* time_37_tcp - started (PID 12152)  
* echo_7_udp - started (PID 12158)
```

Si può notare come nella sezione Listening On ci apparirà proprio l'indirizzo IP della macchina in questione ovvero Kali che era quello che ci serviva al fine di ottenere la pagina web `epicode.internal`

4. Successivamente andiamo a fare un test da Windows per vedere effettivamente se la macchina pinga la pagina epicode.internal:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Domenico>ping epicode.internal

Pinging epicode.internal [192.168.32.100] with 32 bytes of data:
Reply from 192.168.32.100: bytes=32 time=2ms 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

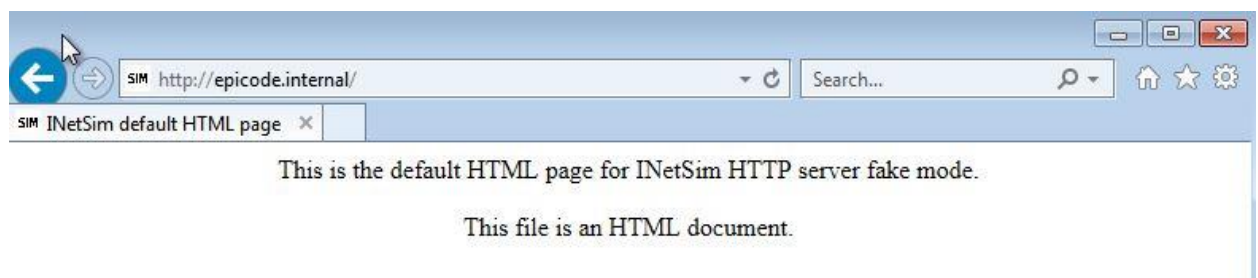
Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Domenico>
```

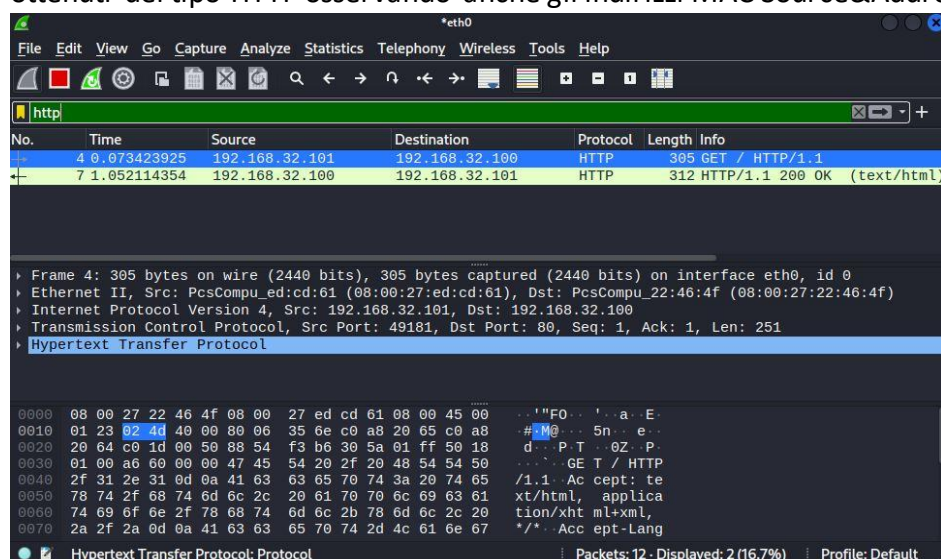
Come si può notare la macchina riesce a pingare epicode.internal di fatti abbiamo 4 pacchetti inviati e 4 ricevuti con 0 persi.

5. Pertanto possiamo ora andare a testare se effettivamente il Browser di internet ci fornisce la pagina web “epicode.internal”. Il test verrà effettuato sia per HTTPS con analisi dei pacchetti e sia per HTTP.

- HTTP



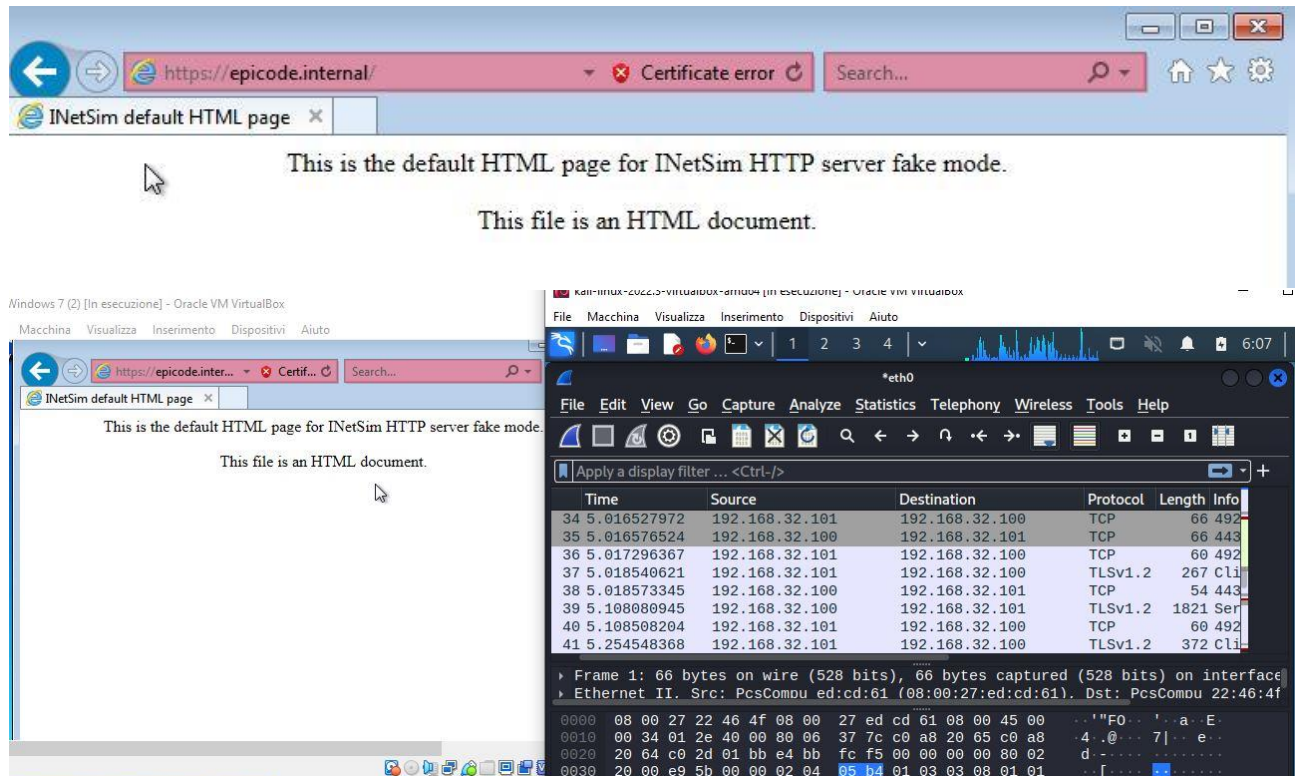
Andando ora in Wireshark da Kali, poi su eth0 possiamo andare ad analizzare i pacchetti ottenuti del tipo HTTP osservando anche gli indirizzi MAC Source&Address



Come possiamo notare i pacchetti trovati sono 2 con dicitura su “Info 200” (ovvero OK/andato a buon fine). Osservando gli indirizzi MAC possiamo notare come sono rispettivamente quello di

Windows su richiesta mentre destinazione quello di Kali, viceversa su risposta.

- HTTPS:



Anche in questo caso possiamo andare ad analizzare i pacchetti ottenuti dalla ricerca della pagina HTTPS di `epicode.internal`, i quali sono da analizzare principalmente i pacchetti del tipo TLS che sono proprio quelli relativi all'HTTPS. Anche in tal caso si è notato come l'indirizzo MAC sorgente è proprio quello relativo a Windows che fa appunto richiesta a Kali, con quest'ultimo che riceve la risposta e risponde a sua volta inviando un nuovo pacchetto con richiesta avvenuta per permettere così la trasmissione via Web.