

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 Linux). 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.

Impostare IP statico a Kali Linux (192.168.32.100)

Per configurare un indirizzo ip statico su Kali Linux bisogna innanzitutto accedere a terminale, successivamente bisogna digitare i seguenti comandi:

```
sudo nano /etc/network/interfaces
```

Una volta digitate i comandi vedremo la seguente schermata

```
File Actions Edit View Help
GNU nano 7.2
# 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
```

Una volta arrivati alla schermata di configurazione ci basterà digitare l'ip address come da consegna (192.168.32.100) e il conseguente Default Gateway (192.168.32.1).

Attivazione servizi DNS, http, HTTPS su Kali Linux

Per attivare i servizi richiesti dalla traccia quali: HTTP, HTTPS e DNS, utili a richiamare le pagine web da Windows 7, innanzitutto è necessario configurare il servizio "inetSim" da Kali Linux.

Da terminale bisogna digitare i seguenti comandi per accedere alla pagina di configurazione:

```
sudo nano /etc/inetsim/inetsim.conf
```

Per attivare i servizi richiesti bisogna cancellare l' "#"

dai servizi che vogliamo attivare. In questo caso ci basterà attivi i servizi in bianco nell'immagine in basso.

```
# 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, 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
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
```

Successivamente per associare un IP ad inetSim è necessario decommentare la voce “service_bind_address”. In questo caso siamo andati ad associare l’indirizzo 0.0.0.0 in modo da permettere all’applicazione di comunicare a tutti gli ip disponibili in base alle schede di rete configurate.

```
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
service_bind_address 0.0.0.0
```

```
#dns_default_hostname somehost  
  
#####  
# dns_default_domainname  
#  
# Default domain name to return with DNS replies  
#  
# Syntax: dns_default_domainname <domain name>  
#  
# Default: inetsim.org  
#  
dns_default_domainname domain.name  
  
#####  
# 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 epicode.internal 192.168.32.100
```

Per attivare il servizio DNS statico sarà necessario decommentare la voce “dns_static” (come da immagine in alto) andando ad inserire la richiesta della traccia in quanto la chiamata deve essere fatta su “epicode.internal” relativo all’indirizzo IP 192.168.32.100 che sarà concomitante all’indirizzo associato a Kali in quanto quest’ultimo dovrà fungere da server application.

```
(kali@kali)-[/etc/network]
$ 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:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 5920 (5.7 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
```

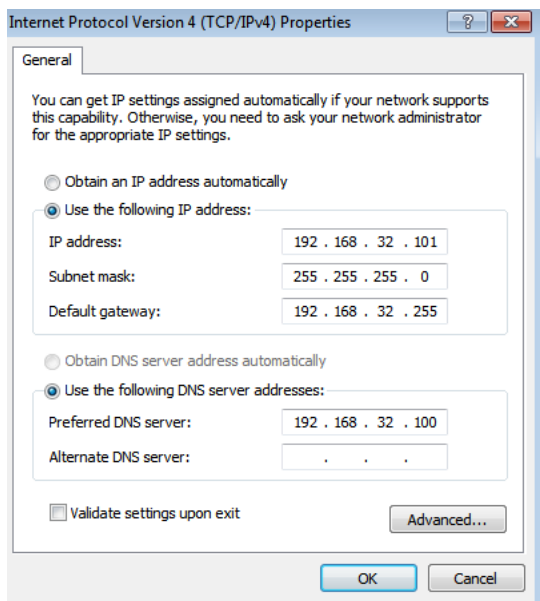
Una volta configurati i servizi, come da richiesta, è possibile verificare la corretta esecuzione dei comandi precedenti digitando da terminale il comando “ifconfig” come da figura in alto verificando la corretta associazione dell’IP statico.

Impostare Ip Statico Windows 7 (192.168.32.101)

Per impostare un IP statico su Windows 7 sarà necessario modificare i parametri di default seguendo il percorso in basso:

Pannello di controllo -> Network and Internet -> Change adapter settings
-> Tasto destro Local Area Connection -> Properties -> Internet protocol
Version 4 (TCP/IPv4) -> Properties:

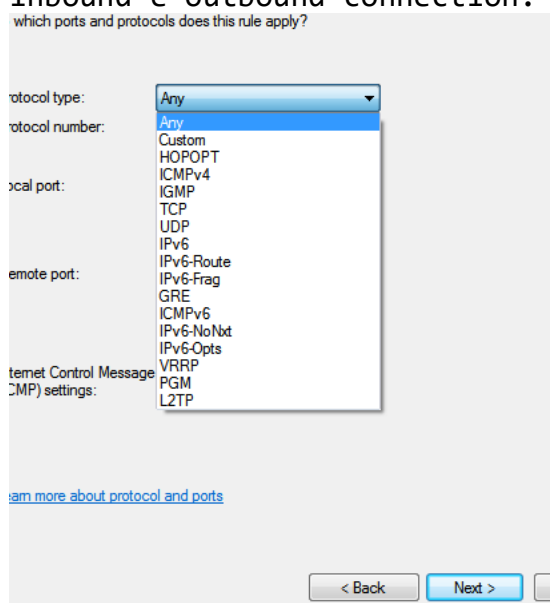
Una volta arrivati alla finestra di configurazione andremo ad inserire nella voce IP Address, l’IP statico che vogliamo associare alla macchina, il default Gateway di riferimento (il default Gateway è il canale di comunicazione che consente ad un dispositivo di collegarsi in rete tramite IP) e l’indirizzo IP statico associato al servizio DNS su Kali Linux per permettere al sistema Windows 7 di collegarsi a tale servizio. Ricordiamo che il DNS Domain è utile a mascherare un indirizzo IP in un indirizzo testuale.



Attivare regole Firewall Windows

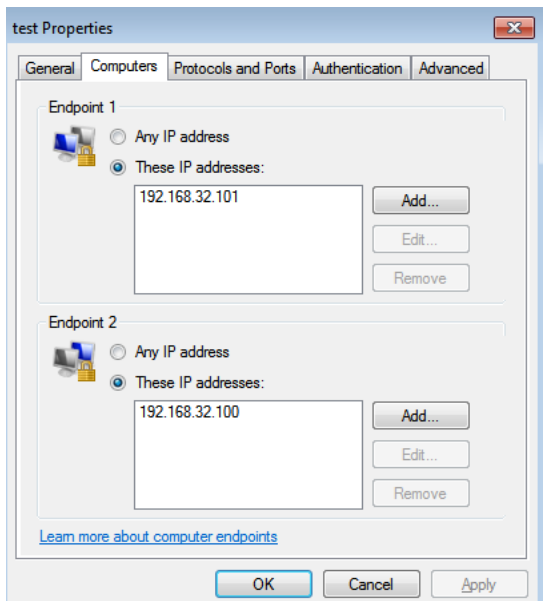
Per consentire la connessione tra le due macchine virtuali è necessario abilitare la regola di connessione entrata\uscita tramite firewall Windows seguendo il percorso descritto in basso:

Control Panel -> System and Security -> advanced settings -> impostare inbound e outbound connection.



In questo abbiamo lasciato any in quanto su Windows, nella voce "Protocol Type" non è presente il protocollo IPv4 (come da immagine in alto), ossia il protocollo che noi stiamo andando ad autorizzare.

Di seguito le impostazioni "inbound" e "outbound" connection.



Infine, digitando “ipconfig” da terminale è possibile verificare la corretta esecuzione dei comandi precedentemente spiegati e come da immagine in basso possiamo dire che la procedura è stata eseguita correttamente.

```

C:\Users\vbboxuser>ip config
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\vbboxuser>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e039:aede:df5c:6393%11
    IPv4 Address. . . . . : 192.168.32.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.32.255
                                192.168.32.1

Tunnel adapter isatap.{C99DAB66-CED0-4028-97B9-486103A1EF2A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\vbboxuser>

```

Lettura Mac Address Kali Linux e Windows

Per verificare i MAC Address, ossia gli indirizzi univoci associati ad ogni dispositivo fisico su windows sarà necessario rientrare nel comando “ipconfig” coma da immagine. In questo caso il nostro MAC Address sarà: **08-00-27-12-5C-B9**.

```
Command Prompt
C:\Users\ vboxuser>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Windows
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Physical Address. . . . . : 08-00-27-12-5C-B9
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e039:aede:df5c:6393%11(Preferred)
    IPv4 Address. . . . . : 192.168.32.101(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.32.255
                                192.168.32.1
    DHCPv6 IAID . . . . . : 235405351
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-CC-EC-59-08-00-27-12-5C-B9

    DNS Servers . . . . . : 192.168.32.100
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{C99DAB66-CED0-4028-97B9-486103A1EF2A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

C:\Users\ vboxuser>^!+_
```

Per quanto riguarda il MAC Address di Kali Linux digitando “ifconfig” da terminale sarà possibile visualizzare tra le varie informazioni il MAC Address associato: **08:00:27:cb:7e:f5**

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ /sbin/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:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 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)-[~]
└─$
(kali@kali)-[~]
└─$
```

Avvio inetSim services

Per avviare i servizi HTTP, HTTPS e DNS bisognerà entrare in terminale da Kali Linux e digitare

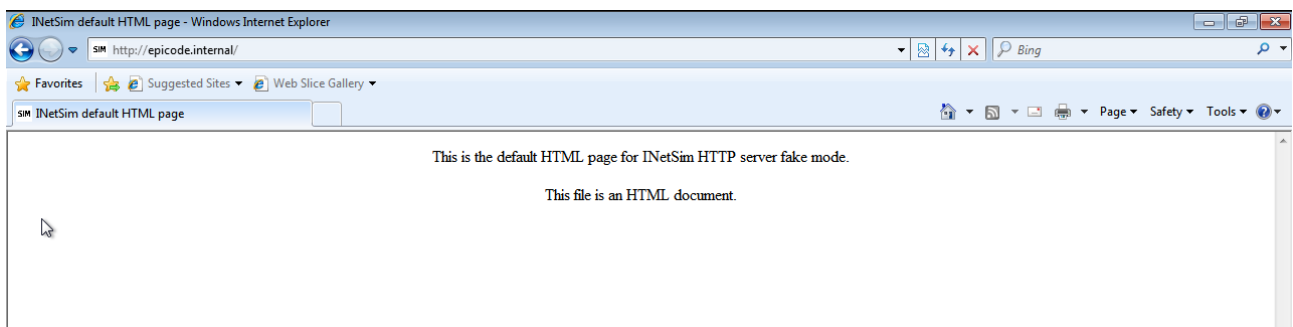
```
sudo inetsim
```

Una volta digitato il comando sarà possibile verificare l'avvio dei servizi "inetSim" come da immagine sottostante.

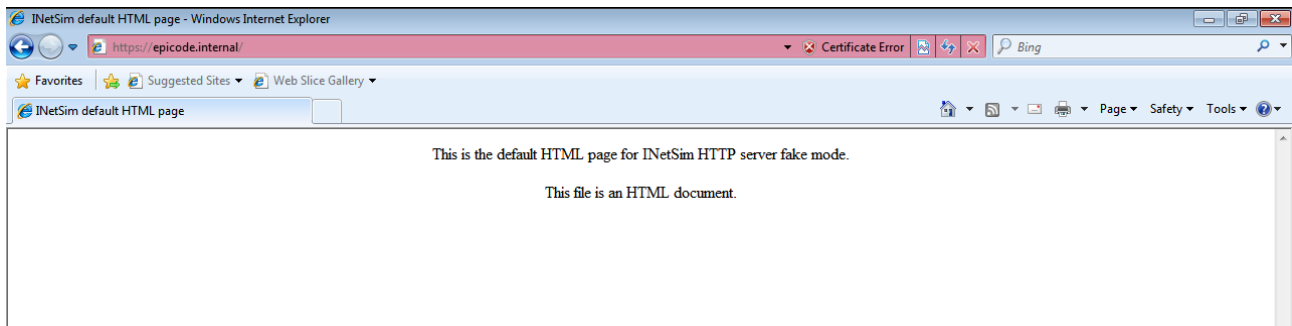
```
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:    /var/log/inetsim/
Using data directory:   /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 8206) ===
Session ID:      8206
Listening on:    0.0.0.0
Real Date/Time:  2023-11-18 07:36:00
Fake Date/Time:  2023-11-18 07:36:00 (Delta: 0 seconds)
Forking services...
 * dns_53_tcp_udp - started (PID 8216)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 39
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 39
 * http_80_tcp - started (PID 8217)
 * https_443_tcp - started (PID 8218)
done.
Simulation running.
```

Richiesta servizi da Windows

Una volta avviata la simulazione inetSim bisognerà andare sul SO Windows 7, aprire una pagina con un web browser, ad esempio, Internet Explorer e richiamare il dominio "http://epicode.internal" come da immagine rispondendo ai quesiti di attivazione servizi HTTP e DNS su Kali Linux.



Inoltre, digitando nella barra di inserimento “https://epicode.internal” risponderemo ai quesiti di attivazione dei servizi HTTPS e DNS su Kali nonché la corretta comunicazione delle due macchine.



Intercettazione comunicazione con WireShark (http)

Prima di effettuare la ricerca da barra degli indirizzi da Windows sarà necessario innanzitutto aprire WireShark su Kali Linux e avviare la registrazione del traffico, dopodiché potremo andare su Windows ed effettuare la chiamata, da browser, HTTP. Seguita questa procedura WireShark registrerà il traffico di rete come da Immagine in basso. Innanzitutto, possiamo dire che il dispositivo chiamante ha indirizzo IP 192.168.32.101 mentre il dispositivo che risponde ha come indirizzo IP 192.168.32.100. Come si può vedere alla riga numero 7 si legge una chiamata HTTP “GET” e la successiva risposta del server “200 OK”.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000443057	192.168.32.101	192.168.32.100	TCP	60	49170 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000472280	192.168.32.100	192.168.32.101	TCP	60	80 → 49170 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000891212	192.168.32.101	192.168.32.100	TCP	60	49170 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001483748	192.168.32.101	192.168.32.100	HTTP	340	GET / HTTP/1.1
7	0.001490509	192.168.32.100	192.168.32.101	TCP	54	80 → 49170 [ACK] Seq=1 Ack=287 Win=64128 Len=0
8	0.025076973	192.168.32.100	192.168.32.101	TCP	204	80 → 49170 [PSH, ACK] Seq=1 Ack=287 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.031700031	192.168.32.101	192.168.32.100	TCP	54	49170 → 80 [ACK] Seq=287 Ack=410 Win=65292 Len=0
10	0.032812551	192.168.32.101	192.168.32.100	TCP	60	49170 → 80 [ACK] Seq=287 Ack=410 Win=65292 Len=0
11	0.033070908	192.168.32.101	192.168.32.100	TCP	60	49170 → 80 [FIN, ACK] Seq=287 Ack=410 Win=65292 Len=0
12	0.033109573	192.168.32.100	192.168.32.101	TCP	54	80 → 49170 [ACK] Seq=410 Ack=288 Win=64128 Len=0

Analizzando la chiamata sulla voce Ethernet 2 potremo verificare la corretta associazione del MAC Address (sia in http che in https).

```

▶ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▼ Ethernet II, Src: PcsCompu_12:5c:b9 (08:00:27:12:5c:b9), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  ▶ Destination: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  ▶ Source: PcsCompu_12:5c:b9 (08:00:27:12:5c:b9)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▶ Transmission Control Protocol, Src Port: 49171, Dst Port: 443, Seq: 0, Len: 0

```

Intercettazione comunicazione con Wireshark (https)

Stessa procedura si può eseguire per il protocollo HTTPS. In questo caso però vedremo delle differenze

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.100	TCP	66	49168 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WScale=0 SACK_PERM
2	0.000000223	192.168.32.100	192.168.32.101	TCP	66	443 → 49168 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000040122	192.168.32.101	192.168.32.100	TCP	60	49168 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.001944910	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
5	0.001964340	192.168.32.100	192.168.32.101	TCP	54	443 → 49168 [ACK] Seq=1 Ack=162 Win=64128 Len=0
6	0.128826309	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7	0.134921146	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.134987850	192.168.32.100	192.168.32.101	TCP	54	443 → 49168 [ACK] Seq=1320 Ack=296 Win=64128 Len=0
9	0.135775202	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	0.343394809	192.168.32.101	192.168.32.100	TCP	60	49168 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
15	3.279835413	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xc0e4 A wpad
17	3.381412163	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xc0e4 A wpad
18	3.588764801	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD:00>
19	4.331886347	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD:00>
20	5.078592433	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD:00>
26	8.968295617	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x2009 A wpad
28	9.066483871	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x2009 A wpad
30	9.270140607	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD:00>
31	10.016510908	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD:00>
32	10.764028635	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD:00>
34	12.534539396	192.168.32.101	192.168.32.100	TLSv1	379	Application Data
35	12.552810585	192.168.32.100	192.168.32.101	TLSv1	235	Application Data
36	12.556844777	192.168.32.100	192.168.32.101	TLSv1	384	Application Data, Encrypted Alert
37	12.557651901	192.168.32.101	192.168.32.100	TCP	60	49168 → 443 [ACK] Seq=021 Ack=1891 Win=65700 Len=0
38	12.558183368	192.168.32.101	192.168.32.100	TCP	60	49168 → 443 [FIN, ACK] Seq=621 Ack=1891 Win=65700 Len=0
39	12.558128628	192.168.32.100	192.168.32.101	TCP	54	443 → 49168 [ACK] Seq=1891 Ack=622 Win=64128 Len=0

- è possibile vedere la differenza tra protocolli in quanto la chiamata HTTPS è criptata, in quanto successivamente al three-way-handshake (SYN, SYN-ACK, ACK -> riga 1 -3) vengono scambiati pacchetti TLSv1 (TLS ricordiamo che consiste in “Transport Layer Security” ossia il protocollo di trasporto che fornisce sicurezza e integrità dei dati nelle comunicazioni in rete), nella riga 4 troviamo la risposta del server al client “Hello”, riga 6 il server scambia la chiave con il client e alla riga 7 troviamo lo scambio client server. Questo scambio di chiavi ci fa capire immediatamente che la richiesta è di tipo https e non http;

- per quanto riguarda lo scambio http nell' immagine sopra (Sez. Intercettazione comunicazione con WireShark (http)) possiamo notare una richiesta GET con successiva risposta del server -> 200 OK. Inoltre, analizzando nel dettaglio la risposta del server è possibile visualizzare il contenuto delle pagine html in quanto la comunicazione, nelle richieste http, non è criptata.

Conclusioni

Possiamo dire che viste le immagini viene specificato:

- l'assegnazione degli indirizzi IP statici alle macchine;
- la comunicazione tra le due macchine;
- l'attivazione dei servizi richiesti (HTTP, HTTPS e DNS) su inetSim;
- la comunicazione di Windows con i servizi attivati in Kali Linux attraverso web browser;
- la registrazione delle chiamate HTTP e HTTPS tramite WireShark;
- la corrispondenza dei MAC Address;