INTRODUZIONE ALLA SICUREZZA NEI SISTEMI OPERATIVI

Simulazione client-server in laboratorio virtuale

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.

---

1. Impostare le schede di rete delle macchine virtuali su rete interna dalle impostazioni di rete di VirtualBox

In modo tale che le macchine riescano a comunicare tra loro

2. Impostare l'IP 192.168.32.100 su macchina Kali Linux

- accedere al terminale
- aprire il file con il comando '`sudo nano /etc/network/interfaces`'
- immettere l'IP 192.168.32.100 accanto alla voce "address"
- una volta modificato il file salvare ed uscire con i comandi 'enter'(salva) 'ctrl x'(esci)
- '`ifconfg`' per verificare che l'IP sia stato impostato correttamente

```
┌──(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:fec7:e136  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 279  bytes 32888 (32.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 115  bytes 28759 (28.0 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 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Impostare l'IP 192.168.32.101 su macchina Windows 7

- accedere al pannello di configurazione delle reti
- scegliere la voce 'change adapter setting' situato in alto a sinistra della schedina
- selezionare la scheda di rete
- tasto destro del mouse > proprietà > internet > protocol 4 (TCP/IPv4)
- modifcare i campi e assegnare un IP di 192.168.32.101 alla macchina
- riavviare la macchine
- da 'cmd' digitare 'ipconfig' per verificare che l'IP sia stato configurato correttamente

```
C:\Users\Jessi      ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6ce1:acff:2660:d74e%11
   IPv4 Address. . . . . . . . . . . : 192.168.32.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.32.2
```

4. Verificare che le due macchine riescano a comunicare tra loro regolarmente

Ping da Windows 7(192.168.32.101) a Kali Linux(192.168.32.100)

```
C:\Users\Jessica      ping 192.168.32.100

Pinging 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
```

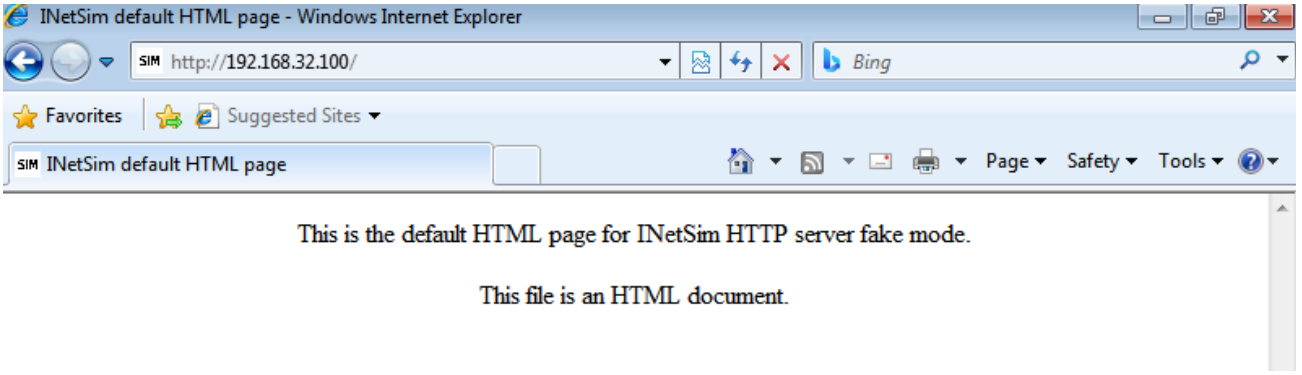
5. Configurazione hostname 'epicode.internal' nel file di configurazione dell'utility Inetsim

```
##########################################
# 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
```

6. Avvio l'utility di Inetsim con servizi di DNS e HTTPS

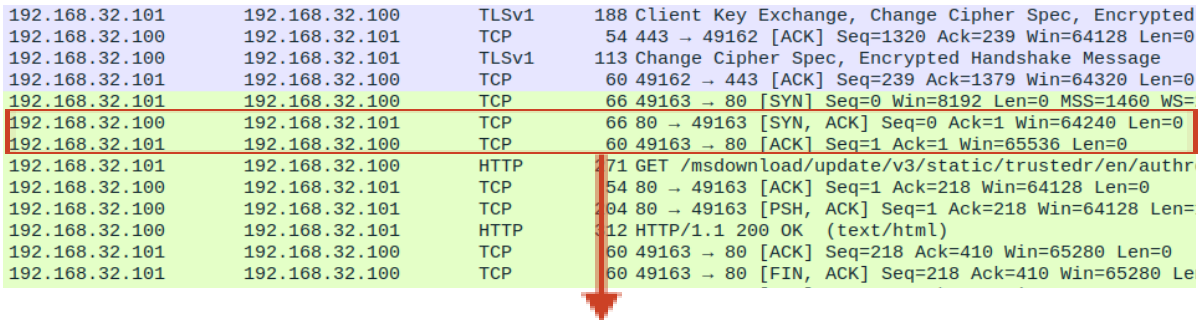
```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1963) ===
Session ID:     1963
Listening on:   192.168.32.100
Real Date/Time: 2023-06-18 10:38:27
Fake Date/Time: 2023-06-18 10:38:27 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 1965)
  * https_443_tcp - started (PID 1966)
 done.
Simulation running.
```

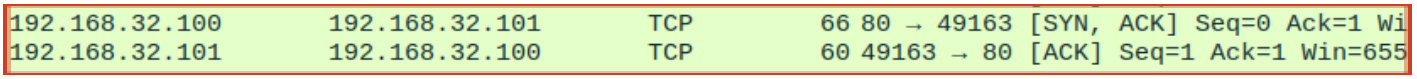
7. Da macchina Windows7 invio la richiesta epicode.internal



8. Intercettazione pacchetti con Wireshark (HTTP)

Capisco che sto catturando il pacchetto dal protocollo HTTP in quanto utulizza la porta 80





9. Intercettazione pacchetti con Wireshark (HTTPS)

Capisco che sto catturando il pacchetto dal protocollo HTTPS in quanto utilizza la porta 443