PROGETTO 1

Gelosa Matteo

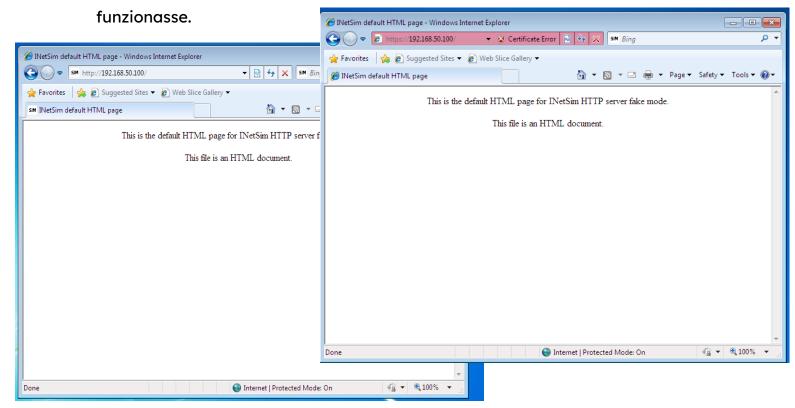
Per questo esercizio,ho inizialmente verificato che le due macchine Kali(192.168.50.100) e Win7(192.168.50.102) comunicassero tra loro tramite il comando ping essendo su rete interna. Il risultato è stato positivo, con questo breve test mi sono assicurato di poter procedere correttamente con l'esercizio.

Successivamente, grazie al tool Inetsim presente su Kali Linux (Esso è in grado di simulare molteplici server sulla nostra rete interna) ho configurato il tool in modo che simulasse server http,https e dns.

```
#
start_service dns
start_service http
start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service ftps
```

Ho rimosso il cancelletto che ha il compito di commentare il testo e non renderlo eseguibile. Rimuovendolo dal testo desiderato esso può essere eseguito.

Successivamente ho eseguito richieste http e https dalla macchina Win7 per verificare che il tutto



Per far sì che la macchina Win7 riuscisse a visualizzare il "server" http e https ho dovuto impostare un bind address di 0.0.0.0 . Quest'ultimo infatti permette a tutti gli ip della rete interna di visualizzare il server quando si effettua la richiesta.

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

Successivamente ho impostato il server DNS.

Sulla macchina Win7 ho impostato come indirizzo DNS l'indirizzo della macchina Kali (192.168.50.100) nonchè la macchina che ospita il server. Eseguendo questo passaggio sono sicuro che digitando il dominio epicode.internal nella barra di ricerca la macchina Win7 sarà in grado di raggiungerlo.

ternet Protocol Version 4 (TCP/IPv4)) Properties
General	
You can get IP settings assigned auto this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatica	illy
Use the following IP address: —	
IP address:	192 . 168 . 50 . 102
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 50 . 1
Obtain DNS server address auto	matically
Use the following DNS server add	dresses:
Preferred DNS server:	192 . 168 . 50 . 100
Alternate DNS server:	
Validate settings upon exit	Advanced
	OK Cancel

Spostandomi sulla macchina Kali ho effettuato queste modifiche:

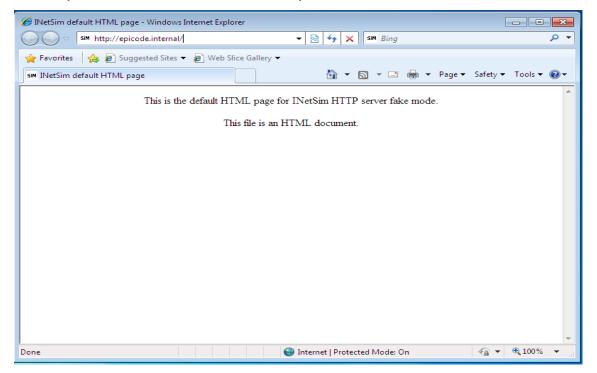
Ho impostato un ip di default al server DNS (192.168.50.100) nonchè l'indirzzo ip della macchina Kali.

Facendo questo chiunque faccia una chiamata col dominio associato all'indirizzo ip del server DNS avrà come risposta la pagina corretta.

```
# 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 192.168.50.100
```

Infine ho impostato il dominio di default per il server DNS (epicode.internal), questo mi ha permesso di poter digitare nella barra di ricerca della macchina win7 il dominio per ricevere come risposta la pagina desiderata.

Questa è l'immagine della barra di ricerca con il dominio epicode.internal, come si può notare riscontro risultato positivo.



Successivamente ho utilizzato il tool Wireshark per intercettare i pacchetti e per visualizzare i MAC address della macchina sorgente e macchena destinatario.

```
Frame 82: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_d4:8f:5e (08:00:27:d4:8f:5e)

Destination: PcsCompu_d4:8f:5e (08:00:27:d4:8f:5e)

Address: PcsCompu_d4:8f:5e (08:00:27:d4:8f:5e)
```

Che corrispondono con quelli della macchina Kali e Win7

```
inet6 fe80::a00:27ff:fecb:7ef5 prefixlen 64
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Eth
RX packets 2249 bytes 207799 (202.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
```

Infine ho provato ad intercettare sempre utilizzando il tool Wireshark lo scambio di pacchetti tra le varie richieste http e https.

Ho notato come nelle richieste http il traffico in transito sia visibile mentre con la richiesta https il traffico viene criptato e dunque non comprensibile.

Richiesta http:

```
' - - ^ - · E ·
000
     08 00 27 cb 7e f5 08 00
                                 27 d4 8f 5e 08 00 45 00
    01 c3 06 8d 40 00 80 06
                                                             . . . . @ . . .
                                                                      · · · · 2f · ·
010
                                0c 8d c0 a8 32 66 c0 a8
                                                             2d · · · P] · ( · { · JHP · @) · · · · GE T / HTTP
020 32 64 c0 a4 00 50 5d af
                                 28 82 7b 17 4a 48 50 18
     40 29 0f ca 00 00 47 45
                                54 20 2f 20 48 54 54 50
030
040
     2f 31 2e 31 0d 0a 41
                            63
                                 63 65 70 74
                                             3a 20 69 6d
                                                             /1.1 · Ac cept: im
                                 2c 20 61 70 70 6c 69 63 age/jpeg , applic
050 61 67 65 2f 6a 70 65 67
060 61 74 69 6f 6e 2f 78 2d
                                6d 73 2d 61 70 70 6c 69 ation/x-ms-appli
070
     63 61 74 69 6f 6e 2c 20
                                 69 6d 61 67 65 2f 67 69
                                                             cation,
                                                                       image/gi
                                                 6e 2f 78
080
     66 2c 20 61 70 70 6c 69
                                 63 61 74 69 6f
                                                             f, appli cation/x
                                 20 69 6d 61 67 65 2f 70
                                                           aml+xml,
090 61 6d 6c 2b 78 6d 6c 2c
                                                                       image/p
0a0 6a 70 65 67 2c 20 61 70
                                 70 6c 69 63 61 74 69 6f
                                                             jpeg, ap plicatio
0b0
    6e 2f 78 2d 6d 73 2d 78
                                 62 61 70 2c 20 2a 2f 2a
                                                             n/x-ms-x bap, */
                                                             · · Accept - Languag
0c0
    0d 0a 41 63 63 65 70
                            74
                                 2d 4c 61
                                          6e 67
                                                 75 61 67
0d0 65 3a 20 69 74 2d 49
                            54
                                 0d 0a 55
                                              65
                                                    2d
                                                       41
                                                             e: it-IT
                                                                      ··User-
                                           73
                                                 72
                                                             gent: Mo zilla/4
0e0
     67
        65 6e
                  3a 20
                         4d
                            6f
                                 7a 69 6c 6c 61
                                                    34 2e
                                                 3b 20 4d
0f0
     30 20 28
               63 6f 6d
                                   69 62
                                                             0 (compa tible; N
                                                             SIE 8.0;
100
        49 45
                         30
                                 20 57
                                              64
                                                 6f
                                                                        Windows
110
     20 4e 54 20 36 2e 31
                                 20 54 72 69 64
                                                 65 6e
                                                                        Trident
                                                             /4.0; SL CC2; .NE
T CLR 2. 0.50727;
.NET CL R 3.5.30
                                                 2e 4e 45
120
     2f 34 2e 30 3b 20 53
     54 20 43 4c 52 20 32 2e
20 2e 4e 45 54 20 43 4c
                                 30 2e 35 30 37
52 20 33 2e 35
130
                                                       30
140
     37 32 39 3b 20 2e 4e
                                                             729; .NE T CLR 3
150
                            45
                                 54 20 43 4c
                                                 20 33 2e
                                                       43
                                                             0.30729;
                                                                        Media (
160
     30 2e 33 30 37 32
                            3b
                                 20 4d 65 64 69
170
     65 6e 74 65
                                 20 36 2e
                                             29 0d 0a
                                                        41
                                                             enter PC
                                                                       6.0)··A
                                 63 6f 64 69 6e 67 3a 20
     63 63 65 70 74 2d 45 6e
                                                             ccept-En coding:
180
                                                             gzip, de flate H
190
     67 7a 69 70 2c 20 64 65
                                 66 6c 61 74 65 0d 0a 48
     6f 73 74 3a 20 65 70 69
                                 63 6f 64 65 2e 69 6e 74
1a0
                                                             ost: epi code.int
1b0
     65 72 6e 61 6c 0d 0a 43
                                 6f 6e 6e 65 63 74 69 6f
                                                             ernal .. C onnectio
1c0
     6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d
                                                             n: Keep- Alive · · ·
1d0
```

Possiamo notare come alla nostra destra il traffico sia comprensibile.

Richiesta https:

```
| No. | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128 | 128
```

In questo caso possiamo notare come il traffico alla destra sia completamente incomprensibile e quindi cifrato.