

w4d4 benchmark

Traccia: Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client (con indirizzo 192.168.32.101 Windows) 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

step 1 configurazioni :

- **procediamo alla configurazione di un web server su Kali linux**
utilizzeremo come programma per il web server inetsim.
procediamo dunque con le seguenti impostazioni sul file di configurazione che si chiama /etc/inetsim/inetsim.conf.

per prima cosa andremo a disattivare tutti i servizi ad eccezione di

```
# quoted_udp, chargen_tcp, chargen_udp,  
# ident, syslog, dummy_tcp, dummy_udp,  
# ftps, irc, https  
#  
#start_service dns  
#start_service http  
start_service https  
#start_service smtp  
#start_service smtps  
#start_service pop3  
https #start service pop3s
```

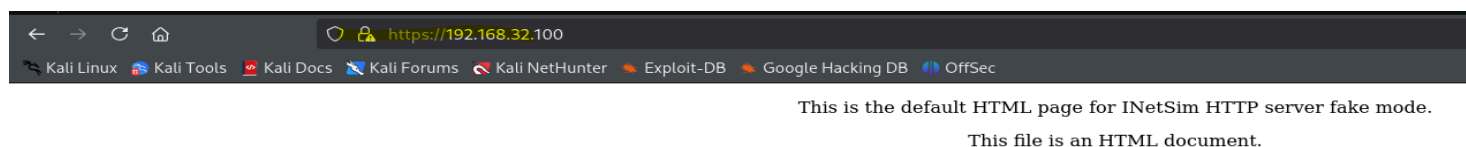
e successivamente andiamo ad impostare il binding degli indirizzi Ip

```
#####
# service_bind_address
# ~ kali@kali: ~
# IP address to bind services to
# NetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas
# Syntax: service_bind_address <IP/ address>
# sing data directory: /var/lib/inetsim/
# Default: 127.0.0.1ry: /var/log/inetsim/report/
# sing configuration file: /etc/inetsim/inetsim.conf
service_bind_address 192.168.32.100
Configuration file parsed successfully.
=== INetSim main process started (PID 1765) ===
#####
# service_run_as_user 68.32.100
```

questa stringa così impostata associerà il servizio https al nostro indirizzo Ip 192.168.32.100/24.

infine andremo ad eseguire il programma interim con i privilegi di amministratore, digitando il comando **sudo inetsim**.

il Web server ora è raggiungibile sia sull'indirizzo di loopback 127.0.0.1 sia sull'interfaccia di rete eth0



step 2 DNS server:

Il Domain name system è servizio che serve a risolvere nomi di dominio in indirizzi ip pubblici o privati.

avendo riscontrato errori nel funzionamento del Dns server di inetsim propongo due soluzioni alternative

1) configurare manualmente l'associazione dell'ip del web server al nome di dominio nel file di host sulla VM windows 7 .

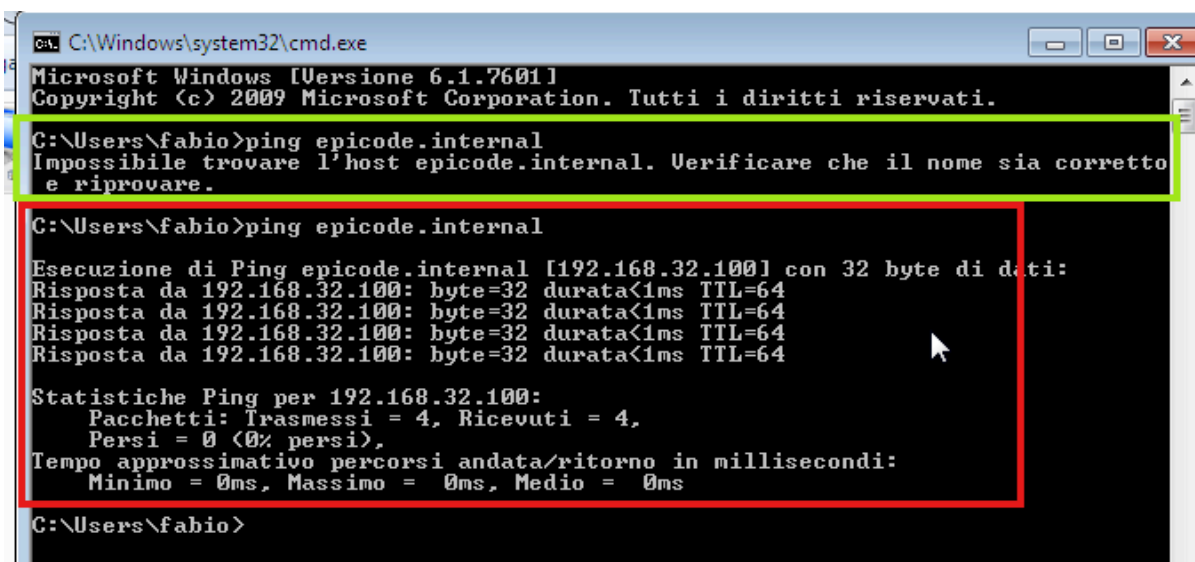
Sostanzialmente in assenza un Dns server associato la macchina Host andrà a controllare nel proprio Filesystem un eventuale corrispondenza col nome di dominio Epicode.internal.

Questa configurazione piuttosto semplice consiste nell'andare a modificare il file host nel path C:\\windows\\System32\\drivers\\etc\\ e andando ad inserire l'ip associato al nome di dominio come in screenshot.

for example:

```
102.54.94.97      rhino.acme.com          # source server
38.25.63.10       x.acme.com             # x client host
192.168.32.100    epicode.internal
localhost name resolution is handled within DNS itself.
127.0.0.1         localhost
::1               localhost
```

N.B per modificare il file è necessario avere i privilegi di admin



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\fabio>ping epicode.internal
Impossibile trovare l'host epicode.internal. Verificare che il nome sia corretto
e riprovare.

C:\Users\fabio>ping epicode.internal

Esecuzione di Ping epicode.internal [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 = 0ms, Medio = 0ms

C:\Users\fabio>
```

in verde il ping non andato a buon fine prima della modifica del file di host, mentre in rosso il ping eseguito con successo dopo.

2) Configurare un dns server alternativo

questa sarebbe la soluzione migliore in quanto consente in futuro di associare più domini a diversi host senza dover aggiungere manualmente tutti i domini ad ogni altra nuova macchina virtuale.

Nel mio caso ho deciso di usare dnsmasq. Il programma purtroppo non è presente di default nella macchina Kali, dunque va installato da internet. Semplicemente si imposta la scheda di rete in **bridge** su Virtualbox e successivamente configuriamo **eth0** in **dhcp**, digitiamo infine **sudo apt install dnsmasq -y**.

Installato il programma lo configuriamo inserendo il dominio di epicode e l'ip della macchina Kali, le configurazioni vengono impostate nel file **/etc/dnsmasq.conf**

```
# Add domains which you want to force to an IP address here.  
# The example below send any host in double-click.net to a local  
# web-server. rd for kali:  
address=/epicode.internal/192.168.32.100
```

a questo punto possiamo eseguire il server con il comando **sudo dnsmasq** ed andiamo impostare il server dns sulla macchina host

Proprietà - Protocollo Internet versione 4 (TCP/IPv4)



Generale

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP: 192 . 168 . 32 . 102

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 50 . 1

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito: 192 . 168 . 32 . 100

Server DNS alternativo: . . .

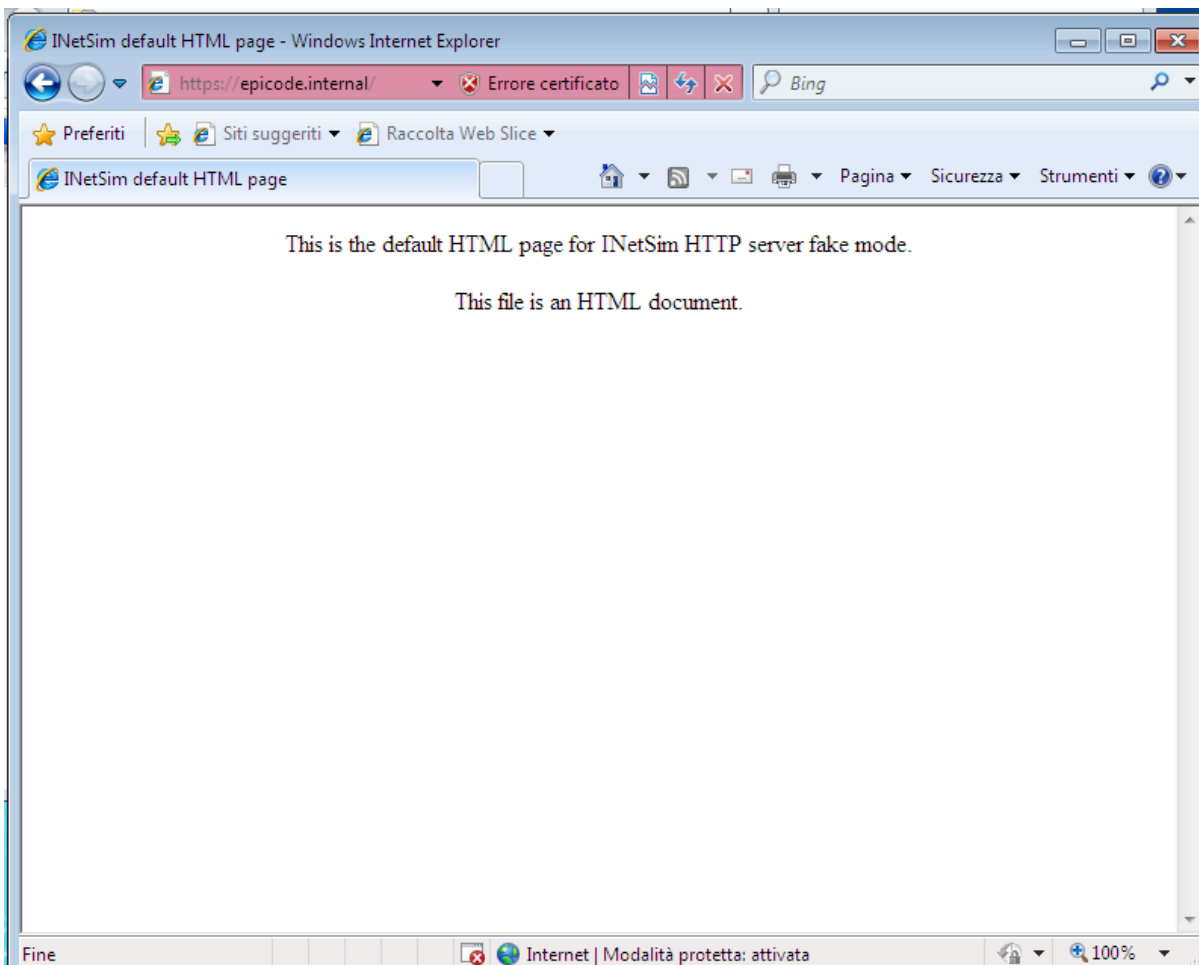
☐ Convalida impostazioni all'uscita

Avanzate...

OK

Annulla

ora è tutto settato e la macchina Win7 risolve correttamente il nome di dominio epicode.internal



3) intercettazione del traffico con wireshark

procediamo ora con l'analisi del traffico selezionando l'interfaccia eth0

nella prima fase la richiesta Dns

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.102
2	0.000018013	PCSSystemtec_6e:13:...	PCSSystemtec_5b:75:...	ARP	42	192.168.32.100 is at 08:00:27:6e:13:6e
3	0.000228132	192.168.32.102	192.168.32.100	DNS	76	Standard query 0xe3ab A epicode.internal
4	0.000314657	192.168.32.100	192.168.32.102	DNS	92	Standard query response 0xe3ab A epicode.internal A 192.168.32.100
5	0.000848644	192.168.32.102	192.168.32.100	TCP	66	49157 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
6	0.000864061	192.168.32.100	192.168.32.102	TCP	66	443 → 49157 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128

Frame 3: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)

Destination: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)

Source: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7)

Type: IPv4 (0x0000)

[Stream index: 1]

Internet Protocol Version 4, Src: 192.168.32.102, Dst: 192.168.32.100

User Datagram Protocol, Src Port: 57607, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xe3ab

Flags: 0x0100 Standard query

0... .. = Response: Message is a query

.000 0... .. = Opcode: Standard query (0)

... ..0 = Truncated: Message is not truncated

... ..1 = Recursion desired: Do query recursively

... ..0 = Z: reserved (0)

... ..0 = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

epicode.internal: type A, class IN

[Response In: 4]

in rosso evidenziato il 2Nd livello della pila iso/osi ovvero il destinatione e il source mac address

in arancione evidenziato il livello network ovvero Ip di destinazione e di sorgente

in magenta il livello di trasporto e qui ci viene evidenziato che la richiesta dns viene fatta sulla porta 53 e che viene usato il protocollo di trasporto UDP

in fine a livello applicativo abbiamo la query DNS per il dominio Epicode.internal

11	27.927114413	192.168.32.102	192.168.32.100	TCP	66	49161 → 443	[SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
12	27.927146429	192.168.32.100	192.168.32.102	TCP	66	443 → 49161	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
13	27.927398167	192.168.32.102	192.168.32.100	TCP	66	49161 → 443	[ACK] Seq=1 Ack=1 Win=65700 Len=0
14	27.927545296	192.168.32.102	192.168.32.100	TLSv1	215	Client Hello	[SNI=epicode.internal]
15	27.927554538	192.168.32.100	192.168.32.102	TCP	54	443 → 49161	[ACK] Seq=1 Ack=162 Win=64128 Len=0
16	27.951921250	192.168.32.100	192.168.32.102	TLSv1	1373	Server Hello	Certificate, Server Key Exchange, Server Hello Done
17	27.962597980	192.168.32.102	192.168.32.100	TLSv1	188	Client Key Exchange	Change Cipher Spec, Encrypted Handshake Message
18	27.963475162	192.168.32.100	192.168.32.102	TLSv1	113	Change Cipher Spec	Encrypted Handshake Message
19	27.967826429	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.1?	Tell 192.168.32.102
20	28.166483618	192.168.32.102	192.168.32.100	TCP	60	49161 → 443	[ACK] Seq=296 Ack=1379 Win=64320 Len=0
21	28.868025193	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.1?	Tell 192.168.32.102
22	29.869329558	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.1?	Tell 192.168.32.102
23	31.095302430	192.168.32.102	224.0.0.252	LLMNR	64	Standard query 0x70c7	A wpad
24	31.192709996	192.168.32.102	224.0.0.252	LLMNR	64	Standard query 0x70c7	A wpad
25	31.393007119	192.168.32.102	192.168.32.255	NBNS	92	Name query NB WPAD<00>	
26	32.144595791	192.168.32.102	192.168.32.255	NBNS	92	Name query NB WPAD<00>	
27	32.896257699	192.168.32.102	192.168.32.255	NBNS	92	Name query NB WPAD<00>	
28	33.102749964	PCSSystemtec_6e:13:...	PCSSystemtec_5b:75:...	ARP	42	Who has 192.168.32.102?	Tell 192.168.32.100
29	33.103116514	PCSSystemtec_5b:75:...	PCSSystemtec_6e:13:...	ARP	60	192.168.32.102 is at 08:00:27:5b:75:b7	
30	33.651235364	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.1?	Tell 192.168.32.102
31	34.378703992	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.1?	Tell 192.168.32.102
32	35.370202214	PCSSystemtec_5b:75:...	Broadcast	ARP	60	Who has 192.168.32.1?	Tell 192.168.32.102

Source: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.32.102, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49161, Dst Port: 443, Seq: 0, Len: 0
Source Port: 49161
Destination Port: 443
[Stream index: 0]
[Stream Packet Number: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)

0000 08 00 27 6e 13 6e 08 00 27 5b 75 b7 08 00 45 00 ... 'n' n ... 'u' ... E
0010 00 34 01 67 40 00 00 06 37 42 c0 a8 20 66 c0 a8 4 g @ ... 7 B ... f ...
0020 20 64 00 09 01 bb 91 af 51 3d 00 00 00 00 80 02 d Q =
0030 20 00 e8 49 00 00 02 04 05 b4 01 03 03 02 01 01 - i
0040 94 02 ..

Transmission Control Protocol (tcp), 32 bytes

Packets: 53

successivamente troviamo il three-way handshake tra i due host, si possono evidenziare i mac address

31	34.378703992	PCSSystemtec_5b:75:...	Broadcast
32	35.370202214	PCSSystemtec_5b:75:...	Broadcast

Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7), Dst: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
Destination: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
Source: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7)
Type: IPv4 (0x0800)
[Stream index: 0]

gli Ip

TIME TO LIVE: 128
Protocol: TCP (6)
Header Checksum: 0x3742 [validation disabled] [Header checksum status: Unverified]
Source Address: 192.168.32.102
Destination Address: 192.168.32.100
[Stream index: 0]
Transmission Control Protocol, Src Port: 49161,

ed infine il protocollo di trasporto con le relative porte


```
Internet Protocol Version 4, Src: 192.168.32.102, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49161, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 49161
  Destination Port: 443
  [Stream index: 0]
  [Stream Packet Number: 1]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2444185917
```

da notare l'uso della porta di destinazione 443 ovvero la specifica del protocollo https

differenze tra HTTP e HTTPS

```
1 0.000000000 192.168.32.102 192.168.32.100 TCP 66 49165 -> 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
2 0.000049958 192.168.32.100 192.168.32.102 TCP 66 80 -> 49165 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3 0.000244480 192.168.32.102 192.168.32.100 TCP 60 49165 -> 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4 0.000395469 192.168.32.102 192.168.32.100 HTTP 354 GET / HTTP/1.1
5 0.000413401 192.168.32.100 192.168.32.102 TCP 54 80 -> 49165 [ACK] Seq=1 Ack=301 Win=64128 Len=0
6 0.010005293 192.168.32.100 192.168.32.102 TCP 204 80 -> 49165 [PSH, ACK] Seq=1 Ack=301 Win=64128 Len=150 [TCP PDU reassembled in 7]
7 0.019888863 192.168.32.100 192.168.32.102 HTTP 312 HTTP/1.1 200 OK (text/html)
8 0.020071487 192.168.32.102 192.168.32.100 TCP 60 49165 -> 80 [ACK] Seq=301 Ack=410 Win=65292 Len=0
9 0.020225523 192.168.32.102 192.168.32.100 TCP 60 49165 -> 80 [FIN, ACK] Seq=301 Ack=410 Win=65292 Len=0
10 0.020248126 192.168.32.100 192.168.32.102 TCP 54 80 -> 49165 [ACK] Seq=410 Ack=302 Win=64128 Len=0
11 0.033425892 192.168.32.102 192.168.32.100 DNS 77 Standard query response 0xf640 Refused A urs.microsoft.com
12 0.033528385 192.168.32.100 192.168.32.102 DNS 77 Standard query response 0xf640 Refused A urs.microsoft.com
13 0.034020263 192.168.32.102 192.168.32.100 DNS 77 Standard query response 0x49c1 Refused A urs.microsoft.com
14 0.034070161 192.168.32.100 192.168.32.102 DNS 77 Standard query response 0x49c1 Refused A urs.microsoft.com
15 0.034557548 192.168.32.102 192.168.32.100 DNS 77 Standard query response 0xfa01 Refused A urs.microsoft.com
16 0.034607276 192.168.32.100 192.168.32.102 DNS 77 Standard query response 0xfa01 Refused A urs.microsoft.com
17 0.034970077 192.168.32.102 192.168.32.100 DNS 77 Standard query response 0xa32b Refused A urs.microsoft.com
18 0.035019013 192.168.32.100 192.168.32.102 DNS 77 Standard query response 0xa32b Refused A urs.microsoft.com
19 19.250229694 fe80::a00:27ff:fe6e::ff02::2 ICMPv6 70 Router Solicitation from 08:00:27:0e:13:6e

Frame 4: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7), Dst: PCSSystemtec_6e:13:6e (08:00:27:0e:13:6e)
Internet Protocol Version 4, Src: 192.168.32.102, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49165, Dst Port: 80, Seq: 1, Ack: 1, Len: 300
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Language: it-IT\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
  Accept-Encoding: gzip, deflate\r\n
  Host: epicode.internal\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Response in frame: 7]
  [Full request URI: http://epicode.internal/]
0010 01 54 01 99 40 00 80 06 35 f0 c0 a8 20 66 c0 a8 T...Pu...5...f...
0020 20 64 00 00 00 50 75 87 67 14 04 14 dc 65 50 16 d...Pu...g...eH...
0030 40 29 35 6c 06 06 47 45 54 20 2f 20 48 54 54 50 01l...GE T / HTTP
0040 2f 31 2e 31 00 0a 41 63 65 70 74 3a 20 2a 2f /11...Ac cept: /*
0050 2a 0d 0a 41 63 63 65 79 74 2d 4c 61 6e 67 75 61 *...Accep t-Langua
0060 67 65 3a 20 69 74 2d 49 54 0d 0a 55 73 65 72 2d ge: it-I T User-
0070 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 Agent: M ozilla/4
0080 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 .0 (comp atible;
0090 4d 53 49 45 20 30 2e 30 3b 20 57 69 6e 64 6f 77 MSIE 8.0 ; Window
00a0 73 20 4e 54 20 36 2e 31 3b 20 54 72 09 64 65 6e s NT 6.1 ; Triden
00b0 74 2f 34 2e 30 3b 20 53 4c 43 43 32 3b 20 2e 4e t/4.0; S LCC2; .N
00c0 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 37 ET CLR 2 .0.50727
00d0 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 ; .NET C LR 3.5.3
00e0 30 37 32 39 3b 20 2e 4e 45 54 20 43 4c 52 20 33 0729; .N ET CLR 3
00f0 2e 30 2e 33 30 37 32 39 3b 20 40 65 64 69 61 20 .0.30729; Media
0100 43 65 6e 74 65 72 20 50 43 20 36 2e 30 29 0d 0a Center P C 6.0) .
0110 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding:
0120 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate;
0130 48 6f 73 74 3a 20 65 70 60 65 64 65 20 60 60 Next-av tions: 10
```

le differenze più evidenti sono che il protocollo cifrato TLS ora non è più presente dunque il protocollo HTTP viene mostrato in chiaro è anche possibile vedere proprio la programmazione HTLM del file index di inetsim

```
0000 08 00 27 5b 75 b7 08 00 27 6e 13 6e 08 00 45 00 ...[U...n.n..E.
0010 01 2a 2f 55 40 00 40 06 48 5e c0 a8 20 64 c0 a8 ...*/U@.@. H^.. d..
0020 20 66 00 50 c0 0e 2c 9c 13 75 e4 7a ed 98 50 19 ...f.P... .u.z..P.
0030 01 f5 c3 37 00 00 3c 68 74 6d 6c 3e 0a 20 20 3c ...7...<html>.. <
0040 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 head>.. <title
0050 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74 >INetSim default
0060 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c HTML pa ge</titl
0070 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c e>.. </h ead>.. <
0080 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70 body>.. <p></p>
0090 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22 >.. <p align="
00a0 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20 center"> This is
00b0 74 68 65 20 64 65 66 61 75 6c 74 20 48 54 4d 4c the defa ult HTML
00c0 20 70 61 67 65 20 66 6f 72 20 49 4e 65 74 53 69 page fo r INetSi
00d0 6d 20 48 54 54 50 20 73 65 72 76 65 72 20 66 61 m HTTP s erver fa
00e0 6b 65 20 6d 6f 64 65 2e 3c 2f 70 3e 0a 20 20 20 ke mode. </p>..
00f0 20 3c 70 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 <p alig n="cente
0100 72 22 3e 54 68 69 73 20 66 69 6c 65 20 69 73 20 r">This file is
0110 61 6e 20 48 54 4d 4c 20 64 6f 63 75 6d 65 6e 74 an HTML document
0120 2e 3c 2f 70 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a .</p>.. </body>..
0130 3c 2f 68 74 6d 6c 3e 0a </html>..
```

e questa è la get che viene effettuata al server HTTP

```
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: it-IT\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
    Accept-Encoding: gzip, deflate\r\n
    Host: epicode.internal\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Response in frame: 7]
    [Full request URI: http://epicode.internal/]
```

Infine l'altra grande differenza riguarda la porta di destinazione che nel HTTP è la n° 80

```
▶ Frame 4: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface eth0, id
▶ Ethernet II, Src: PCSSystemtec_5b:75:b7 (08:00:27:5b:75:b7), Dst: PCSSystemtec_6e:13:6e (08:
▶ Internet Protocol Version 4, Src: 192.168.32.102, Dst: 192.168.32.100
▼ Transmission Control Protocol, Src Port: 49166, Dst Port: 80, Seq: 1, Ack: 1, Len: 300
  Source Port: 49166
  Destination Port: 80
  [Stream index: 0]
```