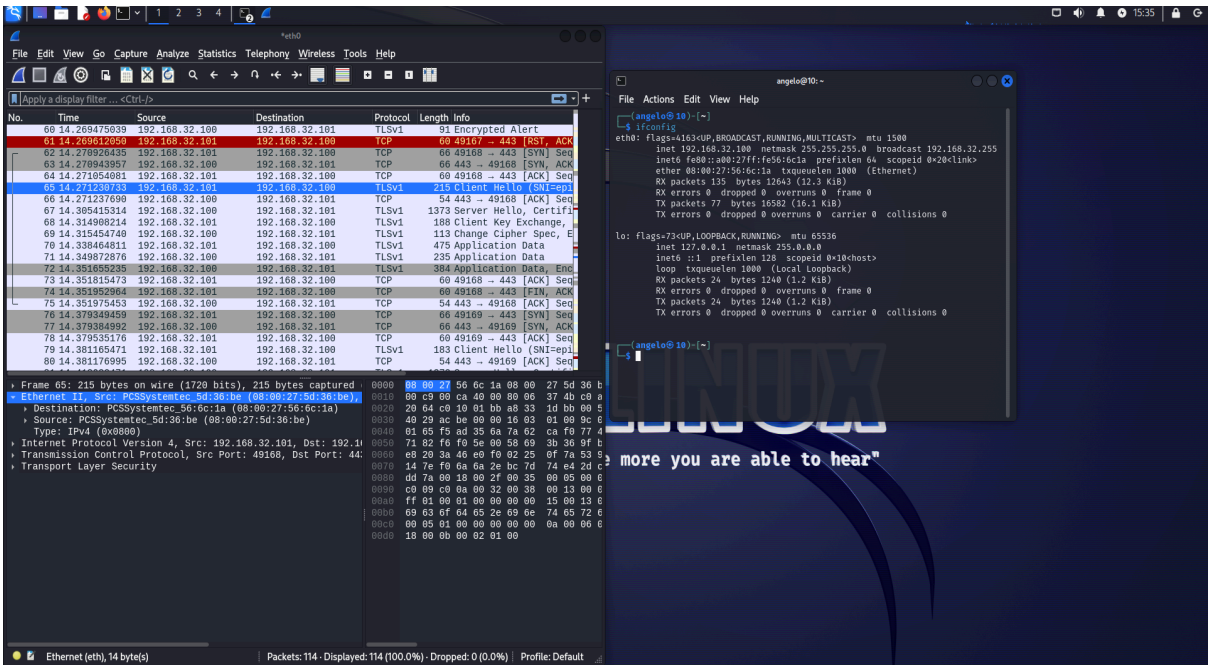
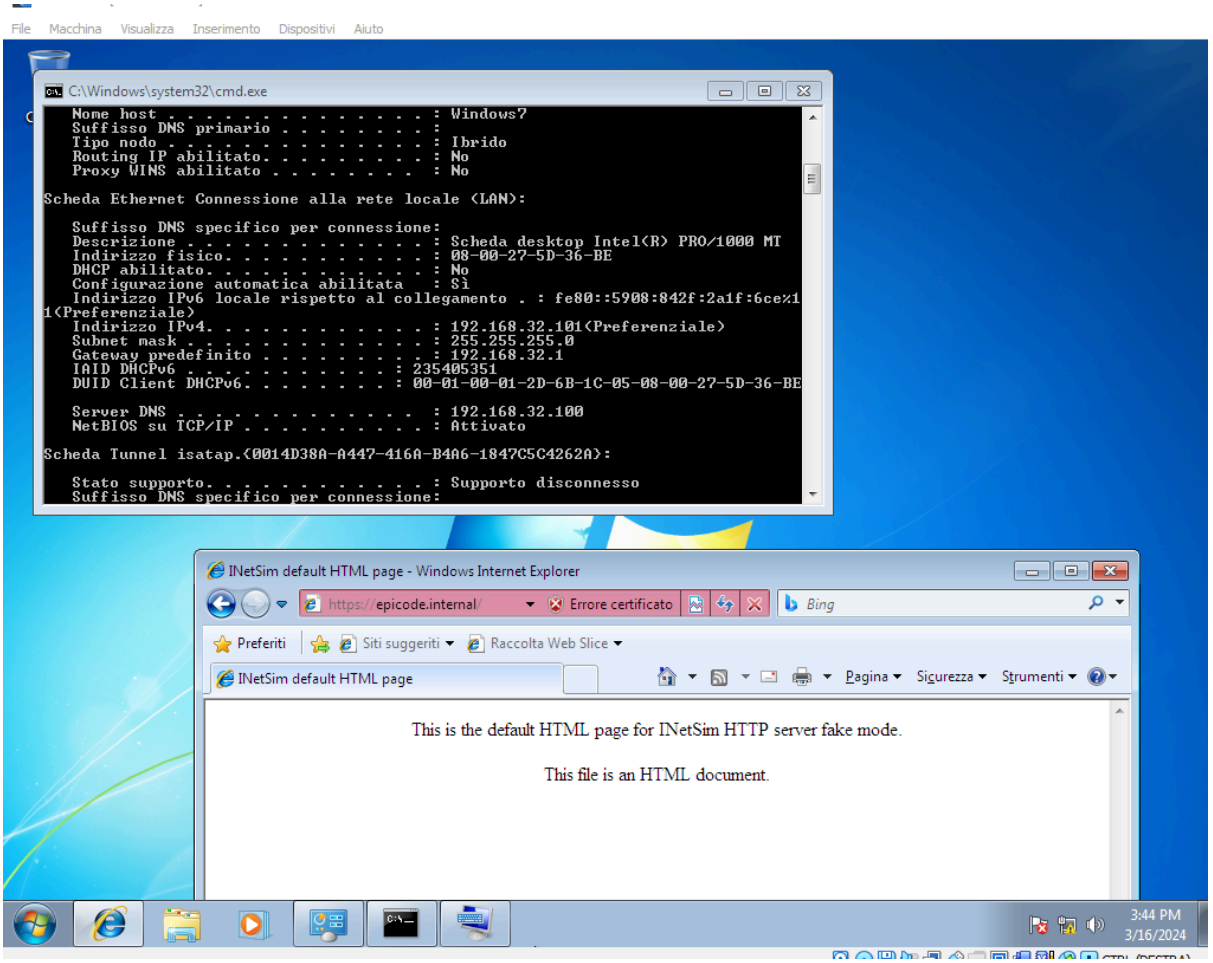
Progetto D'esame W4 D4

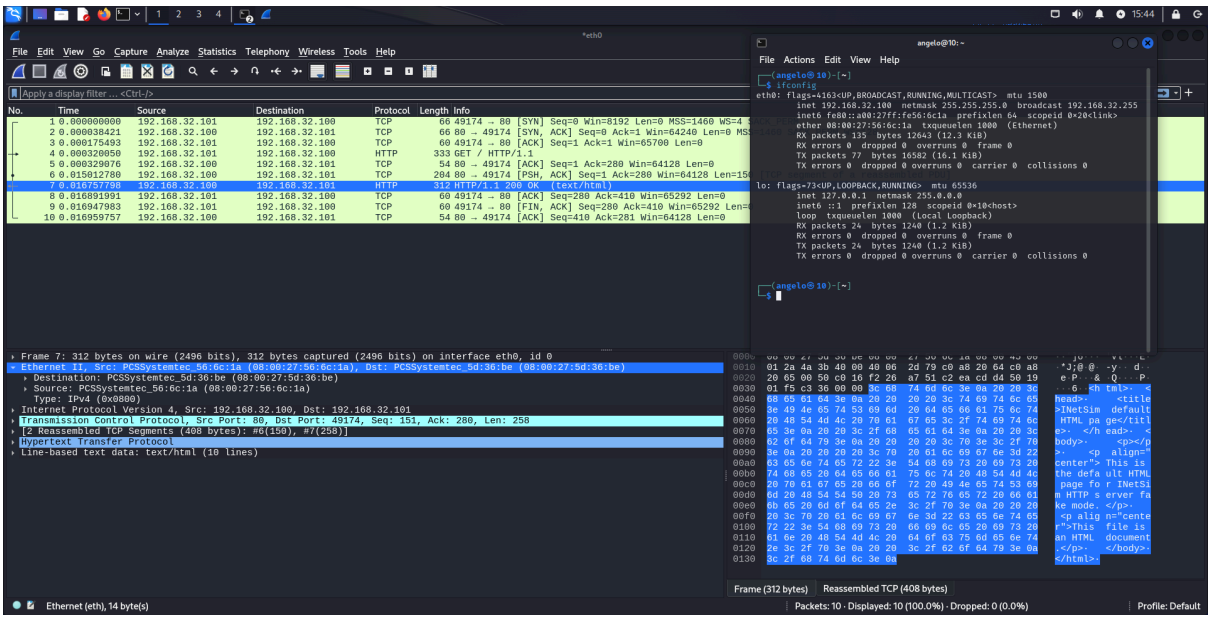
Come possiamo notare grazie a questo progetto, abbiamo capito quale differenza c'è tra un HTTP e un HTTPS.
A primo impatto grazie anche all'applicazione Wireshark possiamo notare che Avviando la ricerca in HTTPS ci sono meno informazioni al pacchetto perchè è criptato.
Cosa contraria quando si effettua una ricerca in HTTP perchè come si può notare anche in foto in allegato ci sono scritte tutte le informazioni che io sto visualizzando nella pagina web in quel momento e anche che tipo di broswer si sta utilizzando.

Mac Address (Kali): 08:00:27:56:6c:1a
Mac Address (Windows): 08:00:27:5d:36:be
IP (Kali): 192.168.32.100
IP (Windows): 192.168.32.101

Allegato 1: Pacchetti wireshark in HTTPS + Mac address linux
Allegato 2: Mac address Windows + Motore di ricerca epicode.interal
Allegato 3: Pacchetti wireshark in HTTP + Mac address linux


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
60 14.269475039 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
61 14.269612050 192.168.32.101 192.168.32.100 TCP 60 49167 → 443 [RST, ACK
62 14.270926435 192.168.32.101 192.168.32.100 TCP 66 49168 → 443 [SYN] Seq
63 14.270943957 192.168.32.100 192.168.32.101 TCP 66 443 → 49168 [SYN, ACK
64 14.271054081 192.168.32.101 192.168.32.100 TCP 60 49168 → 443 [ACK] Seq
65 14.271230753 192.168.32.101 192.168.32.100 TLSv1 219 Client Hello (SNI=epi
66 14.271237690 192.168.32.100 192.168.32.101 TCP 54 443 → 49168 [ACK] Seq
67 14.305415314 192.168.32.100 192.168.32.101 TLSv1 1373 Server Hello, Certifi
68 14.314908214 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange,
69 14.315454740 192.168.32.101 192.168.32.100 TLSv1 113 Change Cipher Spec, E
70 14.338464811 192.168.32.101 192.168.32.100 TLSv1 475 Application Data
71 14.349872876 192.168.32.100 192.168.32.101 TLSv1 235 Application Data
72 14.351655235 192.168.32.100 192.168.32.101 TLSv1 384 Application Data, Enc
73 14.351815473 192.168.32.101 192.168.32.100 TCP 60 49168 → 443 [ACK] Seq
74 14.351952964 192.168.32.100 192.168.32.101 TCP 60 49168 → 443 [FIN, ACK
75 14.351975453 192.168.32.101 192.168.32.100 TCP 54 443 → 49168 [ACK] Seq
76 14.379349459 192.168.32.101 192.168.32.100 TCP 66 49169 → 443 [SYN] Seq
77 14.379384992 192.168.32.100 192.168.32.101 TCP 66 443 → 49169 [SYN, ACK
78 14.379535176 192.168.32.101 192.168.32.100 TCP 60 49169 → 443 [ACK] Seq
79 14.381165471 192.168.32.101 192.168.32.100 TLSv1 183 Client Hello (SNI=epi
80 14.381176995 192.168.32.100 192.168.32.101 TCP 54 443 → 49169 [ACK] Seq
Frame 65: 215 bytes on wire (1720 bits), 215 bytes captured
Ethernet II, Src: PCSSystemtec_5d:36:be (08:00:27:5d:36:be),
Destination: PCSSystemtec_56:6c:1a (08:00:27:56:6c:1a)
Source: PCSSystemtec_5d:36:be (08:00:27:5d:36:be)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.1
Transmission Control Protocol, Src Port: 49168, Dst Port: 44
Transport Layer Security
Ethernet (eth), 14 byte(s)
Packets: 114 · Displayed: 114 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
angelo@10: ~
File Actions Edit View Help
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:fe56:6c1a prefixlen 64 scopeid 0x20<link>
ether 08:00:27:56:6c:1a txqueuelen 1000 (Ethernet)
RX packets 135 bytes 12643 (12.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 77 bytes 16582 (16.1 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
more you are able to hear"


File Macchina Visualizza Inserimento Dispositivi Aiuto
C:\Windows\system32\cmd.exe
Nome host . . . . . : Windows7
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
Indirizzo fisico. . . . . : 08-00-27-5D-36-BE
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::5908:842f:2a1f:6ce%11(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.32.101(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.1
IAID DHCPv6 . . . . . : 235405351
DUID Client DHCPv6. . . . . : 00-01-00-01-2D-6B-1C-05-08-00-27-5D-36-BE
Server DNS . . . . . : 192.168.32.100
NetBIOS su TCP/IP . . . . . : Attivato
Scheda Tunnel isatap.{0014D38A-A447-416A-B4A6-1847C5C4262A}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Errore certificato
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
3:44 PM
3/16/2024


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.32.101 192.168.32.100 TCP 66 49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2 0.000038421 192.168.32.100 192.168.32.101 TCP 66 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3 0.000175493 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4 0.000320050 192.168.32.101 192.168.32.100 HTTP 333 GET / HTTP/1.1
5 0.000329076 192.168.32.100 192.168.32.101 TCP 54 80 → 49174 [ACK] Seq=1 Ack=280 Win=64128 Len=0
6 0.015012780 192.168.32.100 192.168.32.101 TCP 204 80 → 49174 [PSH, ACK] Seq=1 Ack=280 Win=64128 Len=150
7 0.016767780 192.168.32.100 192.168.32.101 HTTP 312 HTTP/1.1 200 OK (text/html)
8 0.016891991 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [ACK] Seq=280 Ack=410 Win=65292 Len=0
9 0.016947983 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [FIN, ACK] Seq=280 Ack=410 Win=65292 Len=0
10 0.016959757 192.168.32.100 192.168.32.101 TCP 54 80 → 49174 [ACK] Seq=410 Ack=281 Win=64128 Len=0
Frame 7: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_56:6c:1a (08:00:27:56:6c:1a), Dst: PCSSystemtec_5d:36:be (08:00:27:5d:36:be)
Destination: PCSSystemtec_5d:36:be (08:00:27:5d:36:be)
Source: PCSSystemtec_56:6c:1a (08:00:27:56:6c:1a)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49174, Seq: 151, Ack: 280, Len: 258
[2 Reassembled TCP Segments (408 bytes): #6(150), #7(258)]
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
Frame (312 bytes)
Reassembled TCP (408 bytes)
Ethernet (eth), 14 byte(s)
Packets: 10 · Displayed: 10 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
angelo@10: ~
File Actions Edit View Help
$ 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:fe56:6c1a prefixlen 64 scopeid 0x20<link>
ether 08:00:27:56:6c:1a txqueuelen 1000 (Ethernet)
RX packets 135 bytes 12643 (12.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 77 bytes 16582 (16.1 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
$