Report simulazione rete

In base all'esercizio svolto le presento dettagliatamente il report sulla simulazione da lei assegnata. Utilizzando protocolli HTTPS/HTTP simulando un client-server.

Introduzione

-Impostazione indirizzo ip Kali-Linux

-Impostazione indirizzo ip Windows 7

-Https- Attivo

-Servizio Dns/Attivo

-Configurazione Dns---(epicode.internal) (Tramite i duei indirizzi ip)

-Comunicazione Wireshark-- IMAC/sorgente/destinazione/HTTPS/HTTP

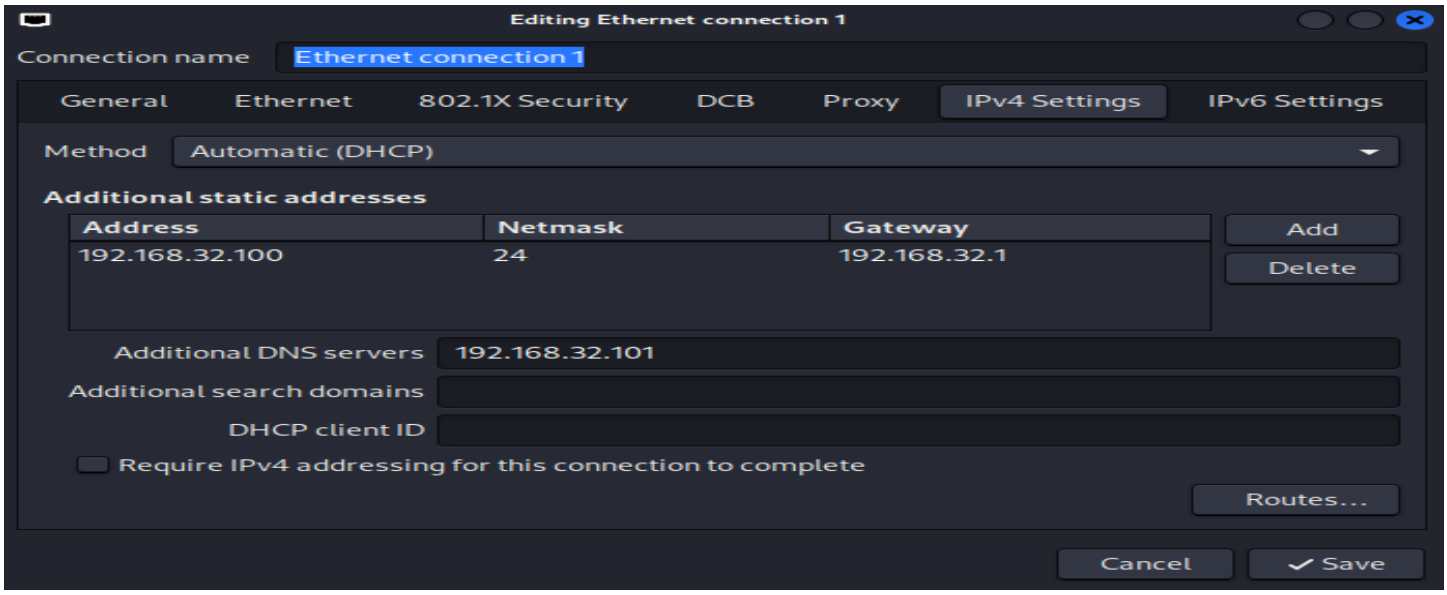
L’impostazione dell’indirizzo ip su Kali-linux si effettua tramite rete, inserendo dei Parametri sulla voce iPv4 settings aggiungendo sull’apposita tabella;

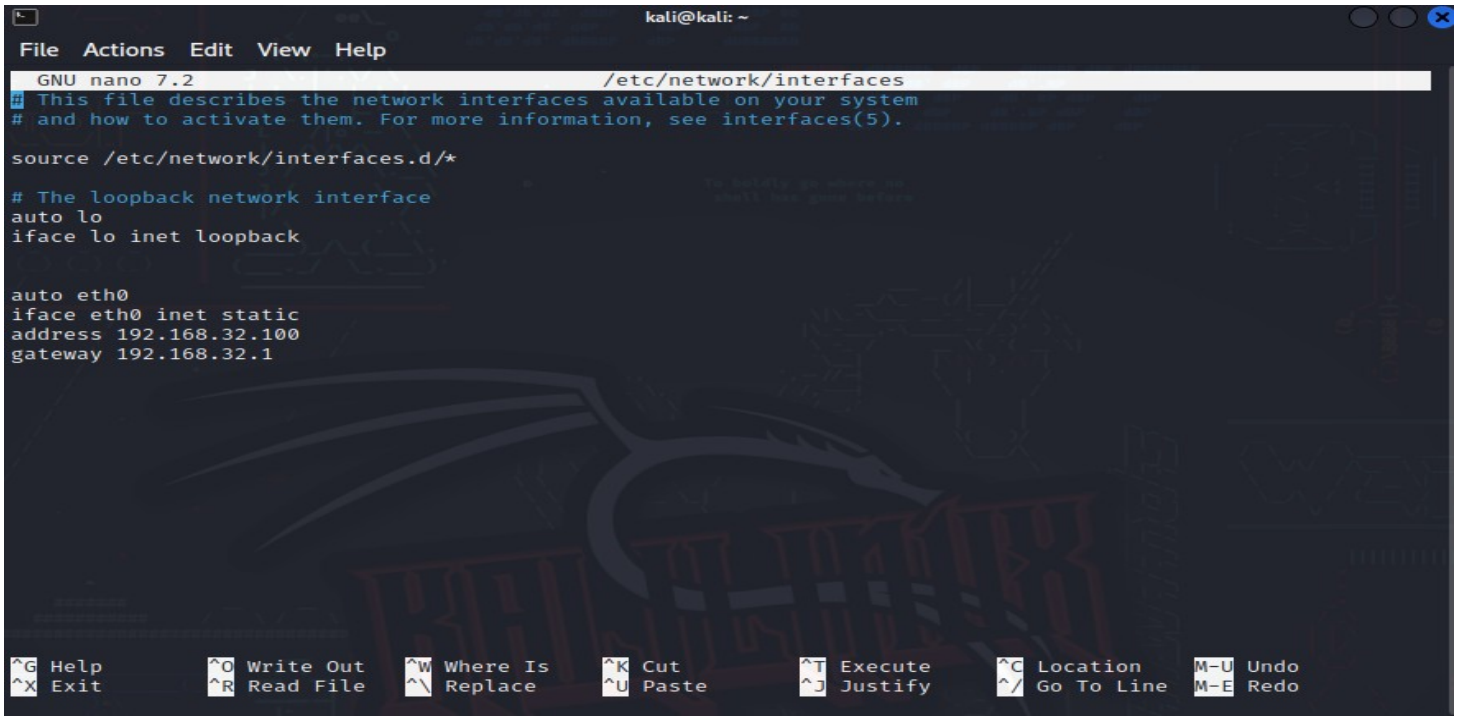
-l’indirizzo

-netmask

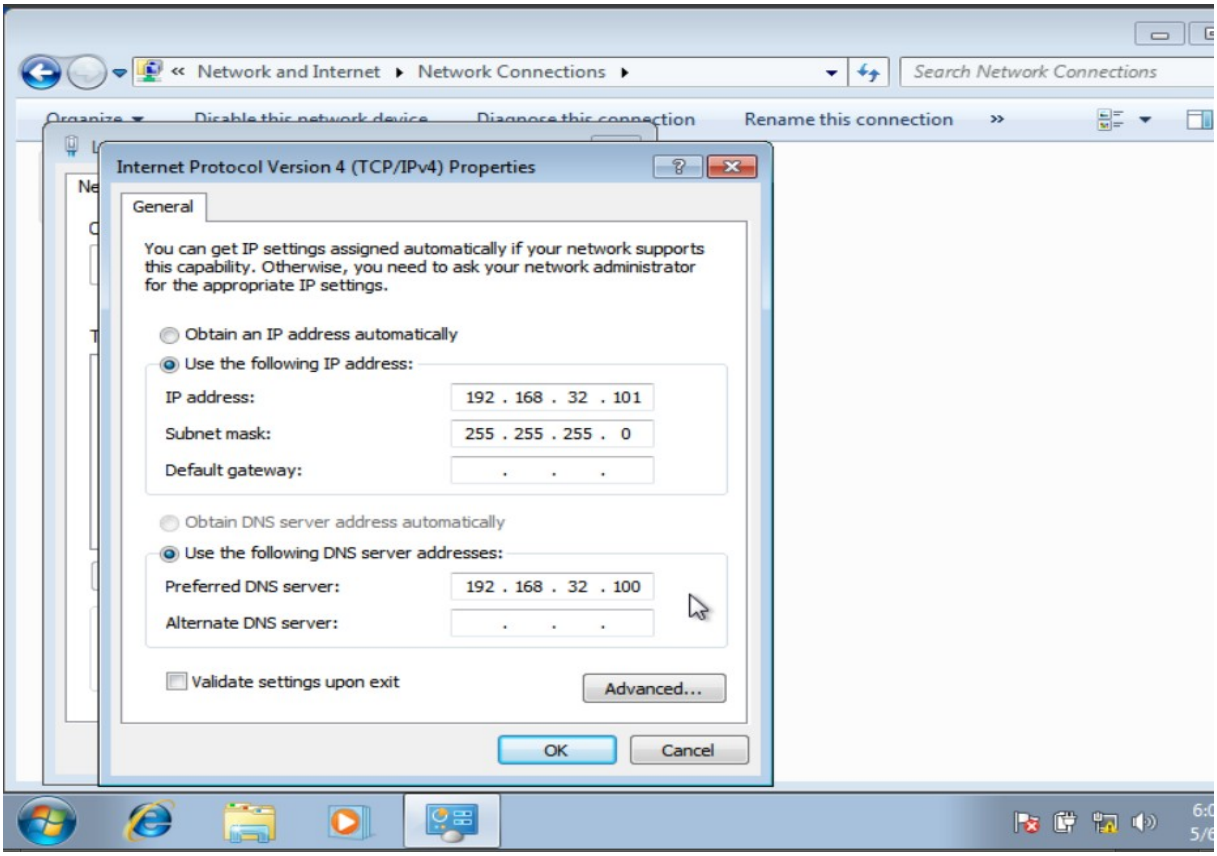
-Gateway.

Effettuare la medesima operazione tramite terminale.

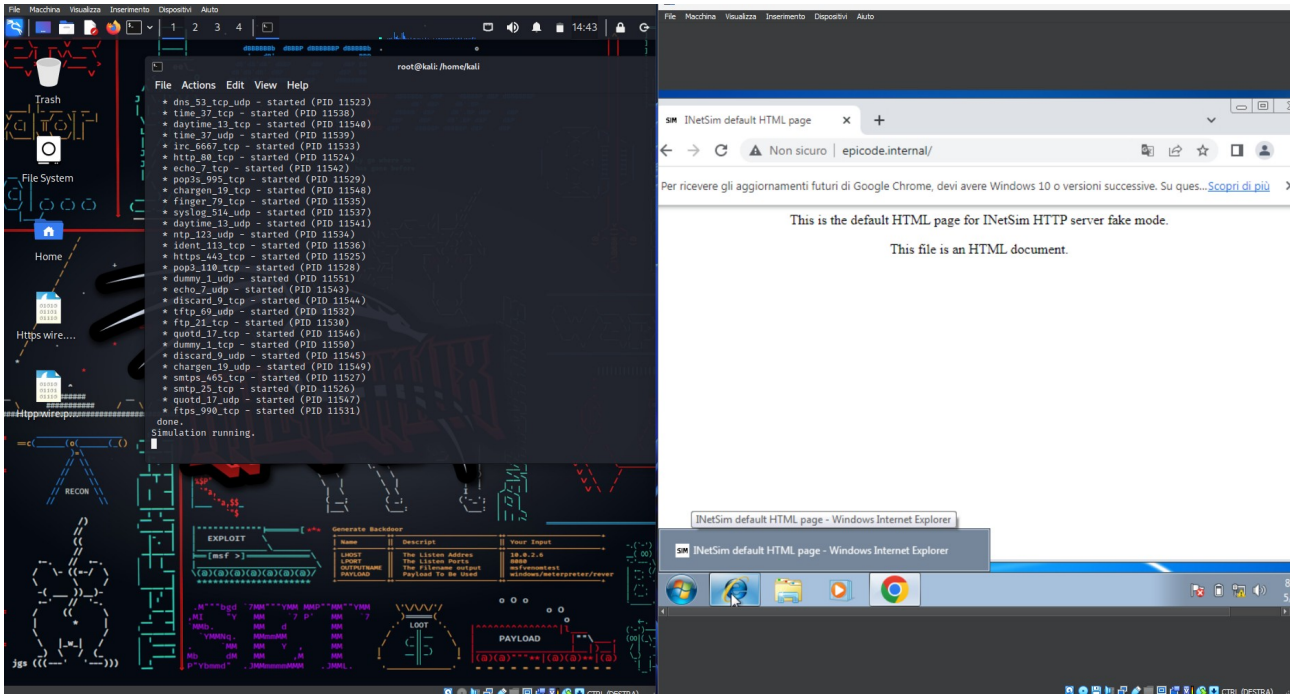




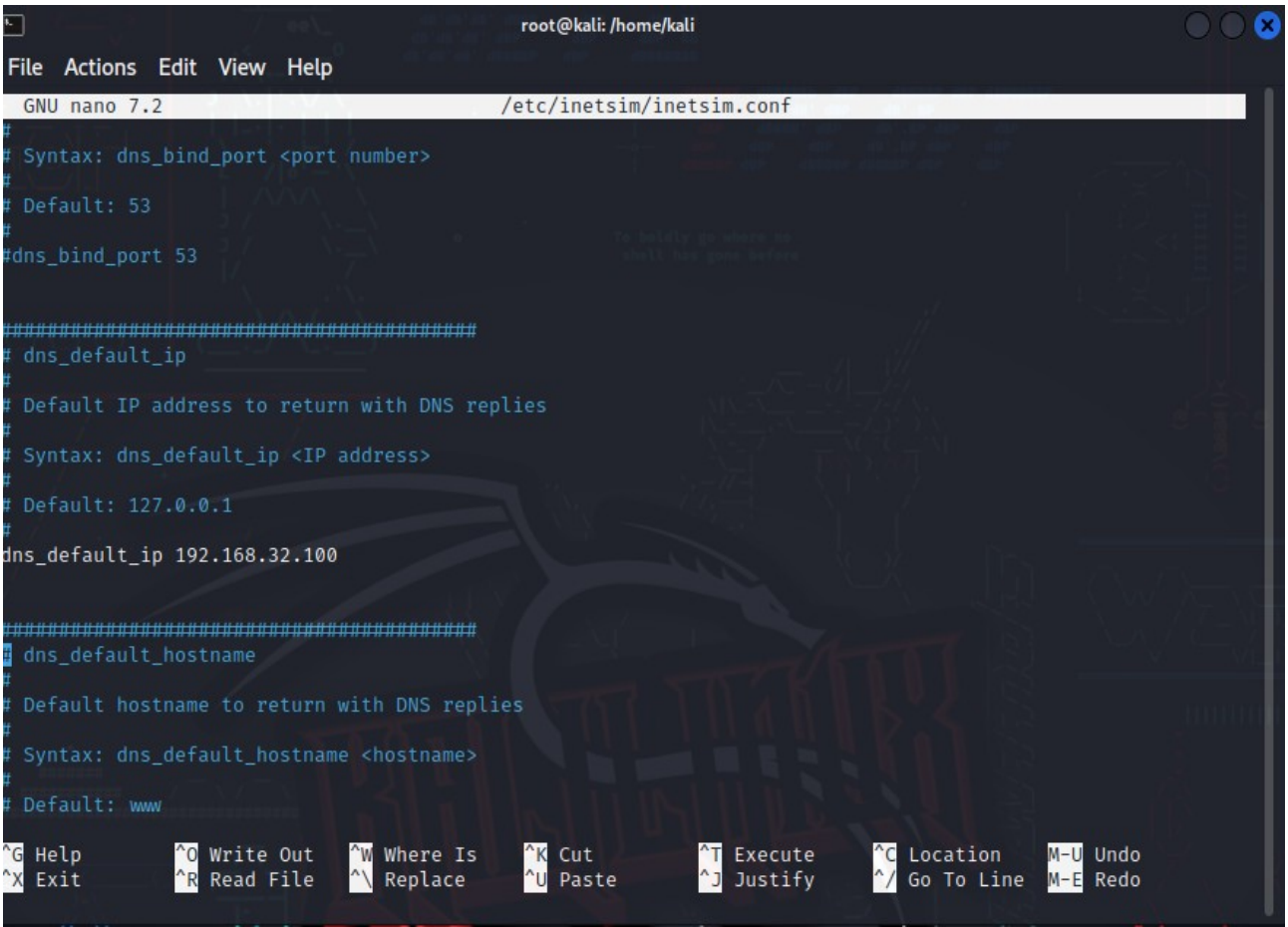
Replicare la medesima operazione su windows accedendo alle impostazioni e modificando iPv4.



Bisogna modificare gli indirizzi (192.168.32.100) per Kali e per Windows (192.168.32.101) che sono fondamentali per una comunicazione sicura tra il client e il server simulato.



Configurando il Dns tramite file di comunicazione,possiamo mettere in contatto,tramite web browser una risorsa all'hostname epicode.internal che risponde all'ip 192.168.32.100



Comunicazione tramite Wireshark.

Wireshark è un programma che permette di intercettare pacchetti,in questo caso bisogna evidenziare l’indirizzo MAC address e la destinazione della richiesta HTTPS.

Tale comunicazione si e svolta tramite il protocollo HTTPS (Hyper text trasfer protocol secure),quest’ultimo garantisce un trasferimento dei dati tra client e server in modo sicuro rispettando la privacy.
Il controllo del traffico effettuato con l’utilizzo di wireshark,abbiamo rilevato gli indirizzi MAC notando che il contenuto HTTPS è crittografato.
ip.addr == 192.168.32.101 || tcp.port == 443

Nella seconda parte dell’esercizio il server HTTPS è stato sostituito con HTTP emulando

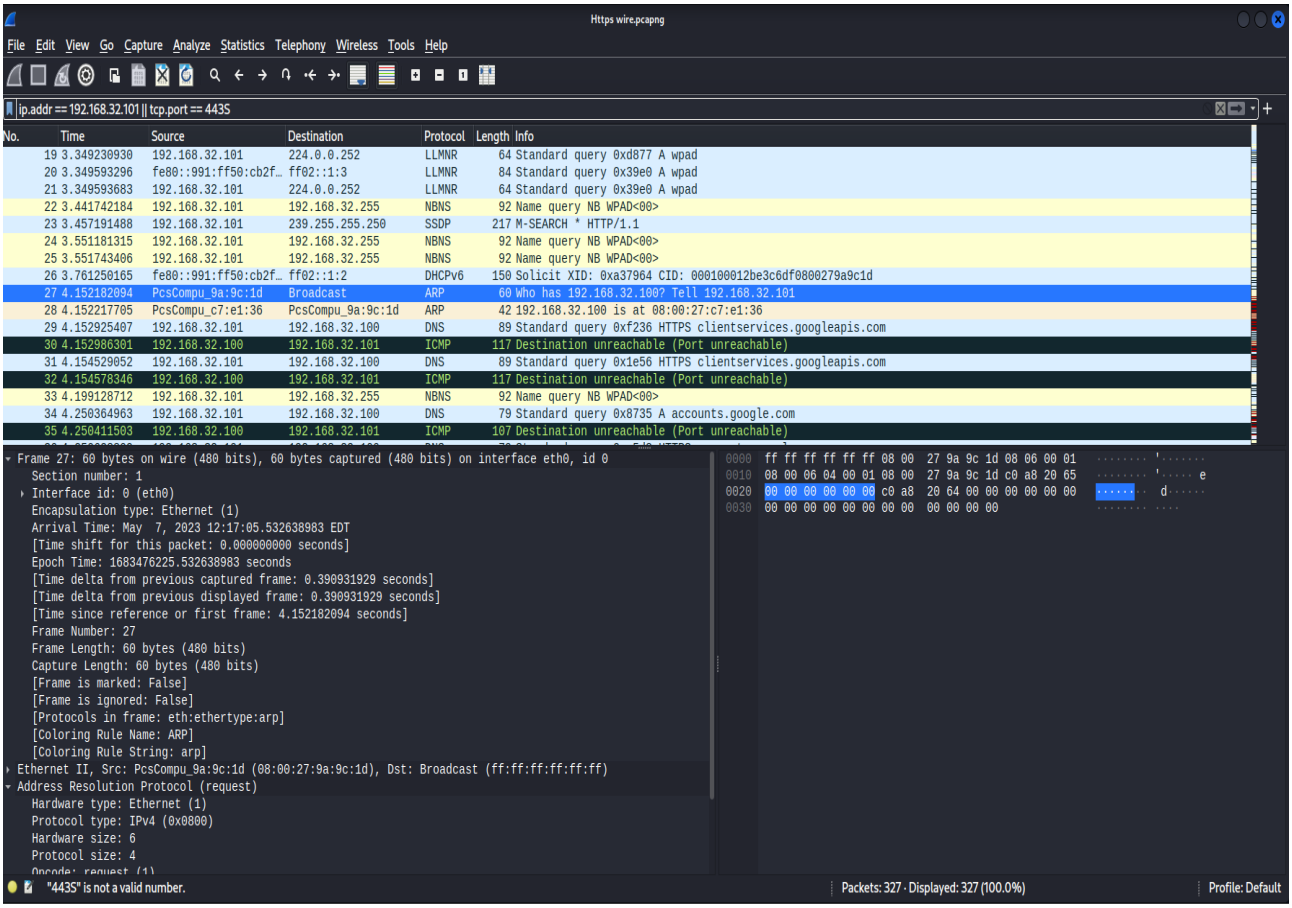
lo stesso comportamento per evidenziare le differenze tra i due.

Le principali differenze tra i due sono la crittografia che avviene tramite connessione ssl/tls e la sicurezza dei dati,cosa che non avviene nell'HTTP ,che al contrario è possibile vedere i dati senza crittografia.
ip.addr == 192.168.32.101 || tcp.port == 80

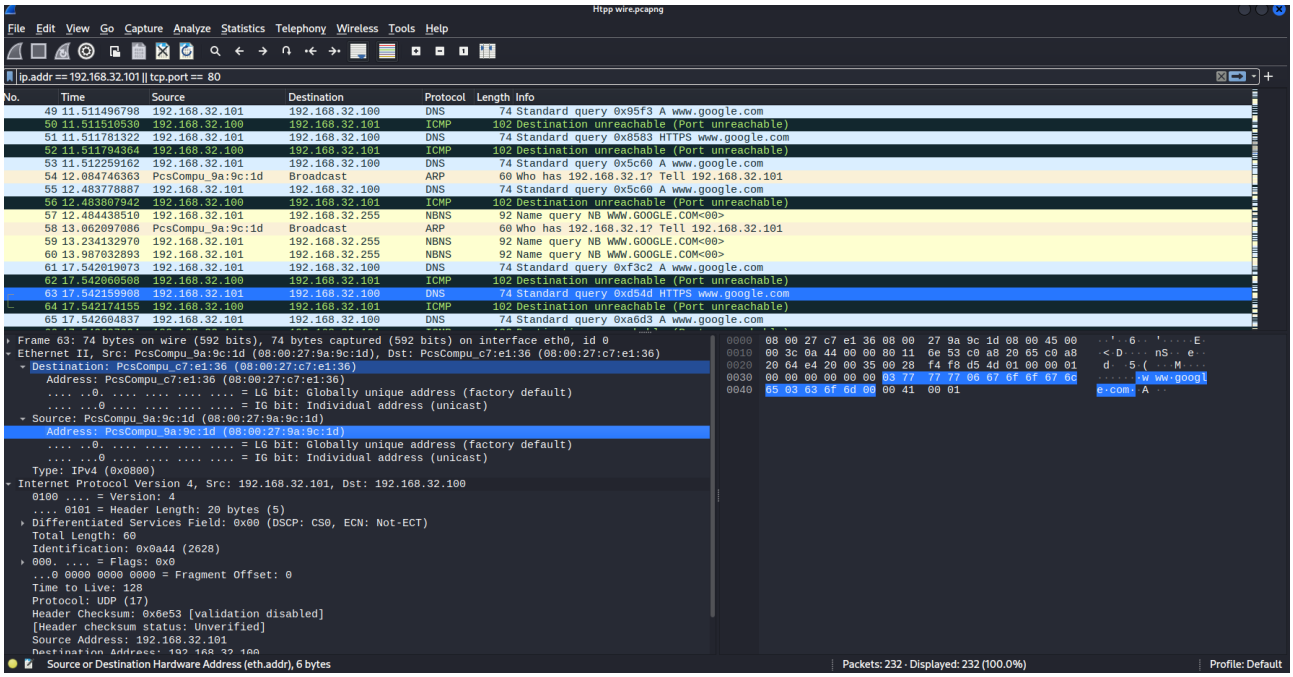
Nel momento in cui è stato intercettato il traffico HTTP con wireshark ,si e potuto notare che i dati erano ben visibili.
La mancanza di crittografia rende più vulnerabile il furto di dati sensibili.

Con tale vulnerabilità è possibile risalire a password,indirizzi,conti bancari ed informazioni personali.

Pertanto conviene utilizzare il protocollo HTTPS che scongiura i problemi sopra citati e garantisce l'integrità dei dati in generale.


Https wire.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.32.101 || tcp.port == 4435
No. Time Source Destination Protocol Length Info
19 3.349230930 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xd877 A wpad
20 3.349593296 fe80::991:ff50:cb2f… ff02::1:3 LLMNR 84 Standard query 0x39e0 A wpad
21 3.349593683 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0x39e0 A wpad
22 3.441742184 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
23 3.457191488 192.168.32.101 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
24 3.551181315 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
25 3.551743406 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
26 3.761250165 fe80::991:ff50:cb2f… ff02::1:2 DHCPv6 150 Solicit XID: 0xa37964 CID: 000100012be3c6df0800279a9c1d
27 4.152182094 PcsCompu_9a:9c:1d Broadcast ARP 60 Who has 192.168.32.100? Tell 192.168.32.101
28 4.152217705 PcsCompu_c7:e1:36 PcsCompu_9a:9c:1d ARP 42 192.168.32.100 is at 08:00:27:c7:e1:36
29 4.152925407 192.168.32.101 192.168.32.100 DNS 89 Standard query 0xf236 HTTPS clientservices.googleapis.com
30 4.152986301 192.168.32.100 192.168.32.101 ICMP 117 Destination unreachable (Port unreachable)
31 4.154529052 192.168.32.101 192.168.32.100 DNS 89 Standard query 0x1e56 HTTPS clientservices.googleapis.com
32 4.154578346 192.168.32.100 192.168.32.101 ICMP 117 Destination unreachable (Port unreachable)
33 4.199128712 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
34 4.250364963 192.168.32.101 192.168.32.100 DNS 79 Standard query 0x8735 A accounts.google.com
35 4.250411503 192.168.32.100 192.168.32.101 ICMP 107 Destination unreachable (Port unreachable)
Frame 27: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Section number: 1
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: May 7, 2023 12:17:05.532638983 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1683476225.532638983 seconds
[Time delta from previous captured frame: 0.390931929 seconds]
[Time delta from previous displayed frame: 0.390931929 seconds]
[Time since reference or first frame: 4.152182094 seconds]
Frame Number: 27
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
0000 ff ff ff ff ff ff 08 00 27 9a 9c 1d 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 9a 9c 1d c0 a8 20 65
0020 00 00 00 00 00 00 c0 a8 20 64 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
"4435" is not a valid number.
Packets: 327 · Displayed: 327 (100.0%)
Profile: Default


Epoch Time: 1683476225.532638983 seconds
[Time delta from previous captured frame: 0.390931929 seconds]
[Time delta from previous displayed frame: 0.390931929 seconds]
[Time since reference or first frame: 4.152182094 seconds]
Frame Number: 27
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory defaul…
....1 .... = IG bit: Group address (multicast/broadcast)
Source: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d)
Address: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
0000 ff ff ff ff ff ff 08 00 27 9a 9c 1d 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 9a 9c 1d c0 a8 20 65
0020 00 00 00 00 00 00 c0 a8 20 64 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00


Htpp wire.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.32.101 || tcp.port == 80
No. Time Source Destination Protocol Length Info
49 11.511496798 192.168.32.101 192.168.32.100 DNS 74 Standard query 0x95f3 A www.google.com
50 11.511510530 192.168.32.100 192.168.32.101 ICMP 102 Destination unreachable (Port unreachable)
51 11.511781322 192.168.32.101 192.168.32.100 DNS 74 Standard query 0x8583 HTTPS www.google.com
52 11.511794364 192.168.32.100 192.168.32.101 ICMP 102 Destination unreachable (Port unreachable)
53 11.512259162 192.168.32.101 192.168.32.100 DNS 74 Standard query 0x5c60 A www.google.com
54 12.084746363 PcsCompu_9a:9c:1d Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
55 12.483778887 192.168.32.101 192.168.32.100 DNS 74 Standard query 0x5c60 A www.google.com
56 12.483807942 192.168.32.100 192.168.32.101 ICMP 102 Destination unreachable (Port unreachable)
57 12.484438510 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WWW.GOOGLE.COM<00>
58 13.062097086 PcsCompu_9a:9c:1d Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
59 13.234132970 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WWW.GOOGLE.COM<00>
60 13.987032893 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WWW.GOOGLE.COM<00>
61 17.542019073 192.168.32.101 192.168.32.100 DNS 74 Standard query 0xf3c2 A www.google.com
62 17.542060508 192.168.32.100 192.168.32.101 ICMP 102 Destination unreachable (Port unreachable)
63 17.542159908 192.168.32.101 192.168.32.100 DNS 74 Standard query 0xd54d HTTPS www.google.com
64 17.542174155 192.168.32.100 192.168.32.101 ICMP 102 Destination unreachable (Port unreachable)
65 17.542604837 192.168.32.101 192.168.32.100 DNS 74 Standard query 0xa6d3 A www.google.com
Frame 63: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
Address: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d)
Address: PcsCompu_9a:9c:1d (08:00:27:9a:9c:1d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x0a44 (2628)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x6e53 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.32.101
0000 08 00 27 c7 e1 36 08 00 27 9a 9c 1d 08 00 45 00
0010 00 3c 0a 44 00 00 80 11 6e 53 c0 a8 20 65 c0 a8
0020 20 64 e4 20 00 35 00 28 f4 f8 d5 4d 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c
0040 65 03 63 6f 6d 00 00 41 00 01
Source or Destination Hardware Address (eth.addr), 6 bytes
Packets: 232 · Displayed: 232 (100.0%)
Profile: Default