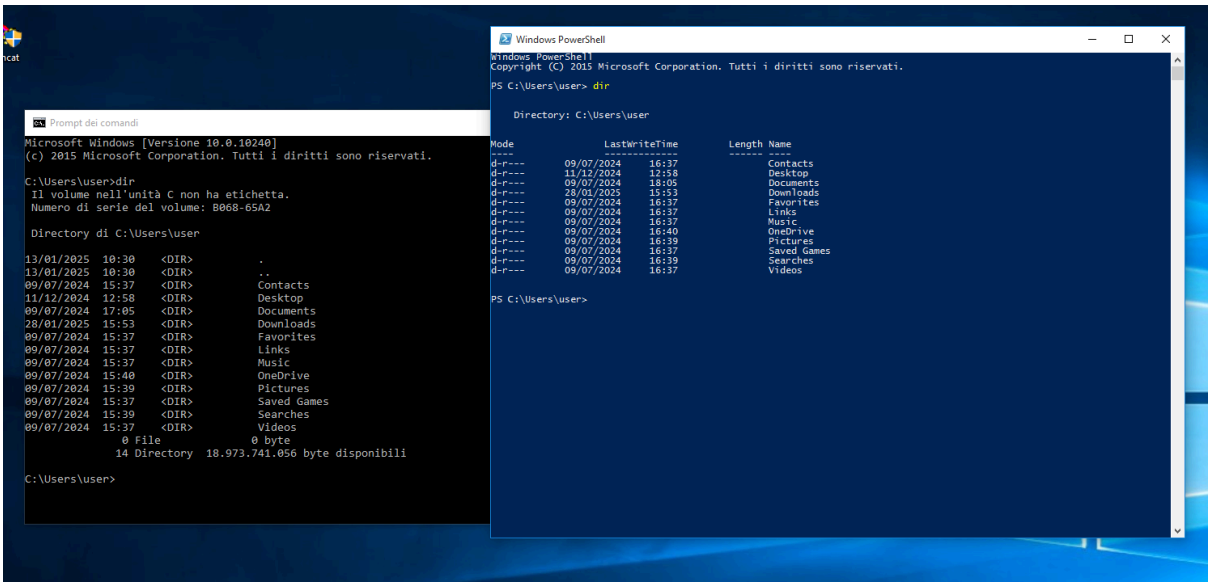
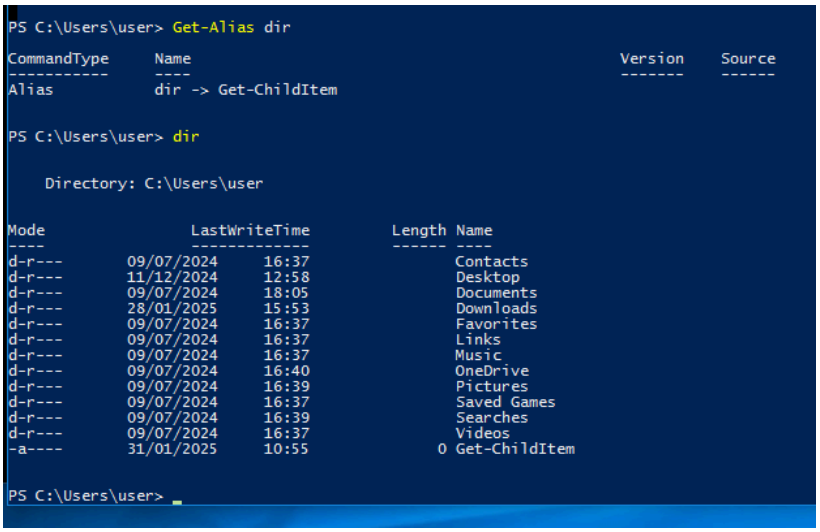
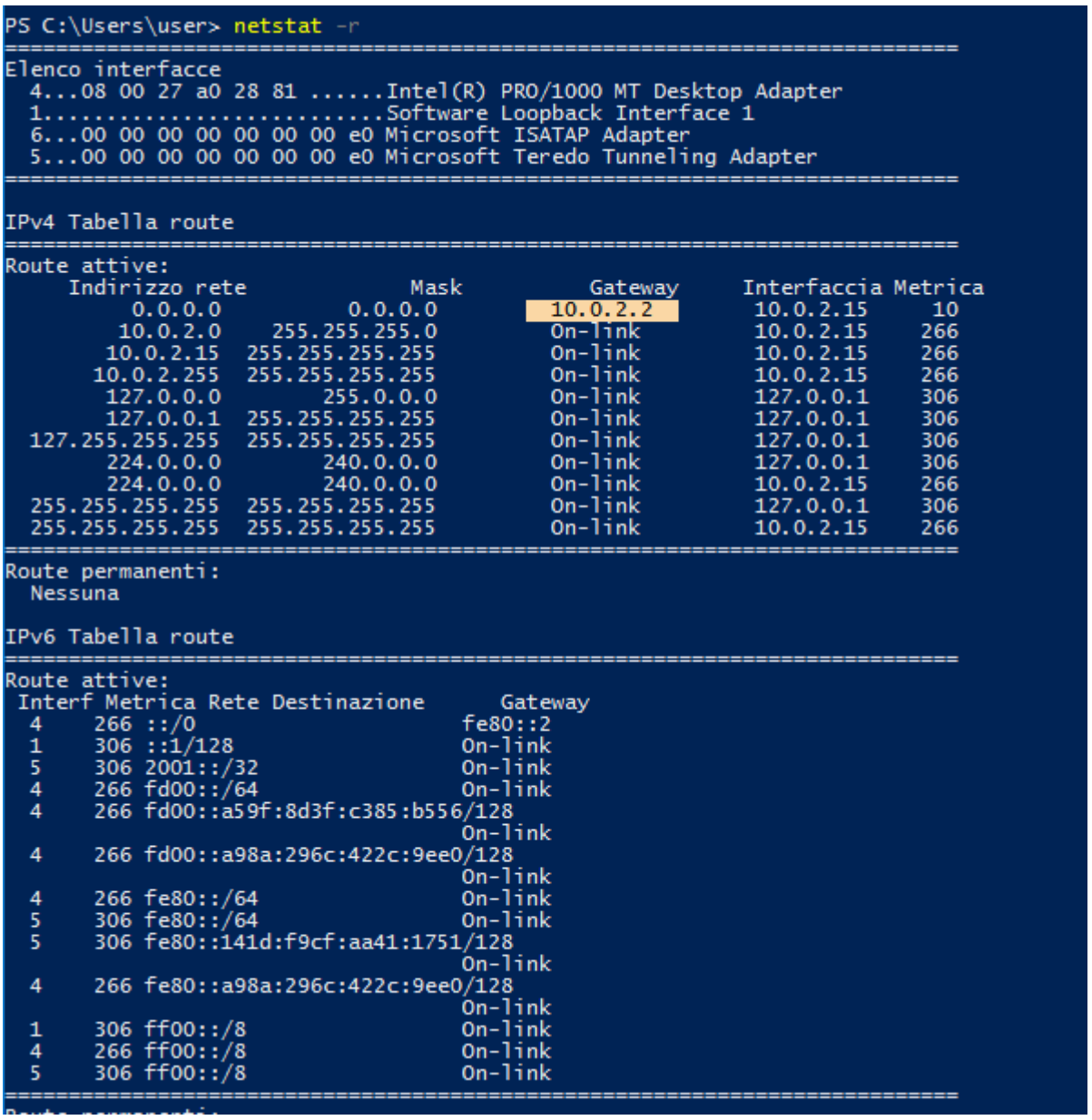
Esame S11L5
Laboratorio - Utilizzo di Windows PowerShell

Data una macchina windows sono andata a svolgere i comandi richiesti dall'esercizio guidato.
Ho aperto Powershell e Command Prompt e richiesto il comando dir



e provato vari altri comandi come cd, ipconfig ecc.
Il risultato da entrambi è praticamente lo stesso.
Ho successivamente utilizzato il comando Get-Alias dir, Aliasdir -> Get-ChillItem per avere come risultato al comando dir Get.ChildItem

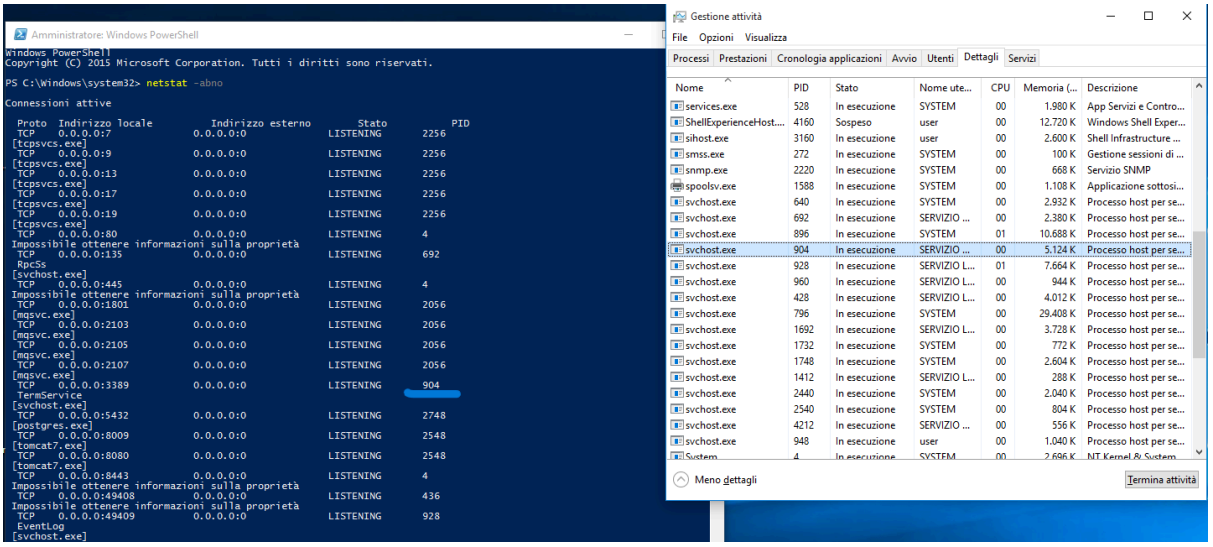




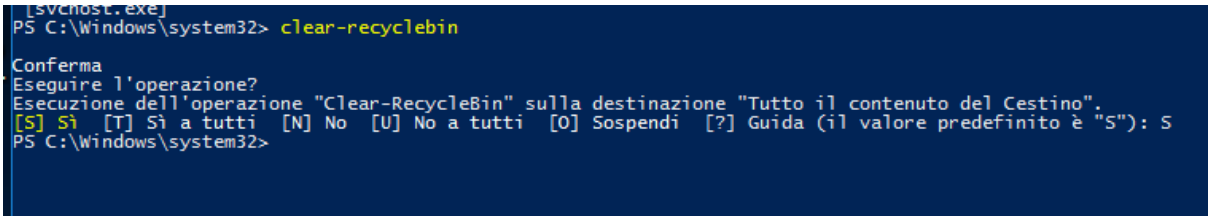
```
PS C:\Users\user> netstat -r
===========================================================================
Elenco interfacce
  4...08 00 27 a0 28 81 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  5...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0        10.0.2.2       10.0.2.15     10
         10.0.2.0    255.255.255.0         On-link        10.0.2.15    266
        10.0.2.15  255.255.255.255         On-link        10.0.2.15    266
       10.0.2.255  255.255.255.255         On-link        10.0.2.15    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link        10.0.2.15    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link        10.0.2.15    266
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  4    266 ::/0                     fe80::2
  1    306 ::1/128                  On-link
  5    306 2001::/32                On-link
  4    266 fd00::/64                On-link
  4    266 fd00::a59f:8d3f:c385:b556/128
                                    On-link
  4    266 fd00::a98a:296c:422c:9ee0/128
                                    On-link
  4    266 fe80::/64                On-link
  5    306 fe80::/64                On-link
  5    306 fe80::141d:f9cf:aa41:1751/128
                                    On-link
  4    266 fe80::a98a:296c:422c:9ee0/128
                                    On-link
  1    306 ff00::/8                 On-link
  4    266 ff00::/8                 On-link
  5    306 ff00::/8                 On-link
===========================================================================
```

netstat-r per mostrare le routing tables con le routing attive. In questo caso riusciamo a constatare che l'ip del gateway è 10.0.2.2

Apro poi un altra powershell con permessi da amministratore e richiedo il comando netstat -abno ed in contemporanea apro il Task Manager>Dettagli per visualizzare i servizi in esecuzione e confrontarli tra le due.

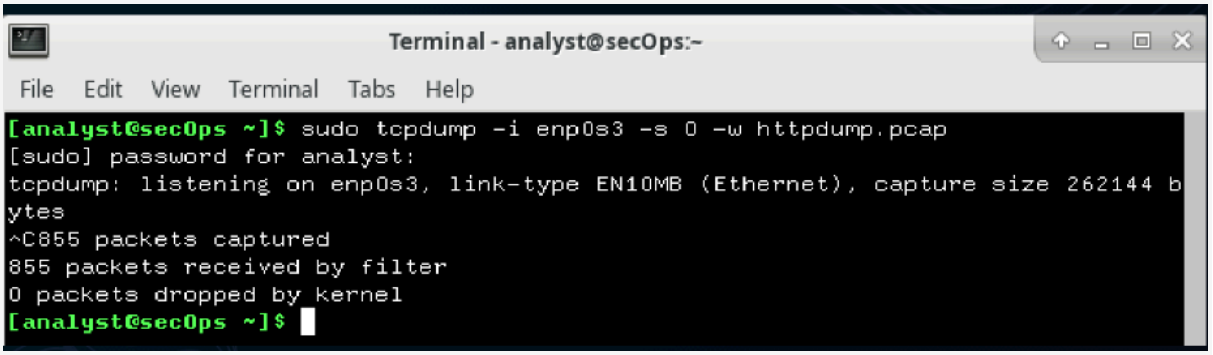


Il Pid 904 è associato con svchost.exe in esecuzione, il nome utente è servizio di rete ed occupa una memoria di 5,124 k.

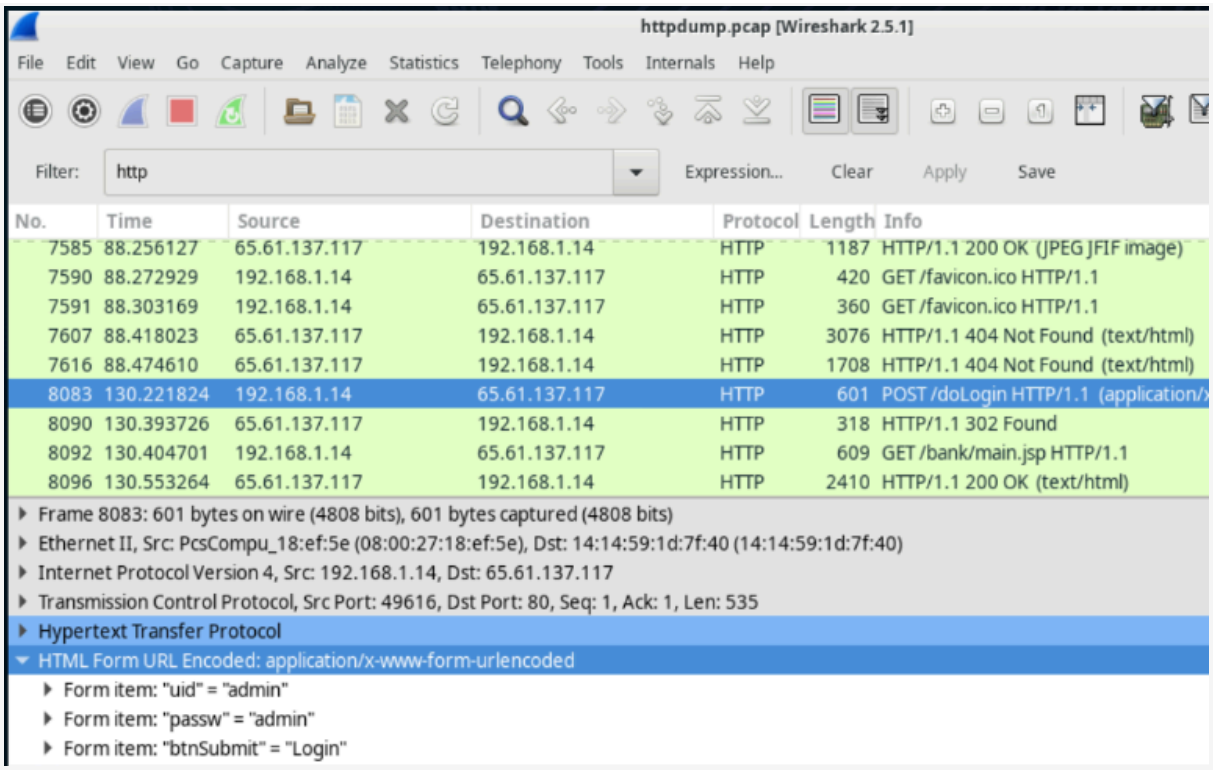


Laboratorio - Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

Sulla macchina CyberOps VM andiamo ad eseguire il seguente comando: `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`
ci mettiamo in ascolto su una determinata porta o interfaccia salvando poi un file denominato “httpdump.pcap”
Ci colleghiamo in HTTP su un sito ed effettuando il login.



tramite wireshark ci risulteranno in chiaro le credenziali di accesso del login

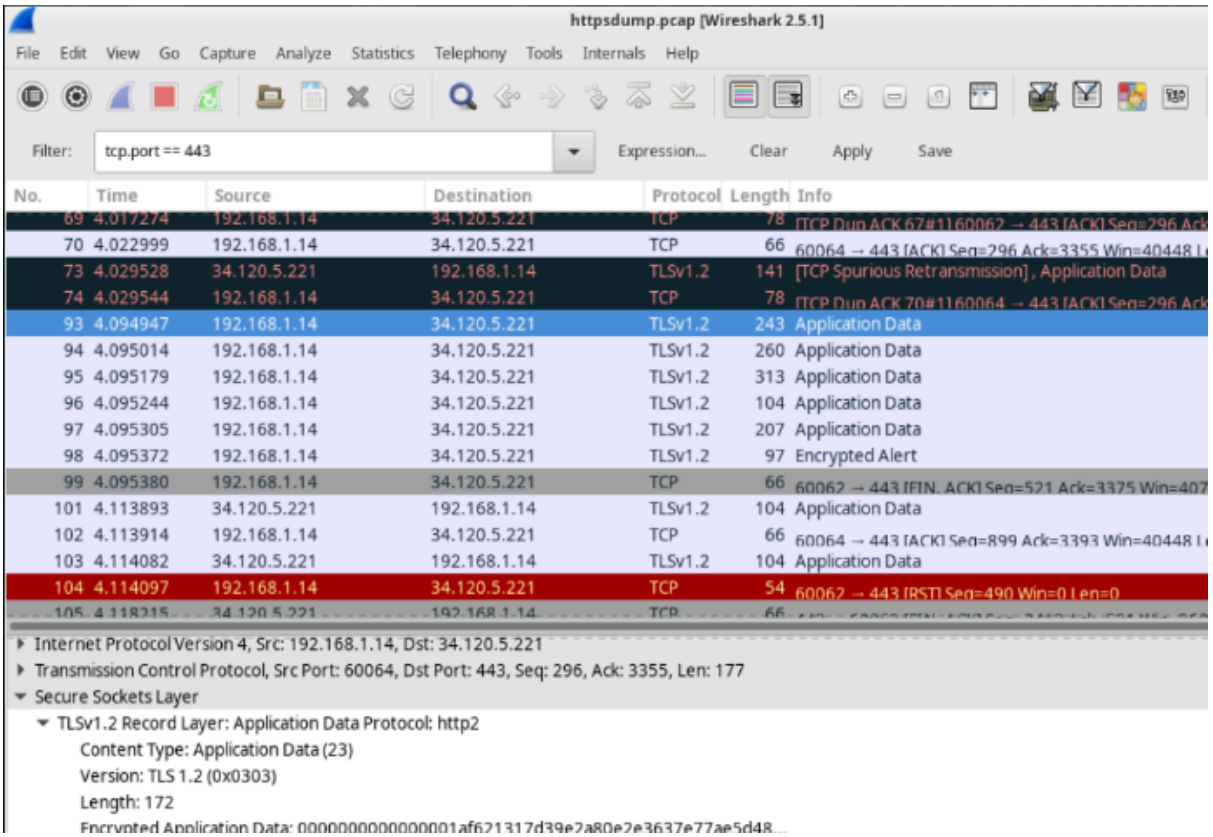


Stesso procedimento lo svolgo per il traffico HTTPS e le differenze tra traffico criptato e non.

Con il comando `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap` saremo di nuovo in ascolto e svolgiamo la stessa procedura fatta con HTTP.

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture
ytes
^C1753 packets captured
1753 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

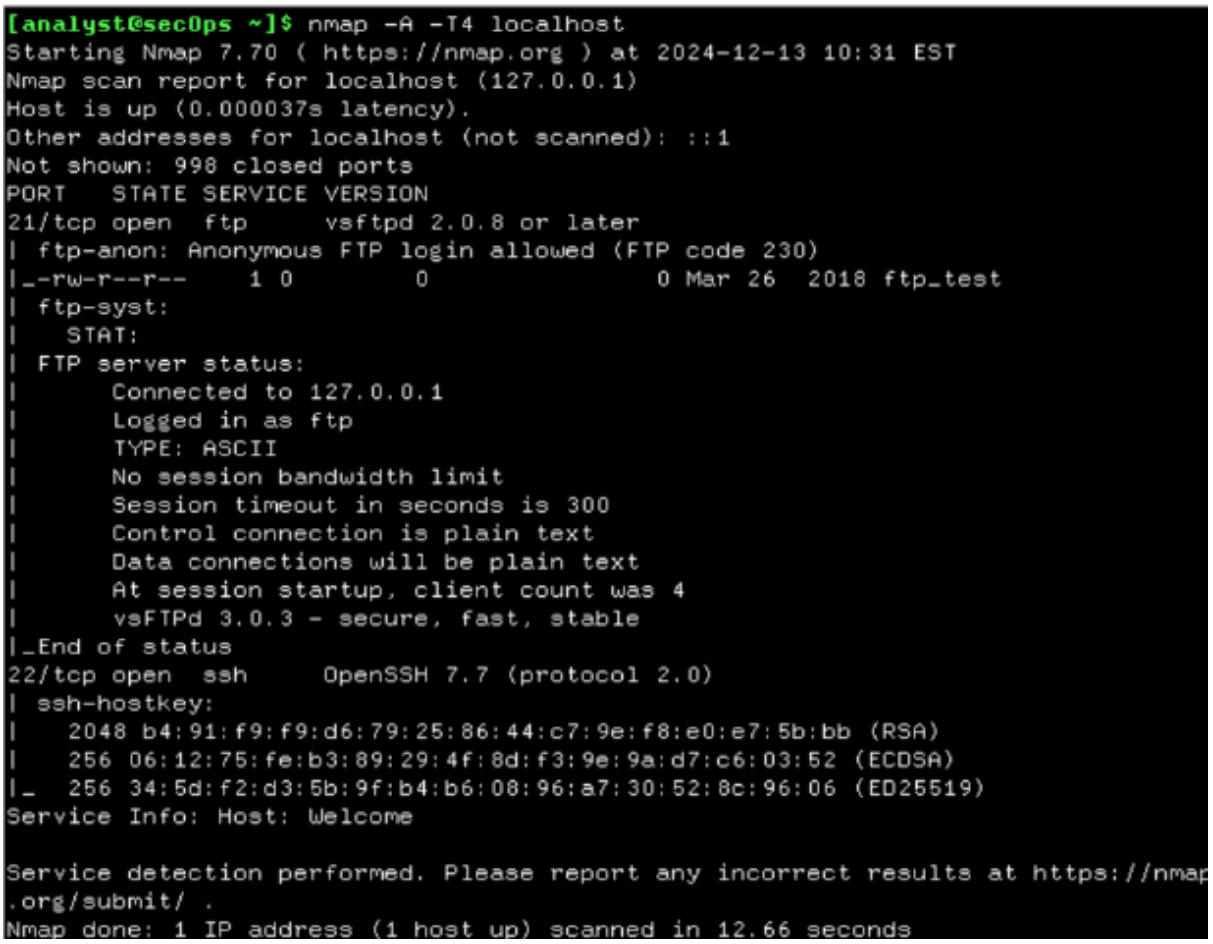
catturiamo il traffico e vediamo una netta differenza rispetto ad HTTP, qui nessun dettaglio del collegamento è visibile.



Nmap Bonus 1

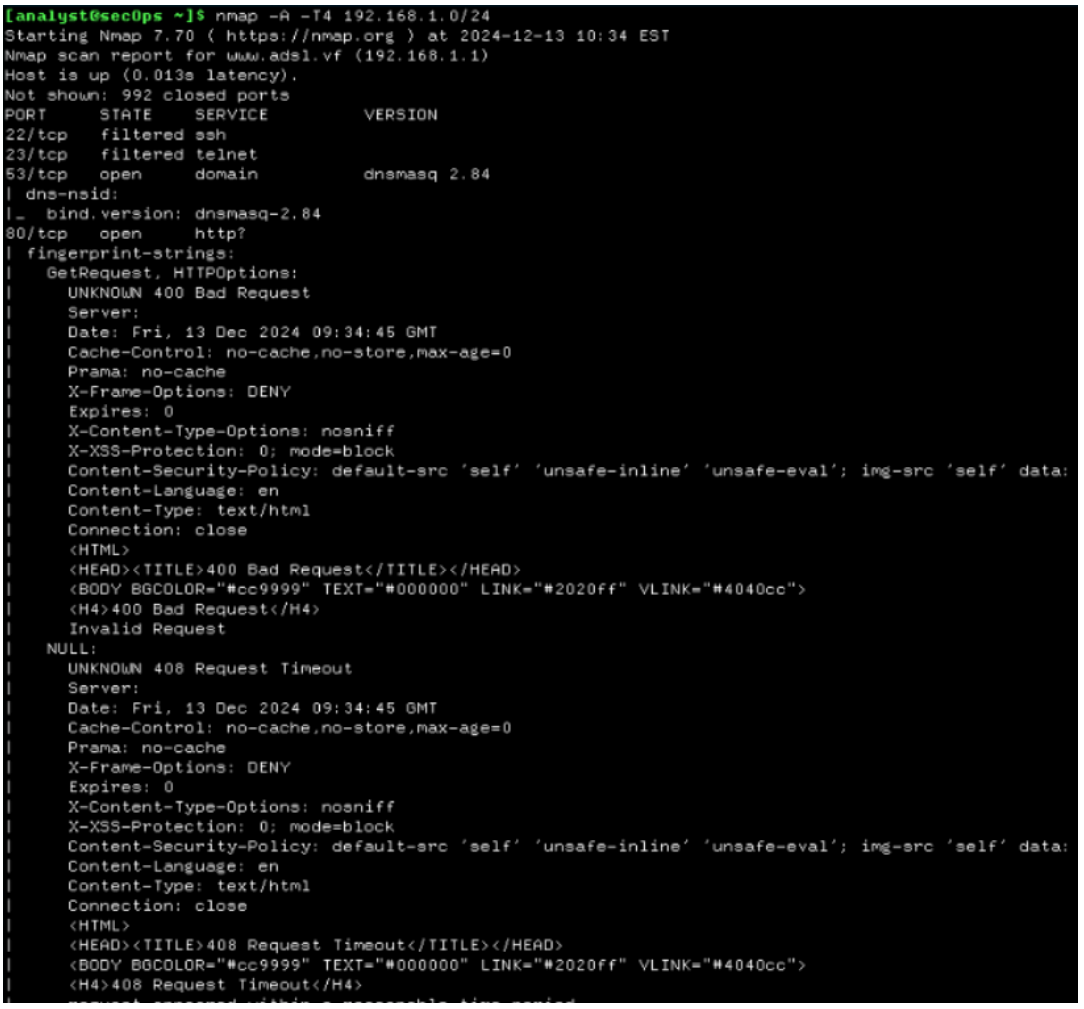
Usando il comando nmap -A -T4 localhost (localhost 127.0.0.1) andiamo ad impostare una scansione avanzata in modo che ci restituisca piu info possibili e con t4 andiamo ad aumentare la velocità.

Le porte aperte dalla scansione sono la 21 e 22.



```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:31 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000037s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 127.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.66 seconds
```

Scansione della sottorete sempre con lo stesso comando cambiando solo l'ip:



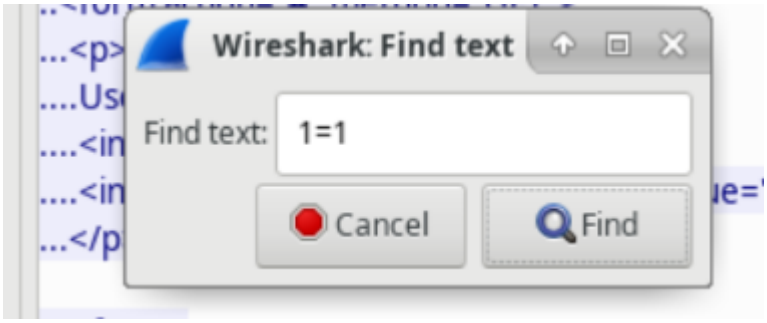
```
[analyst@secOps ~]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:34 EST
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.013s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE         VERSION
22/tcp   filtered ssh
23/tcp   filtered telnet
53/tcp   open     domain          dnsmasq 2.84
| dns-nsid:
|_  bind.version: dnsmasq-2.84
80/tcp   open     http?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     UNKNOWN 400 Bad Request
|     Server:
|     Date: Fri, 13 Dec 2024 09:34:45 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Prama: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 0; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:
|     Content-Language: en
|     Content-Type: text/html
|     Connection: close
|     <HTML>
|     <HEAD><TITLE>400 Bad Request</TITLE></HEAD>
|     <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
|     <H4>400 Bad Request</H4>
|     Invalid Request
|   NULL:
|     UNKNOWN 408 Request Timeout
|     Server:
|     Date: Fri, 13 Dec 2024 09:34:45 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Prama: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 0; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:
|     Content-Language: en
|     Content-Type: text/html
|     Connection: close
|     <HTML>
|     <HEAD><TITLE>408 Request Timeout</TITLE></HEAD>
|     <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
|     <H4>408 Request Timeout</H4>
```

Per la terza richiesta scansioniamo il server web target: scanme.nmap.org

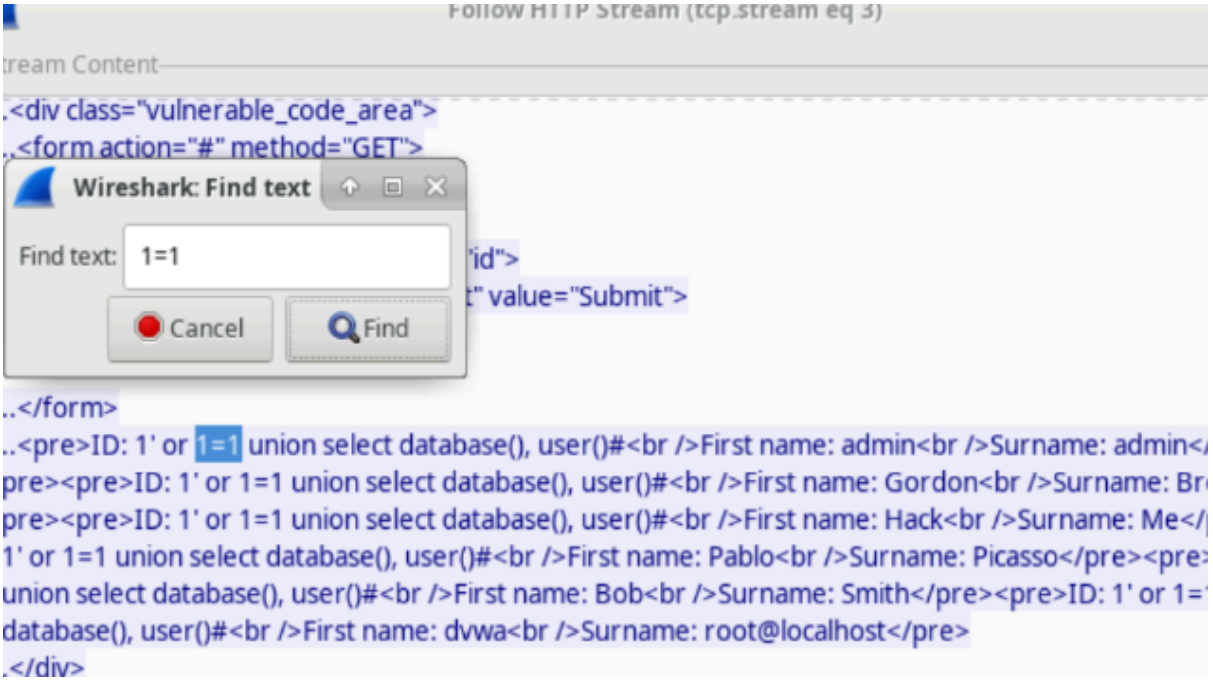
```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:42 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:
Not shown: 995 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubun
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
53/tcp    open  domain     dnsmasq 2.84
| dns-nsid:
|_  bind.version: dnsmasq-2.84
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 44.58 seconds
```

Wireshark and My SQL

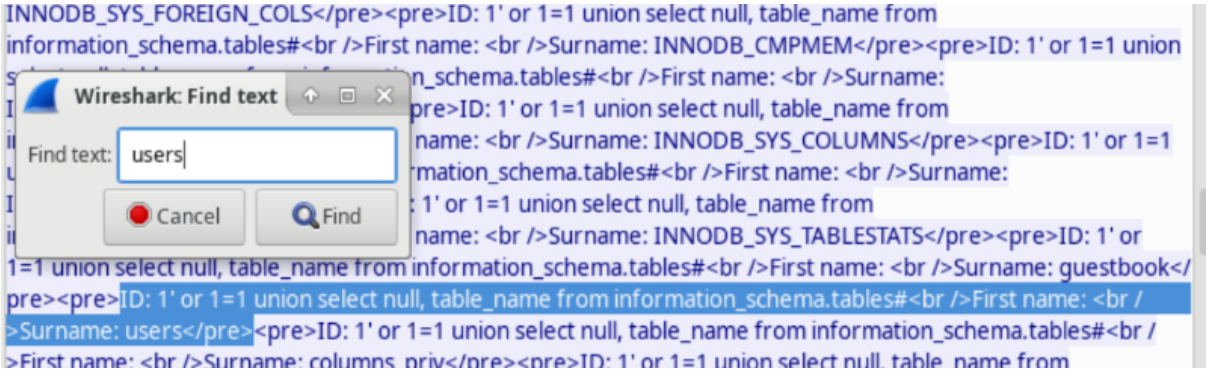
Pertanto dai due indirizzi ip coinvolti 10.0.2.4 (attaccante) e 10.0.2.15 (vittima) andiamo ad aprire una sessione su wireshark per HTTP che ci darà in chiaro la conversazione tra macchina vittima e server.
L'attaccante ha inviato una richiesta per testare se l'applicazione fosse vulnerabile ad un SQL con il comando 1=1 nel campo userID.



A seguire l'attaccante ha utilizzato una query per ottenere piu info dal database.



Ha cercato poi di ottenere una lista delle tabelle del database



ed utilizzato una query per recuperare username e password dalla tabella users.