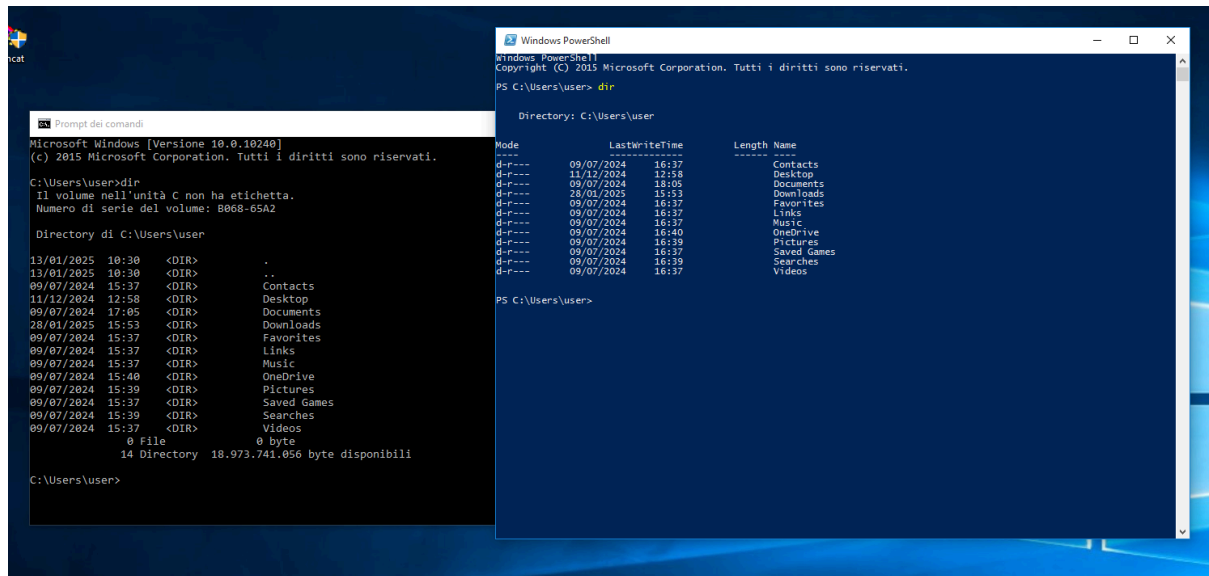


## Esame S11L5

## Laboratorio - Utilizzo di Windows PowerShell

Data una macchina windows sono andata a svolgere i comandi richiesti dall'esercizio guidato.

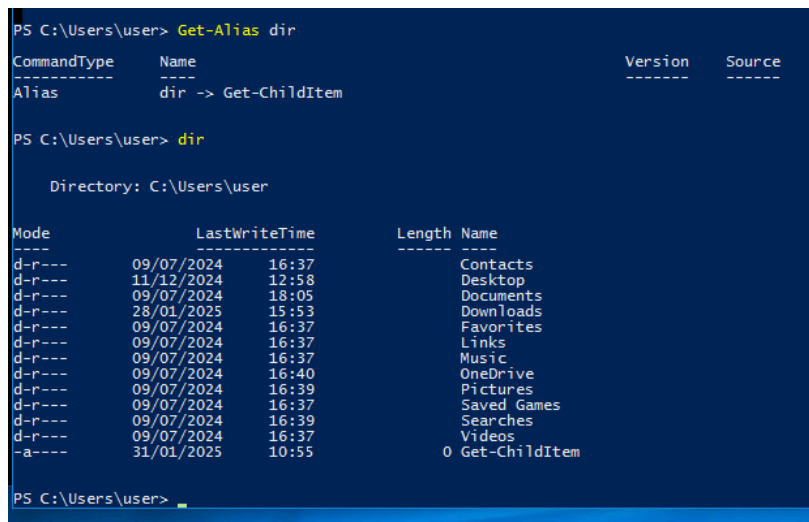
Ho aperto Powershell e Command Prompt e richiesto il comando dir



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-ChildItem 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 e0 Microsoft ISATAP Adapter
5...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
=====
Route permanenti:

```

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

Apri 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.

The screenshot shows two windows. On the left, a Windows PowerShell window displays the output of the `netstat -abno` command, listing active connections. On the right, the Windows Task Manager window shows the 'Dettagli' tab, displaying a list of running processes.

Nome	PID	Stato	Nome utente	CPU	Memoria (K)	Descrizione
services.exe	528	In esecuzione	SYSTEM	00	1.980 K	App Servizi e Contro...
ShellExperienceHost.exe	4160	Sospeso	user	00	12.720 K	Windows Shell Exper...
svchost.exe	3160	In esecuzione	user	00	2.600 K	Shell Infrastructure ...
smss.exe	272	In esecuzione	SYSTEM	00	100 K	Gestione sessioni di ...
snmp.exe	2220	In esecuzione	SYSTEM	00	668 K	Servizio SNMP
spoolsv.exe	1588	In esecuzione	SYSTEM	00	1.108 K	Applicazione sottos...
svchost.exe	640	In esecuzione	SYSTEM	00	2.932 K	Processo host per se...
svchost.exe	692	In esecuzione	SERVIZIO ...	00	2.380 K	Processo host per se...
svchost.exe	896	In esecuzione	SYSTEM	01	10.688 K	Processo host per se...
svchost.exe	904	In esecuzione	SERVIZIO ...	00	5.124 K	Processo host per se...
svchost.exe	928	In esecuzione	SERVIZIO L...	01	7.664 K	Processo host per se...
svchost.exe	960	In esecuzione	SERVIZIO L...	00	944 K	Processo host per se...
svchost.exe	428	In esecuzione	SERVIZIO L...	00	4.012 K	Processo host per se...
svchost.exe	796	In esecuzione	SYSTEM	00	29.408 K	Processo host per se...
svchost.exe	1692	In esecuzione	SERVIZIO L...	00	3.728 K	Processo host per se...
svchost.exe	1732	In esecuzione	SYSTEM	00	772 K	Processo host per se...
svchost.exe	1748	In esecuzione	SYSTEM	00	2.604 K	Processo host per se...
svchost.exe	1412	In esecuzione	SERVIZIO L...	00	288 K	Processo host per se...
svchost.exe	2440	In esecuzione	SYSTEM	00	2.040 K	Processo host per se...
svchost.exe	2540	In esecuzione	SYSTEM	00	804 K	Processo host per se...
svchost.exe	4212	In esecuzione	SERVIZIO ...	00	356 K	Processo host per se...
svchost.exe	948	In esecuzione	user	00	1.040 K	Processo host per se...
System	4	In esecuzione	SYSTEM	00	2.696 K	NT Kernel & System

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.

The screenshot shows a Windows PowerShell window where the command `clear-recyclebin` is being executed. The command prompt shows the command being entered and the confirmation prompt.

```
PS C:\Windows\system32> clear-recyclebin

Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[Y] S [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S
PS C:\Windows\system32>
```

## 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.

The screenshot shows a terminal window with the command `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap` being executed. The output shows the command being run, the password being entered, and the status of the capture.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C855 packets captured
855 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

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

httpdump.pcap [Wireshark 2.5.1]

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
7585	88.256127	65.61.137.117	192.168.1.14	HTTP	1187	HTTP/1.1 200 OK (JPEG JFIF image)
7590	88.272929	192.168.1.14	65.61.137.117	HTTP	420	GET /favicon.ico HTTP/1.1
7591	88.303169	192.168.1.14	65.61.137.117	HTTP	360	GET /favicon.ico HTTP/1.1
7607	88.418023	65.61.137.117	192.168.1.14	HTTP	3076	HTTP/1.1 404 Not Found (text/html)
7616	88.474610	65.61.137.117	192.168.1.14	HTTP	1708	HTTP/1.1 404 Not Found (text/html)
8083	130.221824	192.168.1.14	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
8090	130.393726	65.61.137.117	192.168.1.14	HTTP	318	HTTP/1.1 302 Found
8092	130.404701	192.168.1.14	65.61.137.117	HTTP	609	GET /bank/main.jsp HTTP/1.1
8096	130.553264	65.61.137.117	192.168.1.14	HTTP	2410	HTTP/1.1 200 OK (text/html)

▶ Frame 8083: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)  
 ▶ Ethernet II, Src: PcsCompu\_18:ef:5e (08:00:27:18:ef:5e), Dst: 14:14:59:1d:7f:40 (14:14:59:1d:7f:40)  
 ▶ Internet Protocol Version 4, Src: 192.168.1.14, Dst: 65.61.137.117  
 ▶ Transmission Control Protocol, Src Port: 49616, Dst Port: 80, Seq: 1, Ack: 1, Len: 535  
 ▶ Hypertext Transfer Protocol  
 ▼ HTML Form URL Encoded: application/x-www-form-urlencoded  
 ▶ Form item: "uid" = "admin"  
 ▶ Form item: "passwd" = "admin"  
 ▶ Form item: "btnSubmit" = "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 size 65535 bytes
^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.

htpsdump.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port == 443 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
69	4.017274	192.168.1.14	34.120.5.221	TCP	78	TCP Dup ACK 67#1160062 → 443 [ACK] Seq=296 Ack=3355 Win=0 Len=0
70	4.022999	192.168.1.14	34.120.5.221	TCP	66	60064 → 443 [ACK] Seq=296 Ack=3355 Win=40448 Len=0
73	4.029528	34.120.5.221	192.168.1.14	TLSv1.2	141	[TCP Spurious Retransmission], Application Data
74	4.029544	192.168.1.14	34.120.5.221	TCP	78	TCP Dup ACK 70#1160064 → 443 [ACK] Seq=296 Ack=3355 Win=0 Len=0
93	4.094947	192.168.1.14	34.120.5.221	TLSv1.2	243	Application Data
94	4.095014	192.168.1.14	34.120.5.221	TLSv1.2	260	Application Data
95	4.095179	192.168.1.14	34.120.5.221	TLSv1.2	313	Application Data
96	4.095244	192.168.1.14	34.120.5.221	TLSv1.2	104	Application Data
97	4.095305	192.168.1.14	34.120.5.221	TLSv1.2	207	Application Data
98	4.095372	192.168.1.14	34.120.5.221	TLSv1.2	97	Encrypted Alert
99	4.095380	192.168.1.14	34.120.5.221	TCP	66	60062 → 443 [FIN, ACK] Seq=521 Ack=3375 Win=40736 Len=0
101	4.113893	34.120.5.221	192.168.1.14	TLSv1.2	104	Application Data
102	4.113914	192.168.1.14	34.120.5.221	TCP	66	60064 → 443 [ACK] Seq=899 Ack=3393 Win=40448 Len=0
103	4.114082	34.120.5.221	192.168.1.14	TLSv1.2	104	Application Data
104	4.114097	192.168.1.14	34.120.5.221	TCP	54	60062 → 443 [RST] Seq=490 Win=0 Len=0
105	4.118715	34.120.5.221	192.168.1.14	TCP	66	443 → 60062 [ACK] Seq=3393 Ack=899 Win=0 Len=0

▶ Internet Protocol Version 4, Src: 192.168.1.14, Dst: 34.120.5.221

▶ Transmission Control Protocol, Src Port: 60064, Dst Port: 443, Seq: 296, Ack: 3355, Len: 177

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http2

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 172

Encrypted Application Data: 0000000000000001af621317d39e2a80e2e3637e77ae5d48...

## 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@sec0ps ~]$ 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>
```



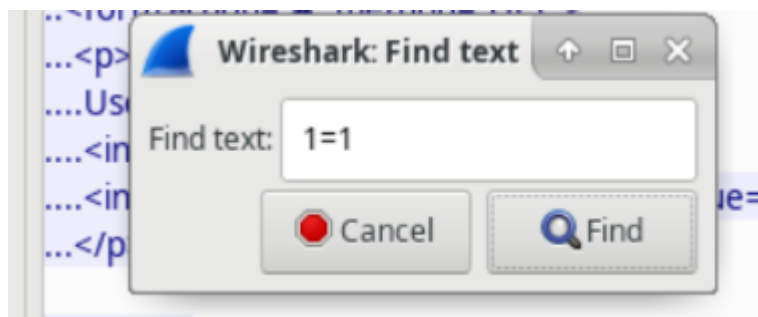
Per la terza richiesta scansioniamo il server web target:  
scanme.nmap.org

```
[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 (Ubuntu)
| 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
```

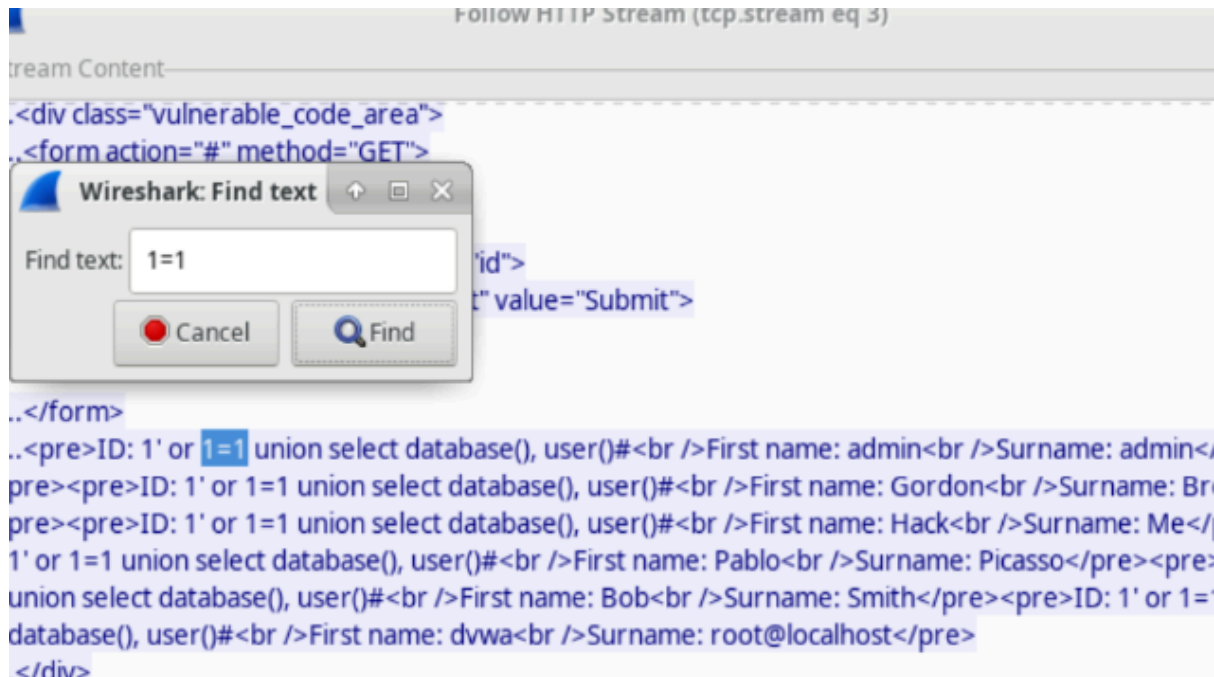
## Wireshark and My SQL

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.

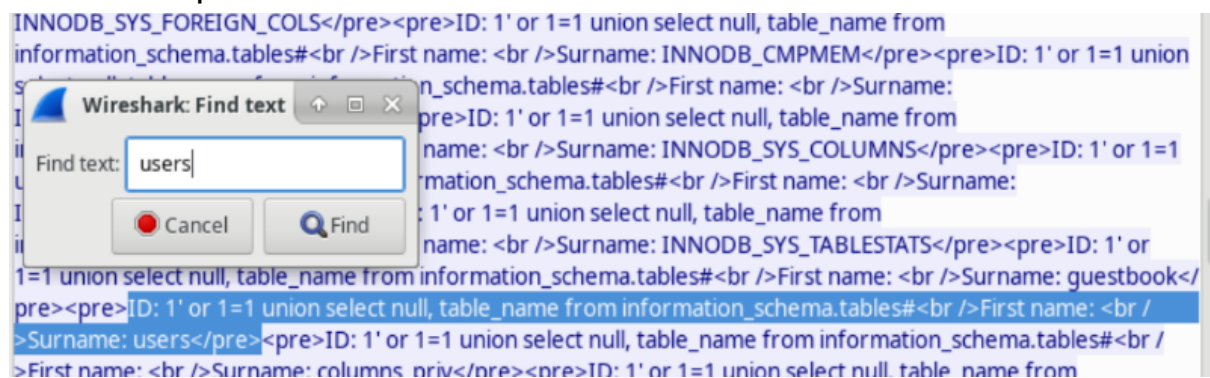


A seguire l'attaccante ha utilizzato una query per ottenere più info dal database.





Ha cercato poi di ottenere una lista delle tabelle del database



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