

# Progetto

## Laboratorio - Utilizzo di Windows PowerShell

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell.

### Obiettivi

---

L'obiettivo del lab è esplorare alcune delle funzioni di PowerShell.

- **Parte 1: Accedere alla console di PowerShell.**
- **Parte 2: Esplora il prompt dei comandi e i comandi di PowerShell.**
- **Parte 3: Esplorare i cmdlet.**
- **Parte 4: Esplorare il comando netstat usando PowerShell.**
- **Parte 5: Svuotare il cestino utilizzando PowerShell.**

### Contesto / Scenario

---

PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo lab si userà la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell dispone anche di funzioni in grado di creare script per automatizzare le attività e lavorare insieme al sistema operativo Windows.

### Risorse necessarie

---

- 1 PC Windows con PowerShell installato e accesso a Internet

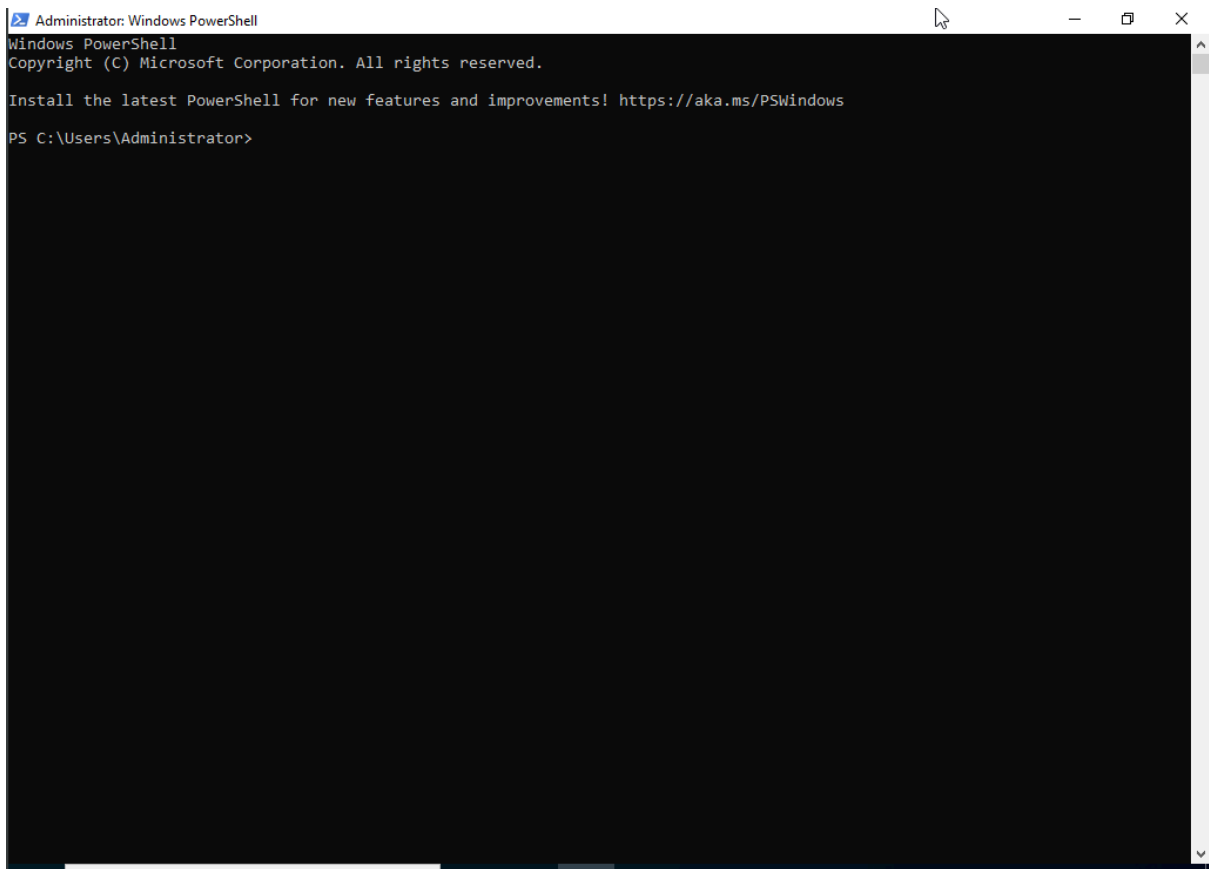
### Disposizioni

---

#### **Parte 1: Accedere alla console di PowerShell.**

Fare clic su **Avvia**. Cerca e seleziona **PowerShell**.

Fare clic su **Start**. Cerca e seleziona il **prompt dei comandi**.



## Parte 2: Esplora il prompt dei comandi e i comandi di PowerShell.

Immettere **dir** al prompt in entrambe le finestre.

```
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

Quali sono gli output del comando? **dir**

Entrambe le finestre forniscono un elenco di sottodirectory e file e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell vengono visualizzati anche gli attributi/le modalità.

Prova un altro comando che hai utilizzato nel prompt dei comandi, come **ping**, **cd** e **ipconfig**.

```

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>

```

Quali sono i risultati?

L'output in entrambe le finestre è simile.

### Parte 3: Esplorare i cmdlet.

I comandi di PowerShell, cmdlets, vengono costruiti sotto forma di stringa *verbo-sostantivo*. Per identificare il comando di PowerShell per elencare le sottodirectory e i file in una directory, immettere **Get-Alias dir** al prompt di PowerShell.

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

CommandType	Name	Version	Source
Alias	dir -> Get-ChildItem		

Qual è il comando PowerShell per **dir**?

## Get-ChildItem

Per informazioni più dettagliate sui cmdlet, eseguire una ricerca su Internet per i **cmdlet di Microsoft PowerShell**.

The screenshot shows the PowerShell documentation website. The top navigation bar includes links like 'Panoramica', 'DSC', 'PowerShellGet', 'Moduli di utilità', 'Browser dei moduli', 'API Browser', and 'Più'. The main header shows 'PowerShell 7.5' and a search filter. The left sidebar lists various topics under 'Scrittura di un cmdlet di PowerShell', with 'Cenni preliminari sui cmdlet' selected. The main content area is titled 'Cenni preliminari sui cmdlet' and includes a table of contents with links to 'Cmdlet', 'Termini dei cmdlet', 'Differenze tra i cmdlet e i comandi', and 'Classi di base dei cmdlet'. The main text explains that a cmdlet is a lightweight command used in the PowerShell environment, and it is called by the PowerShell runtime in the context of automation scripts. It also mentions that cmdlets can be binary (C#), advanced script functions, CDXML, or workflow flows.

Al termine, chiudere la finestra del prompt dei comandi.

## Parte 4: Esplorare il comando netstat usando PowerShell.

Al prompt di PowerShell, immettere per visualizzare le opzioni disponibili per il comando **netstat -h**

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

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables host
           multiple independent components, and in these cases the
           sequence of components involved in creating the connection
           or listening port is displayed. In this case the executable
           name is in [] at the bottom, on top is the component it called,
           and so forth until TCP/IP was reached. Note that this option
           can be time-consuming and will fail unless you have sufficient
           permissions.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-i          Displays the time spent by a TCP connection in its current state.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
           be associated with an active connection.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
           the -p option may be used to specify a subset of the default.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
           endpoints.
-y          Displays the TCP connection template for all connections.
```

Per visualizzare la tabella di routing con i percorsi attivi, immettere al prompt **netstat -r**

```

PS C:\Users\Administrator> netstat -r
=====
Interface List
  9...08 00 27 ec ed 94 .....Intel(R) PRO/1000 MT Desktop Adapter
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.50.1     192.168.50.2     281
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
192.168.50.0                255.255.255.0    On-link          192.168.50.2     281
192.168.50.2                255.255.255.255  On-link          192.168.50.2     281
192.168.50.255              255.255.255.255  On-link          192.168.50.2     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.50.2     281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.50.2     281
=====
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
  0.0.0.0                  0.0.0.0    192.168.50.1    Default
=====

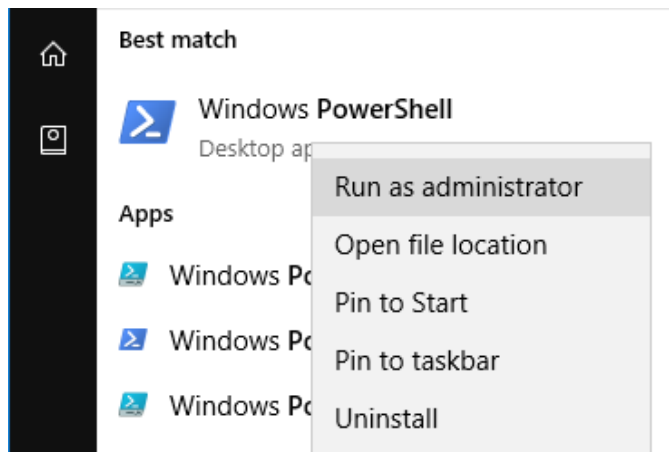
IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    331 ::1/128                      On-link
9    281 fe80::/64                  On-link
9    281 fe80::f108:973a:94cf:70b3/128
                                     On-link
1    331 ff00::/8                      On-link
9    281 ff00::/8                      On-link
=====
Persistent Routes:
None

```

Che cos'è il gateway IPv4?

Le risposte possono variare. In questo esempio, il gateway è 192.168.50.1.

Aprire ed eseguire un secondo PowerShell con privilegi elevati. Fare clic su **Avvia**. Cerca PowerShell e fai clic con il pulsante destro del mouse su **Windows PowerShell** e seleziona **Esegui come amministratore**. Fare clic su **Sì** per consentire all'app di apportare modifiche al dispositivo.



nb: nel nostro caso siamo già Administrator.

Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Immettere il al prompt. **netstat -abno**

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

Active Connections

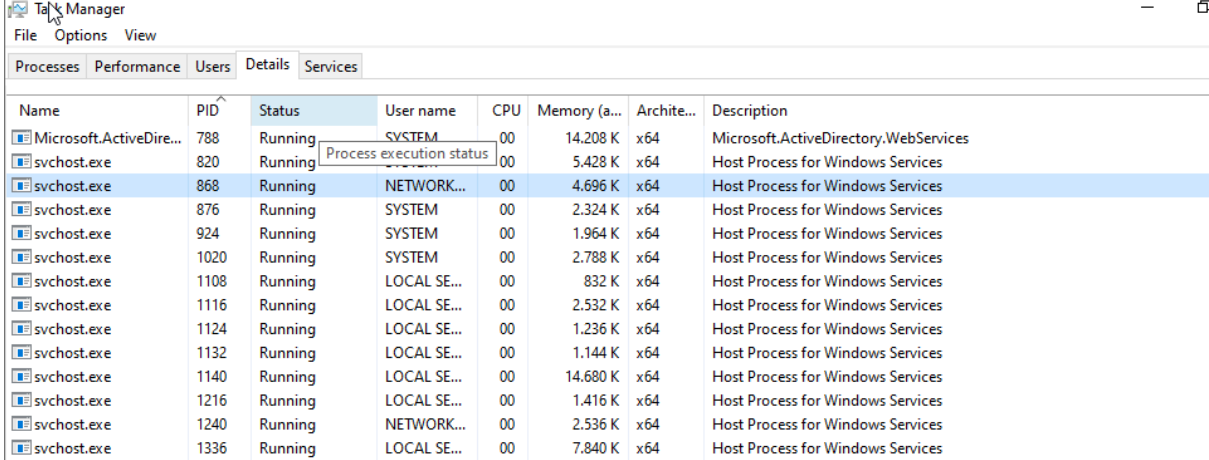
  Proto Local Address           Foreign Address         State       PID
  TCP    0.0.0.0:88              0.0.0.0:0               LISTENING   628
  [lsass.exe]
  TCP    0.0.0.0:135             0.0.0.0:0               LISTENING   868
  RpcSs
  [svchost.exe]
  TCP    0.0.0.0:389             0.0.0.0:0               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
```

Apri il Task Manager. Passare alla scheda **Dettagli**. Fare clic sull'intestazione **PID** in modo che i PID siano in ordine.



Selezionare uno dei PID dai risultati di netstat -abno. In questo esempio viene utilizzato il PID 868.

Individua il PID selezionato nel Task Manager. Fare clic con il pulsante destro del mouse sul PID selezionato in Gestione attività per aprire la finestra di dialogo **Proprietà** per ulteriori informazioni.



Name	PID	Status	User name	CPU	Memory (a...	Archite...	Description
Microsoft.ActiveDire...	788	Running	SYSTEM	00	14.208 K	x64	Microsoft.ActiveDirectory.WebServices
svchost.exe	820	Running	SYSTEM	00	5.428 K	x64	Host Process for Windows Services
svchost.exe	868	Running	NETWORK...	00	4.696 K	x64	Host Process for Windows Services
svchost.exe	876	Running	SYSTEM	00	2.324 K	x64	Host Process for Windows Services
svchost.exe	924	Running	SYSTEM	00	1.964 K	x64	Host Process for Windows Services
svchost.exe	1020	Running	SYSTEM	00	2.788 K	x64	Host Process for Windows Services
svchost.exe	1108	Running	LOCAL SE...	00	832 K	x64	Host Process for Windows Services
svchost.exe	1116	Running	LOCAL SE...	00	2.532 K	x64	Host Process for Windows Services
svchost.exe	1124	Running	LOCAL SE...	00	1.236 K	x64	Host Process for Windows Services
svchost.exe	1132	Running	LOCAL SE...	00	1.144 K	x64	Host Process for Windows Services
svchost.exe	1140	Running	LOCAL SE...	00	14.680 K	x64	Host Process for Windows Services
svchost.exe	1216	Running	LOCAL SE...	00	1.416 K	x64	Host Process for Windows Services
svchost.exe	1240	Running	NETWORK...	00	2.536 K	x64	Host Process for Windows Services
svchost.exe	1336	Running	LOCAL SE...	00	7.840 K	x64	Host Process for Windows Services

Quali informazioni è possibile ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

PID 868 è associato a svchost.exe processo. L'utente per questo processo è NETWORK SERVICE e utilizza 4696K di memoria.

## Parte 5: Svuotare il cestino utilizzando PowerShell.

I comandi di PowerShell possono semplificare la gestione di una rete di computer di grandi dimensioni. Ad esempio, se si desidera implementare una nuova soluzione di sicurezza in tutti i server della rete, è possibile utilizzare un comando o uno script di PowerShell per implementare e verificare che i servizi siano in esecuzione. È anche possibile eseguire comandi di PowerShell per semplificare le azioni che richiederebbero più passaggi per l'esecuzione utilizzando gli strumenti desktop grafici di Windows.

Apri il Cestino. Verifica che siano presenti elementi che possono essere eliminati definitivamente dal tuo PC. In caso contrario, ripristina quei file.

Se non sono presenti file nel Cestino, creare alcuni file, ad esempio un file di testo utilizzando Blocco note, e inserirli nel Cestino.

In una console di PowerShell, immettere al prompt. `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"): _
```

Cosa è successo ai file nel Cestino?

I file nel Cestino vengono eliminati definitivamente.

## Domanda di riflessione

---

PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Utilizzando Internet, ricerca comandi che potresti utilizzare per semplificare le tue attività di analista della sicurezza. Registra i tuoi risultati.

PowerShell è uno strumento utile per semplificare le attività quotidiane di un analista della sicurezza. Ecco alcuni comandi principali:

- **Get-NetFirewallRule**: visualizza le regole del firewall.
- **netstat -abno**: mostra le connessioni di rete attive.
- **Get-EventLog**: accede ai log di sistema per rilevare attività sospette.
- **Get-Process** e **Stop-Process**: gestisce i processi in esecuzione.
- **New-LocalUser** e **Add-LocalGroupMember**: crea nuovi utenti e gestisce i gruppi.
- **Compress-Archive** e **Move-Item**: automatizza la gestione dei file di log.

Questi comandi ti permettono di monitorare, gestire e rispondere rapidamente alle minacce di sicurezza.

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

In questo laboratorio, completa i seguenti obiettivi:

- Catturare e visualizzare il traffico HTTP
- Catturare e visualizzare il traffico HTTPS

### Obiettivi

---

- **Parte 1: Acquisire e visualizzare il traffico HTTP**
- **Parte 2: Acquisire e visualizzare il traffico HTTPS**

### Contesto / Scenario

---

HyperText Transfer Protocol (HTTP) è un protocollo a livello di applicazione che presenta i dati tramite un browser web. Con HTTP, non esiste alcuna protezione per i dati scambiati tra due dispositivi di comunicazione.

Con HTTPS, la crittografia viene utilizzata tramite un algoritmo matematico. Questo algoritmo nasconde il vero significato dei dati che vengono scambiati. Questa operazione viene eseguita tramite l'uso di certificati che possono essere visualizzati in un secondo momento in questo laboratorio.

Indipendentemente da HTTP o HTTPS, si consiglia di scambiare dati solo con siti Web di cui ci si fida. Solo perché un sito utilizza HTTPS non significa che sia un sito affidabile. Gli attori delle minacce utilizzano comunemente HTTPS per nascondere le loro attività.

In questo laboratorio, esplorerai e acquisirai il traffico HTTP e HTTPS utilizzando Wireshark.

### Risorse necessarie

---

- Kali VM
- Connessione Internet

### Disposizioni

---

## Parte 1: Acquisizione e visualizzazione del traffico HTTP

In questa parte, utilizzerai tcpdump per acquisire il contenuto del traffico HTTP. Utilizzerai le opzioni di comando per salvare il traffico in un file di acquisizione pacchetti (pcap). Questi record possono quindi essere analizzati utilizzando diverse applicazioni che leggono i file pcap, tra cui Wireshark.

Passaggio 1: avviare la macchina virtuale ed effettuare l'accesso.

Avviare la VM Kali. Utilizzare le seguenti credenziali utente:

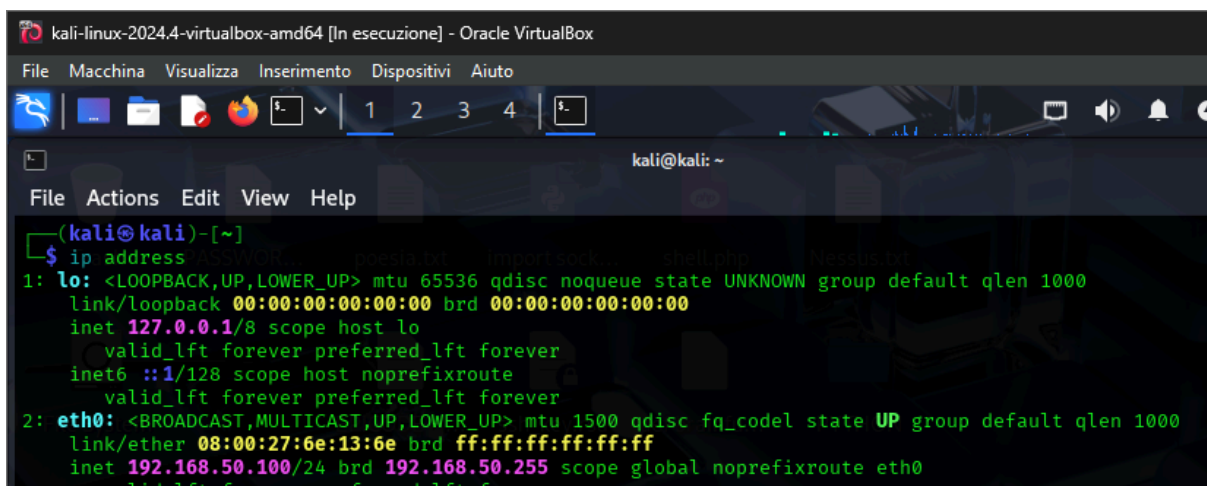
Nome utente: kali

Password: kali

Passaggio 2: apri un terminale e avvia tcpdump.

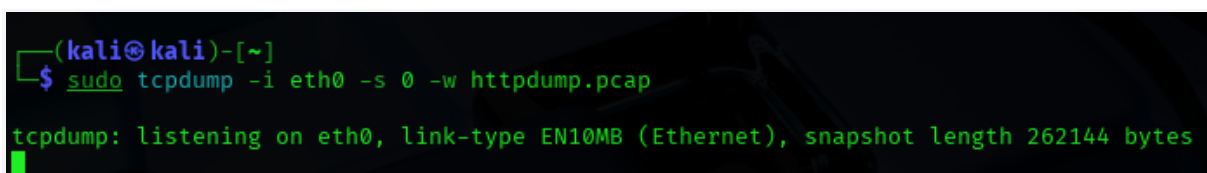
a. Apri un'applicazione terminale e inserisci il comando `.ip address`

b. Elencare le interfacce e i relativi indirizzi IP visualizzati nell'output dell'indirizzo IP.



```
kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
   inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
```

c. Nell'applicazione terminale, immettere il comando `. Immettere la password per Kali quando richiesto.``sudo 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
```

Questo comando avvia tcpdump e registra il traffico di rete sull'interfaccia eth0.

L'opzione di comando consente di specificare l'interfaccia. Se non specificato, tcpdump acquisirà tutto il traffico su tutte le interfacce. **-i**

L'opzione di comando specifica la lunghezza dello snapshot per ogni pacchetto. Dovresti limitare snaplen al numero più piccolo che catturerà le informazioni sul protocollo a cui sei interessato. L'impostazione di snaplen su 0 lo imposta al valore predefinito di 262144, per la compatibilità con le versioni precedenti recenti di tcpdump. **-s**

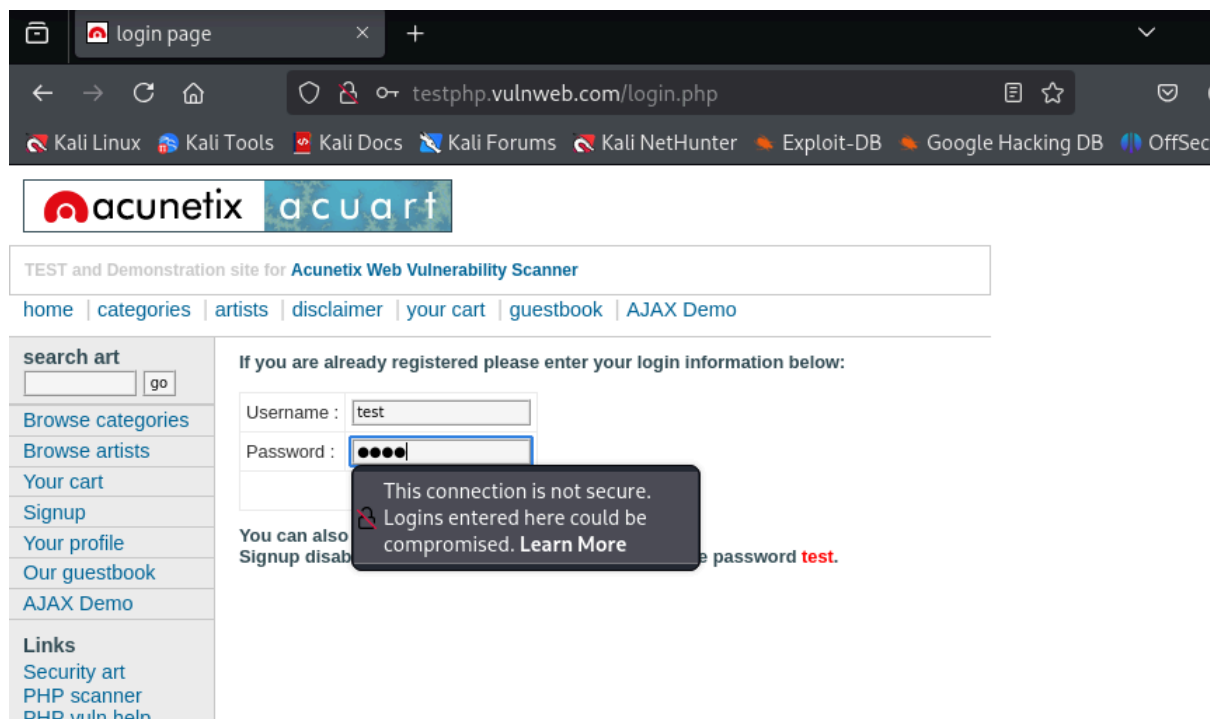
L'opzione command viene utilizzata per scrivere il risultato del comando tcpdump in un file. L'aggiunta dell'estensione .pcap garantisce che i sistemi operativi e le applicazioni siano in grado di leggere su file. Tutto il traffico registrato verrà stampato nel file httpdump.pcap nella home directory dell'analista utente. **-w**

Utilizzare le pagine man per tcpdump per determinare l'uso delle opzioni di comando -s e -w.

d. Aprire un Web browser dalla barra di avvio all'interno della macchina virtuale Kali. Vai a <http://testphp.vulnweb.com/login.php>

e. Inserisci il nome utente Test con la password Test e fai clic su Accedi.

f. Chiudi il browser web.



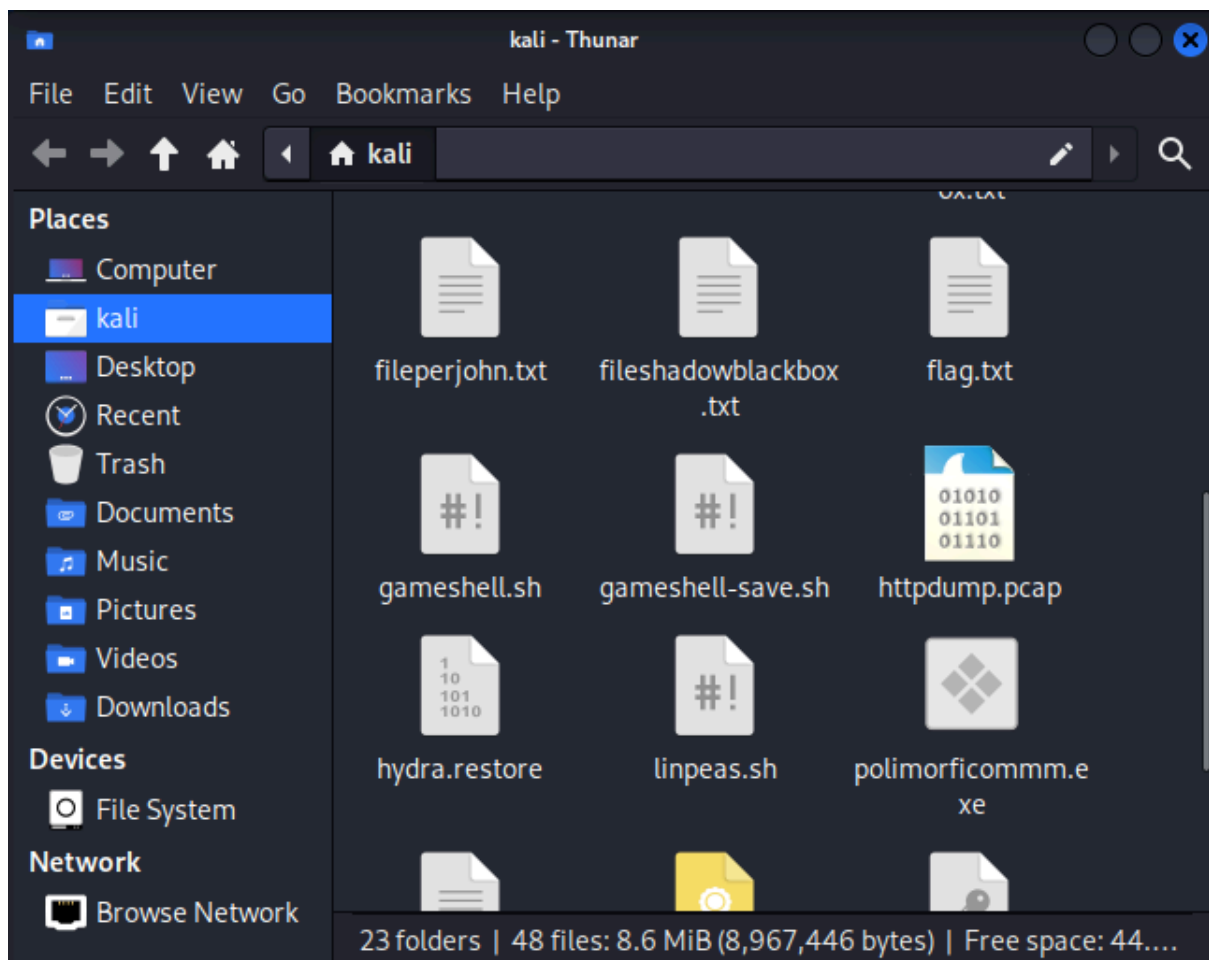
g. Tornare alla finestra del terminale in cui è in esecuzione tcpdump. Immettere CTRL+C per interrompere l'acquisizione del pacchetto.

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C2681 packets captured
2681 packets received by filter
0 packets dropped by kernel
```

Passaggio 3: visualizza l'acquisizione HTTP.

Il tcpdump, eseguito nel passaggio precedente, ha stampato l'output in un file denominato httpdump.pcap. Questo file si trova nel folder di Kali.

a. Fare doppio clic sul file httpdump.pcap.



b. Nell'applicazione Wireshark, filtrare per http e fare clic su Applica.



c. Sfoglia i diversi messaggi HTTP e seleziona il messaggio POST.

d. Nella finestra inferiore viene visualizzato il messaggio. Espandi la sezione URL del modulo HTML codificato: application/x-www-form-urlencoded.

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

Quali sono le due informazioni visualizzate?

### L'uid di Test e la passw di Test

e. Chiudere l'applicazione Wireshark.

## Parte 2: Acquisizione e visualizzazione del traffico HTTPS

A questo punto si utilizzerà tcpdump dalla riga di comando di Kali per acquisire il traffico HTTPS. Dopo aver avviato tcpdump, genererai traffico HTTPS mentre tcpdump registra il contenuto del traffico di rete. Questi record verranno nuovamente analizzati utilizzando Wireshark.

Passaggio 1: avvia tcpdump all'interno di un terminale.

a. Nell'applicazione terminale, immettere il comando . Immettere la password cyberops per l'analista utente quando richiesto. `sudo tcpdump -i eth0 -s 0 -w httpsdump.pcap`

```
(kali@kali)-[~]
$ sudo tcpdump -i eth0 -s 0 -w httpsdump.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

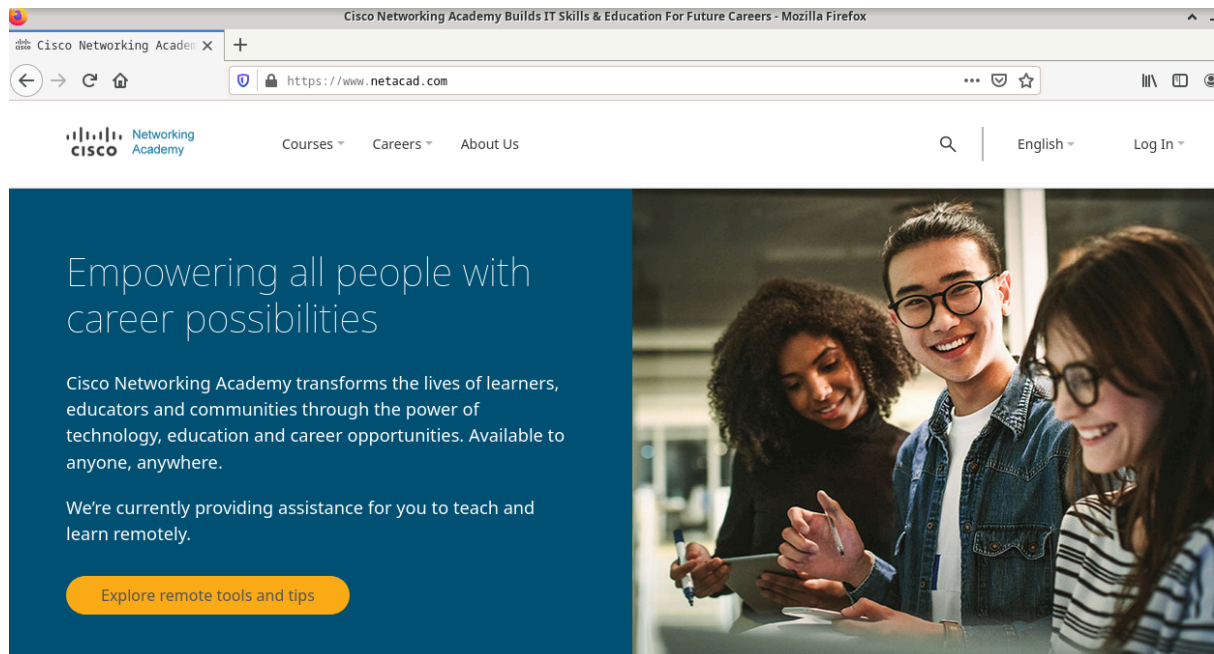
Questo comando avvierà tcpdump e registrerà il traffico di rete sull'interfaccia eth0 della Kali. Se la tua interfaccia è diversa da eth0, modificala quando usi il comando precedente.

Tutto il traffico registrato verrà stampato nel file httpsdump.pcap nel folder di Kali.

b. Aprire un Web browser dalla barra di avvio all'interno della macchina virtuale Kali. Vai a [www.netacad.com](http://www.netacad.com).

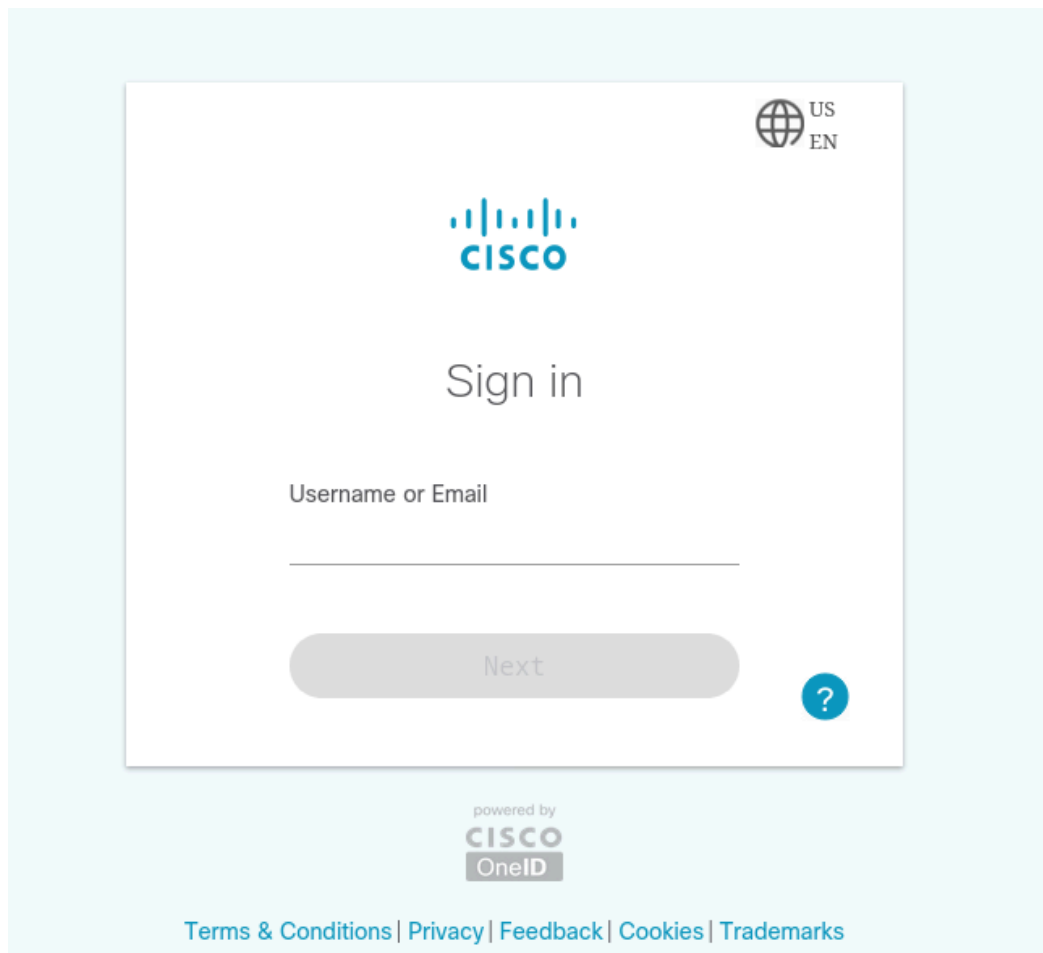
Nota: Se ricevi una pagina Web "Connessione sicura non riuscita", probabilmente significa che la data e l'ora non sono corrette. Aggiorna il giorno e l'ora con il seguente comando, passando al giorno e all'ora correnti:

c. Fare clic su Accedi.



d. Inserisci il tuo nome utente e password NetAcad. Fare clic su Avanti.





e. Chiudere il Web browser nella macchina virtuale.

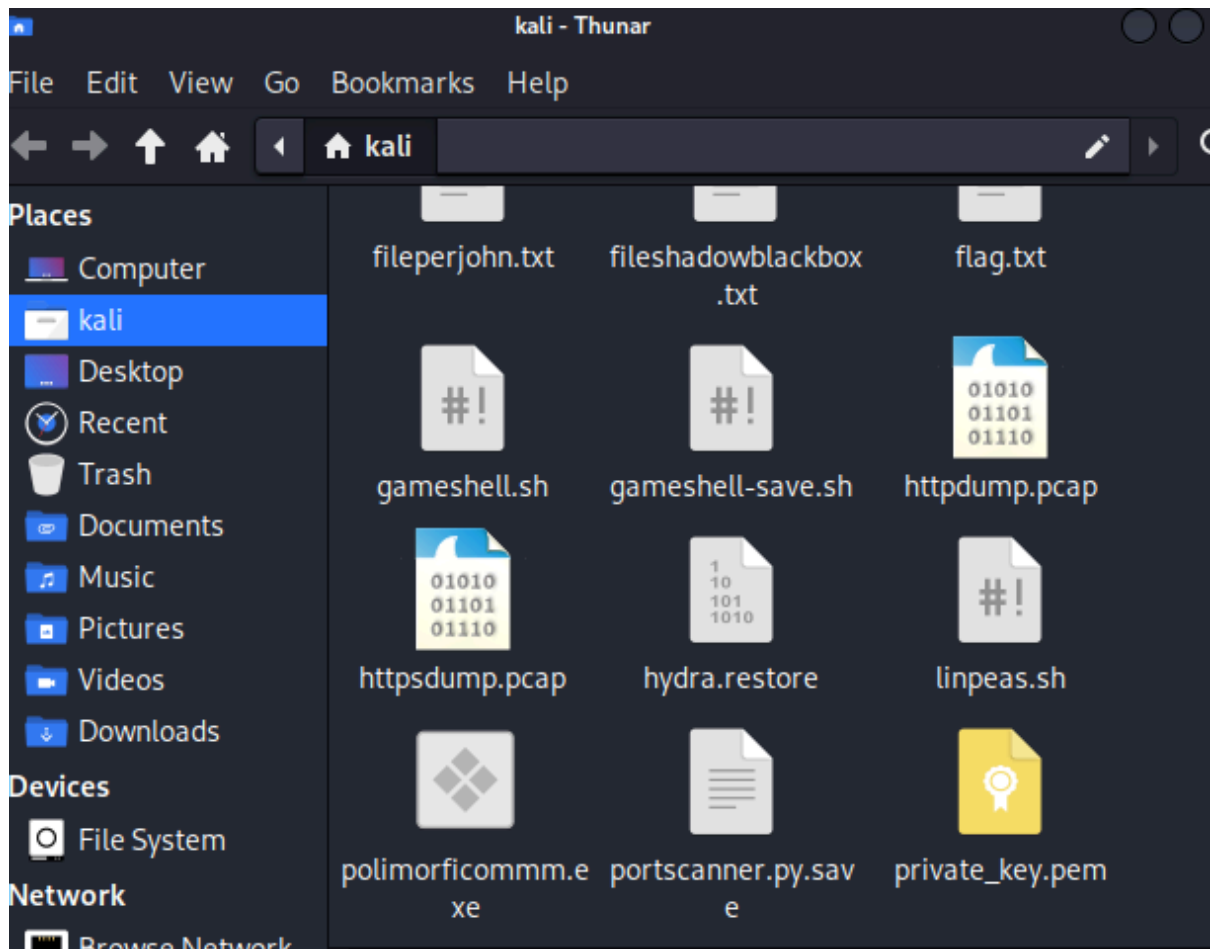
f. Tornare alla finestra del terminale in cui è in esecuzione tcpdump. Immettere CTRL+C per interrompere l'acquisizione del pacchetto.

```
(kali㉿kali)-[~]  
$ sudo tcpdump -i eth0 -s 0 -w httpsdump.pcap  
  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
^C3482 packets captured  
3482 packets received by filter  
0 packets dropped by kernel
```

Passaggio 2: visualizza l'acquisizione HTTPS.

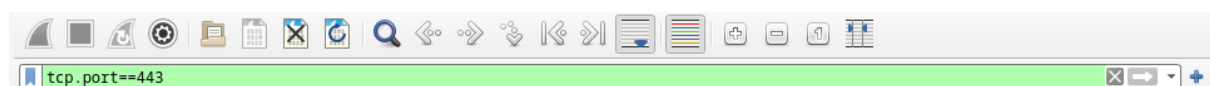
Il tcpdump eseguito nel passaggio 1 ha stampato l'output in un file denominato httpsdump.pcap. Questo file si trova nel folder di Kali.

a. Aprire il file httpsdump.pcap.

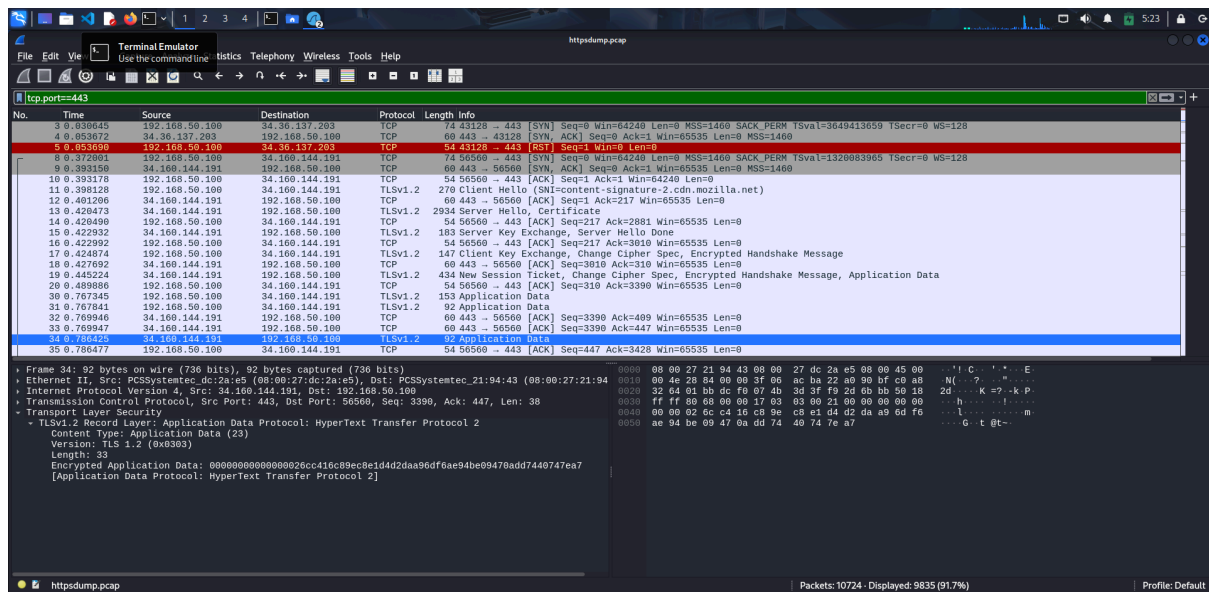


b. Nell'applicazione Wireshark, espandere verticalmente la finestra di acquisizione, quindi filtrare in base al traffico HTTPS tramite la porta 443.

Inserisci `tcp.port==443` come filtro e fai clic su Applica.



c. Sfogliare i diversi messaggi HTTPS e selezionare un messaggio di dati dell'applicazione.

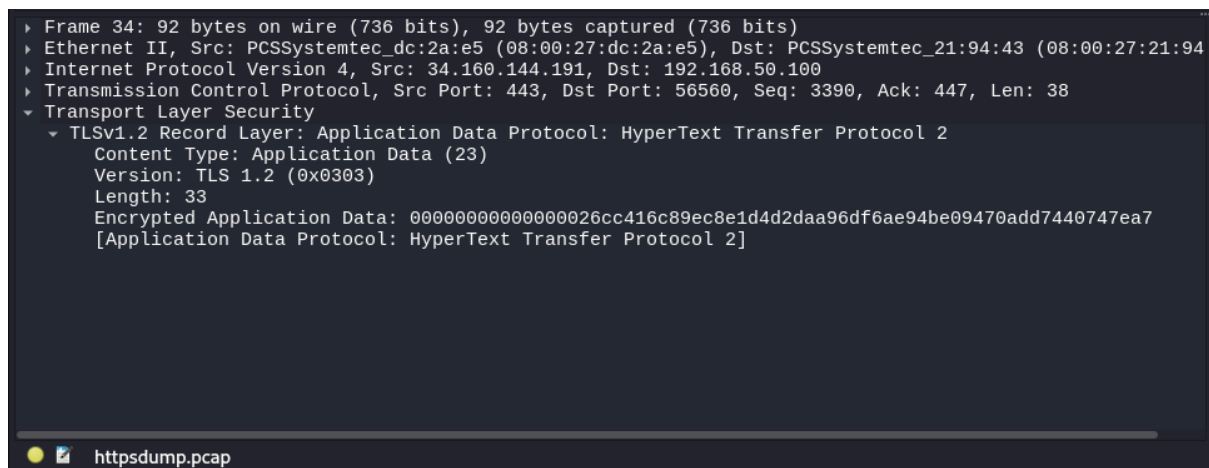


d. Nella finestra inferiore viene visualizzato il messaggio.

Che cosa ha sostituito la sezione HTTP che si trovava nel file di acquisizione precedente?

**Dopo la sezione TCP, ora c'è una sezione Secure Sockets Layer (SSL/TLS 1.2) invece di HTTP.**

e. Espandere completamente la sezione Secure Sockets Layer.



f. Fare clic su Dati dell'applicazione crittografati.

I dati dell'applicazione sono in formato testo normale o leggibile?

**Il payload dei dati viene crittografato utilizzando TLSv1.2 e non può essere visualizzato.**

g. Chiudi tutte le finestre e spegni la macchina virtuale.

## Domande di riflessione

---

### 1. Quali sono i vantaggi dell'utilizzo di HTTPS invece di HTTP?

Quando si utilizza HTTPS, il payload dei dati di un messaggio viene crittografato e può essere visualizzato solo dai dispositivi che fanno parte della conversazione crittografata.

### 2. Tutti i siti web che utilizzano HTTPS sono considerati affidabili?

No, perché i siti Web dannosi possono utilizzare HTTPS per apparire legittimi pur continuando a catturare i dati e gli accessi degli utenti.

## 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

---

- **Parte 1: Esplorare Nmap**
- **Parte 2: Scansione delle porte aperte**

### Contesto / Scenario

---

La scansione delle porte fa solitamente parte di un attacco di ricognizione. È possibile utilizzare una varietà di metodi di scansione delle porte. Esploreremo come utilizzare l'utility Nmap. Nmap è una potente utility di rete che viene utilizzata per il rilevamento della rete e il controllo della sicurezza.

### Risorse necessarie

---

- **Macchina virtuale CyberOps Workstation**
- **Accesso a Internet**

### Disposizioni

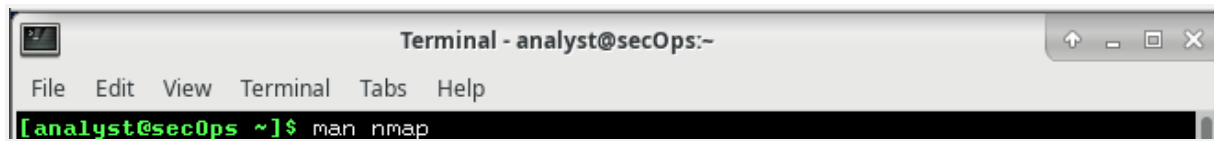
---

#### Parte 1: Esplorare Nmap

In questa parte, utilizzerai le pagine di manuale (o pagine man in breve) per saperne di più su Nmap.

L'uomo [ programma | *utilità* | *funzione* ] visualizza le pagine di manuale associate agli argomenti. Le pagine di manuale sono i manuali di riferimento che si trovano sui sistemi operativi Unix e Linux. Queste pagine possono includere le seguenti sezioni: Nome, Sinossi, Descrizioni, Esempi e Vedi anche.

- a. Avviare la VM CyberOps Workstation.
- b. Apri un terminale.
- c. Al prompt del terminale, immettere `.man nmap`

A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The prompt is "[analyst@secOps ~]\$". The command "man nmap" has been entered at the prompt.

Che cos'è Nmap?

**Nmap è uno strumento di esplorazione della rete e scanner di sicurezza/porte.**

A cosa serve nmap?

**Nmap viene utilizzato per scansionare una rete e determinare gli host e i servizi disponibili offerti nella rete. Alcune delle funzionalità di nmap includono il rilevamento dell'host, la scansione delle porte e il rilevamento del sistema operativo. Nmap può essere comunemente utilizzato per i controlli di sicurezza, per identificare le porte aperte, l'inventario della rete e trovare vulnerabilità nella rete.**

d. Nella pagina man, è possibile utilizzare i tasti freccia su e giù per scorrere le pagine. Puoi anche premere la barra spaziatrice per avanzare di una pagina alla volta.

Per cercare un termine o una frase specifica, utilizzare l'immissione di una barra (/) o di un punto interrogativo (?) seguito dal termine o dalla frase. La barra consente di eseguire la ricerca in avanti nel documento, mentre il punto interrogativo consente di eseguire la ricerca all'indietro nel documento. Il tasto n passa alla corrispondenza successiva.

Digitare /example e premere INVIO. Questo cercherà la parola esempio in avanti attraverso la pagina man.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks
    such as network inventory, managing service upgrade schedules, and
    monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that

Manual page nmap(1) line 1 (press h for help or q to quit)
```

e. Nella prima istanza dell'esempio, vengono visualizzate tre corrispondenze. Per passare alla partita successiva, premere n.

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

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE  SERVICE      VERSION
22/tcp    open   ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open   http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldap
1720/tcp  filtered H.323/Q.931

Manual page nmap(1) line 44 (press h for help or q to quit)
```

Guarda l'esempio 1.

Qual è il comando nmap utilizzato?

## **Nmap -A -T4 scanme.nmap.org**

Utilizza la funzione di ricerca per rispondere alle seguenti domande.

A cosa serve l'interruttore -A?

**-A: Abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute**

Cosa fa l'interruttore -T4?

**-T4 per un'esecuzione più rapida impedendo che il ritardo di scansione dinamica superi i 10 ms per le porte TCP. -T4 è consigliato per una connessione a banda larga o ethernet decente.**

f. Scorri la pagina per saperne di più su nmap. Al termine, digitare q.

## **Parte 2: Scansione delle porte aperte**

In questa parte, utilizzerete gli switch dell'esempio nelle pagine man di Nmap per scansionare il vostro localhost, la vostra rete locale e un server remoto a scanme.nmap.org.

### **Passaggio 1: scansiona il tuo localhost.**

a. Se necessario, aprire un terminale sulla VM. Al prompt, digitare . A seconda della rete locale e dei dispositivi, la scansione richiederà da pochi secondi a pochi minuti. **nmap -A -T4 localhost**



```
[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: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
```

b. Esamina i risultati e rispondi alle seguenti domande.

Quali porti e servizi sono aperti?

**21/TCP: FTP, 22/TCP: SSH**

Per ciascuna delle porte aperte, registrare il software che fornisce i servizi.

**ftp: vsftpd, ssh: OpenSSH**

Passaggio 2: scansiona la tua rete.

Attenzione: Prima di utilizzare Nmap su qualsiasi rete, si prega di ottenere il permesso dei proprietari della rete prima di procedere.

a. Al prompt dei comandi del terminale, premere ENTER per determinare l'indirizzo IP e la subnet mask per questo host. Per questo esempio, l'indirizzo IP per questa macchina virtuale è 192.168.50.153 e la subnet mask è 255.255.255.0. **ip address**

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9a:eb:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.153/24 brd 192.168.50.255 scope global dynamic enp0s3
        valid_lft 7180sec preferred_lft 7180sec
    inet6 fe80::a00:27ff:fe9a:ebbd/64 scope link
        valid_lft forever preferred_lft forever
```

Registrare l'indirizzo IP e la subnet mask per la macchina virtuale.

A quale rete appartiene la macchina virtuale?

**Le risposte possono variare. Questa macchina virtuale ha un indirizzo IP di 192.168.50.153/24 e fa parte della rete 192.168.50.0/24.**

b. Per individuare altri host su questa LAN, immettere . L'ultimo ottetto dell'indirizzo IP deve essere sostituito con uno zero. Ad esempio, nell'indirizzo IP 192.168.50.153, .153 è l'ultimo ottetto. Pertanto, l'indirizzo di rete è 192.168.50.0. Il /24 è chiamato prefisso ed è un'abbreviazione per la netmask 255.255.255.0. Se la macchina virtuale ha una maschera di rete diversa, cercare in Internet una "tabella di conversione CIDR" per trovare il prefisso. Ad esempio, 255.255.0.0 sarebbe /16. In questo esempio viene utilizzato l'indirizzo di rete 192.168.50.0/24

**nmap -A -T4 network address/prefix**

Nota: Questa operazione può richiedere del tempo, soprattutto se si dispone di molti dispositivi collegati alla rete. In un ambiente di test, la scansione ha richiesto circa 4 minuti.

```
[analyst@sec0ps ~]$ 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 fingerprint 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\x06\x81\x85\x01\x00\x00\x00\x07ver
SF:sion\x04bind\x00\x10\x03")%r(DNSStatusRequestTCP,E,"%0\x0c\x00\x90\x0
SF:4\x00\x00\x00\x00");

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
```

Quanti host ci sono?

**3.**

Dai risultati di Nmap, elencare gli indirizzi IP degli host che si trovano sulla stessa LAN della VM. Elencare alcuni dei servizi disponibili negli host rilevati.

**192.168.50.1,192.168.50.100,192.168.50.153. 192.168.50.1:**

**Porta 53/TCP: DNS (Domain Name System)**

**Porta 80/TCP: HTTP (servizio web con titolo "pFSense - Login")**

**192.168.50.153:**

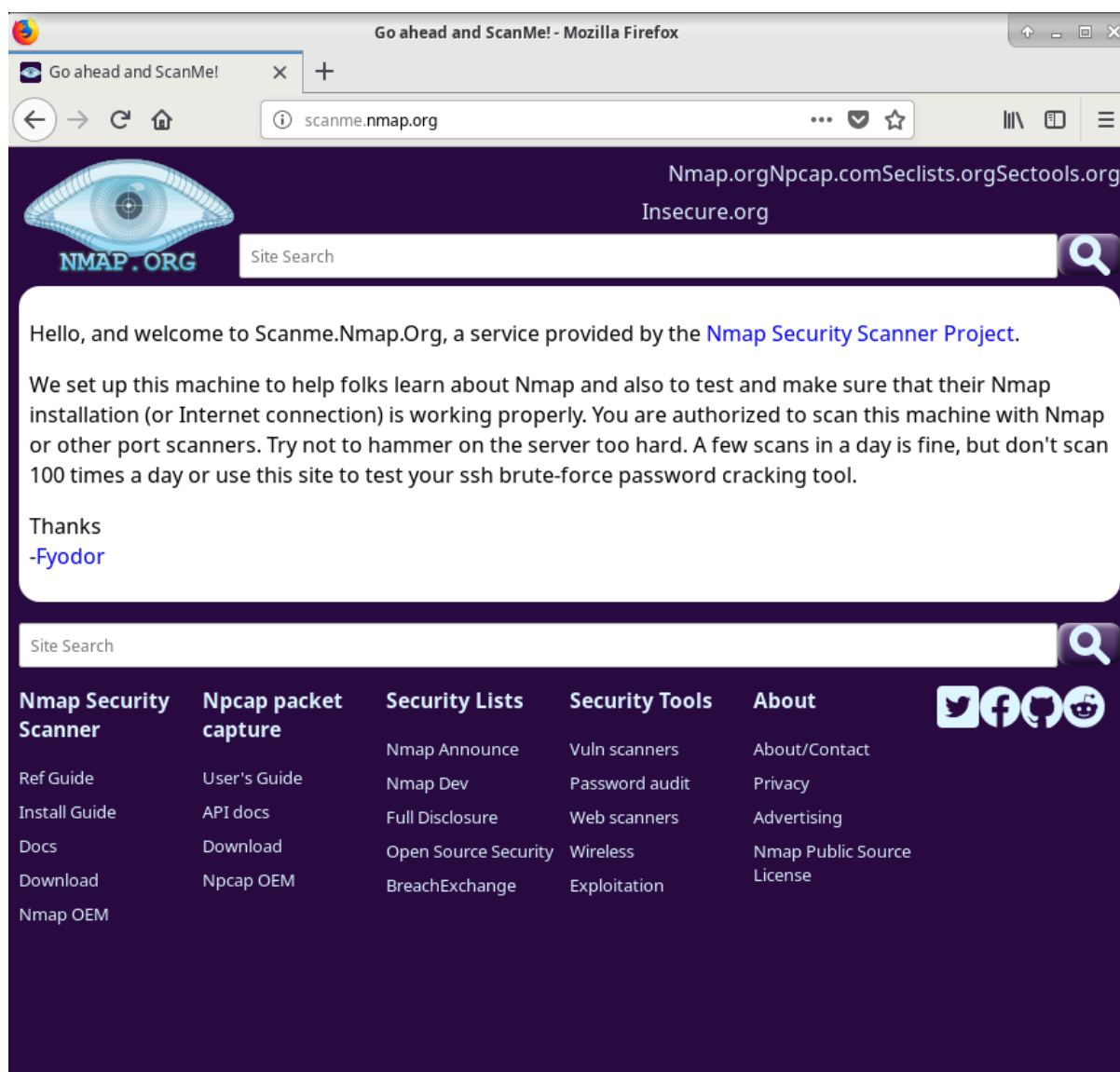
**Porta 21/TCP: FTP (File Transfer Protocol) con login anonimo consentito**

**Porta 22/TCP: SSH (Secure Shell) con OpenSSH 7.7**

**L'host 192.168.50.100 non ha porte aperte rilevate durante la scansione.**

Passaggio 3: eseguire la scansione di un server remoto.

a. Apri un browser Web e vai a [scanme.nmap.org](http://scanme.nmap.org). Si prega di leggere il messaggio pubblicato.



Qual è lo scopo di questo sito?

**Questo sito permette agli utenti di conoscere Nmap e testare la loro installazione di Nmap.**

b. Al prompt del terminale, digitare `.nmap -A -T4 scanme.nmap.org`

```
[analyst@sec0ps ~]$ 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
```

c. Esamina i risultati e rispondi alle seguenti domande.

Quali porti e servizi sono aperti?

**22/TCP: SSH, 9929/TCP: N ping-echo, 31337/TCP: TCPwrapped, 80/TCP: HTTP**

Quali porte e servizi vengono filtrati?

**Porta 25/TCP: smtp (Simple Mail Transfer Protocol)**

**Porta 1875/TCP: westell-stats**

Qual è l'indirizzo IP del server?

**Indirizzo IPv4: 46.33.32.156.**

Qual è il sistema operativo?

**kernel Linux 3.13 - 3.19.**

**Domanda di riflessione**

---

Nmap è un potente strumento per l'esplorazione e la gestione della rete. In che modo Nmap può aiutare con la sicurezza della rete? In che modo Nmap può essere utilizzato da un attore di minacce come strumento nefasto?

**Nmap può essere utilizzato per scansionare una rete interna alla ricerca di specifiche porte aperte per identificare l'entità di una violazione della sicurezza. Può anche essere utilizzato per inventariare una rete per garantire che tutti i sistemi siano probabilmente patchati per problemi di sicurezza. D'altra parte, nmap può essere utilizzato per la ricognizione per determinare le porte aperte e altre informazioni sulla rete.**

## 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.

### Obiettivi

---

In questa esercitazione verrà visualizzato un file PCAP di un attacco precedente a un database SQL.

- Parte 1: Apri Wireshark e carica il file PCAP.
- Parte 2: Visualizza l'attacco SQL injection.
- Parte 3: L'attacco SQL Injection continua...
- Parte 4: L'attacco SQL Injection fornisce informazioni sul sistema.
- Parte 5: L'attacco SQL injection e le informazioni sulla tabella
- Parte 6: L'attacco SQL injection si conclude.

### Contesto / Scenario

---

Gli attacchi SQL injection consentono agli hacker malintenzionati di digitare istruzioni SQL in un sito Web e ricevere una risposta dal database. Ciò consente agli aggressori di manomettere i dati correnti nel database, falsificare le identità e fare altri dispetti.

È stato creato un file PCAP per visualizzare un attacco precedente contro un database SQL. In questo lab verranno visualizzati gli attacchi al database SQL e verranno fornite risposte alle domande.

### Risorse necessarie

---

- **Macchina virtuale CyberOps Workstation**

### Disposizioni

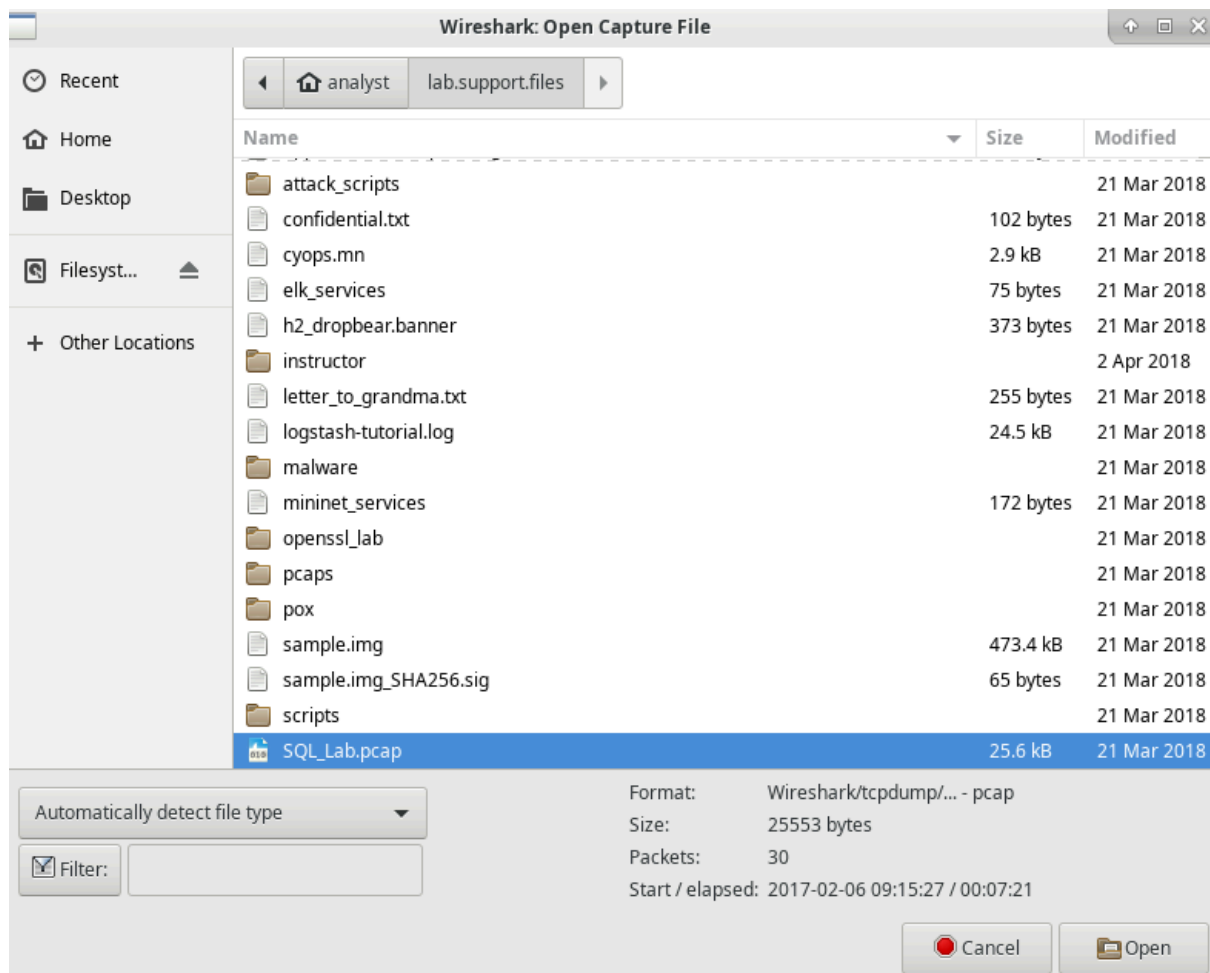
---

Utilizzerai Wireshark, un comune analizzatore di pacchetti di rete, per analizzare il traffico di rete. Dopo aver avviato Wireshark, si aprirà un'acquisizione di rete salvata in precedenza e si visualizzerà un attacco SQL injection passo dopo passo contro un database SQL.

## Parte 1: Apri Wireshark e carica il file PCAP.

L'applicazione Wireshark può essere aperta utilizzando una varietà di metodi su una workstation Linux.

- Avviare la VM CyberOps Workstation.
- Fare clic su Applicazioni > CyberOPS > Wireshark sul desktop e accedere all'applicazione Wireshark.
- Nell'applicazione Wireshark, fare clic su Apri al centro dell'applicazione in File.
- Sfoglia la directory /home/analyst/ e cerca lab.support.files. Nella directory lab.support.files e apri il file **SQL\_Lab.pcap**.



- Il file PCAP si apre all'interno di Wireshark e visualizza il traffico di rete acquisito. Questo file di acquisizione si estende per un periodo di 8 minuti (441 secondi), la durata di questo attacco SQL injection.



SQL\_Lab.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3
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	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3
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)
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

▶ Frame 30: 2091 bytes on wire (16728 bits), 2091 bytes captured (16728 bits)

▶ Ethernet II, Src: PcsCompu\_9f:48:a0 (08:00:27:9f:48:a0), Dst: PcsCompu\_ca:e1:24 (08:00:27:ca:e1:24)

▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 35668, Seq: 1, Ack: 620, Len: 2025

▶ Hypertext Transfer Protocol

▶ Line-based text data: text/html (106 lines)

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

0010 08 1d d4 57 40 00 40 06 46 71 0a 00 02 0f 0a 00 ...W@.@. Fq.....

0020 02 04 00 50 0b 54 02 01 00 00 00 00 00 00 00 ...BT.....

Frame (2091 bytes)    Uncompressed entity body (6215 bytes)

File: "/home/analyst/lab.support.files/...    Packets: 30 · Displayed: 30 (100.0%) · Load time: 0:00.000

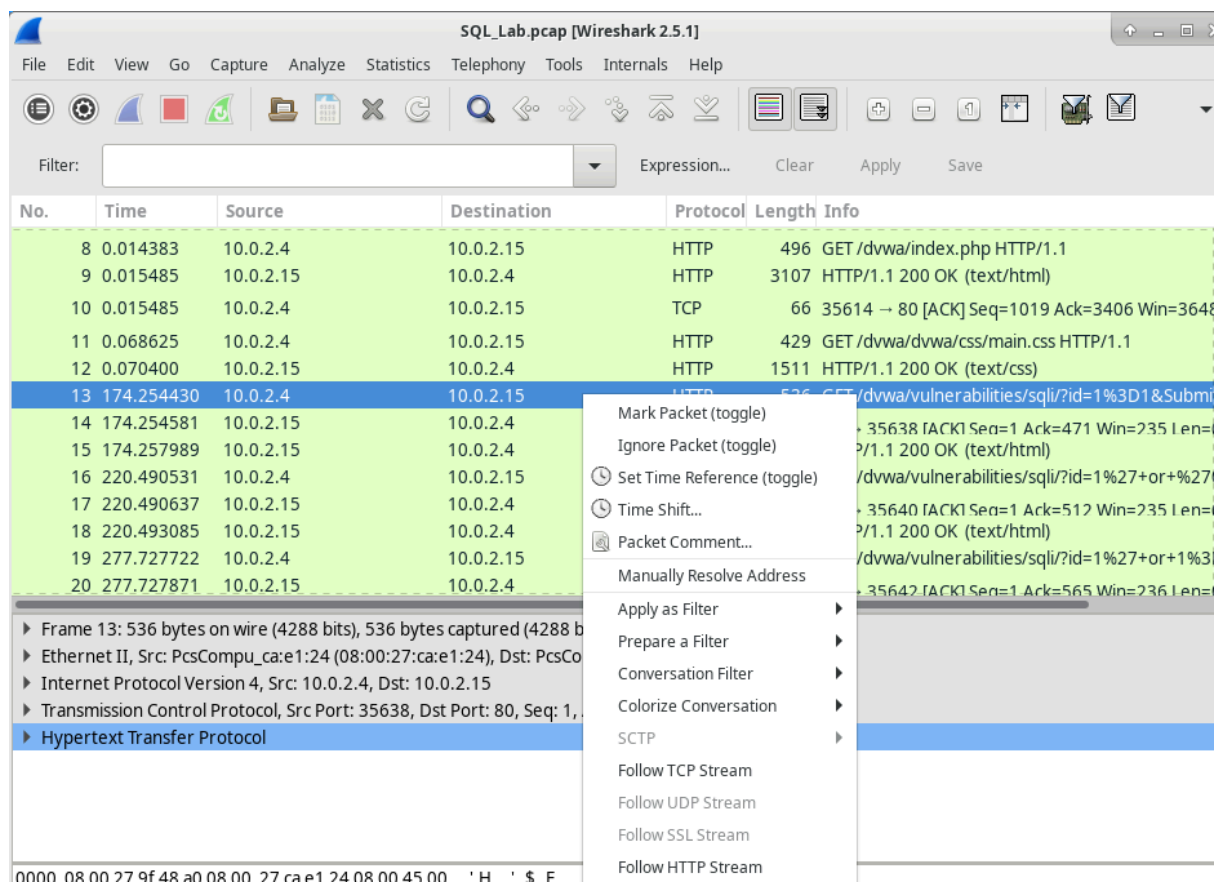
Quali sono i due indirizzi IP coinvolti in questo attacco SQL injection in base alle informazioni visualizzate?

**10.0.2.4 e 10.0.2.15**

## Parte 2: Visualizza l'attacco SQL injection.

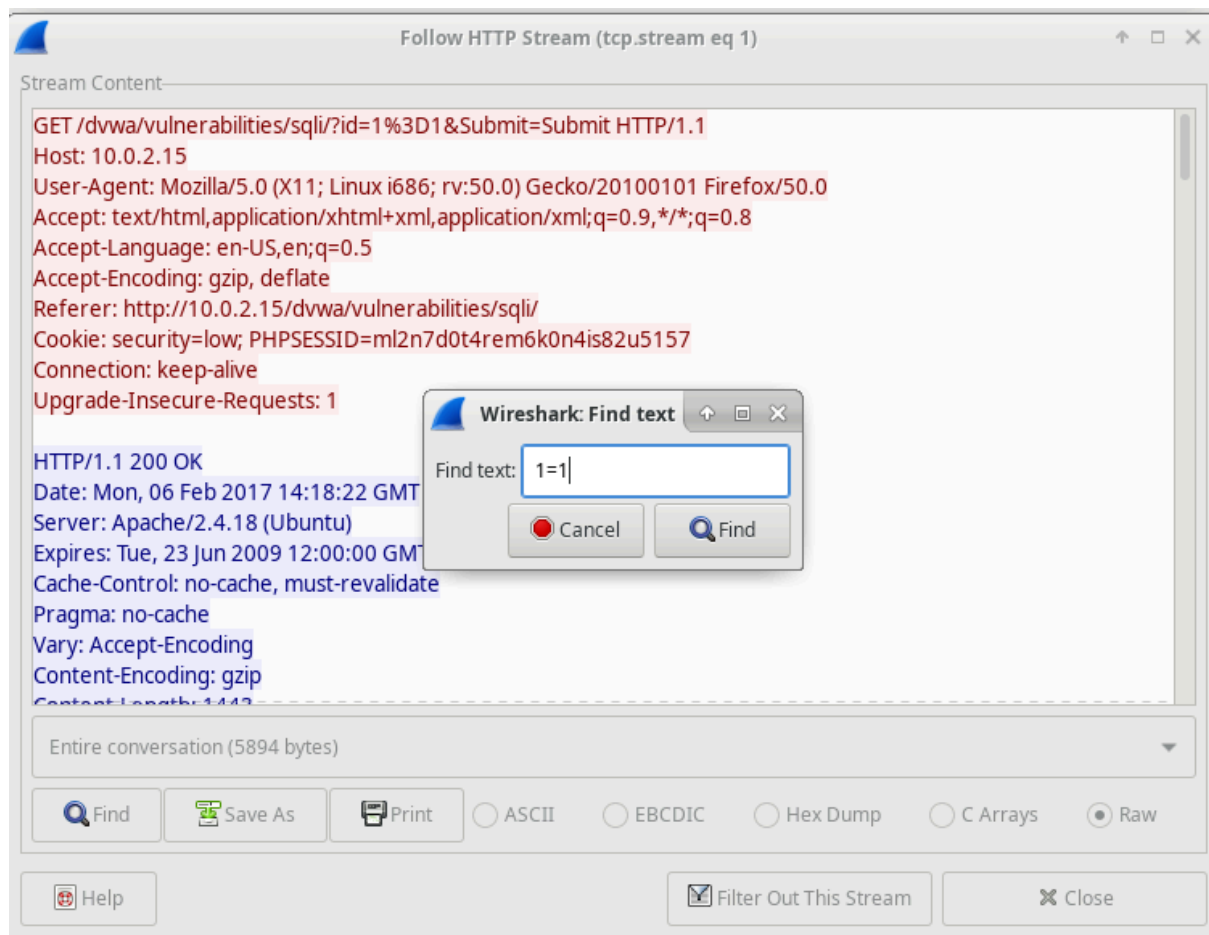
In questo passaggio, visualizzerai l'inizio di un attacco.

a. All'interno dell'acquisizione di Wireshark, fare clic con il pulsante destro del mouse sulla riga 13 e selezionare Segui > flusso HTTP. La riga 13 è stata scelta perché si tratta di una richiesta HTTP GET. Questo sarà molto utile per seguire il flusso di dati man mano che i livelli dell'applicazione lo vedono e porta al test delle query per l'SQL injection.



Il traffico di origine viene visualizzato in rosso. L'origine ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione risponde all'origine.

b. Nel campo Trova, inserisci 1=1. Fare clic su Trova successivo.

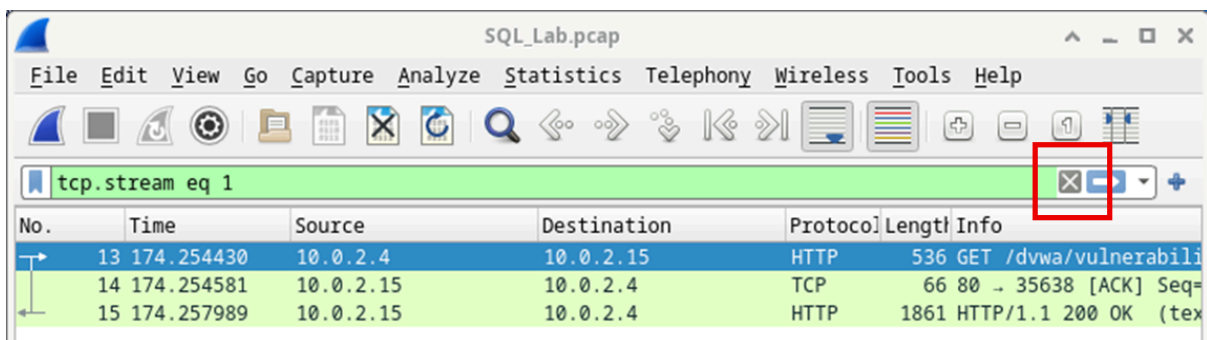


c. L'utente malintenzionato ha inserito una query ( $1=1$ ) in una casella di ricerca UserID sul target 10.0.2.15 per verificare se l'applicazione è vulnerabile all'SQL injection. Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con un record da un database. L'utente malintenzionato ha verificato di poter inserire un comando SQL e il database risponderà. La stringa di ricerca  $1=1$  crea un'istruzione SQL che sarà sempre vera. Nell'esempio, non importa cosa viene inserito nel campo, sarà sempre vero.



d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione Wireshark.



### Parte 3: L'attacco SQL Injection continua...

In questo passaggio, verrà visualizzata la continuazione di un attacco.

un. All'interno dell'acquisizione Wireshark, fare clic con il pulsante destro del mouse sulla riga 19 e scegliere Segui > flusso HTTP.

b. Nel campo Trova, inserisci 1=1. Fare clic su Trova successivo.

c. L'utente malintenzionato ha inserito una query (1' o 1=1 union select database(), user()) in una casella di ricerca UserID sul target 10.0.2.15.

Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con le seguenti informazioni:

The image shows a Wireshark 2.5.1 packet capture window titled 'SQL\_Lab.pcap [Wireshark 2.5.1]'. The filter is set to 'tcp.stream eq 3'. The packet list shows three packets: a GET request (No. 19), a TCP ACK (No. 20), and an HTTP 200 OK response (No. 21). The 'Follow HTTP Stream (tcp.stream eq 3)' window is open, displaying the stream content. A 'Wireshark: Find text' dialog box is overlaid on the stream content, with 'Find text:' set to '1=1'. The stream content shows the HTTP 200 OK response with various headers and a body containing a SQL injection payload.

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%3D1+union+select+data
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)

Stream Content:


```
GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+data
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686;
Accept: text/html,application/xhtml+xml,e
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
Content-Encoding: gzip
```

Wireshark: Find text

Find text: 1=1

Submit=Submit HTTP/1.1



The screenshot shows a window titled "Follow HTTP Stream (tcp.stream eq 3)". The "Stream Content" pane displays the following HTML code:

```
..</form>
..<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre>
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"
target="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>

```

The status bar at the bottom indicates "Entire conversation (6532 bytes)".

Il nome del database è dvwa e l'utente del database è root@localhost. Vengono visualizzati anche più account utente.

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione Wireshark.

## Parte 4: L'attacco SQL Injection fornisce informazioni sul sistema.

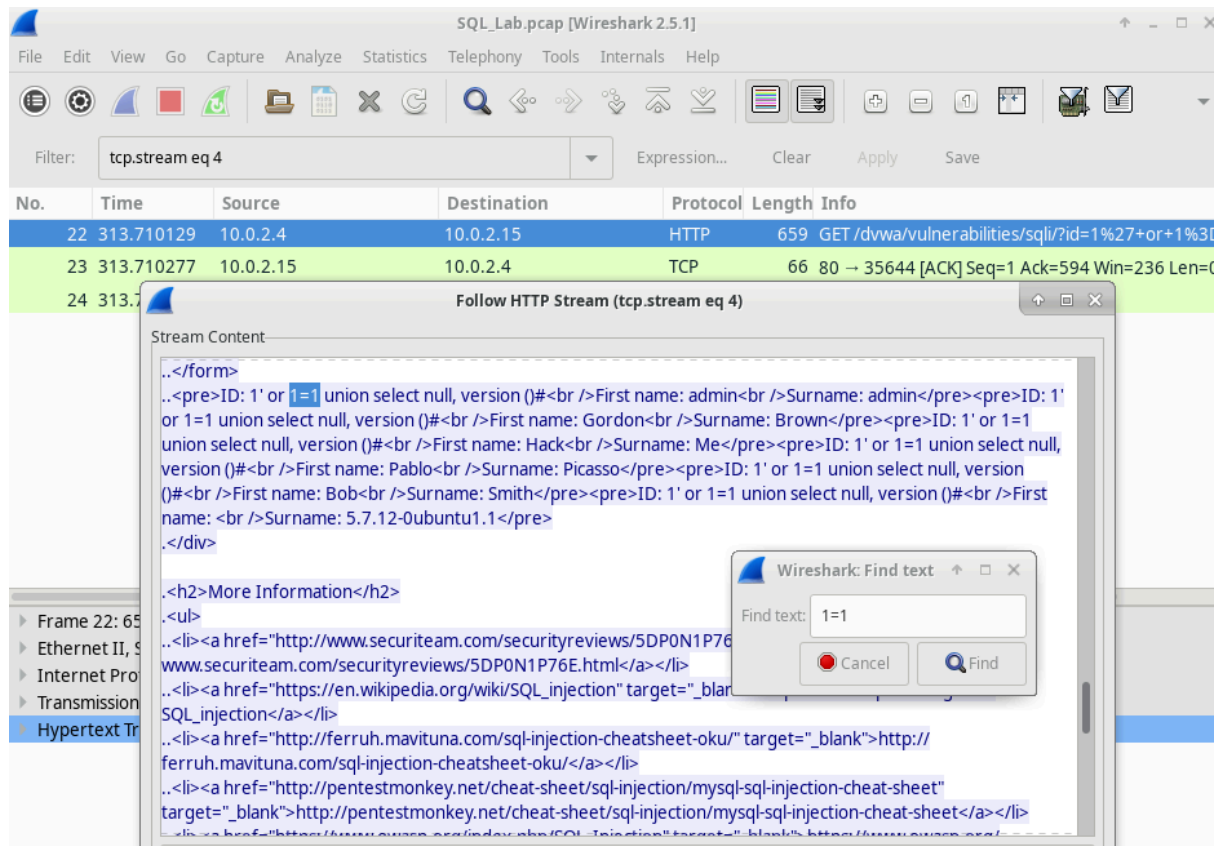
L'aggressore continua e inizia a prendere di mira informazioni più specifiche.

a. All'interno dell'acquisizione di Wireshark, fare clic con il pulsante destro del mouse sulla riga 22 e selezionare Segui > flusso HTTP. In rosso, viene visualizzato il traffico di origine che invia la richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione risponde all'origine.

b. Nel campo Trova, inserisci 1=1. Fare clic su Trova successivo.

c. L'utente malintenzionato ha inserito una query (1' o 1=1 union select null, version ()#) in una casella di ricerca UserID sul target 10.0.2.15 per individuare l'identificatore di versione. Si noti che l'identificatore di versione si

trova alla fine dell'output, subito prima del codice HTML di chiusura `</pre>.</div>`.



Qual è la versione?

**MySQL 5.7.12-0**

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione Wireshark.

## Parte 5: L'attacco SQL injection e le informazioni sulle tabelle.

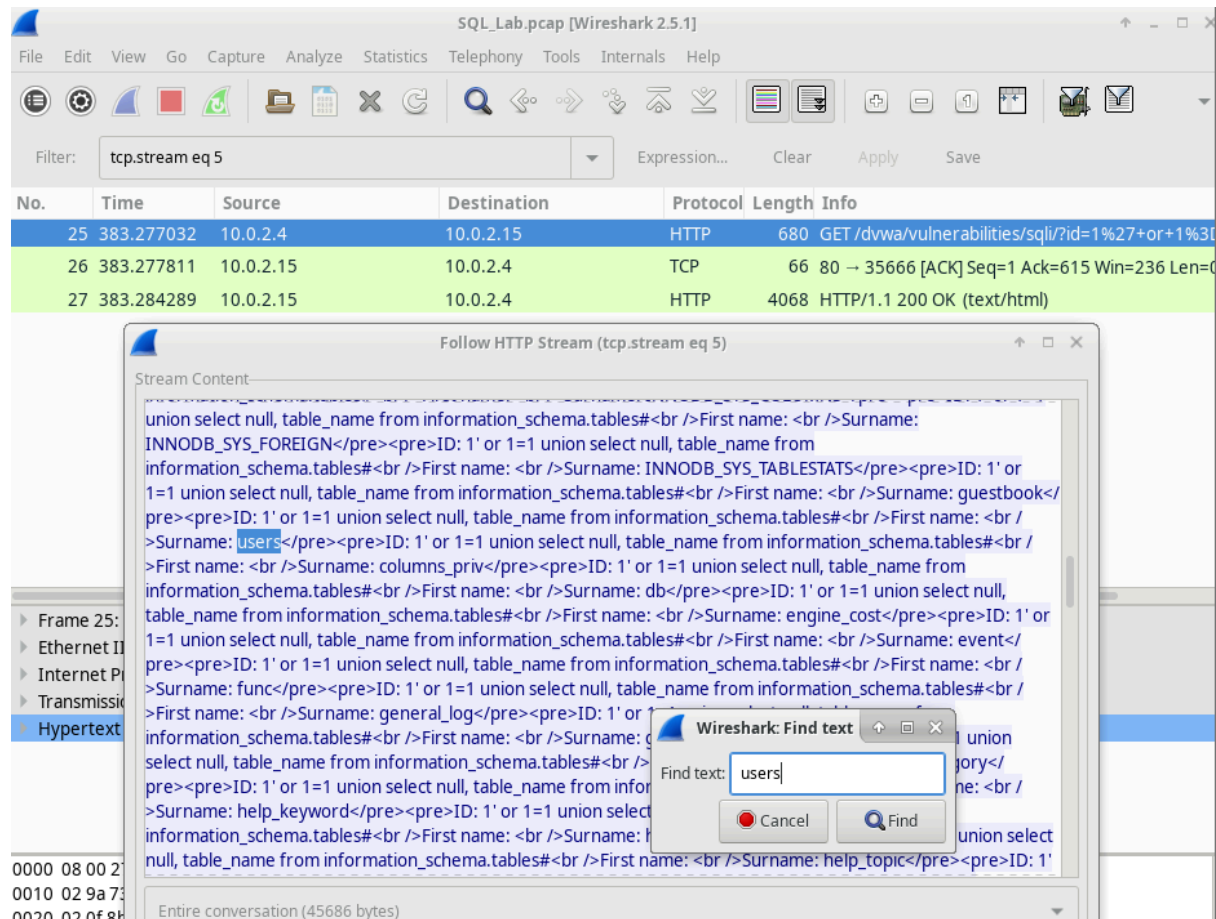
L'aggressore sa che esiste un gran numero di tabelle SQL piene di informazioni. L'aggressore tenta di trovarli.

un. All'interno dell'acquisizione di Wireshark, fare clic con il pulsante destro del mouse sulla riga 25 e selezionare Segui > flusso HTTP. La sorgente è mostrata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione risponde all'origine.

b. Nel campo Trova, inserisci gli utenti. Fare clic su Trova successivo.



c. L'utente malintenzionato ha inserito una query (1' o 1=1 union select null, table\_name da information\_schema.tables#) in una casella di ricerca UserID sulla destinazione 10.0.2.15 per visualizzare tutte le tabelle nel database. Ciò fornisce un enorme output di molte tabelle, poiché l'utente malintenzionato ha specificato "null" senza ulteriori specifiche.



Cosa farebbe per l'aggressore il comando modificato di (1' OR 1=1 UNION SELECT null, column\_name FROM INFORMATION\_SCHEMA.columns WHERE table\_name='users')?

**Il database risponderebbe con un output molto più breve filtrato dall'occorrenza della parola "utenti".**

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su Cancella filtro di visualizzazione per visualizzare l'intera conversazione Wireshark.

## Parte 6: L'attacco SQL injection si conclude.

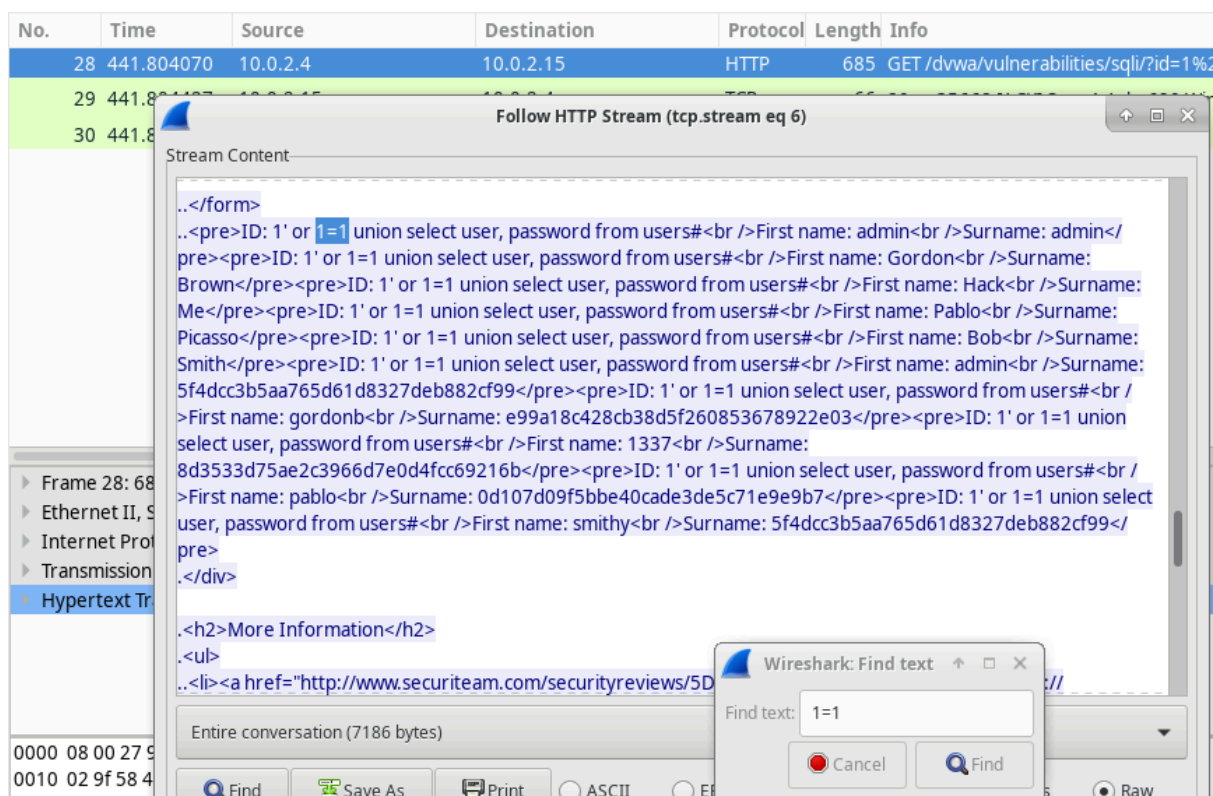
L'attacco si conclude con il miglior premio di tutti; hash delle password.



un. All'interno dell'acquisizione di Wireshark, fare clic con il pulsante destro del mouse sulla riga 28 e selezionare Segui > flusso HTTP. La sorgente è mostrata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione risponde all'origine.

b. Fai clic su Trova e digita 1=1. Cerca questa voce. Una volta individuato il testo, fare clic su Annulla nella casella di ricerca Trova testo.

L'aggressore ha inserito una query (1' o 1=1 unione seleziona utente, password da users#) in una casella di ricerca UserID sul target 10.0.2.15 per estrarre nomi utente e hash delle password!



Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?

1337

c. Utilizzando un sito Web come <https://crackstation.net/>, copia l'hash della password nel cracker dell'hash della password e inizia a decifrare.

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox

https://crackstation.net

# CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

## Free Password Hash Cracker

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

8d3533d75ae2c3966d7e0d4fcc69216b

I'm not a robot

reCAPTCHA

Crack Hashes

**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

Che cos'è la password in testo normale?

**Charley**

d. Chiudere la finestra Segui flusso HTTP. Chiudi tutte le finestre aperte.

## Domande di riflessione

1. Qual è il rischio di avere piattaforme che utilizzano la lingua SQL?

**I siti Web sono comunemente basati su database e utilizzano il linguaggio SQL. La gravità di un attacco SQL injection dipende dall'aggressore.**

2. Naviga in Internet ed esegui una ricerca su "prevenire gli attacchi SQL injection". Quali sono i 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi SQL injection?

**Due metodi per prevenire gli attacchi SQL injection:**

**Utilizzare query parametrizzate (prepared statements) per separare codice e dati.**

**Validare rigorosamente l'input dell'utente per assicurarsi che rispetti il formato atteso.**