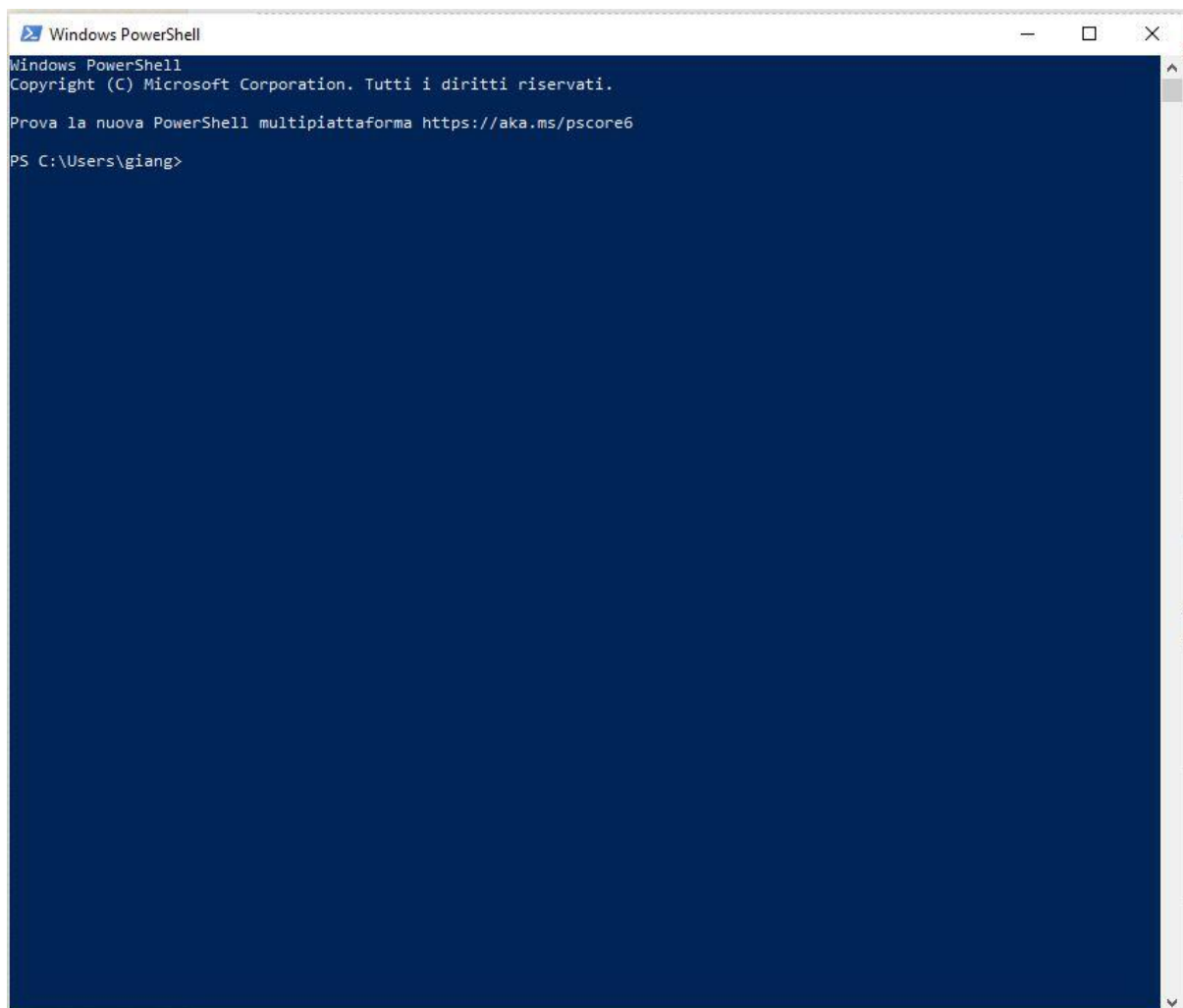


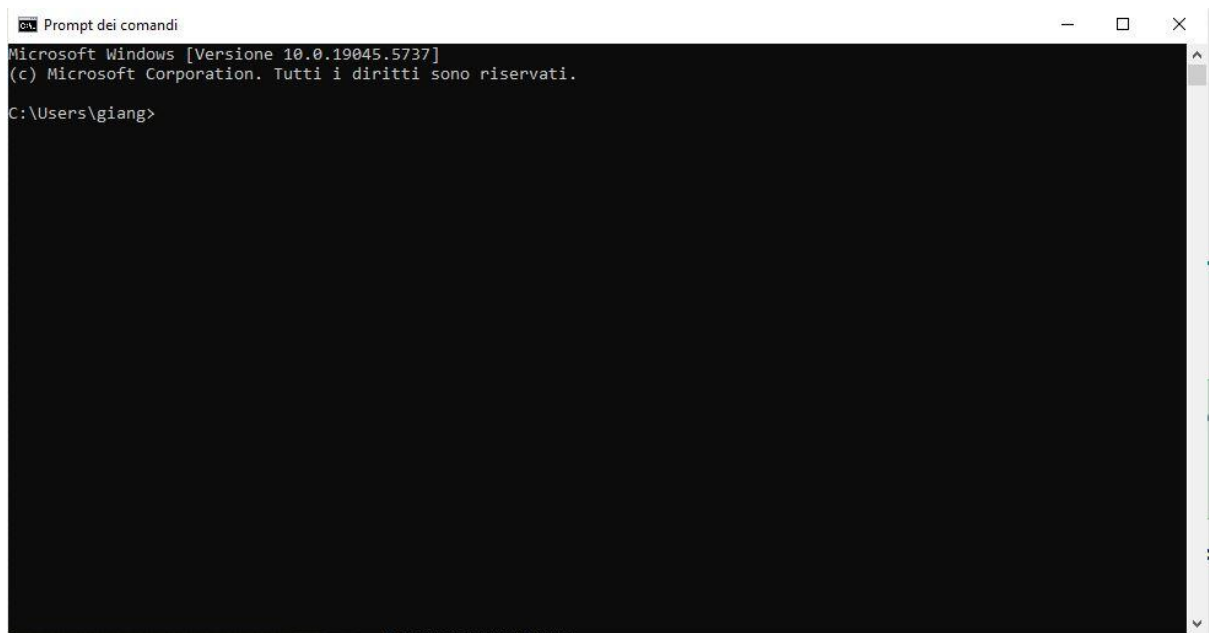
Laboratorio - Utilizzo di Windows PowerShell

Parte 1: accedere alla console di PowerShell.

a. Fare clic su **Start** . Cerca e seleziona **PowerShell** .



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



```
Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.5737]
(c) Microsoft Corporation. Tutti i diritti sono riservati.
C:\Users\giang>
```

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

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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\Users\giang> dir

Directory: C:\Users\giang

Mode                LastWriteTime         Length Name
----                -
d-----          27/02/2025    12:57             .lmstudio
d-----          17/06/2022    20:40             .ms-ad
d-----          30/09/2020     00:24             .Origin
d-----          18/06/2020    13:37             .QtWebEngineProcess
d-----          10/04/2025    14:18             .VirtualBox
d-r-----        19/08/2020    19:50             3D Objects
d-----          15/05/2019    10:39             ansel
d-----          17/02/2025    16:11             Cisco Packet Tracer 8.2.2
d-r-----        19/08/2020    19:50             Contacts
d-r-----        09/04/2025    16:10             Desktop
d-r-----        14/03/2025    15:33             Documents
d-r-----        25/02/2025    14:23             Downloads
d-r-----        19/08/2020    19:50             Favorites
d-----          01/11/2020    11:33             Games
d-----          20/12/2018    13:32             LaunchBox
d-r-----        19/08/2020    19:50             Links
d-r-----        14/03/2023    18:21             Music
d-----          27/03/2025    21:11             Nuova cartella
dar--l          03/04/2025    19:14             OneDrive
d-r-----        28/02/2025    11:16             Pictures
d-----          10/03/2018    17:59             Roaming
d-r-----        06/10/2020    12:16             Saved Games
d-r-----        19/08/2020    19:51             Searches
d-r-----        11/04/2025    08:43             Videos
-a-----          14/03/2025    11:42           210 .gitconfig
-a-----          27/02/2025    11:02           24 .lmstudio-home-pointer
-a-----          17/02/2025    16:10          148 .packettracer
-a-----          29/10/2018     09:41          436 Questo PC - collegamento.lnk

PS C:\Users\giang>
```

C:\ Prompt dei comandi

```
Directory di C:\Users\giang

11/04/2025  08:42    <DIR>          .
11/04/2025  08:42    <DIR>          ..
14/03/2025  12:42                210 .gitconfig
27/02/2025  13:57    <DIR>          .lmstudio
27/02/2025  12:02                24 .lmstudio-home-pointer
17/06/2022  20:40    <DIR>          .ms-ad
30/09/2020  00:24    <DIR>          .Origin
17/02/2025  17:10                148 .packettracer
18/06/2020  13:37    <DIR>          .QtWebEngineProcess
10/04/2025  14:18    <DIR>          .VirtualBox
19/08/2020  19:50    <DIR>          3D Objects
15/05/2019  10:39    <DIR>          ansel
17/02/2025  17:11    <DIR>          Cisco Packet Tracer 8.2.2
19/08/2020  19:50    <DIR>          Contacts
09/04/2025  16:10    <DIR>          Desktop
14/03/2025  16:33    <DIR>          Documents
25/02/2025  15:23    <DIR>          Downloads
19/08/2020  19:50    <DIR>          Favorites
01/11/2020  12:33    <DIR>          Games
20/12/2018  14:32    <DIR>          LaunchBox
19/08/2020  19:50    <DIR>          Links
14/03/2023  19:21    <DIR>          Music
27/03/2025  22:11    <DIR>          Nuova cartella
03/04/2025  19:14    <DIR>          OneDrive
28/02/2025  12:16    <DIR>          Pictures
29/10/2018  10:41                436 Questo PC - collegamento.lnk
10/03/2018  18:59    <DIR>          Roaming
06/10/2020  12:16    <DIR>          Saved Games
19/08/2020  19:51    <DIR>          Searches
11/04/2025  08:43    <DIR>          Videos

         4 File                818 byte
        26 Directory  23.772.299.264 byte disponibili
```

Quali sono gli output del `dir`?

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

b. Prova un altro comando che hai utilizzato nel prompt dei comandi, ad esempio `ping` , `cd` e `ipconfig` .

Quali sono i risultati?

L'output in entrambe le finestre è simile.

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

```
Sintassi: 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]
          [-4] [-6] target_name
```

Opzioni:

-t	Esegue il ping dell'host specificato finché non viene interrotto. Per visualizzare le statistiche e continuare - digitare Control-Break; Per interrompere - digitare Control-C.
-a	Risolve gli indirizzi in nomi host.
-n count	Numero di richieste echo da inviare.
-l size	Dimensioni del buffer di invio.
-f	Imposta il contrassegno per la disattivazione della frammentazione nel pacchetto (solo IPv4).
-i TTL	Durata (TTL, Time To Live).
-v TOS	Tipo di servizio (TOS, Type Of Service) (solo IPv4. Questa impostazione è deprecata e non ha alcun effetto sul campo del tipo di servizio nell'intestazione IP).
-r count	Registra la route per il conteggio degli hop (solo IPv4).
-s count	Timestamp per il conteggio degli hop (solo IPv4).
-j host-list	Route di origine libera lungo l'elenco host (solo IPv4).
-k host-list	Route di origine vincolata lungo l'elenco host (solo IPv4).
-w timeout	Timeout in millisecondi per l'attesa di ogni risposta.
-R	Usa l'intestazione di routing anche per il test del routing inverso (solo IPv6). In base a RFC 5095 l'utilizzo di questa intestazione di routing è deprecato. Alcuni sistemi potrebbero ignorare le richieste echo se viene utilizzata questa intestazione.
-S srcaddr	Indirizzo di origine da utilizzare.
-c compartment	Identificatore del raggruppamento di routing.
-p	Esegue il ping dell'indirizzo di un provider di virtualizzazione di rete di Hyper-V.
-4	Impone l'utilizzo di IPv4.
-6	Impone l'utilizzo di IPv6.

```
PS C:\Users\giang> cd
```

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

Configurazione IP di Windows


```

C:\Users\giang>ping

Sintassi: 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]
           [-4] [-6] target_name

Opzioni:
-t           Esegue il ping dell'host specificato finché non viene
             interrotto. Per visualizzare le statistiche e continuare -
             digitare Control-Break; Per interrompere - digitare
             Control-C.
-a           Risolve gli indirizzi in nomi host.
-n count     Numero di richieste echo da inviare.
-l size      Dimensioni del buffer di invio.
-f           Imposta il contrassegno per la disattivazione della
             frammentazione nel pacchetto (solo IPv4).
-i TTL       Durata (TTL, Time To Live).
-v TOS       Tipo di servizio (TOS, Type Of Service) (solo IPv4).
             Questa impostazione è deprecata e non ha alcun effetto sul
             campo del tipo di servizio nell'intestazione IP).
-r count     Registra la route per il conteggio degli hop (solo IPv4).
-s count     Timestamp per il conteggio degli hop (solo IPv4).
-j host-list Route di origine libera lungo l'elenco host (solo IPv4).
-k host-list Route di origine vincolata lungo l'elenco host (solo IPv4).
-w timeout   Timeout in millisecondi per l'attesa di ogni risposta.
-R           Usa l'intestazione di routing anche per il test del routing
             inverso (solo IPv6). In base a RFC 5095 l'utilizzo di questa
             intestazione di routing è deprecato. Alcuni sistemi
             potrebbero ignorare le richieste echo se viene utilizzata
             questa intestazione.
-S srcaddr   Indirizzo di origine da utilizzare.
-c compartment Identificatore del raggruppamento di routing.
-p           Esegue il ping dell'indirizzo di un provider
             di virtualizzazione di rete di Hyper-V.
-4           Impone l'utilizzo di IPv4.
-6           Impone l'utilizzo di IPv6.

C:\Users\giang>cd
C:\Users\giang

C:\Users\giang>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: station

Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::113c:2a26:ccd:8fad%9
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 10:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 11:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::615f:e7e:1a16:b375%16
    Indirizzo IPv4. . . . . : 192.168.1.7
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Connessione di rete Bluetooth:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

```

Parte 3: Esplora i cmdlet.

a. I comandi di PowerShell, i cmdlet, sono strutturati sotto forma di stringa *verbo-nome* . Per identificare il comando di PowerShell che elenca le sottodirectory e i file in una directory, digitare **Get-Alias dir** al prompt di PowerShell.

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

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

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

Get-ChildItem

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

I cmdlet di **Microsoft PowerShell** sono comandi specializzati progettati per eseguire operazioni specifiche all'interno dell'ambiente PowerShell. Seguono una convenzione di denominazione **Verbo-Sostantivo** (ad esempio, `Get-Process`, `Set-Location`) e restituiscono oggetti .NET, facilitando l'automazione e la gestione del sistema.

Esempi di cmdlet comuni

Ecco alcuni cmdlet frequentemente utilizzati:

Cmdlet	Alias	Descrizione
<code>Get-Help</code>	<code>help</code> , <code>man</code>	Visualizza la guida per cmdlet e concetti.
<code>Get-Command</code>	<code>gcm</code>	Elenca tutti i comandi disponibili.
<code>Get-Process</code>	<code>gps</code> , <code>ps</code>	Mostra i processi in esecuzione.
<code>Set-Location</code>	<code>cd</code> , <code>sl</code>	Cambia la directory corrente.
<code>Get-ChildItem</code>	<code>dir</code> , <code>ls</code>	Elenca file e cartelle.
<code>Copy-Item</code>	<code>cp</code> , <code>copy</code>	Copia file o cartelle.
<code>Remove-Item</code>	<code>rm</code> , <code>del</code>	Elimina file o cartelle.
<code>Select-String</code>	<code>sls</code>	Cerca stringhe nei file (simile a <code>grep</code>).
<code>Invoke-WebRequest</code>	<code>iwr</code> , <code>curl</code>	Esegue richieste HTTP.

Molti di questi cmdlet hanno alias per facilitare la transizione da altri shell come CMD o Bash.

c. Al termine, chiudere la finestra del prompt dei comandi.

Parte 4: Esplora il comando netstat utilizzando PowerShell.

a. Al prompt di PowerShell, premere Invio `netstat -h` per visualizzare le opzioni disponibili per il `netstat` comando.


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

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

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

```
-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
  porta di ascolto. In alcuni casi, host di eseguibili noti
  più componenti indipendenti e in questi casi il
  sequenza di componenti coinvolti nella creazione della connessione
  o la porta in ascolto. In questo caso, l'eseguibile
  il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
  e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
  può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
  autorizzazioni.
-e visualizza le statistiche Ethernet. È possibile combinare
  opzione.
-f Visualizza nomi di dominio completi (FQDN) per stranieri
  indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto
  può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6. Se usato con-s
  opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e i binding
  non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
  essere associato a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono
  visualizzate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
  l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-t Visualizza lo stato corrente di offload della connessione.
-x Visualizza connessioni NetworkDirect, listener e condivisi
  endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
  Non può essere combinato con le altre opzioni.
intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
  tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione
  Statistiche. Se viene omesso, netstat stamperà il
  informazioni di configurazione una volta.
```

b. Per visualizzare la tabella di routing con i percorsi attivi, digitare `netstat -r` al prompt.

```

PS C:\Users\giang> netstat -n
=====
Elenco interfacce
18...10 e7 c6 df 2f 60 .....Realtek PCIe GBE Family Controller
9...0a 00 27 00 00 09 .....VirtualBox Host-Only Ethernet Adapter
7...b8 08 cf ee e3 42 .....Microsoft Wi-Fi Direct Virtual Adapter
11...ba 08 cf ee e3 41 .....Microsoft Wi-Fi Direct Virtual Adapter #3
16...b8 08 cf ee e3 41 .....Intel(R) Dual Band Wireless-AC 7265
19...b8 08 cf ee e3 45 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia Metrica
    0.0.0.0           0.0.0.0    192.168.1.1   192.168.1.7    50
    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
    192.168.1.0        255.255.255.0   On-link       192.168.1.7    306
    192.168.1.7        255.255.255.255   On-link       192.168.1.7    306
    192.168.1.255     255.255.255.255   On-link       192.168.1.7    306
    192.168.56.0       255.255.255.0   On-link       192.168.56.1   281
    192.168.56.1       255.255.255.255   On-link       192.168.56.1   281
    192.168.56.255    255.255.255.255   On-link       192.168.56.1   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       192.168.56.1   281
    224.0.0.0          240.0.0.0   On-link       192.168.1.7    306
    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       192.168.56.1   281
    255.255.255.255    255.255.255.255   On-link       192.168.1.7    306
=====
Route permanenti:
  Nessuna

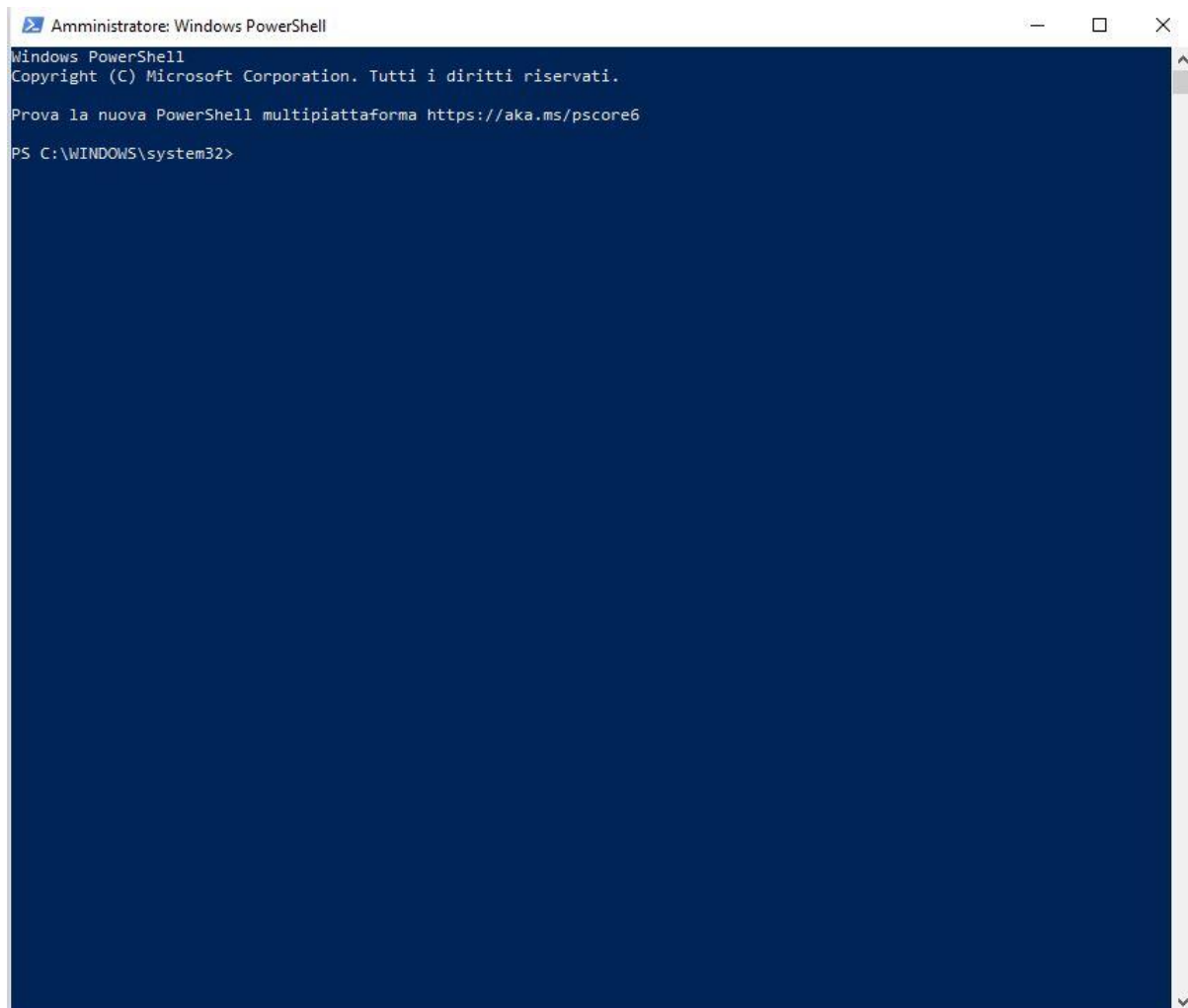
IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
    1      331 ::1/128                On-link
    9      281 fe80::/64                On-link
    16     306 fe80::/64                On-link
    9      281 fe80::113c:2a26:ccd:8fad/128
                                         On-link
    16     306 fe80::615f:e7e:1a16:b375/128
                                         On-link
    1      331 ff00::/8                On-link
    9      281 ff00::/8                On-link
    16     306 ff00::/8                On-link
=====
Route permanenti:
  Nessuna

```

Cos'è il gateway IPv4?

Le risposte possono variare. In questo esempio, il gateway è 192.168.1.1

c. Apri ed esegui una seconda versione di PowerShell con privilegi elevati. Fai clic su **Start** . Cerca PowerShell e fai clic con il pulsante destro del mouse su **Windows PowerShell** , quindi seleziona **Esegui come amministratore** . Fai clic su **Sì** per consentire a questa app di apportare modifiche al dispositivo.



```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\WINDOWS\system32>
```

d. Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Digitare il comando `netstat -abno` al prompt.

```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\WINDOWS\system32> netstat -abno

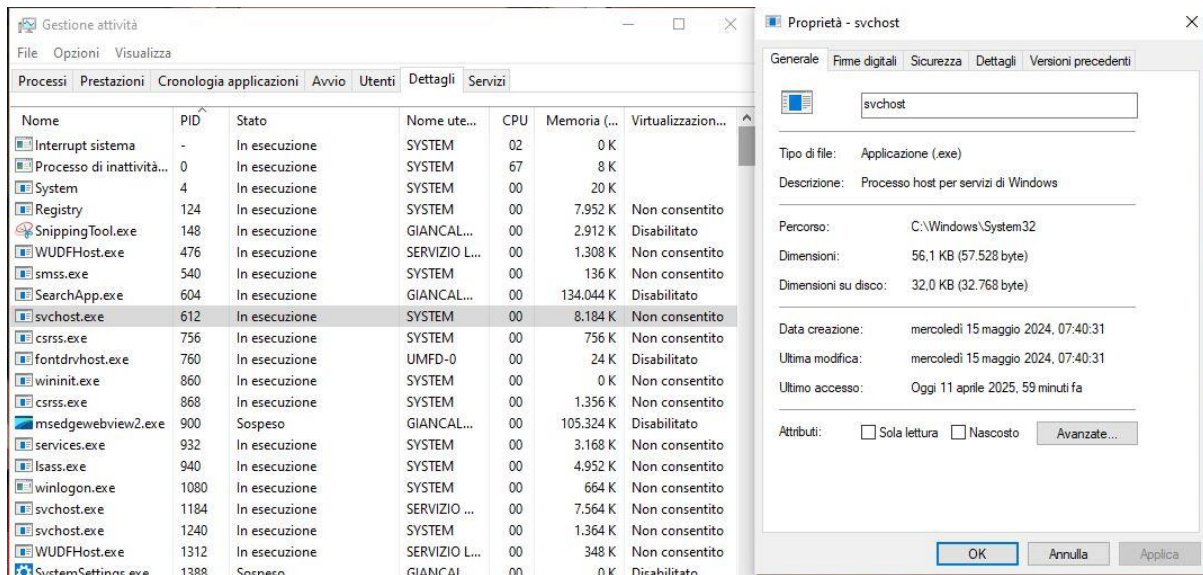
Connessioni attive

Proto Indirizzo locale      Indirizzo esterno  Stato  PID
-----
TCP    0.0.0.0:135              0.0.0.0:0          LISTENING 1184
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040              0.0.0.0:0          LISTENING 9232
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680              0.0.0.0:0          LISTENING 17200
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:8090              0.0.0.0:0          LISTENING 15640
[WinFrmNotification.exe]
TCP    0.0.0.0:10773             0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:27836             0.0.0.0:0          LISTENING 7988
[steam.exe]
TCP    0.0.0.0:49664             0.0.0.0:0          LISTENING 940
[lsass.exe]
TCP    0.0.0.0:49665             0.0.0.0:0          LISTENING 860
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666             0.0.0.0:0          LISTENING 1672
EventLog
[svchost.exe]
TCP    0.0.0.0:49667             0.0.0.0:0          LISTENING 2072
Schedule
[svchost.exe]
TCP    0.0.0.0:49668             0.0.0.0:0          LISTENING 4332
[spoolsv.exe]
TCP    0.0.0.0:49670             0.0.0.0:0          LISTENING 932
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:5354             0.0.0.0:0          LISTENING 4744
[mDNSResponder.exe]
TCP    127.0.0.1:6463             0.0.0.0:0          LISTENING 3360
[Discord.exe]
TCP    127.0.0.1:27060           0.0.0.0:0          LISTENING 7988
[steam.exe]
TCP    127.0.0.1:49701           127.0.0.1:65001     ESTABLISHED 5076
[nvcontainer.exe]
TCP    127.0.0.1:49702           0.0.0.0:0          LISTENING 9152
[NVIDIA Web Helper.exe]
TCP    127.0.0.1:49702           127.0.0.1:49714     ESTABLISHED 9152
[NVIDIA Web Helper.exe]
TCP    127.0.0.1:49714           127.0.0.1:49702     ESTABLISHED 12944
[NVIDIA Share.exe]
TCP    127.0.0.1:49757           127.0.0.1:49758     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49758           127.0.0.1:49757     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49759           127.0.0.1:49760     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49760           127.0.0.1:49759     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49761           127.0.0.1:49762     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49762           127.0.0.1:49761     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49763           127.0.0.1:49764     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49764           127.0.0.1:49763     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49765           127.0.0.1:49766     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49766           127.0.0.1:49765     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49784           127.0.0.1:49785     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49785           127.0.0.1:49784     ESTABLISHED 1904
[CiscoCollabHost.exe]
TCP    127.0.0.1:49823           0.0.0.0:0          LISTENING 7988
[steam.exe]
TCP    127.0.0.1:49823           127.0.0.1:49830     ESTABLISHED 7988
[steam.exe]
TCP    127.0.0.1:49825           0.0.0.0:0          LISTENING 7988
[steam.exe]
TCP    127.0.0.1:49825           127.0.0.1:49829     ESTABLISHED 7988
[steam.exe]
TCP    127.0.0.1:49829           127.0.0.1:49825     ESTABLISHED 15392
[steamwebhelper.exe]
TCP    127.0.0.1:49830           127.0.0.1:49823     ESTABLISHED 15392
[steamwebhelper.exe]
TCP    127.0.0.1:65001           0.0.0.0:0          LISTENING 5076
[nvcontainer.exe]
TCP    127.0.0.1:65001           127.0.0.1:49701     ESTABLISHED 5076
[nvcontainer.exe]
TCP    192.168.1.7:139           0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    192.168.1.7:49745         170.72.238.205:443 ESTABLISHED 8104
[CiscoCollabHost.exe]
```

e. Aprire Gestione Attività. Andare alla scheda **Dettagli** . Fare clic sull'intestazione **PID** per ordinarli.

f. Selezionare uno dei PID dai risultati di netstat -abno. In questo esempio viene utilizzato il PID 612.

g. Individuare il PID selezionato nel Task Manager. Fare clic con il pulsante destro del mouse sul PID selezionato nel Task Manager per aprire la finestra di dialogo **Proprietà** e ottenere ulteriori informazioni.



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

Il PID 612 è associato al processo svchost.exe. L'utente di questo processo è SYSTEM e utilizza 8184 KB di memoria.

Parte 5: Svuotare il cestino tramite 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 su 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 inoltre possibile eseguire comandi di PowerShell per semplificare azioni che richiederebbero più passaggi utilizzando gli strumenti grafici del desktop di Windows.

- Apri il Cestino. Verifica che ci siano elementi che possono essere eliminati definitivamente dal PC. In caso contrario, ripristina i file.
- Se non ci sono file nel Cestino, crea alcuni file, ad esempio un file di testo, utilizzando Blocco note e posizionali nel Cestino.
- In una console di PowerShell, digitare `clear-recyclebin` al prompt.

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

Che fine hanno fatto i 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. Cerca su internet i comandi che potresti utilizzare per semplificare le tue attività di analista della sicurezza. Registra i risultati.

PowerShell è uno strumento fondamentale per gli analisti della sicurezza informatica, grazie alla sua capacità di automatizzare e semplificare numerose attività quotidiane. Ecco alcuni esempi pratici di comandi che possono essere utilizzati:

1. Monitoraggio dei Processi in Esecuzione

Per ottenere informazioni sui processi attualmente in esecuzione sul sistema, è possibile utilizzare il cmdlet `Get-Process`.

2. Analisi dei Log di Sicurezza

Per esaminare i tentativi di accesso non riusciti, è utile analizzare i log di sicurezza. Il cmdlet `Get-EventLog` consente di accedere a questi registri.

3. Verifica dello Stato dei Servizi

Per controllare lo stato di un servizio specifico, come il servizio Windows Update, si può utilizzare il cmdlet `Get-Service`.

4. Test della Connettività di Rete

Per verificare la connettività di rete verso un host remoto, il cmdlet `Test-Connection` può essere molto utile.

5. Gestione dei Criteri di Esecuzione

Per garantire che solo gli script firmati possano essere eseguiti, è possibile impostare il criterio di esecuzione su "AllSigned".

6. Esportazione dei Dettagli dei Processi in Esecuzione

Per creare un report dei processi attivi e salvarlo in un file CSV, il cmdlet Export-Csv può essere utilizzato in combinazione con Get-Process.

7. Ricerca di Stringhe nei File

Per cercare specifiche stringhe all'interno di file di log o altri documenti, il cmdlet Select-String è molto utile.

8. Monitoraggio delle Attività di Rete

Per monitorare le attività di rete e rilevare possibili anomalie, è possibile utilizzare PowerShell per analizzare i pattern di traffico.

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

Parte 1: Acquisizione e visualizzazione del traffico HTTP

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

Avviare la VM CyberOps Workstation. Utilizzare le seguenti credenziali utente:

Nome utente: **analista**

Password: **cyberops**



Passaggio 2: aprire un terminale e avviare tcpdump.

a. Aprire un'applicazione terminale e immettere il comando `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 08:00:27:21:05:f7 brd ff:ff:ff:ff:ff:ff
   inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic enp0s3
       valid_lft 387sec preferred_lft 387sec
   inet6 fe80::a00:27ff:fe21:5f7/64 scope link
       valid_lft forever preferred_lft forever
```

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

lo: 127.0.0.1/8

enp0s3: 192.168.56.107/24

c. Nell'applicazione terminale, digitare il comando `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`. Inserire la password **cyberops** per l'analista utente quando richiesto.

```
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Questo comando avvia tcpdump e registra il traffico di rete sull'interfaccia **enp0s3**.

L' `-i` opzione command consente di specificare l'interfaccia. Se non specificata, tcpdump catturerà tutto il traffico su tutte le interfacce.

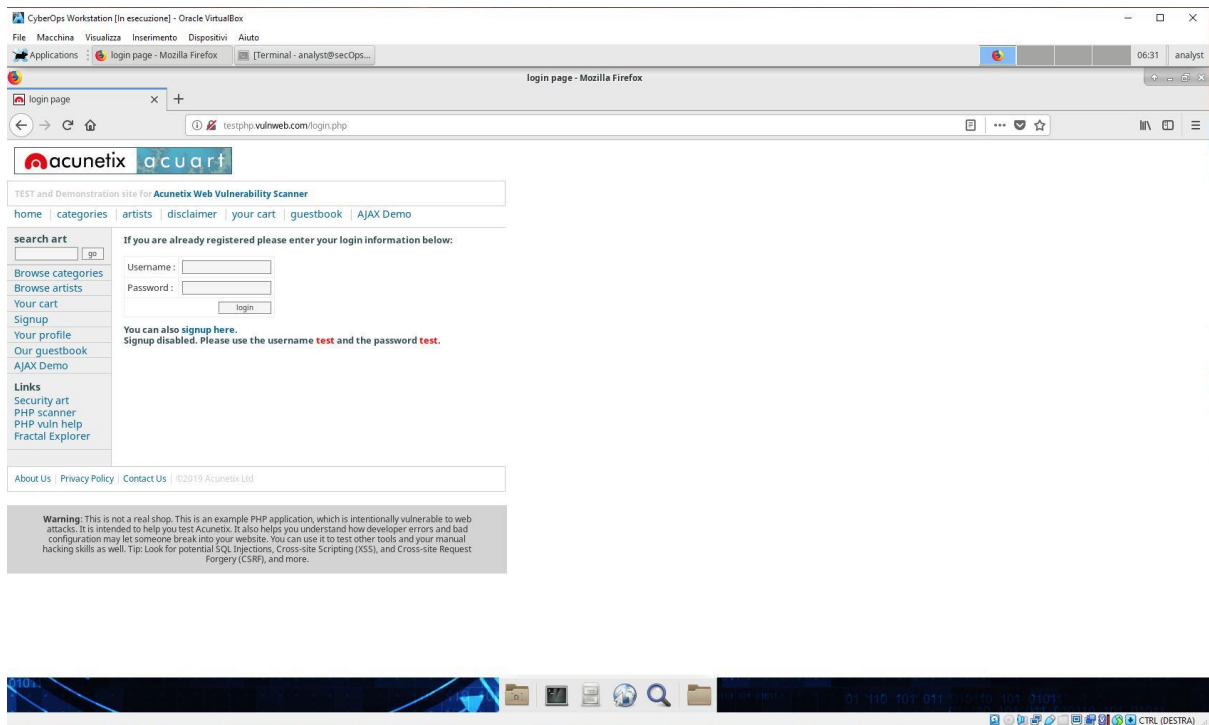
L' `-s` opzione command specifica la lunghezza dello snapshot per ogni pacchetto. È consigliabile limitare snaplen al numero più piccolo che catturi le informazioni di protocollo di interesse. Impostando snaplen a 0, si imposta il valore predefinito di 262144, per garantire la retrocompatibilità con le versioni precedenti di tcpdump.

L' `-w` 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 possano leggere il file. Tutto il traffico registrato verrà visualizzato nel file httpdump.pcap nella directory home dell'analista utente.

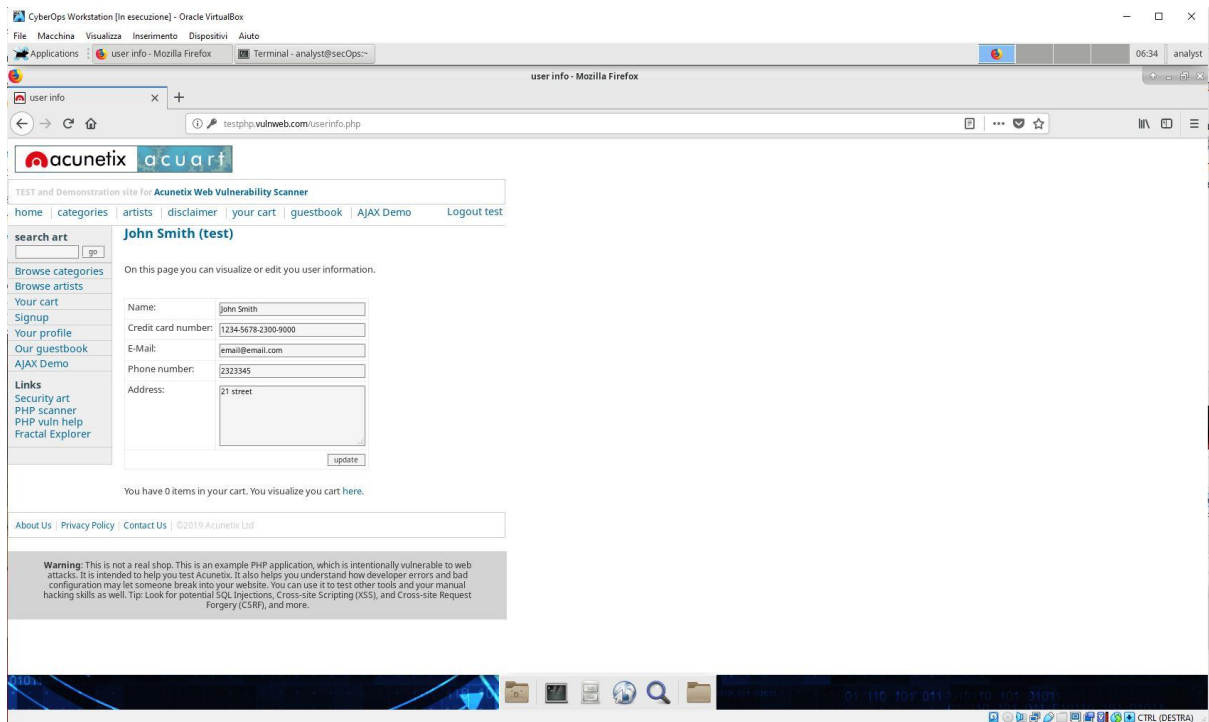
Utilizzare le pagine man di tcpdump per determinare l'utilizzo delle opzioni di comando -s e -w.

d. Aprire un browser web dalla barra di avvio nella VM di CyberOps Workstation. Accedere a <http://testphp.vulnweb.com/login.php>

Poiché questo sito web utilizza HTTP, il traffico non è crittografato. Clicca sul campo Password per visualizzare l'avviso.



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



f. Chiudere il browser web.

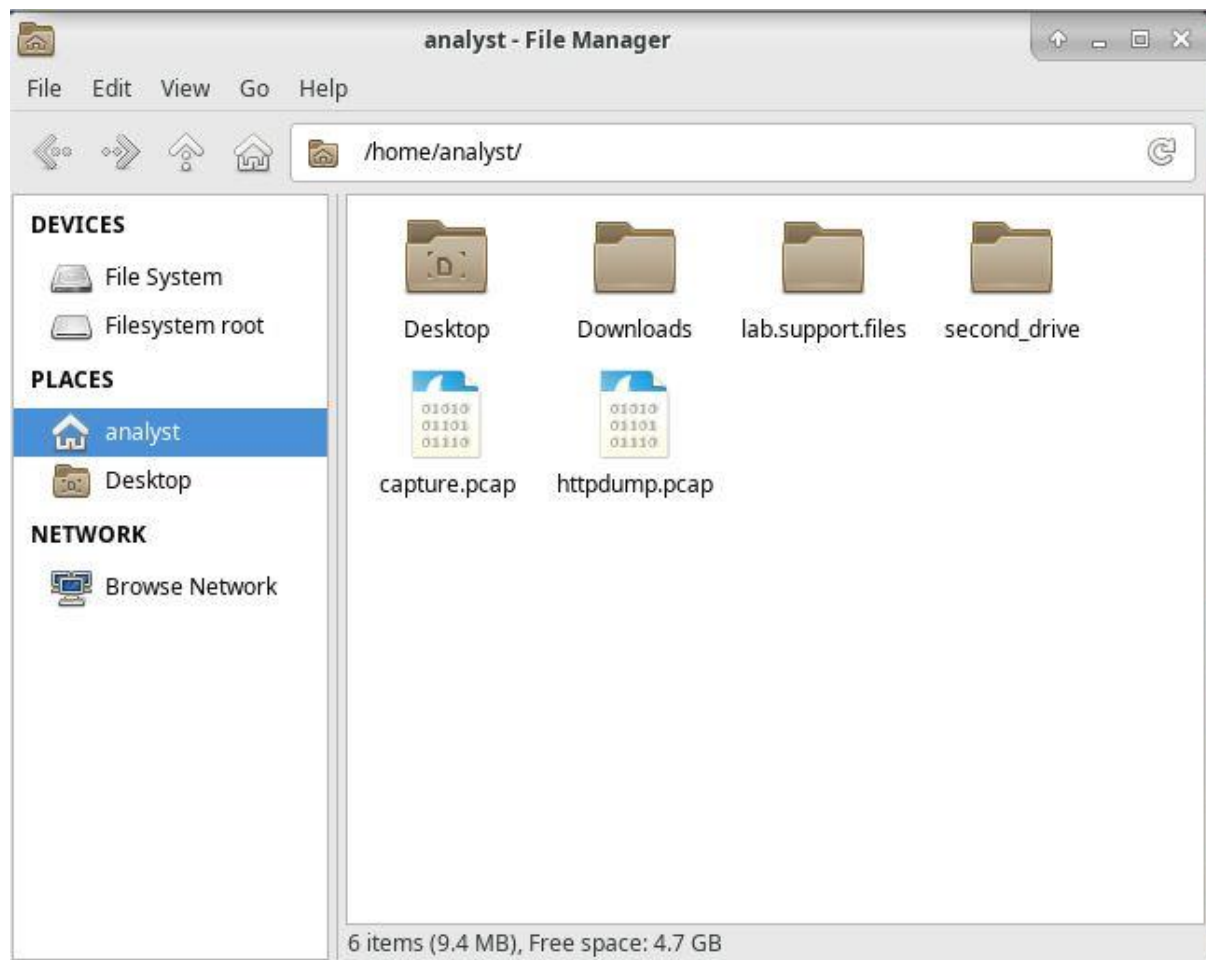
g. Torna alla finestra del terminale in cui è in esecuzione tcpdump. Premi **CTRL+C** per interrompere l'acquisizione dei pacchetti.

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C6927 packets captured
6928 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

Passaggio 3: visualizzare l'acquisizione HTTP.

Il comando tcpdump, eseguito nel passaggio precedente, ha stampato l'output in un file denominato httpdump.pcap. Questo file si trova nella directory home dell'analista **utente** .

a. Fare clic sull'icona del File Manager sul desktop e accedere alla cartella home dell'analista utente . Fare doppio clic sul file **httpdump.pcap** , nella finestra di dialogo Apri con scorrere fino a Wireshark e quindi fare clic su **Apri** .



b. Nell'applicazione Wireshark, filtra per **http** e fai 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** .

CyberOps Workstation [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Applications analyst - File Manager httpdump.pcap [Wireshark ...] [Terminal - analyst@secOps...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4666	300.003733	83.224.69.200	192.168.1.20	OCSP	955	Response
4669	300.007630	83.224.69.200	192.168.1.20	OCSP	955	Response
4949	310.549713	192.168.1.20	44.228.249.3	HTTP	536	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4953	310.738664	44.228.249.3	192.168.1.20	HTTP	342	HTTP/1.1 302 Found (text/html)
4955	310.745825	192.168.1.20	44.228.249.3	HTTP	441	GET /login.php HTTP/1.1
4959	310.937716	44.228.249.3	192.168.1.20	HTTP	2814	HTTP/1.1 200 OK (text/html)
4961	311.077376	192.168.1.20	44.228.249.3	HTTP	463	GET /Flash/add.swf HTTP/1.1
4966	311.262367	44.228.249.3	192.168.1.20	HTTP	1644	HTTP/1.1 206 Partial Content (application/x-shockwave-flash)
5297	338.931150	192.168.1.20	44.228.249.3	HTTP	536	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
5300	339.125100	44.228.249.3	192.168.1.20	HTTP	342	HTTP/1.1 302 Found (text/html)
5301	339.153069	192.168.1.20	44.228.249.3	HTTP	441	GET /login.php HTTP/1.1
5312	339.343555	44.228.249.3	192.168.1.20	HTTP	1374	HTTP/1.1 200 OK (text/html)
5320	339.540663	192.168.1.20	44.228.249.3	HTTP	463	GET /Flash/add.swf HTTP/1.1
5327	339.725881	44.228.249.3	192.168.1.20	HTTP	1644	HTTP/1.1 206 Partial Content (application/x-shockwave-flash)
5538	361.550136	192.168.1.20	44.228.249.3	HTTP	534	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
5563	361.740488	44.228.249.3	192.168.1.20	HTTP	106	HTTP/1.1 200 OK (text/html)
5572	361.876312	192.168.1.20	44.228.249.3	HTTP	493	GET /Flash/add.swf HTTP/1.1
5574	362.079795	44.228.249.3	192.168.1.20	HTTP	2946	[TCP Previous segment not captured] Continuation
5576	362.079850	44.228.249.3	192.168.1.20	HTTP	1644	Continuation
6248	464.463009	192.168.1.20	83.224.69.200	OCSP	497	Request
6250	464.474365	83.224.69.200	192.168.1.20	OCSP	955	Response

▶ Frame 5538: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
 ▶ Ethernet II, Src: PcsCompu_21:05:f7 (08:00:27:21:05:f7), Dst: 14:14:59:38:82:b0 (14:14:59:38:82:b0)
 ▶ Internet Protocol Version 4, Src: 192.168.1.20, Dst: 44.228.249.3
 ▶ Transmission Control Protocol, Src Port: 54902, Dst Port: 80, Seq: 2485, Ack: 15547, Len: 468
 ▶ Hypertext Transfer Protocol
 ▶ HTML Form URL Encoded: application/x-www-form-urlencoded
 ▶ Form item: "uname" = "test"
 ▶ Form item: "pass" = "test"

Quali due informazioni vengono visualizzate?

L'UID dell'amministratore e la password dell'amministratore

e. Chiudere l'applicazione Wireshark.

Parte 2: Acquisizione e visualizzazione del traffico HTTPS

Ora utilizzerai tcpdump dalla riga di comando di una workstation Linux 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: avviare tcpdump da un terminale.

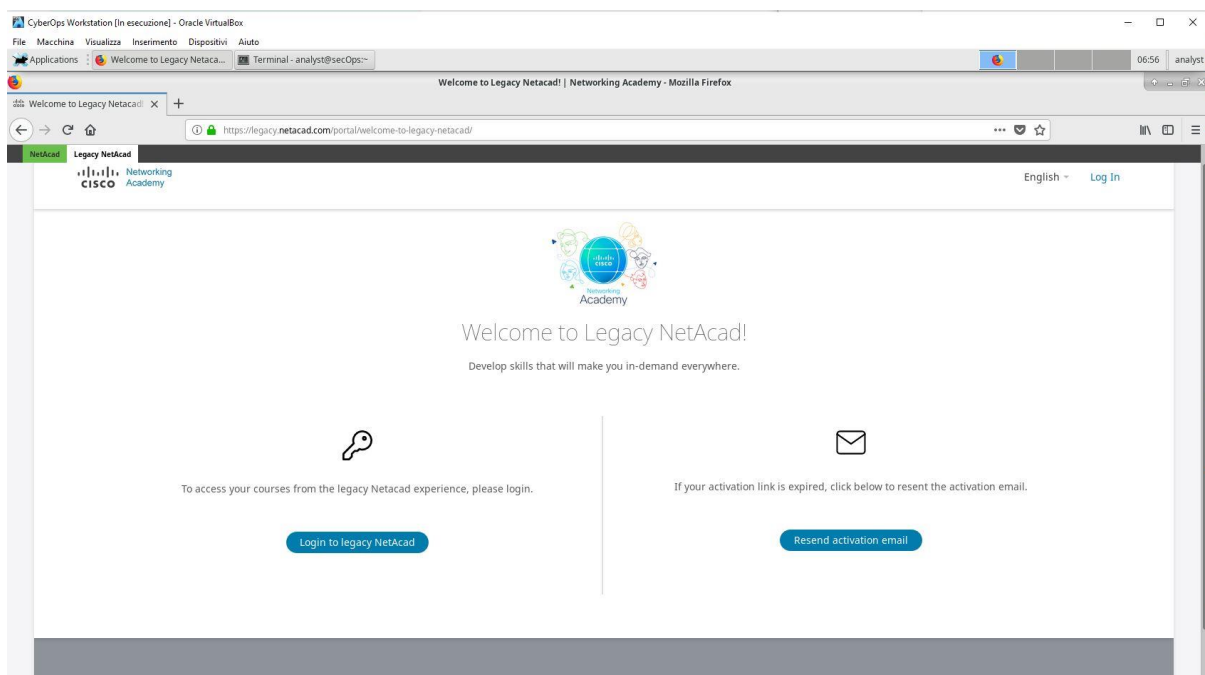
a. Nell'applicazione terminale, digitare il comando `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`. Inserire la password cyberops per l'analista utente quando richiesto.


```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Questo comando avvierà tcpdump e registrerà il traffico di rete sull'interfaccia **enp0s3** della workstation Linux. Se l'interfaccia è diversa da enp0s3, modificarla quando si utilizza il comando precedente.

Tutto il traffico registrato verrà stampato nel file **httpsdump.pcap** nella directory home dell'analista utente.

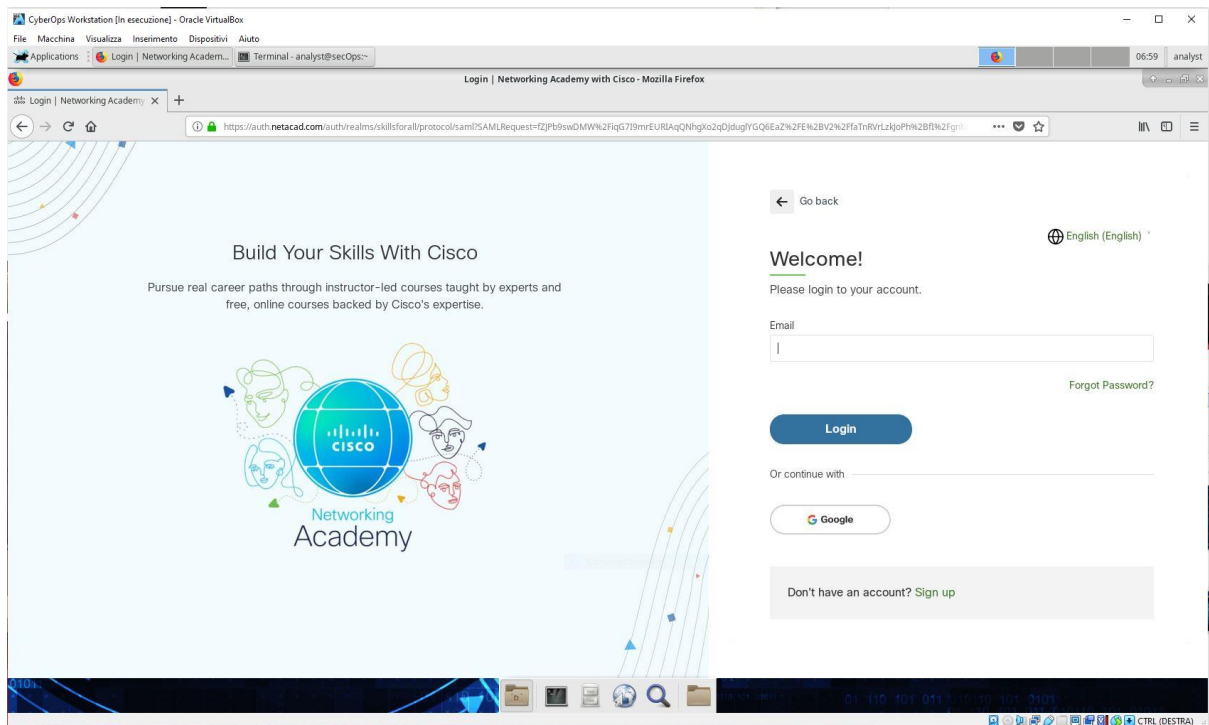
b. Aprire un browser web dalla barra di avvio nella VM di CyberOps Workstation. Accedere a www.netacad.com .



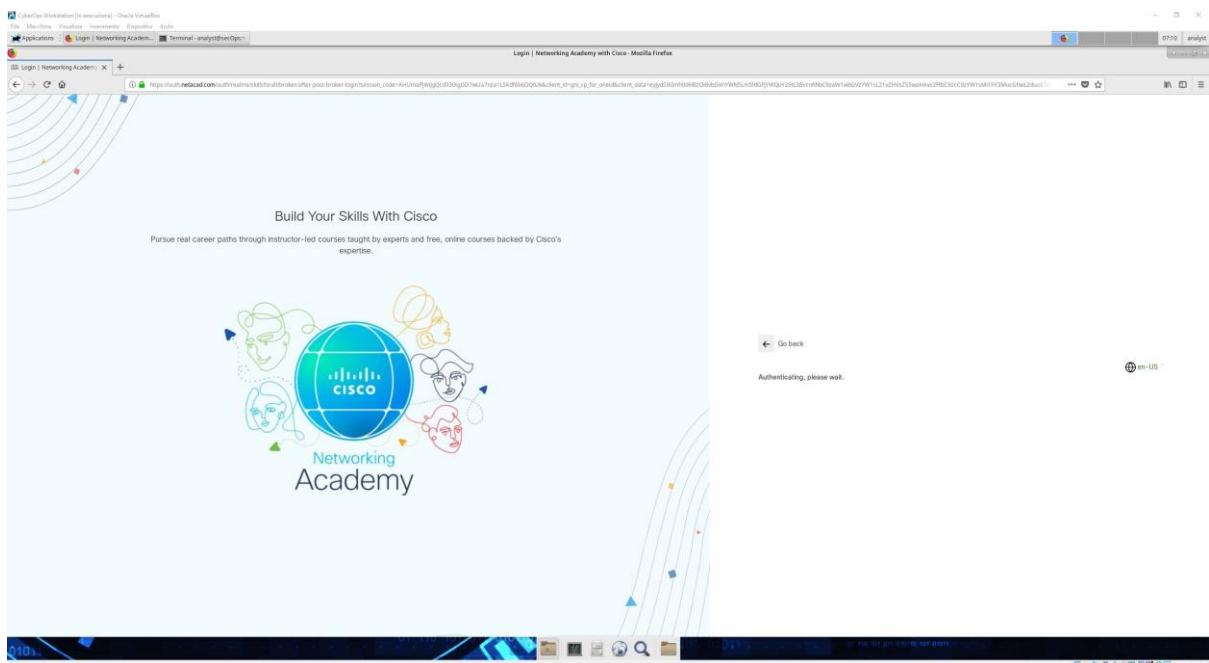
Cosa noti riguardo all'URL del sito web?

Le risposte variano. Il sito web utilizza HTTPS ed è presente un lucchetto.

c. Fare clic su **Accedi** .



d. Inserisci il nome utente e la password. Fai clic su **Avanti** .



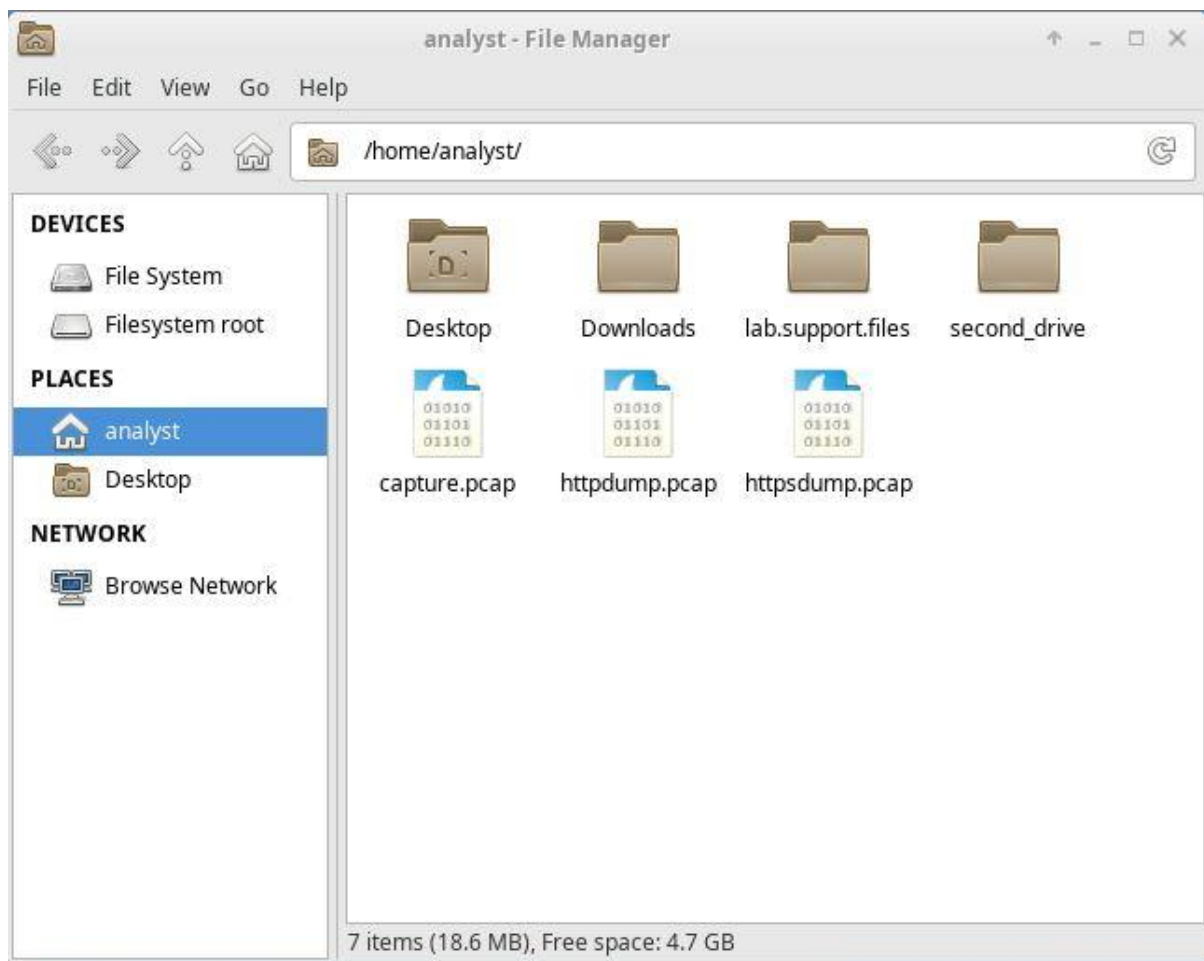
e. Chiudere il browser web nella VM.

f. Tornare alla finestra del terminale in cui è in esecuzione tcpdump. Premere **CTRL+C** per interrompere l'acquisizione dei pacchetti.

Passaggio 2: visualizzare l'acquisizione HTTPS.

Il comando tcpdump eseguito nel passaggio 1 ha stampato l'output in un file denominato httpsdump.pcap. Questo file si trova nella directory home dell'analista **utente** .

a. Fare clic sull'icona del file system sul desktop e accedere alla cartella home dell'analista utente. Aprire il file **httpsdump.pcap** .



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

Immetti **tcp.port==443** come filtro e fai clic su **Applica** .

CyberOps Workstation [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Applications analyst - File Manager httpsdump.pcap [Wireshark...] [Terminal - analyst@secOps...]

httpsdump.pcap [Wireshark]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

No.	Time	Source	Destination	Protocol	Length	Info
189	91.668963	192.168.1.20	34.120.5.221	TCP	74	60006 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=946697059 TSecr=0 WS=1
190	91.669023	192.168.1.20	34.120.5.221	TCP	74	60008 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=946697060 TSecr=0 WS=1
191	91.688154	34.120.5.221	192.168.1.20	TCP	74	443 → 60006 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1752258832 TSecr=0
192	91.688188	192.168.1.20	34.120.5.221	TCP	66	60006 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=946697079 TSecr=1752258832
193	91.690139	34.120.5.221	192.168.1.20	TCP	74	443 → 60008 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1952080491 TSecr=0
194	91.690169	192.168.1.20	34.120.5.221	TCP	66	60008 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=946697081 TSecr=1952080491
195	91.693200	192.168.1.20	34.120.5.221	TLSv1.2	268	Client Hello
196	91.693553	192.168.1.20	34.120.5.221	TLSv1.2	268	Client Hello
197	91.713236	34.120.5.221	192.168.1.20	TCP	66	443 → 60006 [ACK] Seq=1 Ack=203 Win=268800 Len=0 TSval=1752258856 TSecr=946697084
198	91.713408	34.120.5.221	192.168.1.20	TCP	66	443 → 60008 [ACK] Seq=1 Ack=203 Win=268800 Len=0 TSval=1952080514 TSecr=946697084
199	91.715751	34.120.5.221	192.168.1.20	TLSv1.2	1466	Server Hello
200	91.715813	192.168.1.20	34.120.5.221	TCP	66	60008 → 443 [ACK] Seq=203 Ack=1401 Win=32128 Len=0 TSval=946697106 TSecr=1952080517
201	91.716486	34.120.5.221	192.168.1.20	TLSv1.2	1466	Certificate [TCP segment of a reassembled PDU]
202	91.716506	192.168.1.20	34.120.5.221	TCP	66	60008 → 443 [ACK] Seq=203 Ack=2801 Win=35072 Len=0 TSval=946697107 TSecr=1952080517
203	91.716645	34.120.5.221	192.168.1.20	TLSv1.2	301	Server Key Exchange, Server Hello Done
204	91.716658	192.168.1.20	34.120.5.221	TCP	66	60008 → 443 [ACK] Seq=203 Ack=3036 Win=37888 Len=0 TSval=946697107 TSecr=1952080517
205	91.717530	34.120.5.221	192.168.1.20	TLSv1.2	2866	Server Hello, Certificate
206	91.717553	192.168.1.20	34.120.5.221	TCP	66	60006 → 443 [ACK] Seq=203 Ack=2801 Win=34816 Len=0 TSval=946697108 TSecr=1752258860
207	91.718440	34.120.5.221	192.168.1.20	TLSv1.2	301	Server Key Exchange, Server Hello Done
208	91.718462	192.168.1.20	34.120.5.221	TCP	66	60006 → 443 [ACK] Seq=203 Ack=3036 Win=37632 Len=0 TSval=946697109 TSecr=1752258860
209	91.722969	192.168.1.20	34.120.5.221	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
210	91.730847	192.168.1.20	34.120.5.221	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
211	91.750668	34.120.5.221	192.168.1.20	TLSv1.2	377	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
212	91.751651	34.120.5.221	192.168.1.20	TLSv1.2	135	Application Data

Frame 212: 135 bytes on wire (1080 bits). 135 bytes captured (1080 bits)

Ethernet II, Src: 14:14:59:38:82:b0 (14:14:59:38:82:b0), Dst: PcsCompu_21:05:f7 (08:00:27:21:05:f7)

Internet Protocol Version 4, Src: 34.120.5.221, Dst: 192.168.1.20

Transmission Control Protocol, Src Port: 443, Dst Port: 60008, Seq: 3347, Ack: 296, Len: 69

Secure Sockets Layer

TLSv1.2 Record Layer: Application Data Protocol: http2

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 64

Encrypted Application Data: 00000000000000011a9a38ba1394eea2bbc949d366591493...

0000 08 00 27 21 05 f7 14 14 59 38 82 b0 08 00 45 00 ...Y8...E

0010 00 79 12 3c 00 00 76 06 48 32 22 78 05 dd c0 a8 ...y<...v. H2"x...

0020 01 14 01 bb ea 68 ed 00 98 4f 68 8c 23 5e 80 18 ...h...Oh.#^...

0030 04 1a b9 88 00 00 01 01 08 0a 74 5a 62 a1 38 6d ...tZb.8m...

c. Sfoglia i diversi messaggi HTTPS e seleziona un messaggio **Dati applicazione** .

f. Fare clic su **Dati applicazione crittografati** .

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

Il payload dei dati è crittografato tramite TLSv1.2 e non può essere visualizzato.

e. Espandere completamente la sezione **Secure Sockets Layer** .

f. Fare clic su **Dati applicazione crittografati** .

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

Il payload dei dati è crittografato tramite TLSv1.2 e non può essere visualizzato.

g. Chiudere tutte le finestre e arrestare la macchina virtuale.

Domande di riflessione

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

Quando si utilizza HTTPS, il carico di 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 e allo stesso tempo catturare dati e accessi degli utenti.

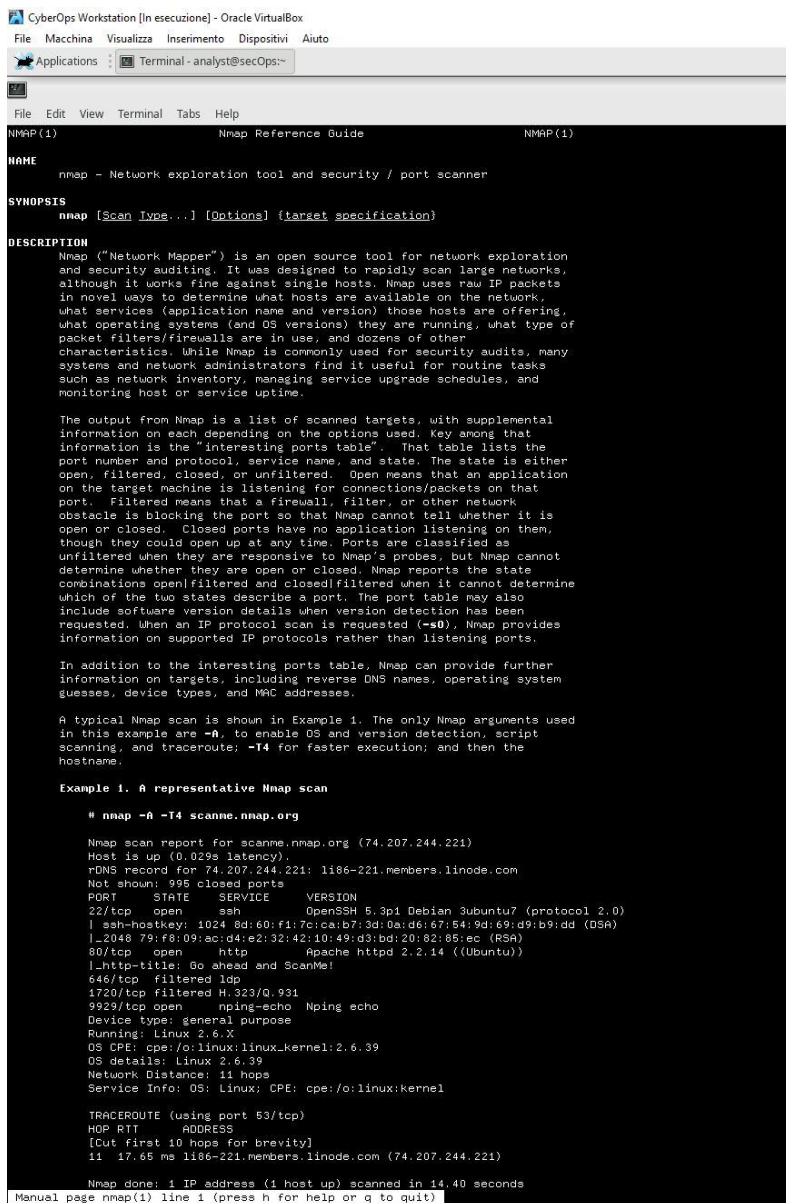
Bonus 1 Laboratorio - Esplorazione di Nmap

Parte 1: Esplorazione di Nmap

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

Il comando **man** [programma | *utilità* | *funzione*] visualizza le pagine di manuale associate agli argomenti. Le pagine di manuale sono i manuali di riferimento disponibili sui sistemi operativi Unix e Linux. Queste pagine possono includere le seguenti sezioni: Nome, Sinossi, Descrizioni, Esempi e Vedere anche.

- Avviare la VM CyberOps Workstation.
- Aprire un terminale.
- Al prompt del terminale, digitare `man nmap`.



```
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Terminal - analyst@secOps:~

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
information is the "interesting ports table". That table lists the
port number and protocol, service name, and state. The state is either
open, filtered, closed, or unfiltered. Open means that an application
on the target machine is listening for connections/packets on that
port. Filtered means that a firewall, filter, or other network
obstacle is blocking the port so that Nmap cannot tell whether it is
open or closed. Closed ports have no application listening on them,
though they could open up at any time. Ports are classified as
unfiltered when they are responsive to Nmap's probes, but Nmap cannot
determine whether they are open or closed. Nmap reports the state
combinations open/filtered and closed/filtered when it cannot determine
which of the two states describe a port. The port table may also
include software version details when version detection has been
requested. When an IP protocol scan is requested (-s0), Nmap provides
information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further
information on targets, including reverse DNS names, operating system
guesses, device types, and MAC addresses.

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: 1186-221.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:ds:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f6:00:ac:d4:c2:32:42:10:49:d3:bd:20:02:65:ee (RSA)
80/tcp    open  http     Apache/2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldp
1720/tcp  filtered H.323/Q.931
9929/tcp  open  nping-echo Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
[Cut first 10 hops for brevity]
11 17.65 ms 1186-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
Manual page nmap(1) line 1 (press h for help or q to quit)
```

Che cosa è Nmap?

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

A cosa serve nmap?

Nmap viene utilizzato per scansionare una rete e determinare gli host disponibili e i servizi offerti al suo interno. Alcune delle funzionalità di Nmap includono la scoperta degli host, la scansione delle porte e il rilevamento del sistema operativo. Nmap può essere comunemente utilizzato per audit di sicurezza, per

identificare porte aperte, effettuare inventari di rete e individuare vulnerabilità nella rete.

d. Nella pagina man, puoi usare 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 una barra (/) o un punto interrogativo (?) seguito dal termine o dalla frase. La barra consente di cercare in avanti nel documento, mentre il punto interrogativo consente di cercare all'indietro. Il tasto n consente di passare alla corrispondenza successiva.

Digita **/example** e premi INVIO. Questo cercherà la parola **example** in avanti nella pagina man

e. Nel primo esempio, vedi tre corrispondenze. Per passare alla corrispondenza successiva, premi n.

Guarda l'esempio 1.

A cosa serve il comando nmap?

```
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

A cosa serve l'interruttore -T4?

-T4 per un'esecuzione più rapida impedendo al ritardo della scansione dinamica di superare i 10 ms per le porte TCP. -T4 è consigliato per una connessione a banda larga o Ethernet adeguata.

f. Scorri la pagina per saperne di più su nmap. Digita **q** al termine.

Parte 2: Scansione delle porte aperte

In questa parte, utilizzerai gli switch dell'esempio nelle pagine man di Nmap per eseguire la scansione del tuo localhost, della tua rete locale e di un server remoto su scanme.nmap.org.

Passaggio 1: esegui la scansione del tuo localhost.

a. Se necessario, aprire un terminale sulla macchina virtuale. Al prompt, digitare `nmap -A -T4 localhost`. A seconda della rete locale e dei dispositivi, la scansione richiederà da pochi secondi a qualche minuto.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:02 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s 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 2
|     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 13.55 seconds
```

b. Rivedi i risultati e rispondi alle seguenti domande.

Quali porte 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: esegui la scansione della rete.

Attenzione: prima di utilizzare Nmap su qualsiasi rete, ottenere l'autorizzazione dei proprietari della rete prima di procedere.

a. Al prompt dei comandi del terminale, digitare Invio `ip address` per determinare l'indirizzo IP e la subnet mask di questo host. In questo esempio, l'indirizzo IP di questa VM è 192.168.1.20/24 e la subnet mask è 255.255.255.0.

```
[analyst@sec0ps ~]$ 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 08:00:27:21:05:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.20/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 80523sec preferred_lft 80523sec
    inet6 fe80::a00:27ff:fe21:5f7/64 scope link
        valid_lft forever preferred_lft forever
[analyst@sec0ps ~]$
```

Registra l'indirizzo IP e la maschera di sottorete della tua VM.

A quale rete appartiene la tua VM?

Le risposte possono variare. Questa macchina virtuale ha un indirizzo IP 192.168.1.20/24 e fa parte della rete 192.168.1.0/24.

b. Per individuare altri host su questa LAN, digitare `nmap -A -T4 network address/prefix`. L'ultimo ottetto dell'indirizzo IP deve essere sostituito con uno zero. Ad esempio, nell'indirizzo IP 192.168.1.20/24 è l'ultimo ottetto. Pertanto, l'indirizzo di rete è 10.0.2.0. /24 è chiamato prefisso ed è un'abbreviazione della netmask 255.255.255.0. Se la macchina virtuale ha una netmask diversa, cercare su 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 10.0.2.0/24.

```
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Terminal - analyst@secOps:~
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:28 EDT
[analyst@secOps ~]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:29 EDT
WARNING: Service 192.168.1.1:49152 had already soft-matched upnp, but now soft-matched rtsp; ignoring second value
WARNING: Service 192.168.1.1:49152 had already soft-matched upnp, but now soft-matched sip; ignoring second value
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.0080s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open  domain      dnsmasq 2.84
| dns-nsid:
|_ bind.version: dnsmasq-2.84
80/tcp    open  http?
|_ fingerprint-strings:
|_ GetRequest, HTTPOptions:
|_   UNKNOWN 400 Bad Request
|_   Server:
|_   Date: Fri, 11 Apr 2025 12:29:57 GMT
|_   Cache-Control: no-cache,no-store,max-age=0
|_   Pragma: no-cache
|_   X-Frame-Options: DENY
|_   Expires: 0
|_   X-Content-Type-Options: nosniff
|_   X-XSS-Protection: 0; mode=block
|_   Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:
|_   Content-Language: en
|_   Content-Type: text/html
|_   Connection: close
|_   <HTML>
|_   <HEAD><TITLE>400 Bad Request</TITLE></HEAD>
|_   <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
|_   <H4>400 Bad Request</H4>
|_   Invalid Request
|_   NULL:
|_   UNKNOWN 408 Request Timeout
|_   Server:
|_   Date: Fri, 11 Apr 2025 12:29:57 GMT
|_   Cache-Control: no-cache,no-store,max-age=0
|_   Pragma: no-cache
|_   X-Frame-Options: DENY
|_   Expires: 0
|_   X-Content-Type-Options: nosniff
|_   X-XSS-Protection: 0; mode=block
|_   Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:
|_   Content-Language: en
|_   Content-Type: text/html
|_   Connection: close
|_   <HTML>
|_   <HEAD><TITLE>408 Request Timeout</TITLE></HEAD>
|_   <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
```

Quanti host sono attivi?

3.

Dai risultati di Nmap, elenca gli indirizzi IP degli host che si trovano sulla stessa LAN della tua VM. Elenca alcuni dei servizi disponibili sugli host rilevati.

3 servizi disponibili.

```
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Applications  Terminal - analyst@secOps:~

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
information is the "interesting ports table". That table lists the
port number and protocol, service name, and state. The state is either
open, filtered, closed, or unfiltered. Open means that an application
on the target machine is listening for connections/packets on that
port. Filtered means that a firewall, filter, or other network
obstacle is blocking the port so that Nmap cannot tell whether it is
open or closed. Closed ports have no application listening on them,
though they could open up at any time. Ports are classified as
unfiltered when they are responsive to Nmap's probes, but Nmap cannot
determine whether they are open or closed. Nmap reports the state
combinations open/filtered and closed/filtered when it cannot determine
which of the two states describe a port. The port table may also
include software version details when version detection has been
requested. When an IP protocol scan is requested (-s0), Nmap provides
information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further
information on targets, including reverse DNS names, operating system
guesses, device types, and MAC addresses.

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: 1186-221.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:ds:67:54:9d:69:d9:b9:dd (DSA)
|_ 2048 79:f6:09:ac:d4:e2:32:42:10:49:d3:bd:20:02:85:ee (RSA)
80/tcp    open  http     Apache/2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered ldap
1720/tcp   filtered H.323/Q.931
9929/tcp   open  nping-echo Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
[Cut first 10 hops for brevity]
11 17.65 ms 1186-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
Manual page nmap(1) line 1 (press h for help or q to quit)
```

```

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:02 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s 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 2
|     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 13.55 seconds

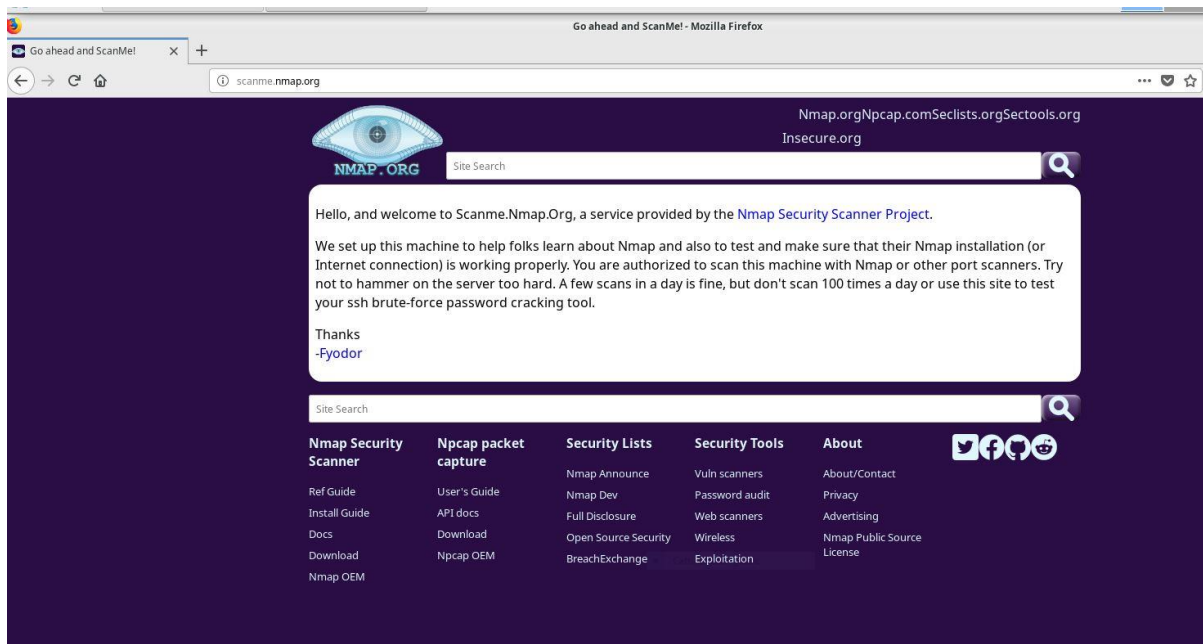
```

Passaggio 3: eseguire la scansione di un server remoto.

a. Apri un browser web e vai su **scanme.nmap.org** . Leggi il messaggio pubblicato.

Qual è lo scopo di questo sito?

Questo sito consente agli utenti di scoprire di più su Nmap e di testarne l'installazione.



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

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 08:45 EDT
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: 995 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)
53/tcp    open  domain       dnsmasq 2.84
|_ dns-nsid:
|_ bind.version: dnsmasq-2.84
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.85 seconds
```

c. Rivedi i risultati e rispondi alle seguenti domande.

Quali porte e servizi sono aperti?

22/tcp: ssh, 9929/tcp: n ping-echo, 31337/tcp: tcpwrapped, 80/tcp: http

Quali porte e servizi vengono filtrati?

Non mi vengono mostrate quelle filtrate

Qual è l'indirizzo IP del server?

Indirizzo IPv4: 45.33.32.156 Indirizzo IPv6: 2600:3c01::f03c:91ff:fe18:bb2f

Qual è il sistema operativo?

Ubuntu Linux

Domanda di riflessione

Nmap è un potente strumento per l'esplorazione e la gestione delle reti. In che modo Nmap può contribuire alla sicurezza delle reti? In che modo Nmap può essere utilizzato da un autore 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 effettuare un inventario di una rete per garantire che tutti i sistemi siano probabilmente aggiornati con le patch di sicurezza. D'altra parte, nmap può essere utilizzato per la ricognizione al fine di individuare porte aperte e altre informazioni sulla rete.

Attacco a un Database MySQL

Parte 1: aprire Wireshark e caricare il file PCAP.

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

a. Avviare la VM CyberOps Workstation.

b. Fare clic su **Applicazioni > CyberOPS > Wireshark** sul desktop e andare all'applicazione Wireshark.

c. Nell'applicazione Wireshark, fare clic su **Apri** al centro dell'applicazione, sotto File.

d. Sfogliare la directory **/home/analyst/** e cercare **lab.support.files** . Nella directory **lab.support.files** , aprire il file **SQL_Lab.pcap** .

e. Il file PCAP si apre in Wireshark e mostra il traffico di rete acquisito.

The screenshot displays the Wireshark 2.5.1 interface. The top pane shows a list of 25 packets. The middle pane shows the details of the selected packet (No. 25), which is an HTTP GET request. The request body contains an SQL injection payload: `id=1∨=1--`. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.00081	10.0.2.4	10.0.2.15	HTTP	454	POST /index.php.php HTTP/1.1 applications/javascript
5	0.002149	10.0.2.15	10.0.2.4	TCP	60	60 --> 35414 [ACK] Seq=1 Ack=383 Win=30236 Len=0 TSV=45838
6	0.005700	10.0.2.4	10.0.2.15	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	HTTP	60	35414 --> 35414 [ACK] Seq=383 Ack=385 Win=30236 Len=0 TSV=45840 TSV=38338
8	0.014145	10.0.2.4	10.0.2.15	HTTP	406	GET /index.php.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	10.0.2.15	10.0.2.15	TCP	60	35414 --> 35414 [ACK] Seq=101 Ack=3408 Win=34480 Len=0 TSV=45843 TSV=38339
11	0.048425	10.0.2.4	10.0.2.15	HTTP	429	GET /index.php.php HTTP/1.1
12	0.050480	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/html)
13	174.254400	10.0.2.4	10.0.2.15	HTTP	530	GET /index.php.php?id=1∨=1--&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	60	--> 35414 [ACK] Seq=1 Ack=417 Win=235 Len=0 TSV=46101 TSV=98114
15	174.254768	10.0.2.4	10.0.2.15	HTTP	1801	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /index.php.php?id=1∨=1--&Submit=Submit HTTP/1.1
17	220.490687	10.0.2.15	10.0.2.4	TCP	60	--> 35440 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSV=46160 TSV=111885
18	220.493895	10.0.2.4	10.0.2.15	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	60	GET /index.php.php?id=1∨=1--&Submit=Submit HTTP/1.1
20	277.727871	10.0.2.15	10.0.2.4	TCP	60	--> 35442 [ACK] Seq=1 Ack=585 Win=236 Len=0 TSV=461793 TSV=129156
21	277.728280	10.0.2.4	10.0.2.15	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.719120	10.0.2.4	10.0.2.15	HTTP	60	GET /index.php.php?id=1∨=1--&Submit=Submit HTTP/1.1
23	313.719277	10.0.2.15	10.0.2.4	TCP	60	--> 35444 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSV=461866 TSV=139951
24	313.72414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277832	10.0.2.4	10.0.2.15	HTTP	680	GET /index.php.php?id=1∨=1--&Submit=Submit HTTP/1.1
26	383.278171	10.0.2.15	10.0.2.4	TCP	60	--> 35446 [ACK] Seq=1 Ack=613 Win=236 Len=0 TSV=462038 TSV=168821
27	383.284209	10.0.2.4	10.0.2.15	HTTP	406	HTTP/1.1 200 OK (text/html)
28	481.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /index.php.php?id=1∨=1--&Submit=Submit HTTP/1.1
29	481.804242	10.0.2.15	10.0.2.4	TCP	60	--> 35448 [ACK] Seq=1 Ack=613 Win=236 Len=0 TSV=462038 TSV=173879
30	481.805708	10.0.2.15	10.0.2.4	HTTP	2001	HTTP/1.1 200 OK (text/html)

Packet Details (No. 25):

- Frame 25 on wire (16728 bits): 2091 bytes captured (16728 bits) on interface 0
- Ethernet II, Src: PcsCom_94:4d:68:02:27:48, Dst: PcsCom_94:4d:68:02:27:48
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
- Transmission Control Protocol, Src Port: 80, Dst Port: 35446, Seq: 1, Ack: 620, Len: 2025
- Hypertext Transfer Protocol
- Line-based text data (text/html) (168 lines)

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

10.0.2.4 e 10.0.2.15

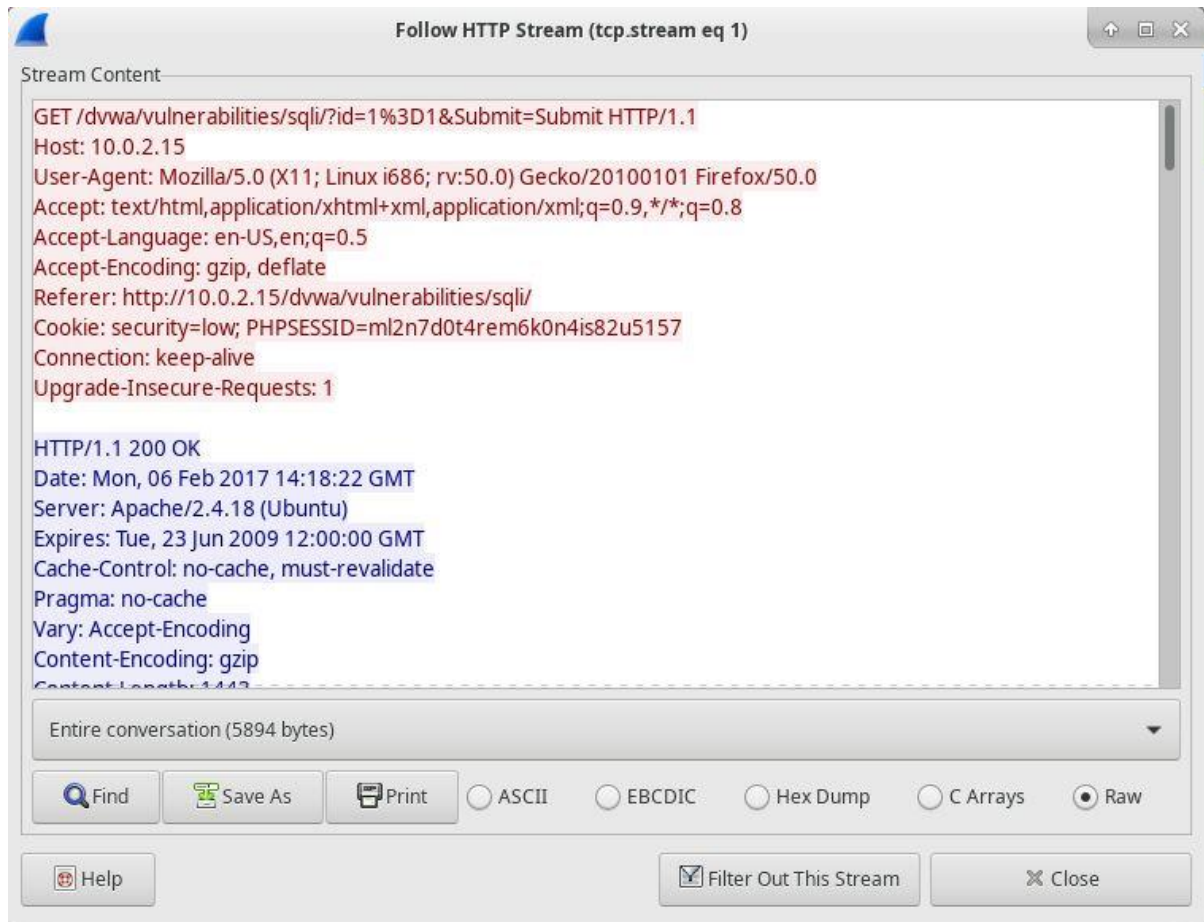
Parte 2: Visualizza l'attacco SQL Injection.

In questa fase, vedrai l'inizio di un attacco.

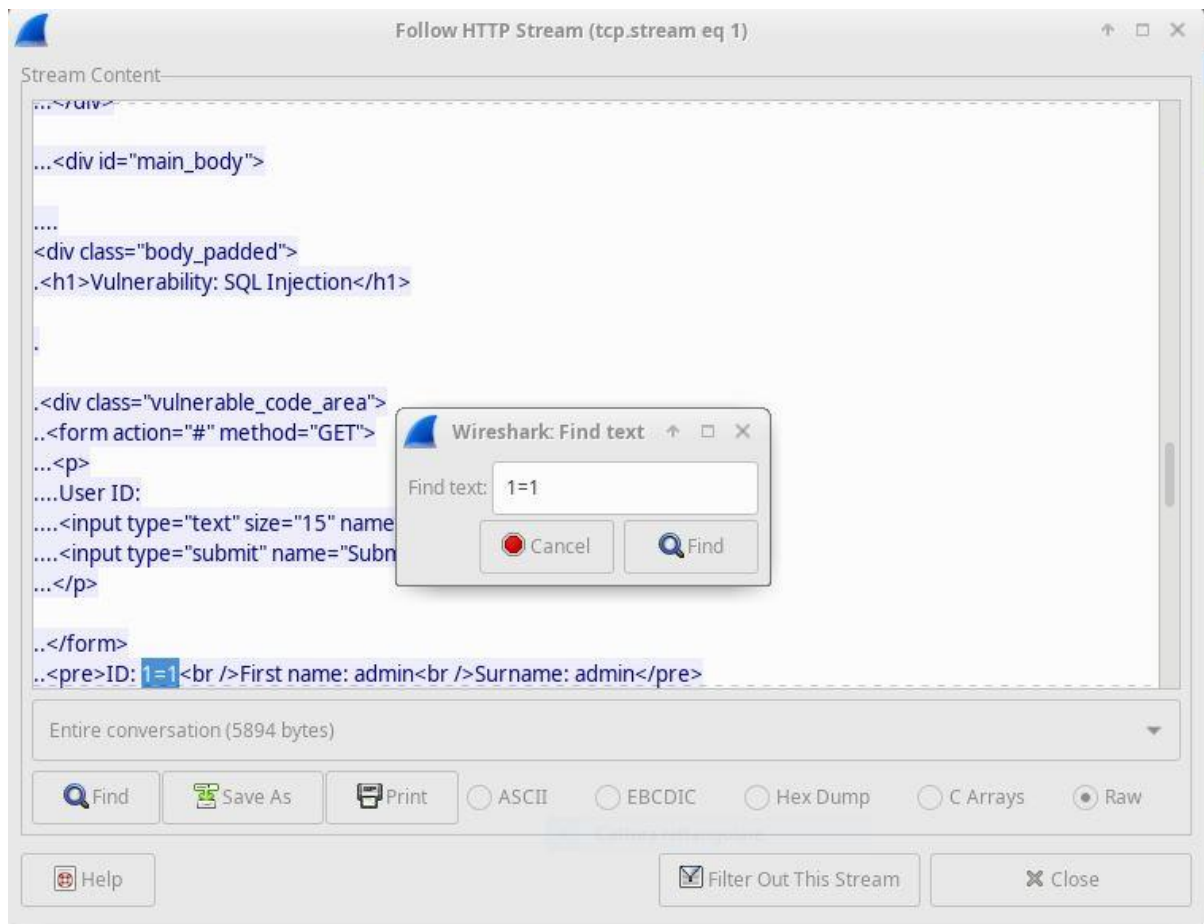
a. All'interno dell'acquisizione Wireshark, fare clic con il pulsante destro del mouse sulla riga 13 e selezionare **Segui > Flusso HTTP** . La riga 13 è stata scelta perché si tratta di una richiesta HTTP GET. Questo sarà molto utile per seguire il flusso di dati così come viene visualizzato dai livelli applicativi e per condurre al test delle query per l'iniezione SQL.

I traffico sorgente è mostrato in rosso. La sorgente ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo **Trova** , inserisci **1=1** .



c. L'attaccante ha inserito una query (1=1) in una casella di ricerca UserID sulla destinazione 10.0.2.15 per verificare se l'applicazione è vulnerabile a SQL injection. Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con un record da un database. L'attaccante ha verificato di poter inserire un comando SQL e il database ha risposto. La stringa di ricerca 1=1 crea un'istruzione SQL che sarà sempre vera. Nell'esempio, indipendentemente da ciò che viene inserito nel campo, sarà sempre vera.



d. Chiudere la finestra Segui flusso HTTP.

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

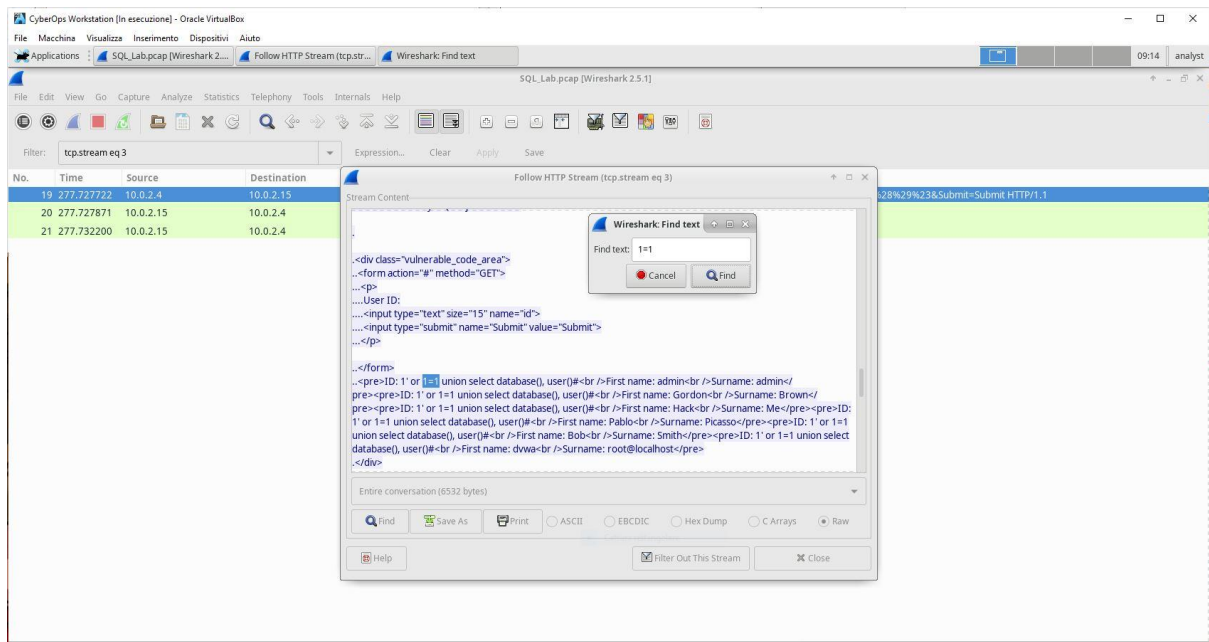
Parte 3: L'attacco SQL Injection continua...

In questa fase, verrà visualizzato il proseguimento di un attacco.

a. 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**. Fai clic su **Trova successivo**.

c. L'attaccante ha inserito una query (1' o 1=1 union select database(), user()#) in una casella di ricerca UserID sulla destinazione 10.0.2.15. Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con le seguenti informazioni:



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 di Wireshark.

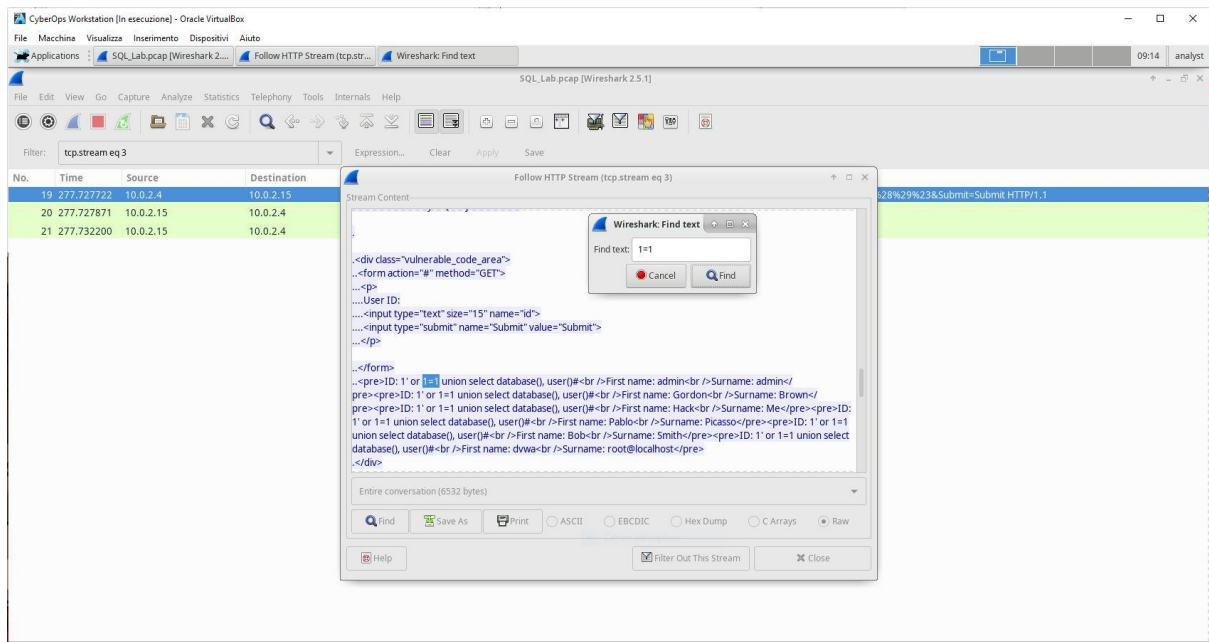
Parte 4: L'attacco SQL Injection fornisce informazioni di sistema.

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

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

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

c. L'attaccante 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'identificativo della versione. Si noti come l'identificativo della versione si trovi 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 di Wireshark.

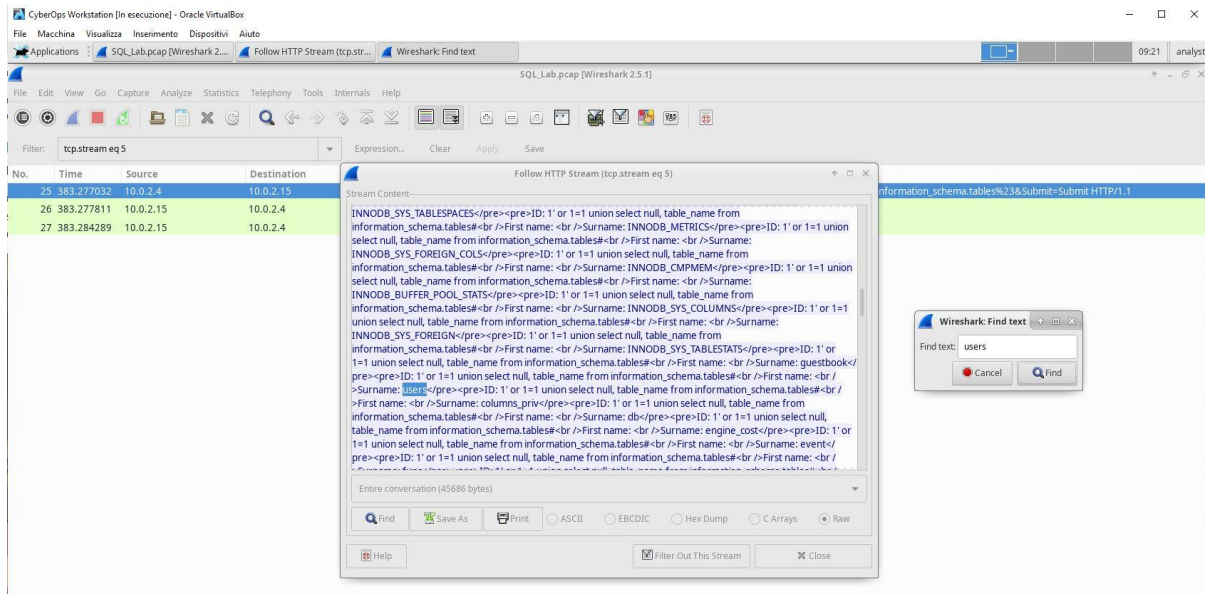
Parte 5: L'attacco SQL Injection e le informazioni della tabella.

L'attaccante sa che esiste un gran numero di tabelle SQL piene di informazioni e cerca di trovarle.

a. All'interno dell'acquisizione Wireshark, fai clic con il pulsante destro del mouse sulla riga 25 e seleziona **Segui > Flusso HTTP** . La sorgente è visualizzata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo **Trova** , inserisci **utenti** . Fai clic su **Trova successivo** .

c. L'attaccante ha inserito una query (1'or 1=1 union select null, table_name from information_schema.tables#) in una casella di ricerca UserID sul target 10.0.2.15 per visualizzare tutte le tabelle del database. Ciò fornisce un output enorme con numerose tabelle, poiché l'attaccante ha specificato "null" senza ulteriori specifiche.



Cosa farebbe il comando modificato (**1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'**) per l'attaccante?

Il database risponderebbe con un output molto più breve, filtrato in base alla presenza della parola "utenti".

d. Chiudere la finestra Segui flusso HTTP.

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

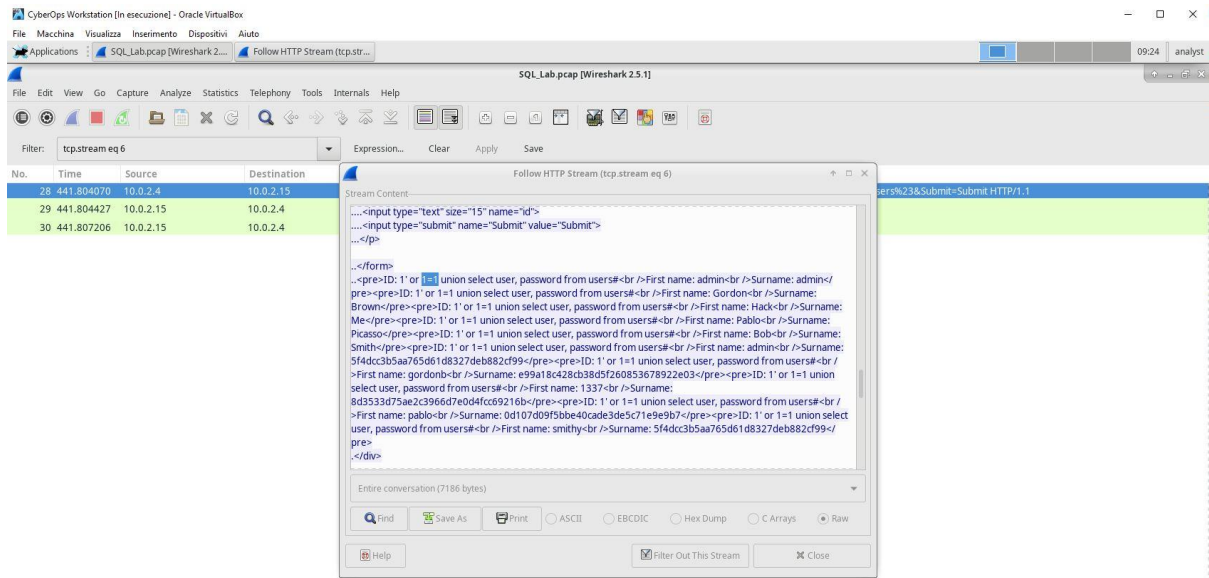
Parte 6: Conclusione dell'attacco SQL Injection.

L'attacco si conclude con il premio più ambito: gli hash delle password.

a. All'interno dell'acquisizione Wireshark, fare clic con il pulsante destro del mouse sulla riga 28 e selezionare **Segui > Flusso HTTP** . La sorgente è visualizzata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Fai clic su **Trova** e digita **1=1** . Cerca questa voce. Una volta trovato il testo, fai clic su **Annulla** nella casella di ricerca "Trova testo".

L'attaccante ha inserito una query (1'or 1=1 union select user, password from users#) in una casella di ricerca UserID sulla destinazione 10.0.2.15 per estrarre nomi utente e hash delle password!



Quale utente ha l'hash della password 8d3533d75ae2c3966d7e0d4fcc69216b?

1337

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

Qual è la password in chiaro?

Charley

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

Domande di riflessione

1. Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?

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

2. Naviga su internet e cerca "prevenire attacchi SQL injection". Quali sono due metodi o misure che si possono adottare per prevenire gli attacchi SQL injection?

Le risposte possono variare, ma dovrebbero includere: filtrare l'input dell'utente, implementare un firewall per applicazioni web, disabilitare funzionalità/capacità del database non necessarie, monitorare le istruzioni SQL, utilizzare parametri con procedure archiviate e utilizzare parametri con SQL dinamico.