**S11-L5 Lab – Utilizzo di Windows PowerShell**

**INDICE**

Laboratorio 1……………………………………………………pg 1

accedere alla console di PowerShell……………………pg 2

Esplora i comandi…………………………………………….pg 3

Esplora i cmdlet……………………………………………….pg 4

comando netstat utilizzando PowerShell……………..pg 5

Svuotare il cestino tramite PowerShell…………………pg 7

Laboratorio 2…………………………………………………...pg 8

Cattura http ………………………………………………..…..pg 8

Cattura https………………………………………….………..pg 11

Bonus 1………………………………………………….……….pg 14

Bonus 2……………………………………………………………pg 20

**LABORATORIO 1**

**OBIETTIVI**

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

**ISTRUZIONI**

Parte 1: accedere alla console di PowerShell.

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

Parte 3: Esplora i cmdlet.

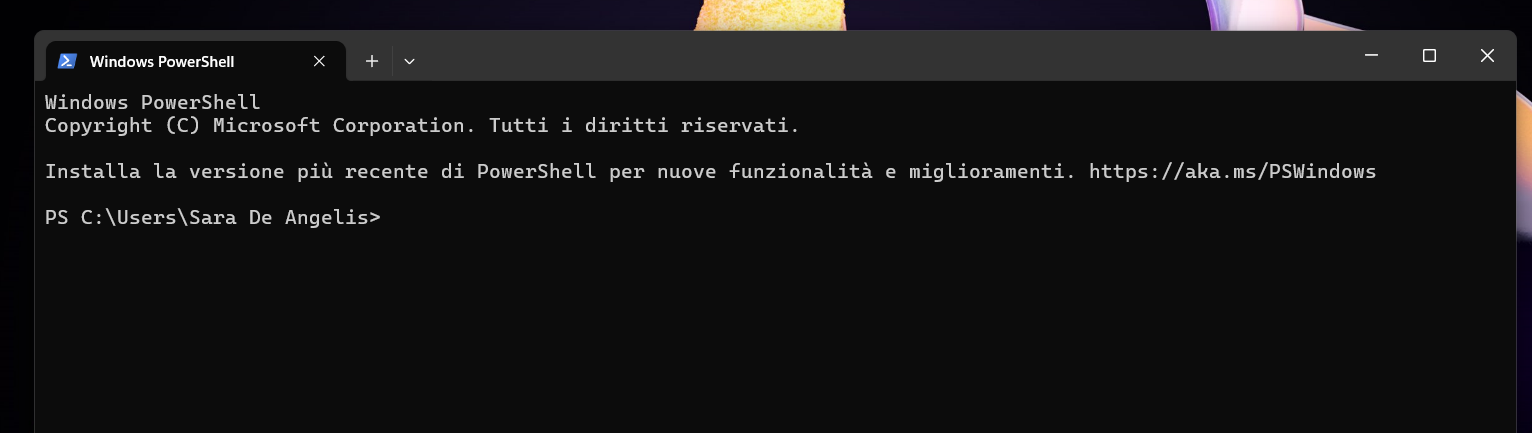
Parte 4: Esplora il comando netstat utilizzando PowerShell.

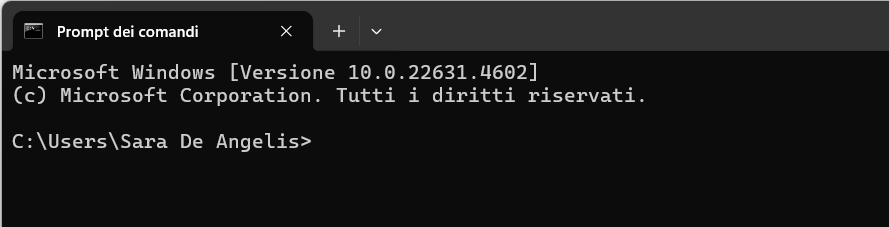
Parte 5: Svuotare il cestino tramite PowerShell.

**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 .



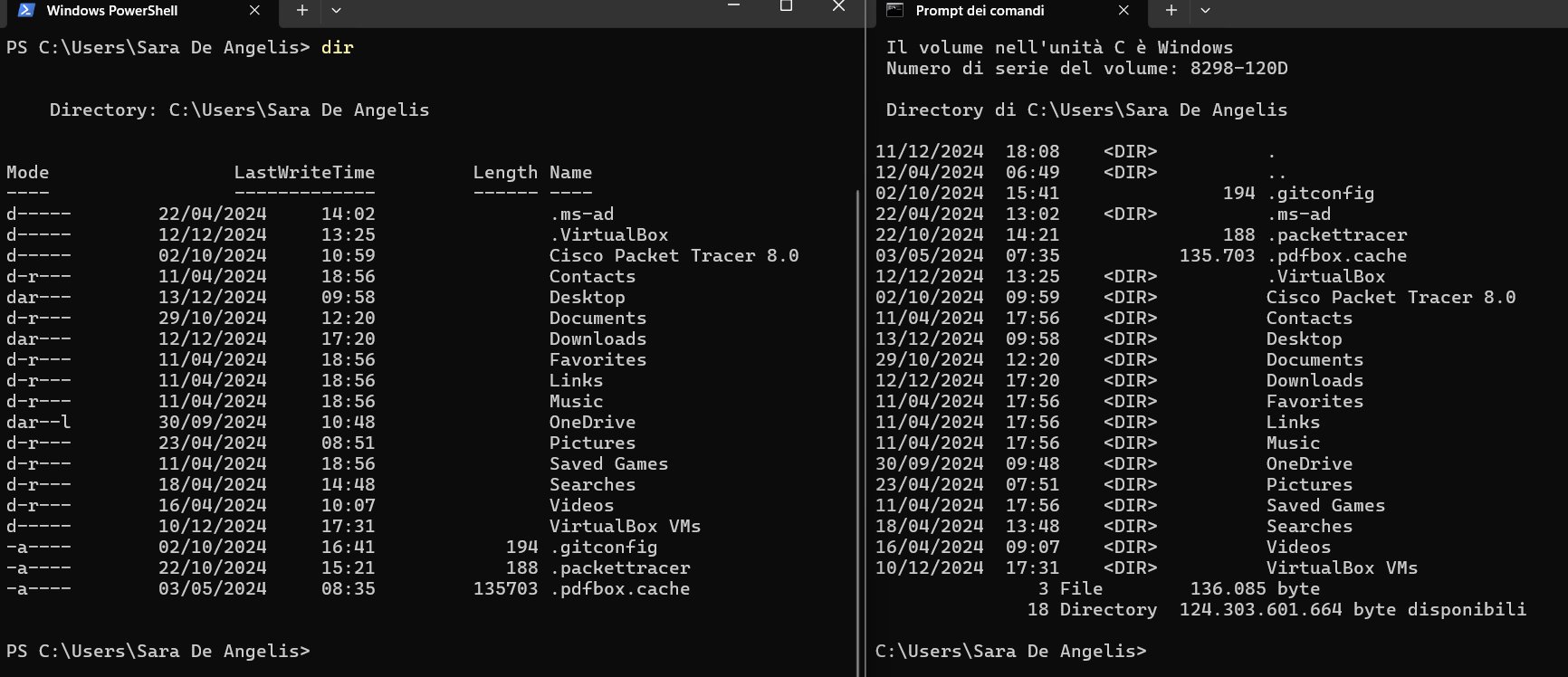


**Parte 2: Esplora i comandi del prompt dei comandi e di PowerShell.**

a. Immettere dir al prompt in entrambe le finestre.

Quali sono gli output del dircomando?

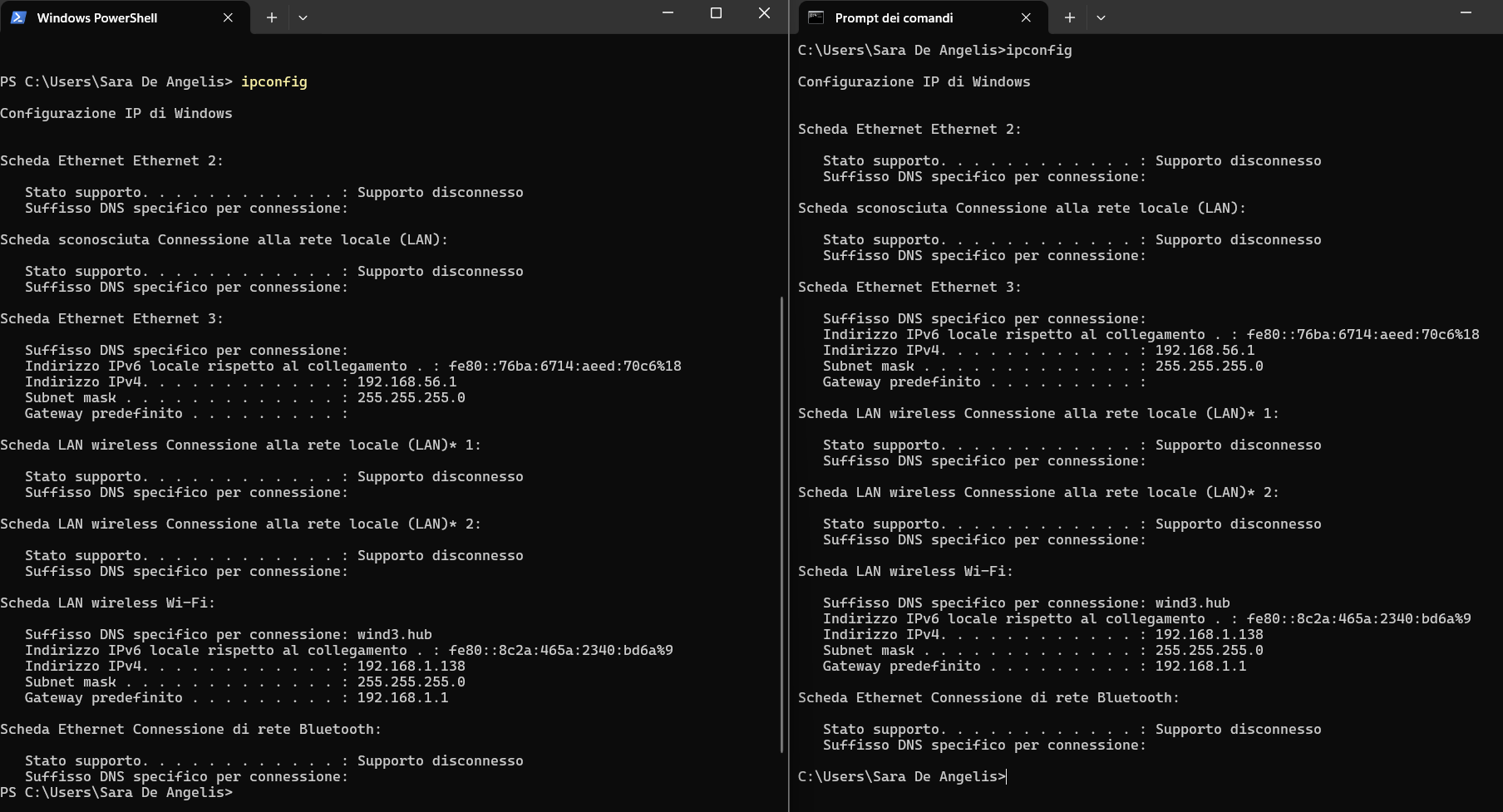
Entrambe le finestre forniscono un elenco di sottodirectory e file, e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell, vengono mostrati anche gli attributi/modalità.



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.



**Parte 3: Esplora i cmdlet.**

a. I comandi PowerShell, cmdlet, sono costruiti sotto forma di stringa verbo-nome . Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, immettere Get-Alias ​​dir al prompt PowerShell.

PS C:\Users\Sara De Angelis> get-alias dir

CommandType Name Version Source

----------- ---- ------- ------

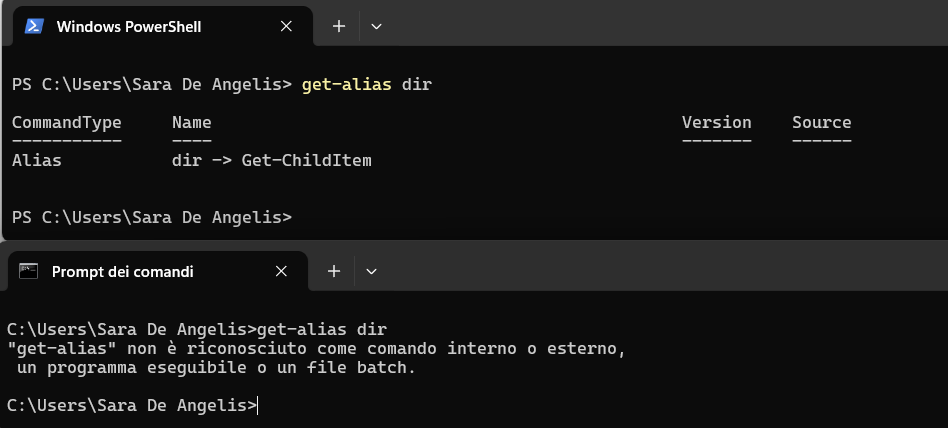
Alias dir -> Get-ChildItem

Qual è il comando PowerShell per dir ?

Ottieni-ChildItem

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

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



**I cmdlet di PowerShell** sono comandi leggeri e modulari che consentono di eseguire operazioni specifiche, spesso su oggetti, all'interno dell'ambiente Windows PowerShell. Ogni cmdlet segue una struttura basata su un verbo e un sostantivo (ad esempio, `Get-Process` per ottenere informazioni sui processi in esecuzione). Questi comandi possono essere utilizzati per attività come la gestione di file, la configurazione del sistema, il monitoraggio della rete e altro ancora.

Alcuni cmdlet comunemente utilizzati includono:

- \*\*`Get-Help`\*\*: Fornisce informazioni su come utilizzare altri cmdlet.

- \*\*`Get-Process`\*\*: Mostra informazioni sui processi attivi.

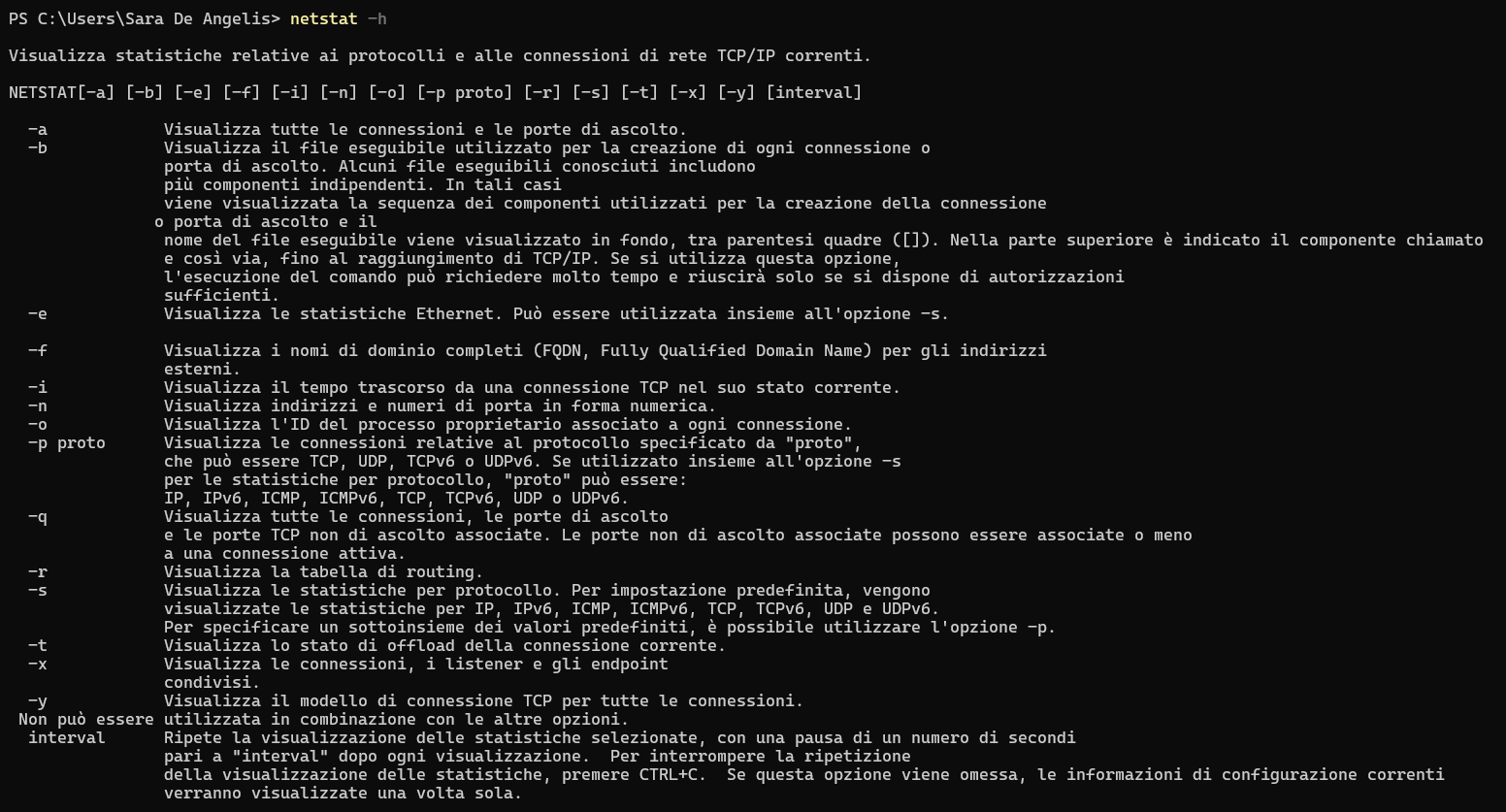
- \*\*`Set-ExecutionPolicy`\*\*: Configura i permessi per l'esecuzione degli script.

- \*\*`Invoke-Command`\*\*: Esegue comandi su computer remoti.

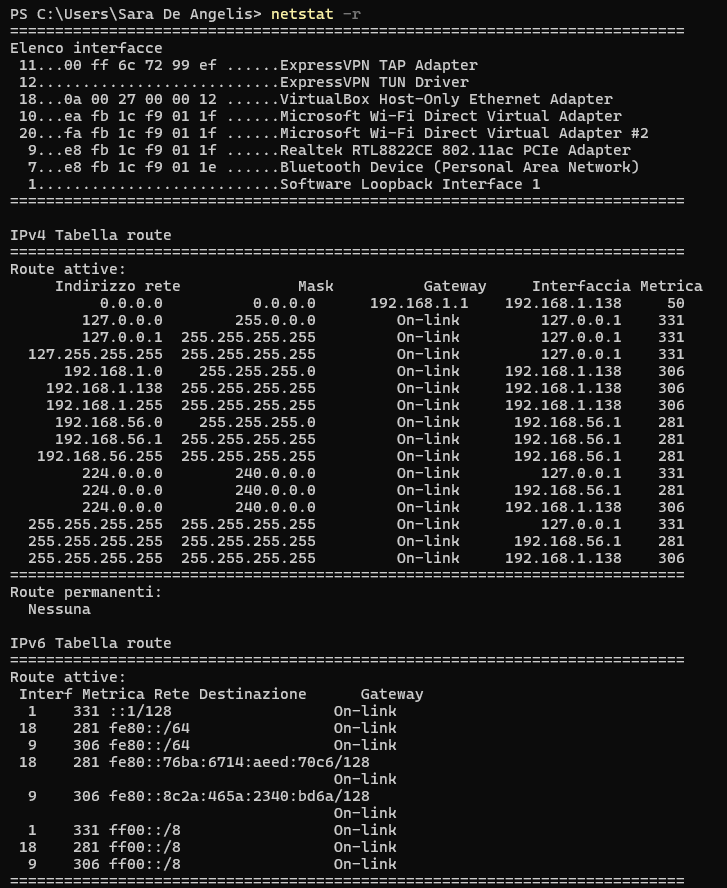
Per un approfondimento sui cmdlet, puoi consultare la guida ufficiale di Microsoft, che include dettagli sulle convenzioni di denominazione, parametri disponibili e modalità di utilizzo avanzate, come il piping e la gestione degli errori. Puoi esplorare i dettagli su [Microsoft Learn](<https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4>).

**Parte 4: Esplora il** **comando netstat utilizzando PowerShell.**

a. Al prompt di PowerShell, premere Invio netstat -hper visualizzare le opzioni disponibili per il netstatcomando.



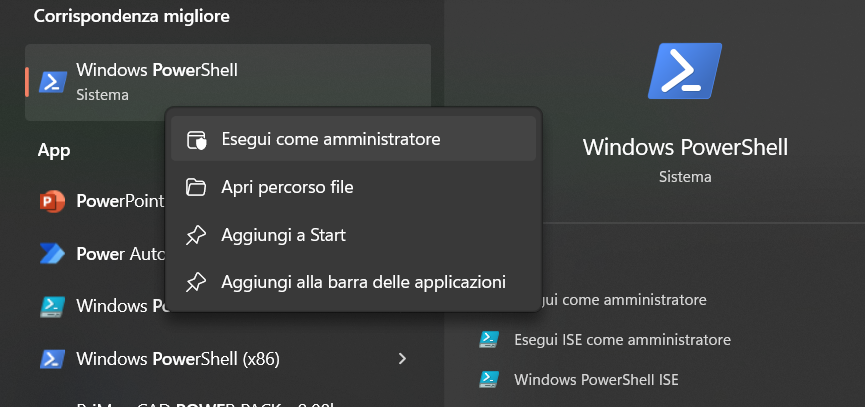
b. Per visualizzare la tabella di routing con i percorsi attivi, digitare netstat -r prompt.



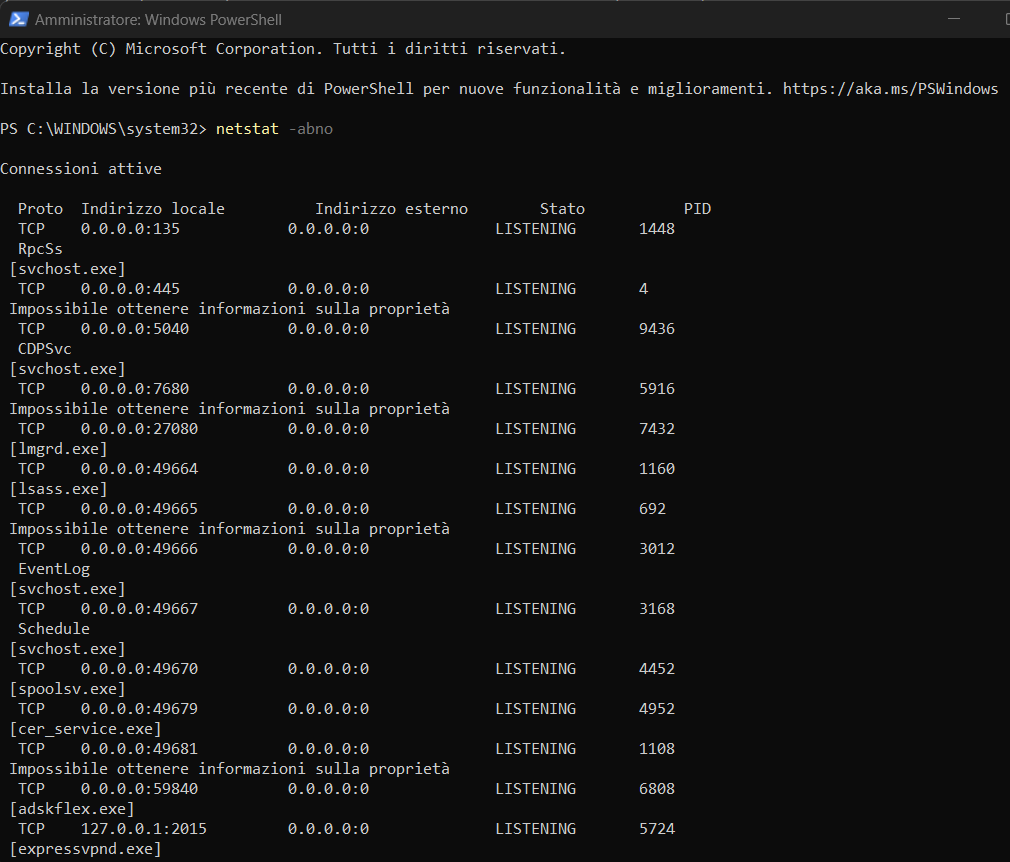
Cos'è il gateway IPv4?

192.168.1.1

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



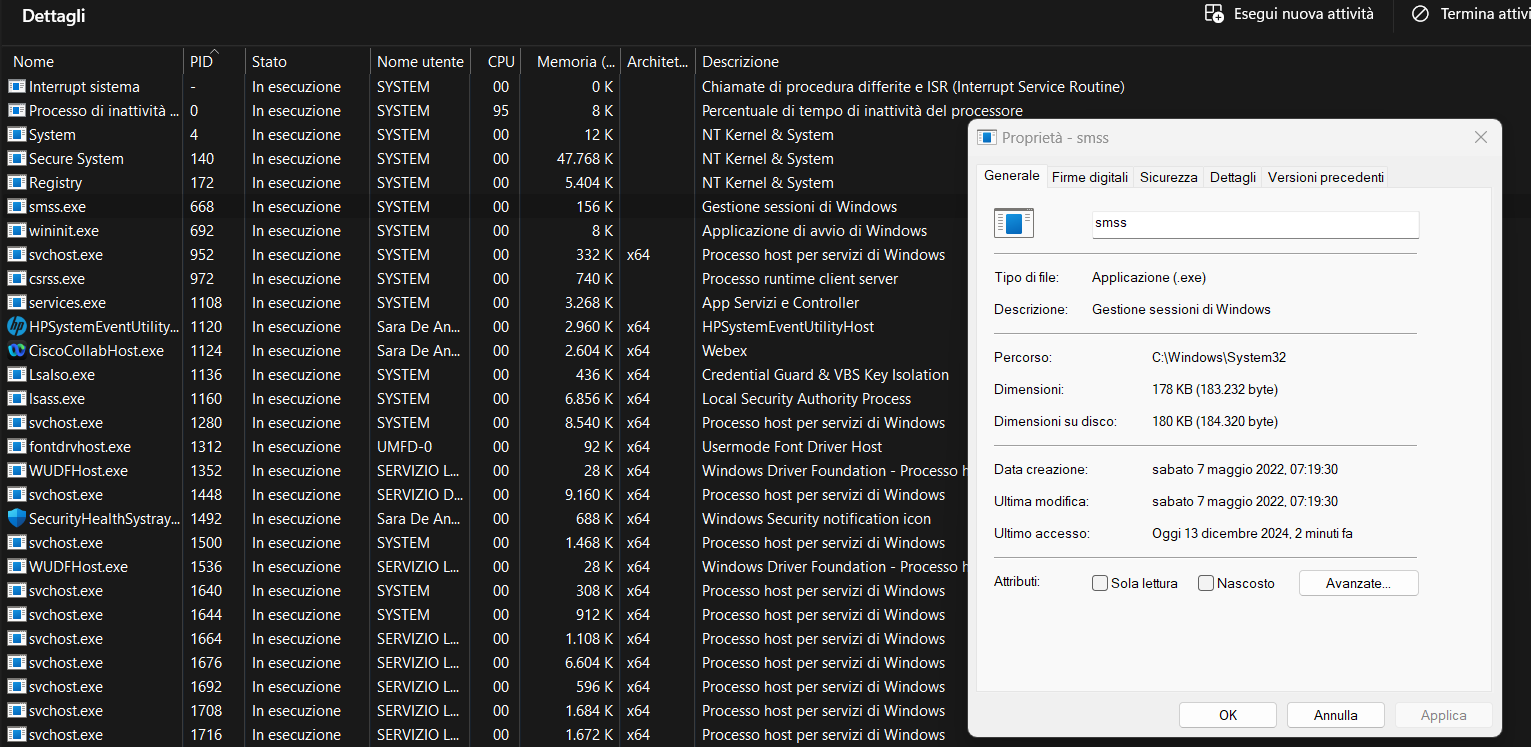
d. Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Digitare al netstat -abno prompt.



e. Apri Task Manager. Vai alla scheda Dettagli . Fai clic sull'intestazione PID in modo che i PID siano in ordine.

f. Selezionare uno dei PID dai risultati di netstat -abno. In questo esempio viene utilizzato il PID 668.

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 per ulteriori informazioni.



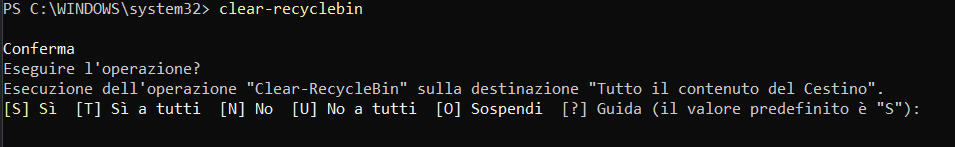
**Parte 5: Svuotare il cestino tramite PowerShell.**

I comandi di PowerShell possono semplificare la gestione di una grande rete di computer. 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 per essere eseguite utilizzando gli strumenti desktop grafici di Windows.

a. Apri il Cestino. Verifica che ci siano elementi che possono essere eliminati in modo permanente dal tuo PC. In caso contrario, ripristina quei file.

b. Se non ci sono file nel Cestino, crea alcuni file, ad esempio un file di testo, utilizzando Blocco note e posizionali nel Cestino.

c. In una console di PowerShell, immettere clear-recyclebinal prompt.



**LABORATORIO 2**

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

**Contesto / Scenario**

HyperText Transfer Protocol (HTTP) è un protocollo di livello applicativo che presenta dati tramite un browser web. Con HTTP, non c'è alcuna salvaguardia per i dati scambiati tra due dispositivi comunicanti.

Con HTTPS, la crittografia viene utilizzata tramite un algoritmo matematico. Questo algoritmo nasconde il vero significato dei dati che vengono scambiati. Ciò avviene tramite l'uso di certificati che possono essere visualizzati più avanti in questo laboratorio.

Indipendentemente da HTTP o HTTPS, è consigliabile scambiare dati solo con siti web di cui ti fidi. Il fatto che un sito utilizzi HTTPS non significa che sia un sito affidabile. Gli attori delle minacce utilizzano comunemente HTTPS per nascondere le proprie attività.

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

**Parte 1: Cattura e visualizza il traffico HTTP**

In questa parte, utilizzerai tcpdump per catturare il contenuto del traffico HTTP. Utilizzerai le opzioni di comando per salvare il traffico in un file di cattura dei 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.

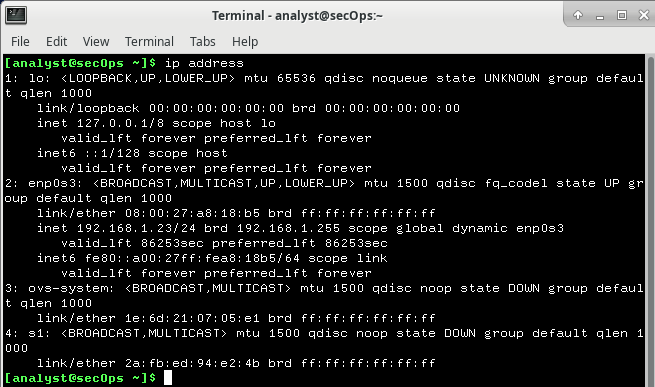
Avviare la VM CyberOps Workstation. Utilizzare le seguenti credenziali utente:

Nome utente: analista

Password: cyberops

Passaggio 2: aprire un terminale e avviare tcpdump.

1. Aprire un'applicazione terminale e immettere il comando ip address.



[analyst@secOps ~]$ indirizzo IP

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

c. Mentre sei nell'applicazione terminale, inserisci il comando sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap. Inserisci la password cyberops per l'analista utente quando richiesto.

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. Dovresti limitare snaplen al numero più piccolo che catturerà le informazioni di protocollo a cui sei interessato. Impostando snaplen su 0 lo imposti al valore predefinito di 262144, per compatibilità con le versioni precedenti più recenti di tcpdump.

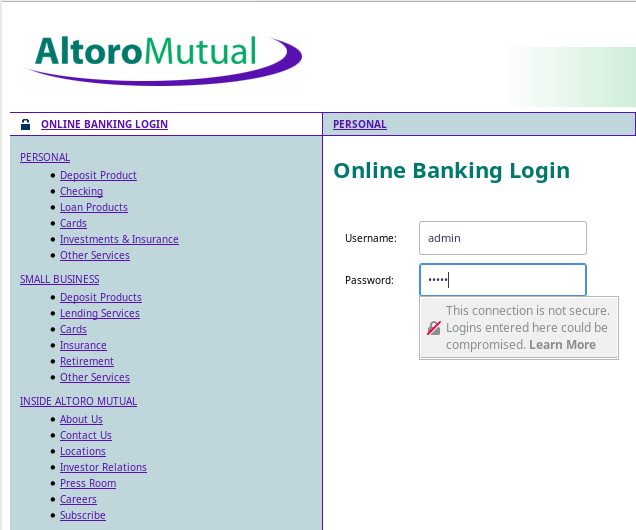
L' -w opzione command viene utilizzata per scrivere il risultato del comando tcpdump in un file. Aggiungendo l'estensione .pcap si garantisce che i sistemi operativi e le applicazioni saranno in grado di leggere il file. Tutto il traffico registrato verrà stampato nel file httpdump.pcap nella directory 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 all'interno della VM CyberOps Workstation. Andare su http://www.altoromutual.com/login.jsp

Poiché questo sito web utilizza HTTP, il traffico non è crittografato. Fai clic sul campo Password per visualizzare l'avviso pop-up.

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



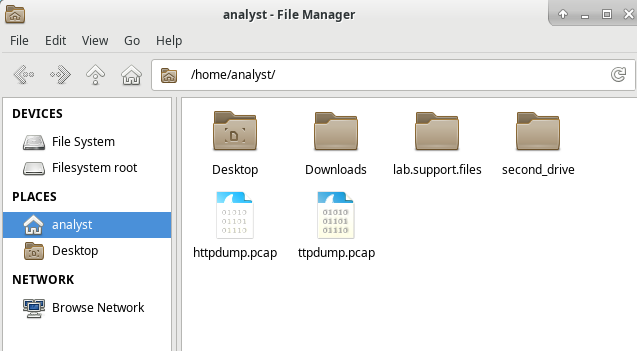
f. Chiudere il browser web.

g. Ritornare alla finestra del terminale in cui è in esecuzione tcpdump. Digitare CTRL+C per interrompere la cattura del pacchetto.

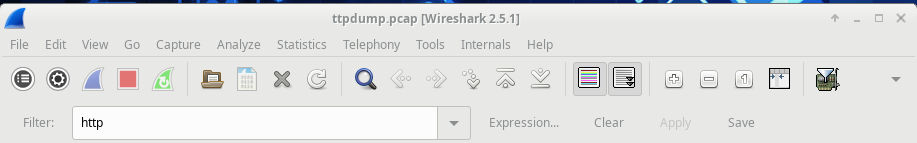
**visualizzare l'acquisizione HTTP.**

Il 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 .

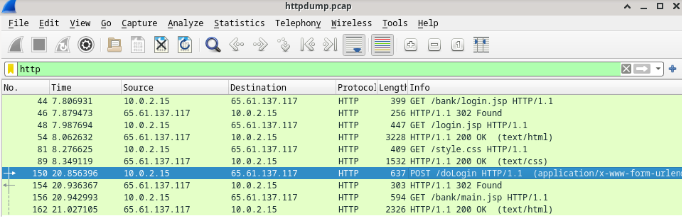
1. Fare clic sull'icona File Manager sul desktop e andare alla cartella home dell'analista utente . Fare doppio clic sul file httpdump.pcap , nella finestra di dialogo Apri con scorrere fino a Wireshark e quindi fare clic su Apri .



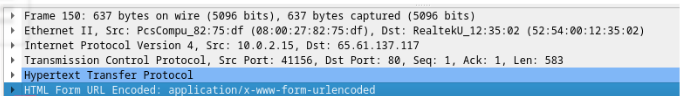
1. Nell'applicazione Wireshark, filtra per http e fai clic su Applica



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



1. Nella finestra inferiore viene visualizzato il messaggio. Espandi la sezione HTML Form URL Encoded: application/x-www-form-urlencoded .



1. Chiudere applicazione di wire shark

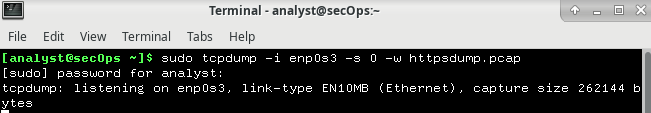
**Parte 2: Cattura e visualizza il traffico HTTPS**

Ora utilizzerai tcpdump dalla riga di comando di una workstation Linux per catturare il traffico HTTPS. Dopo aver avviato tcpdump, genererai traffico HTTPS mentre tcpdump registra il contenuto del traffico di rete. Questi record saranno nuovamente analizzati utilizzando Wireshark.

Passaggio 1: avviare tcpdump da un terminale.

1. Mentre sei nell'applicazione terminale, immetti il ​​comando sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap.

Immetti la password cyberops per l'analista utente quando richiesto.



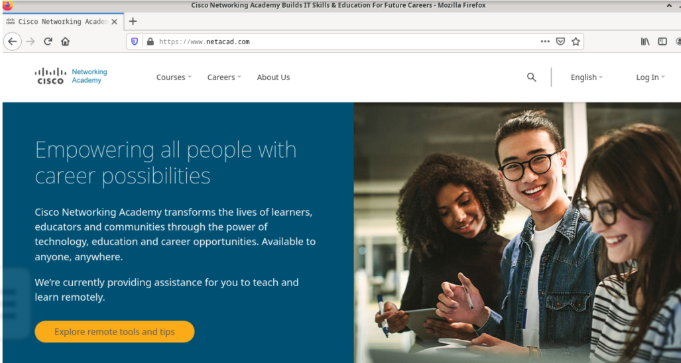
Questo comando avvierà tcpdump e registrerà il traffico di rete sull'interfaccia enp0s3 della workstation Linux. Se la tua interfaccia è diversa da enp0s3, modificala quando usi il comando sopra.

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

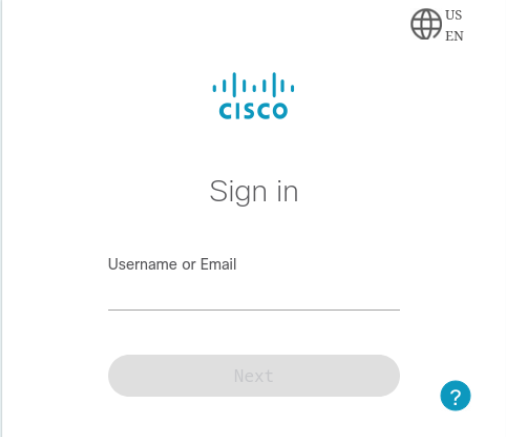
b. Aprire un browser Web dalla barra di avvio all'interno della VM CyberOps Workstation. Andare su www.netacad.com .

Nota: se ricevi una pagina web "Connessione protetta non riuscita", probabilmente significa che la data e l'ora sono errate. Aggiorna il giorno e l'ora con il seguente comando, cambiando il giorno e l'ora correnti

* Fare clic su ACCEDI



* Inserisci il tuo nome utente e password NetAcad. Fai clic su Avanti .



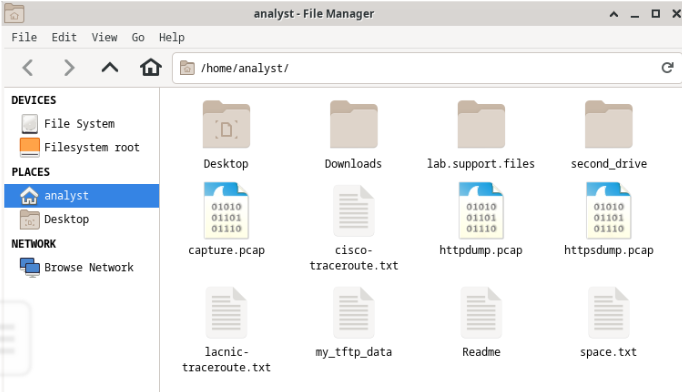
e. Chiudere il browser web nella VM.

1. Ritornare alla finestra del terminale in cui è in esecuzione tcpdump. Digitare CTRL+C per interrompere la cattura del pacchetto.

**Passaggio 2: visualizzare l'acquisizione HTTPS.**

Il 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 .

1. Fai clic sull'icona Filesystem sul desktop e vai alla cartella home dell'analista utente. Apri il file httpsdump.pcap

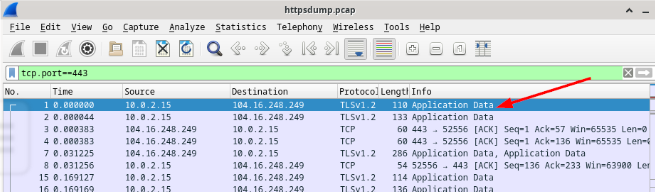


b. Nell'applicazione Wireshark, espandere verticalmente la finestra di acquisizione e quindi filtrare in base al traffico HTTPS tramite la porta 443.

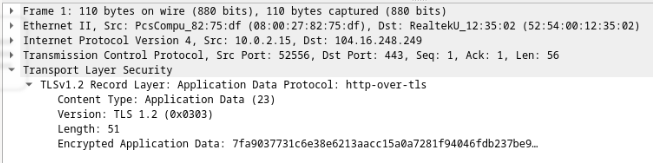
Immetti tcp.port==443 come filtro e fai clic su Applica .



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



1. Nella finestra inferiore viene visualizzato il messaggio.
2. 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.

1. 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**

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

**Contesto / Scenario**

La scansione delle porte è solitamente parte di un attacco di ricognizione. Esistono vari metodi di scansione delle porte che possono essere utilizzati. Esploreremo come utilizzare l'utilità Nmap. Nmap è una potente utilità di rete utilizzata per la scoperta della rete e l'audit di sicurezza.

**Parte 1: Esplorazione di Nmap**

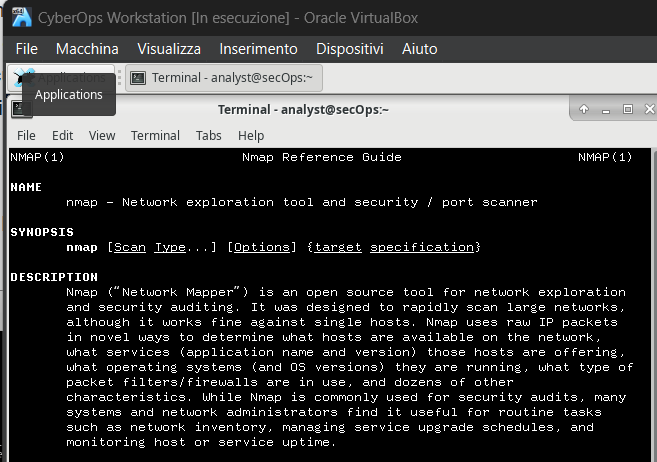
In questa parte, utilizzerai le pagine del manuale (o man page in breve) per saperne di più su Nmap.

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

a. Avviare la VM CyberOps Workstation.

b. Aprire un terminale.

c. Al prompt del terminale, digitare man nmap



Che cos'è Nmap?

Nmap è uno strumento di esplorazione di rete e di scansione di porte e sicurezza.

A cosa serve nmap?

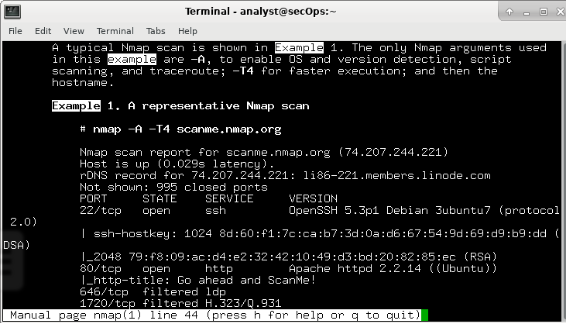
Nmap viene utilizzato per scansionare una rete e determinare gli host disponibili e i servizi offerti nella rete. Alcune delle funzionalità di nmap includono la scoperta degli host, la scansione delle porte e il rilevamento del sistema operativo. Nmap può essere comunemente utilizzato per audit di sicurezza, per identificare porte aperte, inventari di rete e trovare vulnerabilità nella rete.

d. Mentre sei 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, usa 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 nel documento. Il tasto n consente di passare alla corrispondenza successiva.

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

1. 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 scansiona.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 decente.

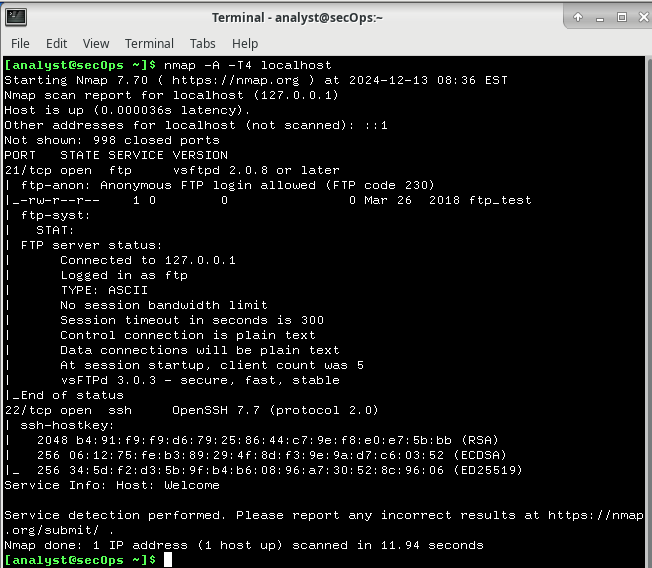
f. Scorri la pagina per saperne di più su nmap. Digita q quando hai finito.

**Parte 1: 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.

1. Se necessario, apri un terminale sulla VM. Al prompt, digita nmap -A -T4 localhost. A seconda della tua rete locale e dei tuoi dispositivi, la scansione richiederà da pochi secondi a qualche minuto.



b. Rivedi i risultati e rispondi alle seguenti domande.

Quali porte e servizi sono aperti?

21/tcp: connessione FTP, 22/tcp: connessione SSH

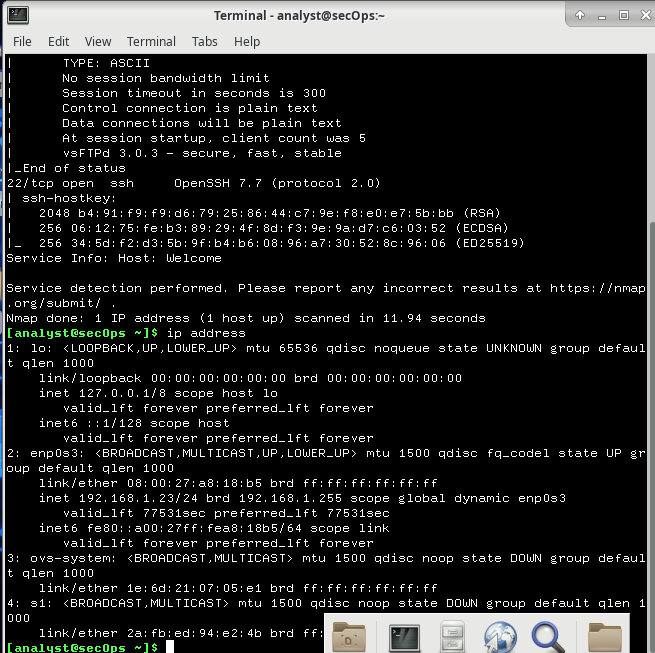
Per ciascuna delle porte aperte, registrare il software che fornisce i servizi.

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.

1. Al prompt dei comandi del terminale, digitare ip addressper determinare l'indirizzo IP e la subnet mask per questo host. Per questo esempio, l'indirizzo IP per questa VM è 10.0.2.15 e la subnet mask è 255.255.255.0.



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

A quale rete appartiene la tua VM?

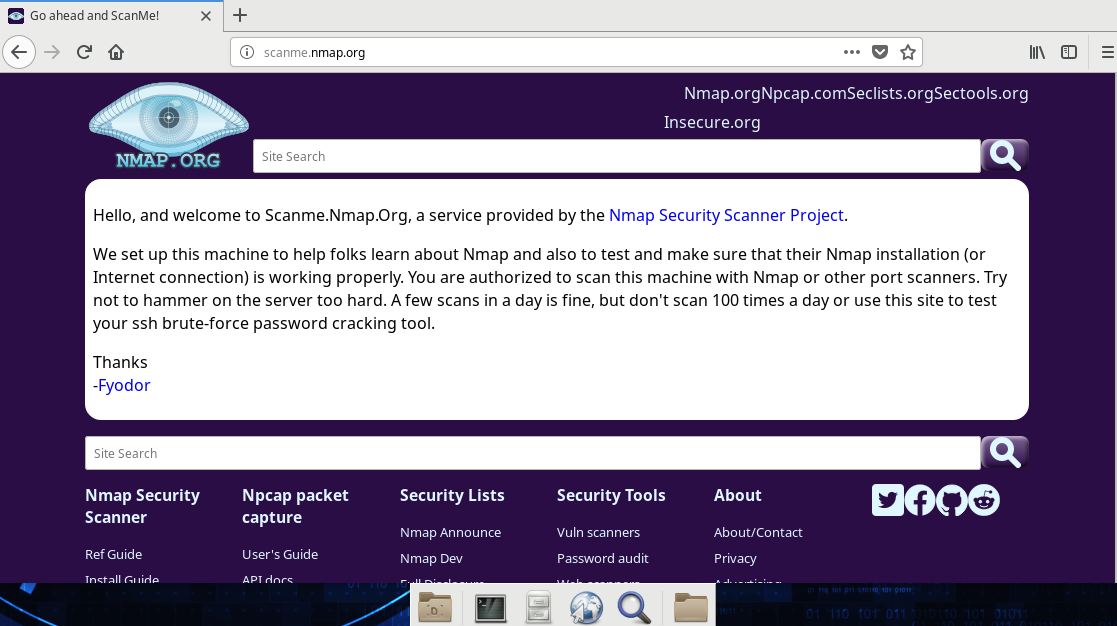
Le risposte possono variare. Questa VM ha un indirizzo IP di 192.168.1.19/24 e fa parte della rete 192.168.1.0/24.

1. Per individuare altri host su questa LAN, immettere nmap -A -T4 network address/prefix. L'ultimo ottetto dell'indirizzo IP deve essere sostituito con uno zero. Ad esempio, nell'indirizzo IP 10.0.2.15, .15 è l'ultimo ottetto. Pertanto, l'indirizzo di rete è 10.0.2.0. /24 è chiamato prefisso ed è una scorciatoia per la netmask 255.255.255.0. Se la tua VM ha una netmask diversa, cerca su Internet una "tabella di conversione CIDR" per trovare il tuo prefisso. Ad esempio, 255.255.0.0 sarebbe /16. In questo esempio viene utilizzato l'indirizzo di rete 10.0.2.0/24

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

**Passaggio 3: eseguire la scansione di un server remoto.**

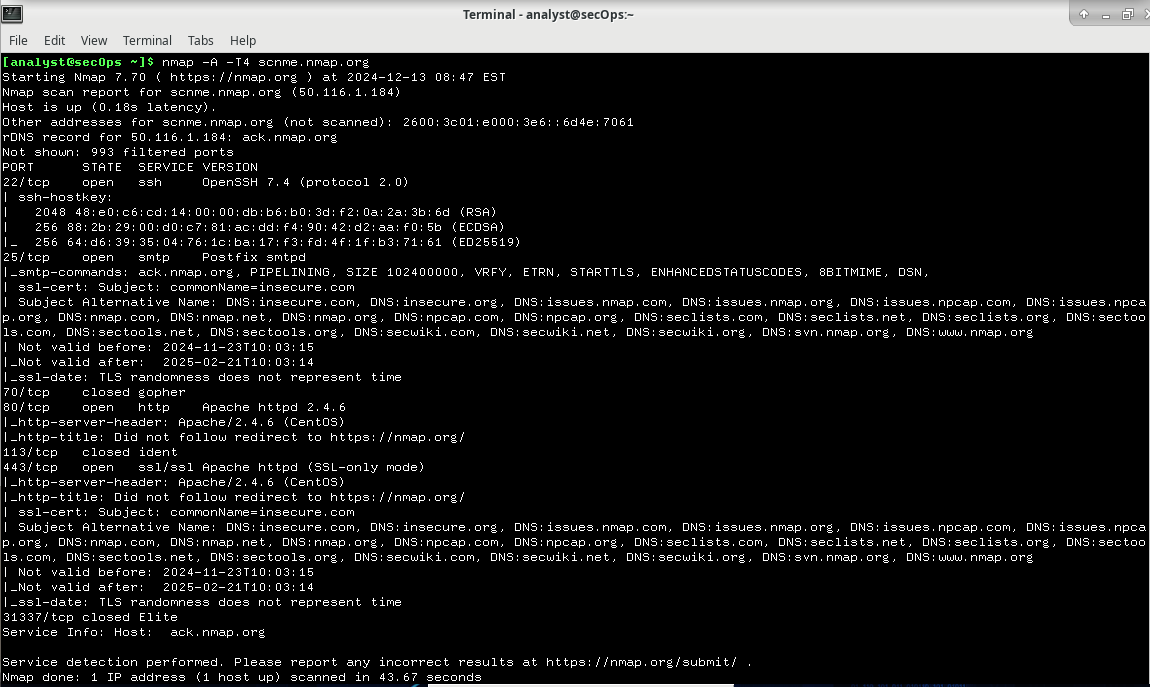
1. Apri un browser web e vai su scanme.nmap.org . Leggi il messaggio pubblicato.



Qual è lo scopo di questo sito?

Questo sito consente agli utenti di conoscere Nmap e di testarne l'installazione.

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



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?

135/tcp: msrpc, 139/tcp: netbios-ssn, 445/tcp: microsoft-ds, 25/tcp: smtp

* 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

**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 threat actor come strumento nefasto?

**Nmap** può essere utilizzato per scansionare una rete interna per porte aperte specifiche per identificare l'entità di una violazione della sicurezza. Può anche essere utilizzato per fare un inventario di una rete per garantire che tutti i sistemi siano probabilmente patchati contro i problemi di sicurezza. D'altro canto, nmap può essere utilizzato per la ricognizione per determinare porte aperte e altre informazioni sulla rete.

**Nmap** (Network Mapper) è uno strumento open-source progettato per il rilevamento delle reti e il controllo della sicurezza. È utilizzato principalmente da amministratori di sistema e professionisti della sicurezza informatica per identificare dispositivi connessi a una rete, mappare la topologia della rete e analizzare potenziali vulnerabilità.

Le sue funzionalità principali includono:

1. \*\*Scansione delle porte: identifica quali porte su un host sono aperte, chiuse o filtrate.

2. \*\*Rilevamento del sistema operativo: consente di determinare il sistema operativo e la versione in uso su un dispositivo.

3. \*\*Identificazione dei servizi: riconosce i servizi in esecuzione sulle porte aperte e ne rileva le versioni.

4. \*\*Rilevamento della rete: individua dispositivi e subnet connessi.

Nmap supporta diverse tecniche di scansione, come la scansione SYN, UDP, e la scansione di tipo ACK. Inoltre, può eseguire script personalizzati tramite il motore NSE (Nmap Scripting Engine), per attività avanzate come la ricerca di vulnerabilità note.

È compatibile con vari sistemi operativi (Windows, Linux, macOS) ed è disponibile sia in modalità a riga di comando sia con interfaccia grafica (Zenmap). Nmap è uno strumento essenziale per analisi di rete, ma il suo utilizzo deve rispettare le normative legali e il consenso dei proprietari delle reti analizzate.

**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 questo laboratorio, visualizzerai un file PCAP relativo a un precedente attacco a un database SQL.

Parte 1: aprire Wireshark e caricare 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 di sistema.

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

Parte 6: Conclusione dell'attacco SQL Injection.

**Contesto / Scenario**

Gli attacchi di iniezione SQL 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 danni.

È stato creato un file PCAP per consentirti di visualizzare un attacco precedente contro un database SQL. In questo laboratorio, visualizzerai gli attacchi al database SQL e risponderai alle domande.

**Parte 1: aprire Wireshark e caricare il file PCAP.**

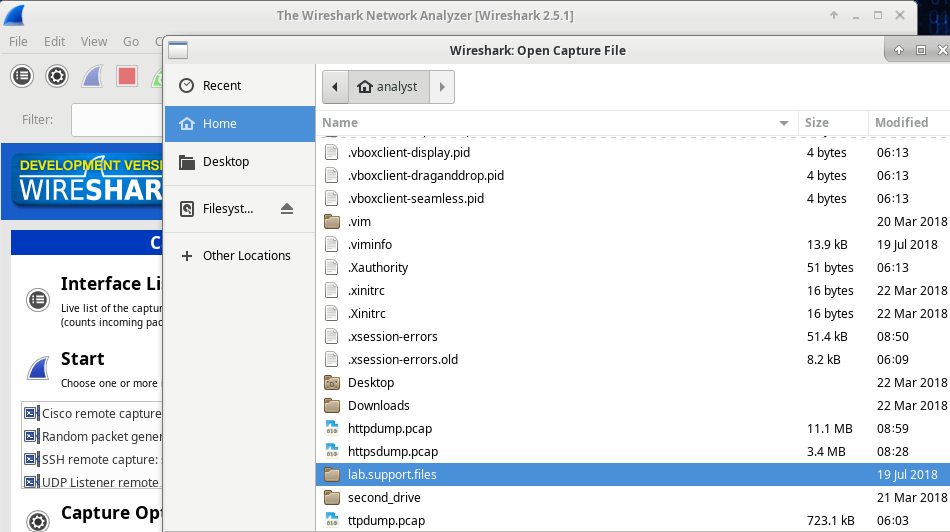
L'applicazione Wireshark può essere aperta utilizzando diversi metodi su una workstation Linux.

a. Avviare la VM CyberOps Workstation.

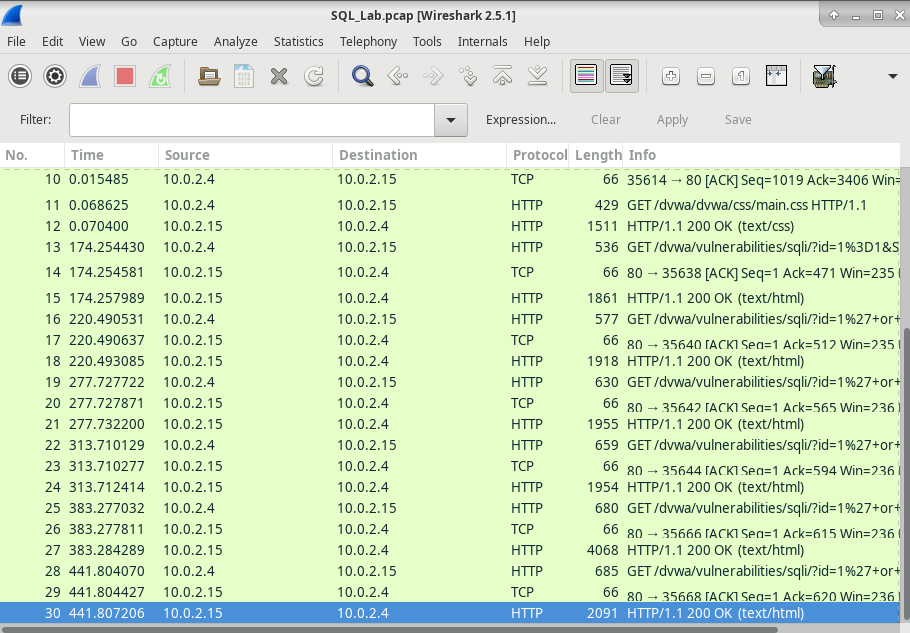
b. Fare clic su Applicazioni > CyberOPS > Wireshark sul desktop e accedere all'applicazione Wireshark.

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

d. Sfoglia la directory /home/analyst/ e cerca lab.support.files . Nella directory lab.support.files apri il file SQL\_Lab.pcap .



1. Il file PCAP si apre all'interno di Wireshark e visualizza il traffico di rete catturato. Questo file di cattura si estende su un periodo di 8 minuti (441 secondi), la durata di questo attacco di iniezione SQL.



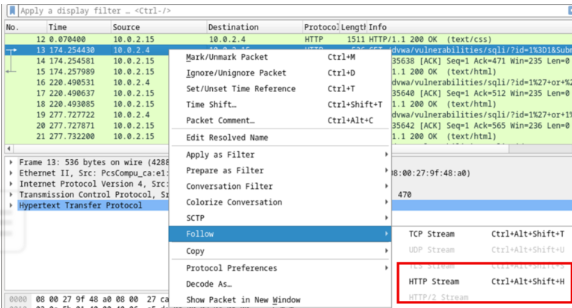
Quali sono i due indirizzi IP coinvolti in questo attacco di iniezione SQL in base alle informazioni visualizzate?

10.0.2.4 e 10.0.2.15

**Parte 2: Visualizza l'attacco SQL Injection.**

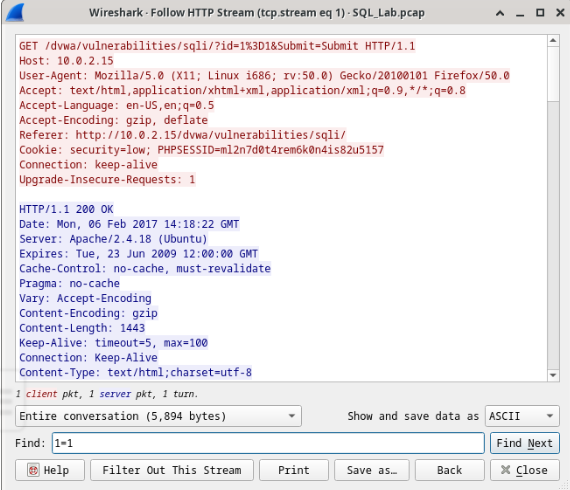
In questa fase, vedrai l'inizio di un attacco.

1. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 13 e seleziona Follow > HTTP Stream . La riga 13 è stata scelta perché è una richiesta HTTP GET. Ciò sarà molto utile per seguire il flusso di dati così come lo vedono i livelli dell'applicazione e porta al test della query per l'iniezione SQL.

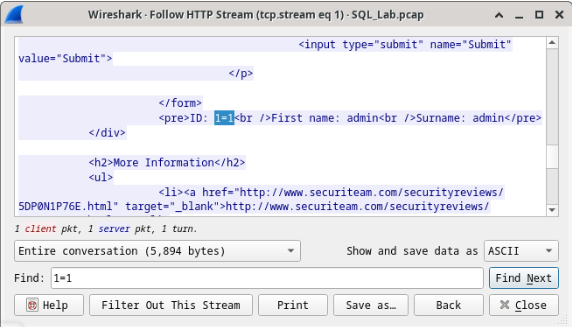


Il traffico sorgente è mostrato in rosso. La sorgente ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

1. Nel campo Trova , immettere 1=1 . Fare clic su Trova successivo



1. L'attaccante ha inserito una query (1=1) in una casella di ricerca UserID sul target 10.0.2.15 per vedere se l'applicazione è vulnerabile all'iniezione SQL. 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 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.

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

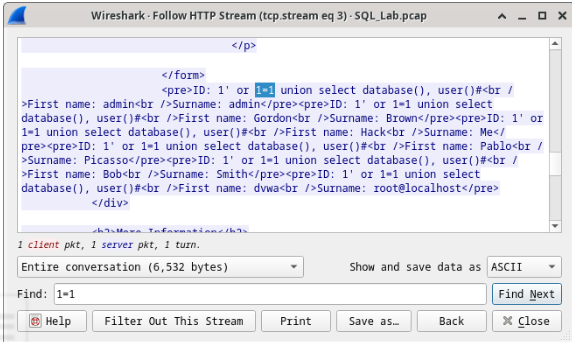
**Parte 3: L'attacco SQL Injection continua**

In questa fase, visualizzerai 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 , immettere 1=1 . Fare clic su Trova successivo .

1. 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 . Sono inoltre visualizzati più account utente.

d. Chiudere la finestra Segui flusso HTTP.

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

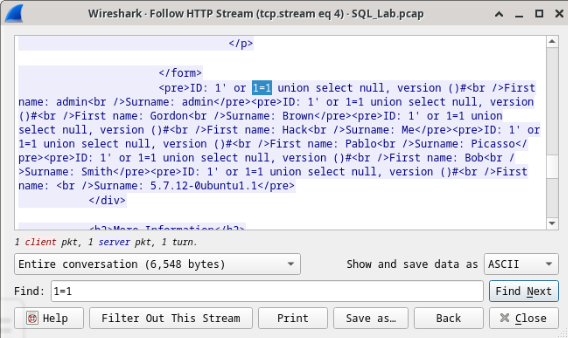
**Parte 4: L'attacco SQL Injection fornisce informazioni di sistema.**

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

a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 22 e seleziona Follow > HTTP Stream . In rosso, viene mostrato 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 , immettere 1=1 . Fare clic su Trova successivo .

1. 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. Notare come l'identificativo della versione si trovi alla fine dell'output, subito prima del codice HTML di chiusura </pre>.</div>.



Versione MySQL 5.7.12-0

d. Chiudere la finestra Segui flusso HTTP.

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

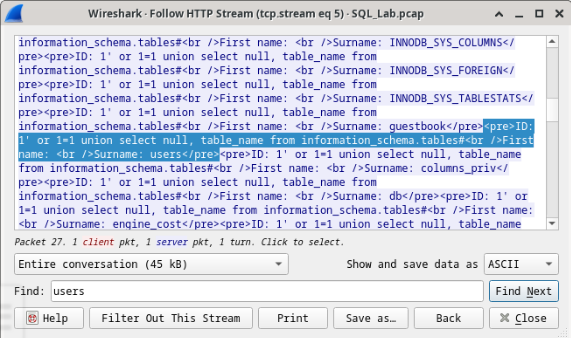
**Parte 5: L'attacco SQL Injection e le informazioni della tabella.**

L'attaccante sa che c'è un gran numero di tabelle SQL piene di informazioni. L'attaccante tenta di trovarle.

a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 25 e seleziona Follow > HTTP Stream . La sorgente è mostrata 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 , immetti utenti . Fai clic su Trova successivo .

1. 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 nel database. Ciò fornisce un output enorme di molte 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”.

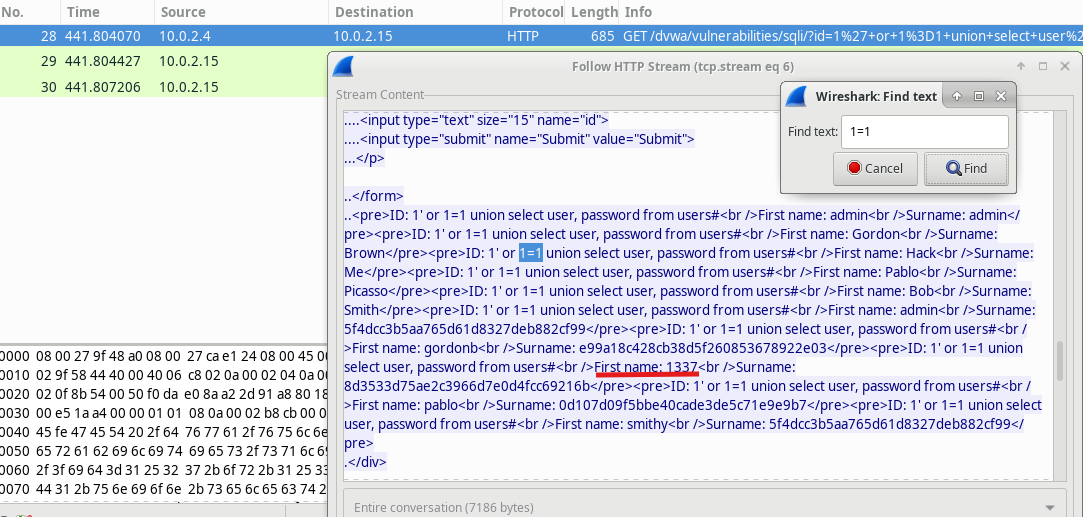
**Parte 6: Conclusione dell'attacco SQL Injection.**

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

a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 28 e seleziona Follow > HTTP Stream . La sorgente è mostrata 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. Quando il testo è stato trovato, fai clic su Annulla nella casella di ricerca Trova testo.

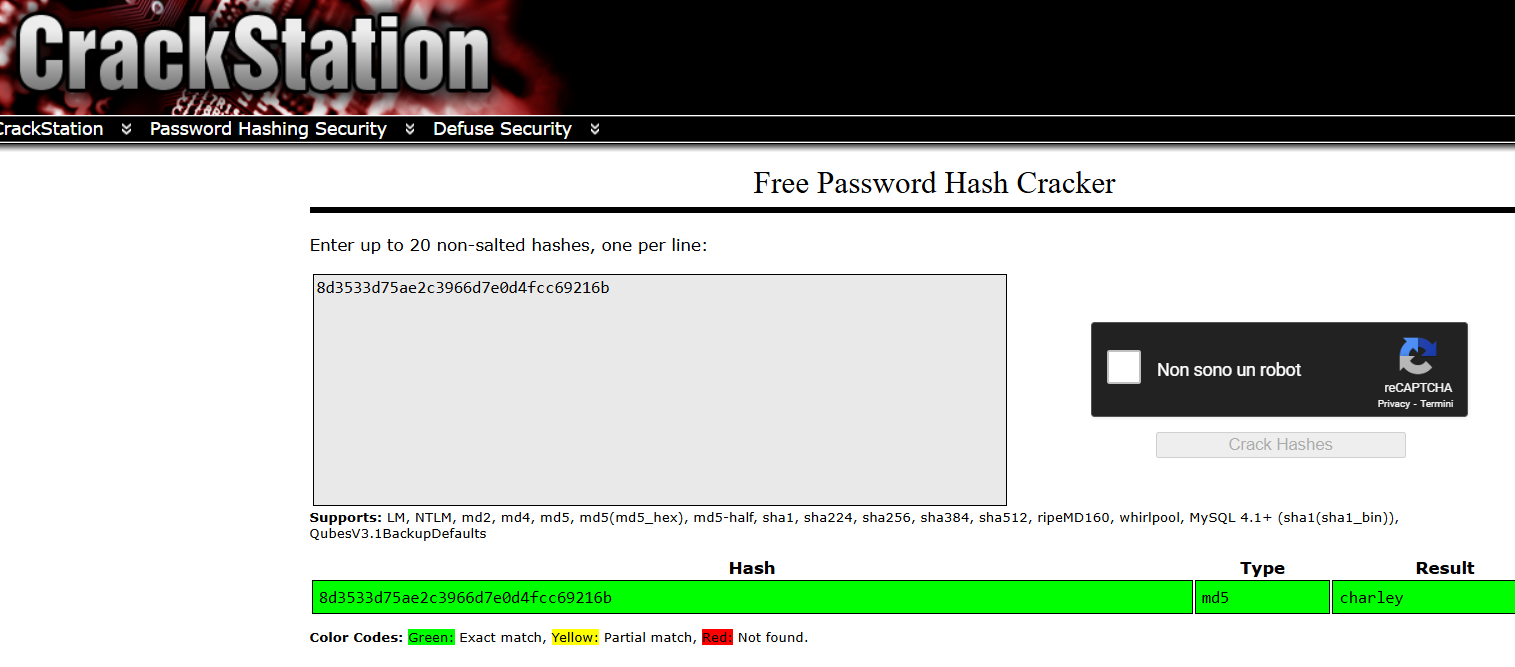
L'aggressore ha inserito una query (1'or 1=1 union select user, password from users#) in una casella di ricerca UserID sulla destinazione 10.0.2.15 per estrarre nomi utente e hash delle password!



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 l'hash della password e inizia a craccare.



Qual è la password in testo normale?

Carlo

1. Chiudere la finestra Segui flusso HTTP. Chiudere tutte le finestre aperte.

**Domande di riflessione**

1. Qual è il rischio di avere piattaforme che utilizzano 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'attaccante.

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

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.

WIRESHARK

Wireshark è uno strumento open-source per l'analisi del traffico di rete, ampiamente utilizzato da amministratori di sistema, ingegneri di rete e professionisti della sicurezza informatica. La sua funzione principale è catturare e analizzare pacchetti di dati che transitano in una rete, fornendo informazioni dettagliate su ogni comunicazione.

Con Wireshark, è possibile:

1. Monitorare il traffico in tempo reale su una rete locale (LAN).

2. Analizzare protocolli di rete come TCP, UDP, HTTP, DNS, e molti altri.

3. Individuare problemi di rete, come latenze elevate, pacchetti persi o configurazioni errate.

4. Rilevare attività sospette, utile per identificare attacchi informatici come spoofing, DoS o intercettazioni di dati.

5. Ispezionare pacchetti dettagliati, inclusi header e payload, per una diagnosi approfondita.

L'interfaccia di Wireshark permette di applicare filtri per focalizzarsi su pacchetti specifici, semplificando l'analisi di grandi volumi di dati. Supporta diversi formati di cattura ed è compatibile con Windows, Linux e macOS.

Wireshark è uno strumento potente ma deve essere usato eticamente, rispettando la privacy e le leggi locali, in quanto consente di visualizzare dati sensibili in transito.