LABORATORI

Traccia:

1. Laboratorio su PowerShell
2. Esaminare traffico HTTP e HTTPS
3. Esplorazione di Nmap
4. Attacco ad un Database MySQL

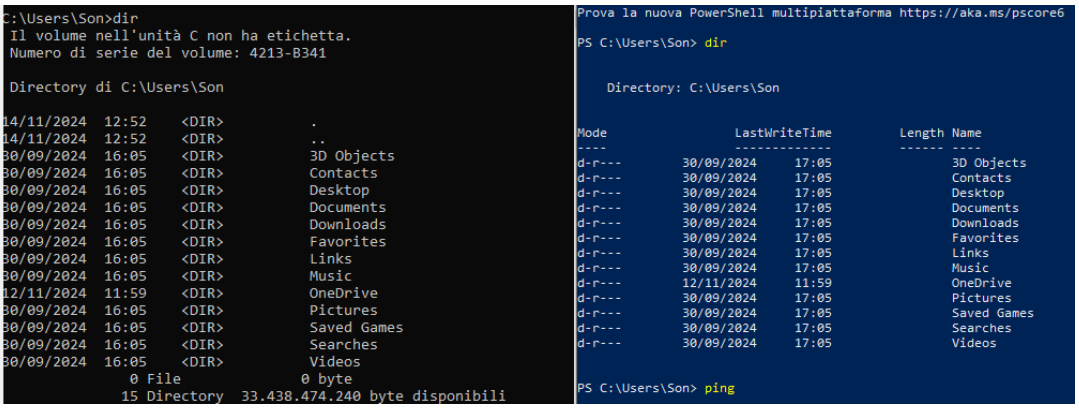
1. Introduzione

In questa esercitazione si andrà ad imparare ad analizzare con diversi strumenti alcuni tipi di attacchi ed esaminare il traffico dati per apprendere quali sono alcune delle attività inerenti ai team di difesa nel SOC.

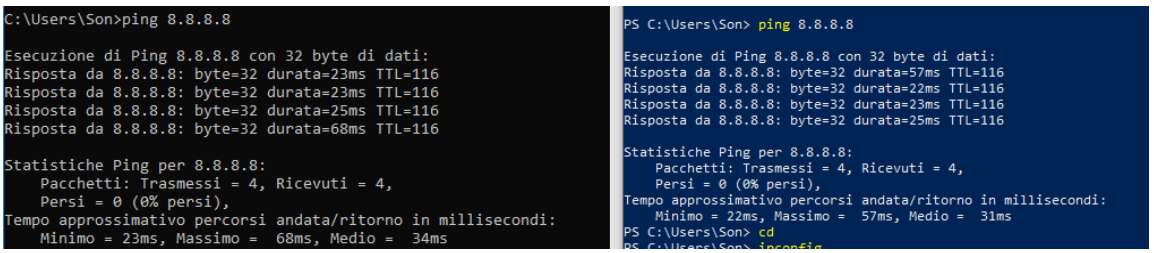
2. Laboratorio su PowerShell

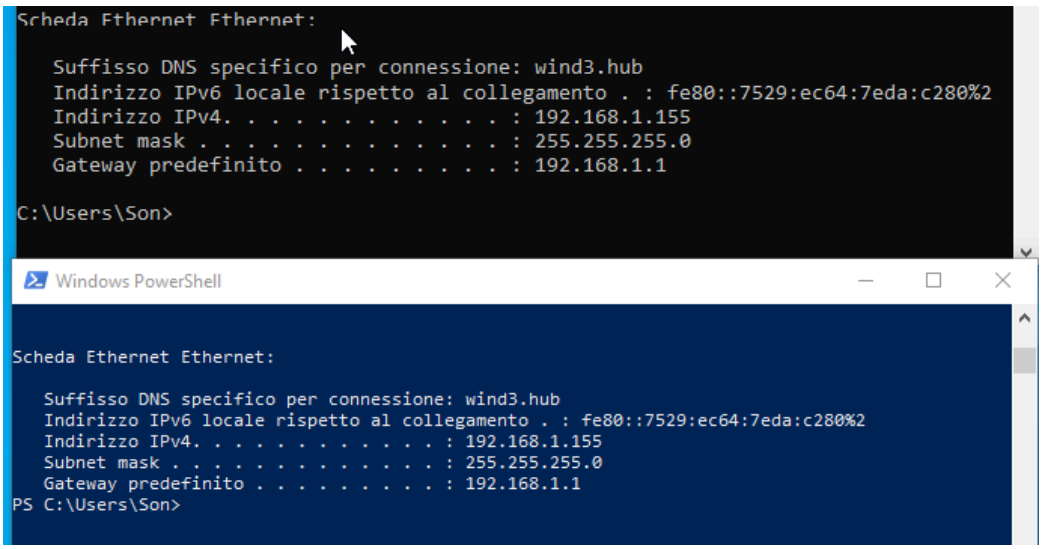
Il primo laboratorio che si è andati ad eseguire è un' esplorazione di PowerShell su un sistema operativo Windows 10.
Quando si parla di PowerShell si intende una riga di comando ed un linguaggio scripting sviluppato da Microsoft, utile per l'automazione delle attività di amministrazione del sistema e la gestione della configurazione.
Il primo passaggio che si è andato ad eseguire è quello di aprire il prompt dei comandi e PowerShell per analizzare le differenze tra gli output.

Di seguito sarà possibile vedere il confronto del comando *dir*, utile per visualizzare la struttura delle directory e delle sotto-directory presenti nel sistema operativo, sarà possibile notare che nella PowerShell (a sinistra) sono presenti i dati relativi ai permessi su ogni directory trovata.

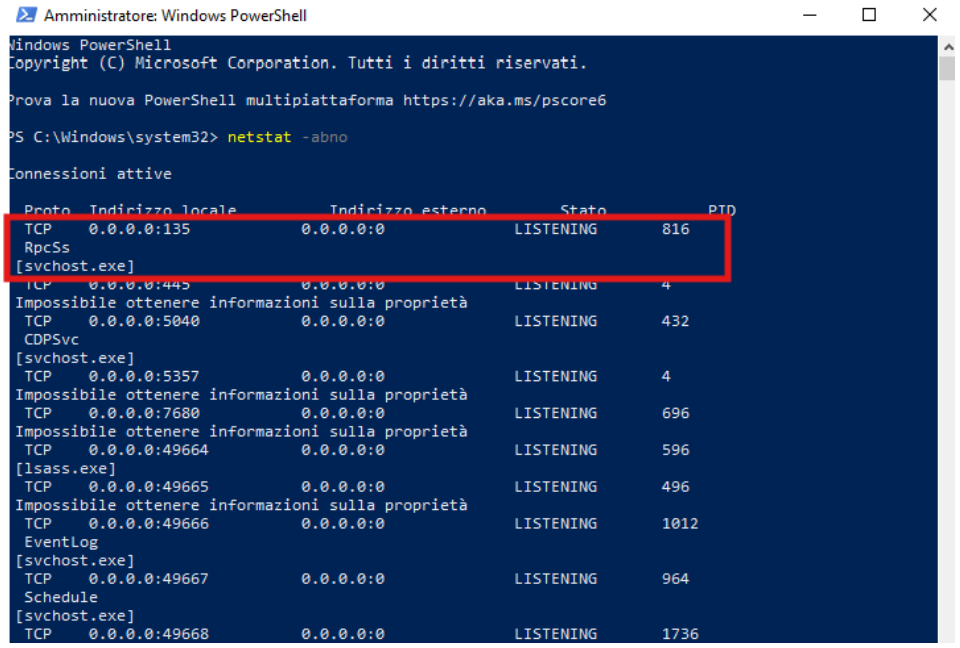


Poi si è eseguito un *ping* per un test di connettività ed un *ifconfig* per verificare le impostazioni di rete. Sarà possibile constatare che non vi è differenza nell'output.

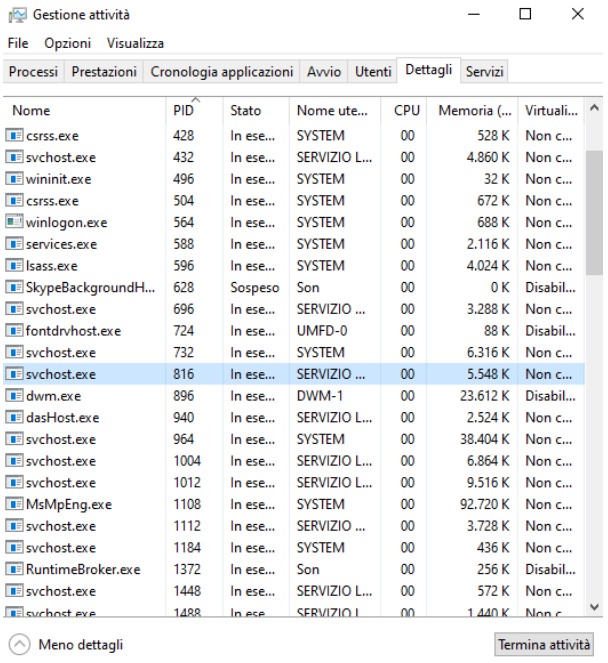




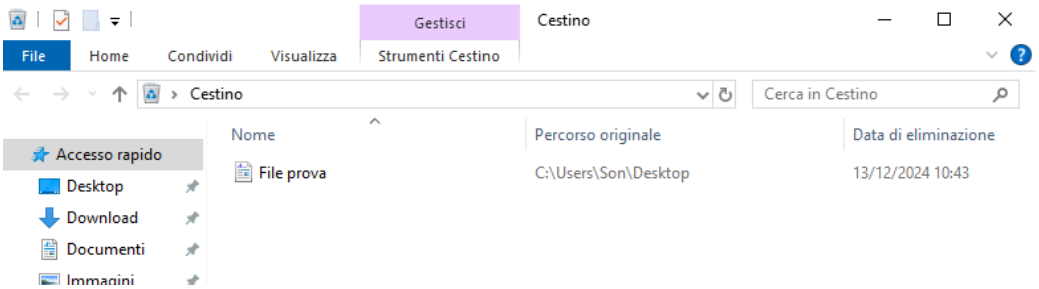
Il passaggio successivo sarà quello di aprire la PowerShell come amministratore per eseguire il comando *netstat -abno.* Questo è un comando di rete utilizzato per visualizzare informazioni dettagliate sulle connessioni di rete e sulle porte aperte, i servizi associati ed i protocolli utilizzati. Sarà scelto ed evidenziato un processo che verrà di seguito individuato nel Task Manager, ovvero il numero 816.



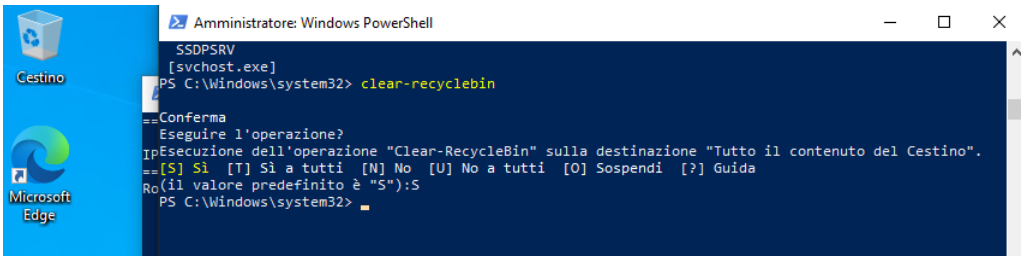
Nel Task Manager andremo a cercare il numero PID, che identifica il processo all'interno della macchina. Potremo vedere che si tratta di un servizio di rete attivo.



Per esplorare ancora le funzionalità di PowerShell si è creato un file che può essere eliminato definitivamente, in questo caso un semplice file di testo. Sarà successivamente eliminato per poterlo visualizzare all'interno del cestino.

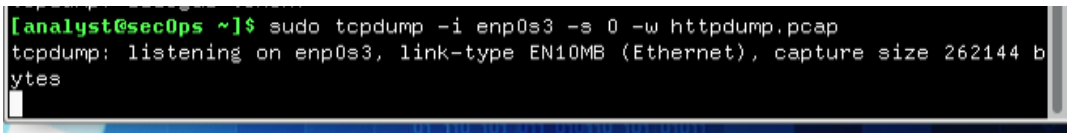


Il comando che verrà eseguito in PowerShell sarà clear-recyclebin, il quale ha la funzione di svuotare il cestino definitivamente.

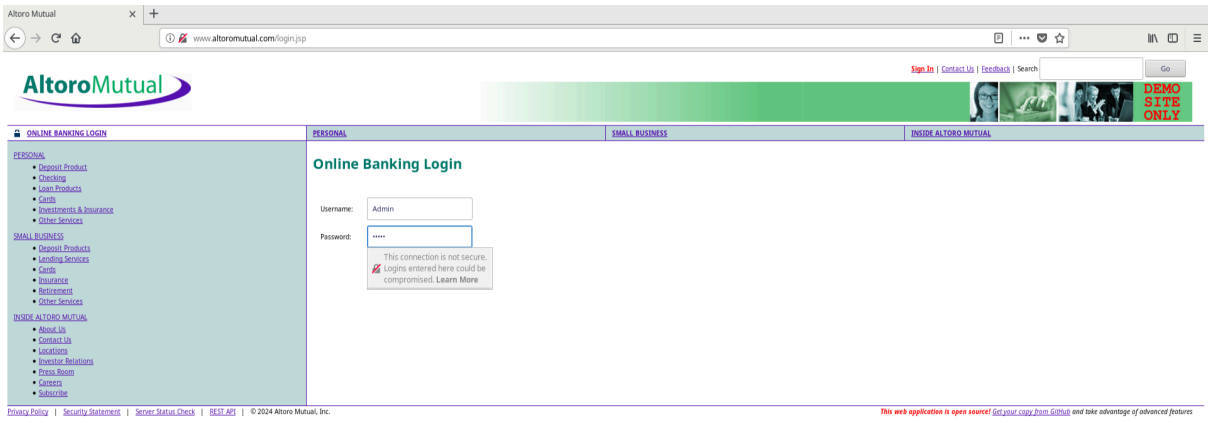


3. Esaminare il traffico HTTP e HTTPS

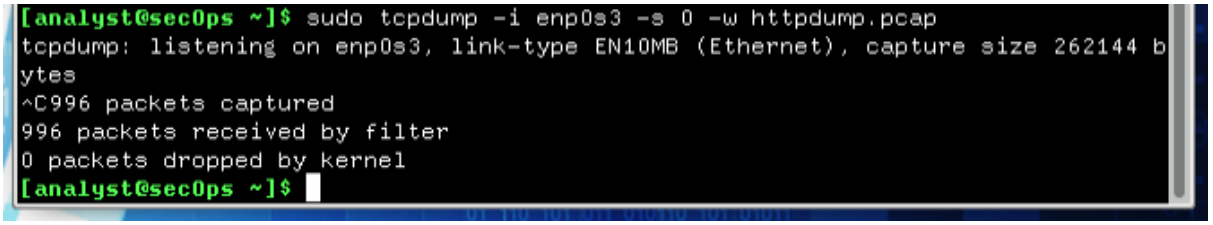
Per eseguire l'analisi del traffico HTTP e HTTPS si è utilizzata la macchina CyberOps Workstation per vederne le differenze in quanto il protocollo HTTP non è criptato, al contrario di HTTPS.
I protocolli HTTP e HTTPS sono quelli che regolamentano la comunicazione tra client e server web.
Il primo passaggio eseguito è stato aprire una connessione in ascolto con tcpdump per effettuare la cattura di una sessione.



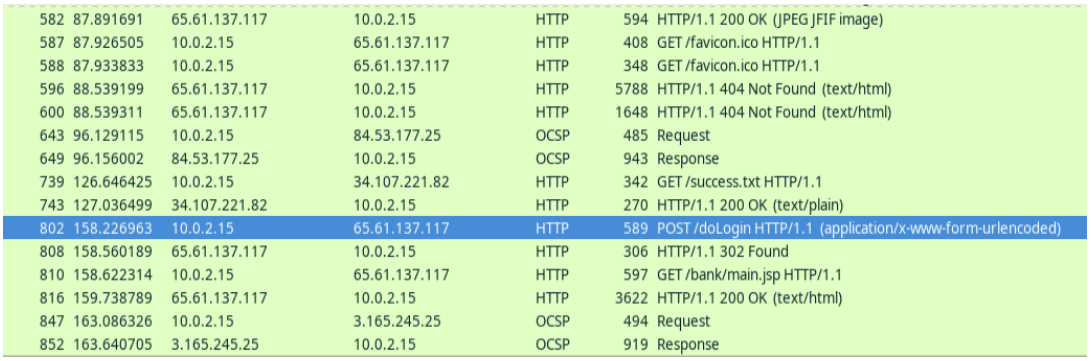
Verrà effettuata la prova connettendosi sul browser ad un sito web non criptato con protocollo HTTP ed effettueremo il login con user Admin e password Admin.



Dopodichè chiuderemo il browser e la cattura del traffico, generando un file .pcap che poi apriremo su Wireshark.

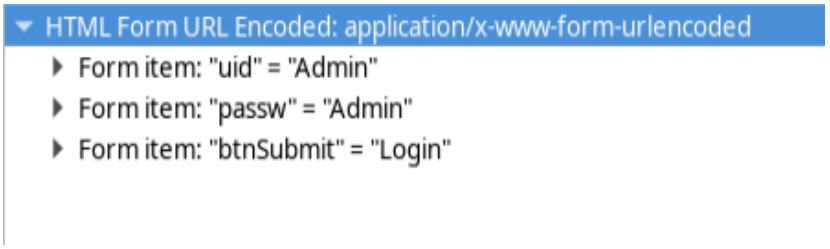


Si andrà ad analizzare il file appena catturato utilizzando il filtro HTTP che renderà visibili tutte le attività che hanno avuto luogo tramite quel protocollo, si cercherà il traffico che evidenzierà il verbo POST.

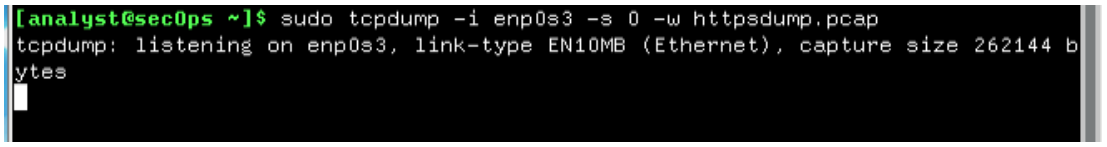


582	87.891691	65.61.137.117	10.0.2.15	HTTP	594	HTTP/1.1 200 OK (JPEG JFIF image)
587	87.926505	10.0.2.15	65.61.137.117	HTTP	408	GET /favicon.ico HTTP/1.1
588	87.933833	10.0.2.15	65.61.137.117	HTTP	348	GET /favicon.ico HTTP/1.1
596	88.539199	65.61.137.117	10.0.2.15	HTTP	5788	HTTP/1.1 404 Not Found (text/html)
600	88.539311	65.61.137.117	10.0.2.15	HTTP	1648	HTTP/1.1 404 Not Found (text/html)
643	96.129115	10.0.2.15	84.53.177.25	OCSP	485	Request
649	96.156002	84.53.177.25	10.0.2.15	OCSP	943	Response
739	126.646425	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
743	127.036499	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
802	158.226963	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
808	158.560189	65.61.137.117	10.0.2.15	HTTP	306	HTTP/1.1 302 Found
810	158.622314	10.0.2.15	65.61.137.117	HTTP	597	GET /bank/main.jsp HTTP/1.1
816	159.738789	65.61.137.117	10.0.2.15	HTTP	3622	HTTP/1.1 200 OK (text/html)
847	163.086326	10.0.2.15	3.165.245.25	OCSP	494	Request
852	163.640705	3.165.245.25	10.0.2.15	OCSP	919	Response

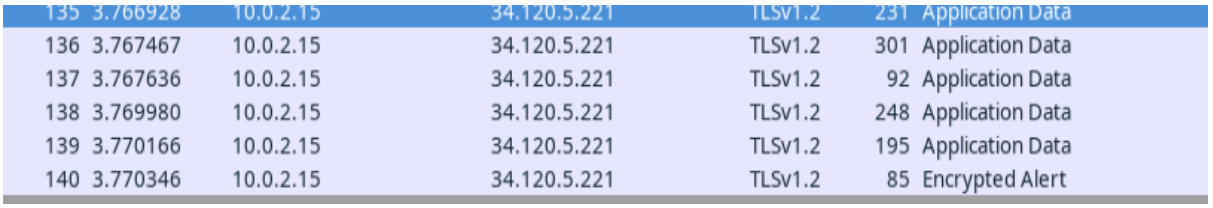
Andando ad analizzare meglio le specifiche di questa attività, sarà possibile individuare Username e Password inseriti in chiaro, esattamente come ci si aspetta dal protocollo HTTP, non criptato.



Di seguito sarà eseguita la stessa operazione, sfruttando una pagina web che usa il protocollo HTTPS, criptato. Si effettuerà il login per poi analizzare cosa tcpdump avrà rilevato.



Nel traffico Wireshark rilevato inseriremo un filtro che ci farà vedere tutto il traffico TCP presente sulla porta 443 (HTTPS) in evidenza. Si andrà a cercare le transazioni Application Data.



Andando a guardare nei dettagli, potremo visualizzare il Secure Socket Layer che non darà in evidenza le credenziali inserite. Inoltre sarà possibile visualizzare un *Encrypted Alert* che darà comunicazione che i dati di questa pagina sono criptati.

4. Esplorazione Nmap

Il terzo laboratorio richiede l'utilizzo del programma Nmap su CyberOps Workstation per analizzare la composizione della rete.
Nmap è uno strumento open-source utilizzato per la scansione delle reti e la mappatura delle porte sui dispositivi connessi ad una rete.
Tramite il comando *man nmap* sarà possibile analizzare un manuale delle istruzioni completo per l'utilizzo del software.

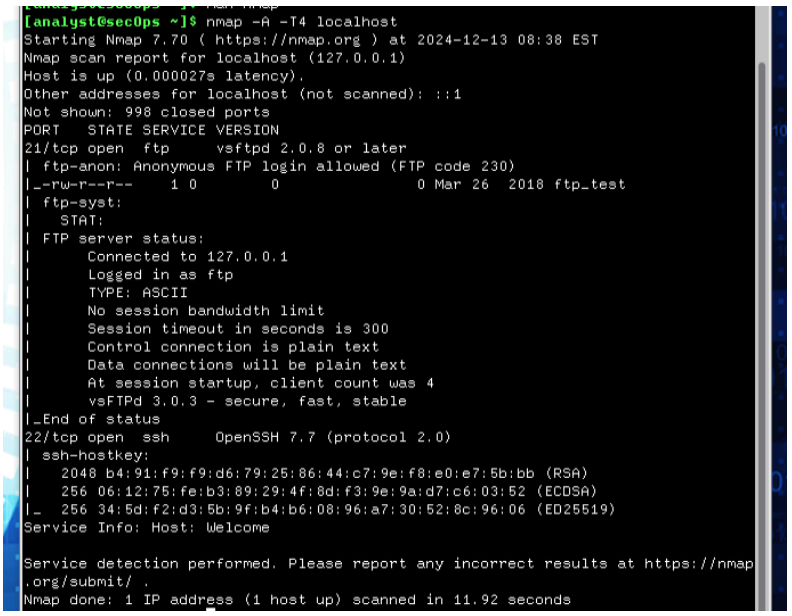
Per capire meglio l'utilizzo dei comandi Nmap si analizza un esempio:

Nmap -A -T4 scanme.nmap.org

In cui:

- -A è il comando che serve alla rilevazione del Sistema Operativo;
- -T4 è il numero di thread analizzati per volta, più alto sarà il valore e maggiore sarà la rilevabilità.

Per fare un test di nmap si eseguirà una scansione dell'host locale, l'otuput che verrà restituito sarà il seguente.



Ciò che è possibile rilevare è l'apertura della porta del servizio FTP (porta 21, servizio vsftdp) e SSH (porta 22, servizio OpenSSH).

Il passaggio successivo prevede l'azione di individuare gli altri host presenti su questa rete.

nmap -A -T4 [indirizzo di rete/subnet mask]

L'output sarà il seguente.

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 08:46 EST
Nmap scan report for 10.0.2.15
Host is up (0.000092s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 27.23 seconds
```

Non sono stati rilevati altri dispositivi su questa rete.

Per andare ad analizzare un server remoto, si aprirà il browser per connettersi al server remoto preso in esame, poi si eseguirà la scansione nmap.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 08:57 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 996 filtered ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pro
tocol 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)
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 51.94 seconds
```

Si potrà analizzare la presenza delle porte aperte SSH (22), HTTP Apache (80), tcpwrapped (9929), tcpwrapped (31337), e la presenza di 996 porte filtrate.

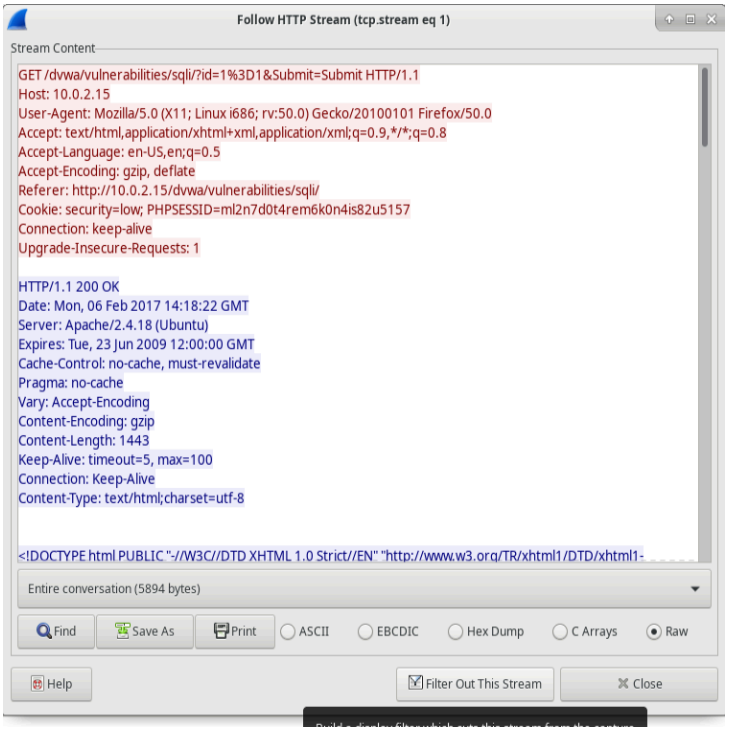
L'indirizzo IP del server è: 45.33.32.156.

5. Attacco ad un Database MySQL

L'ultimo laboratorio riguarda l'esplorazione di un file Wireshark che involve un attacco SQL Injection.
L'SQL Injection è un tipo di attacco di sicurezza informatica che si verifica quando un malintenzionato riesce ad interferire con le query SQL inviate ad un database. Ciò si verifica quando un'applicazione web accetta input dall'utente e li utilizza dinamicamente per creare una query SQL senza convalidarli correttamente o sanificarli in modo sicuro. L'obiettivo di questo attacco è quello di ottenere accesso non autorizzato ai dati, modificarli o eliminarli o compromettere il server.
In questo laboratorio si andrà ad analizzare una cattura già presente su CyberOps Workstation.
La durata di questa cattura è di circa 441 secondi, i due indirizzi IP coinvolti sono 10.0.2.15 e 10.0.2.4.

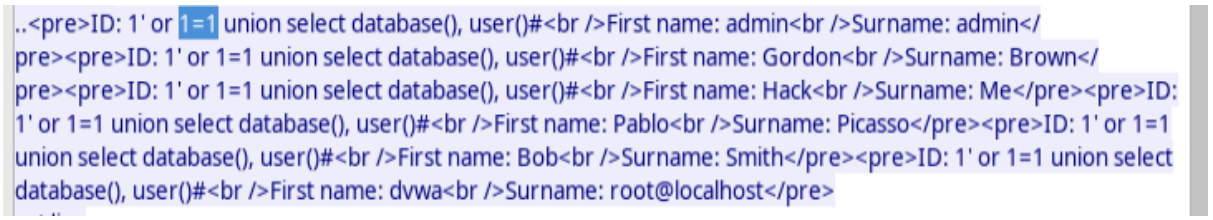
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D%270+&Submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=111985
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=129156
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+version+%28%29%23&Submit=Submit HTTP/1.1
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=139951
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_name+from+information_schema.tables%23&Submit=Submit HTTP/1.1
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=160821
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+user%2C+password+from+users%23&Submit=Submit HTTP/1.1
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

Per vedere più da vicino, sarà selezionata la riga numero 13, ovvero dove ha inizio l'attacco, e sarà analizzato l'HTTP Stream, in rosso sarà segnata la sorgente del traffico, in blu la destinazione.

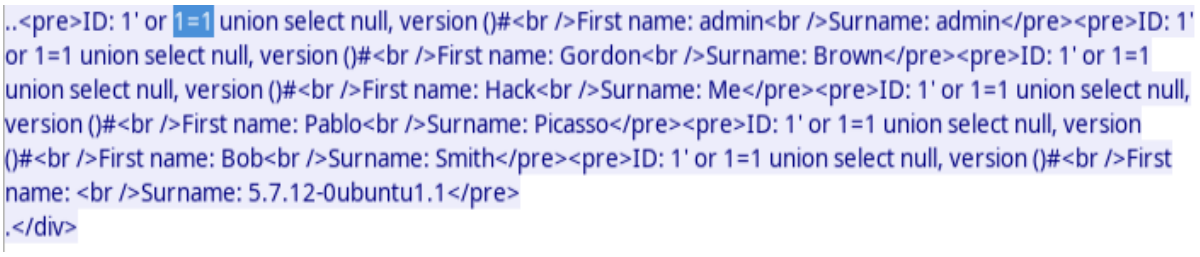


Sarà effettuata una ricerca della porzione in codice SQL “1=1” che ci rivelerà con facilità l’username in chiaro, questa porzione di codice sta a significare che le condizioni saranno sempre vere (1 in codice binario).

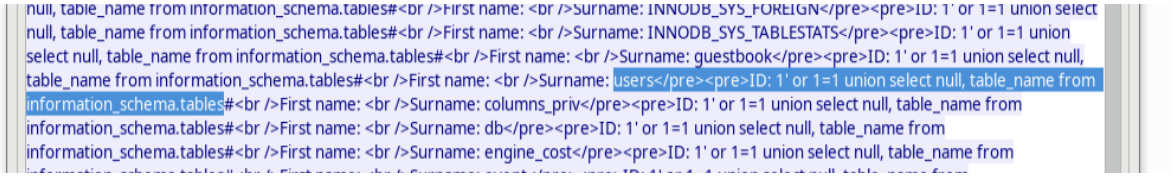
A seguire sarà effettuata una seconda ricerca sulla riga 19 del file .pcap sempre sull’HTTP Stream.



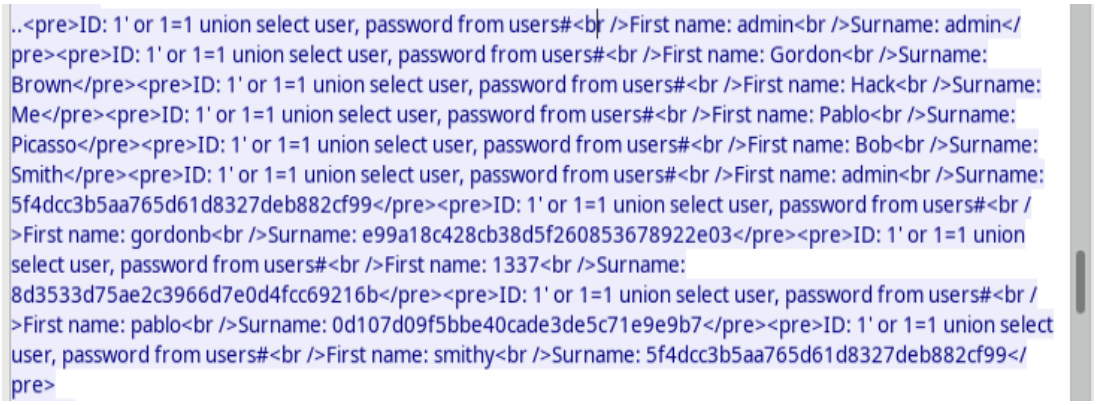
Ciò che si evince da questo output è il database chiamato *dvwa* il cui user sarà *root@localhost*.
La prossima ricerca proseguirà con la stessa analisi sulla riga 22.



L’output che restituirà, evidenzierà che la query immessa avrà come risultato la versione del Sistema Operativo, ovvero la *5.7.12-0ubuntu1.1*.
A questo punto l’attaccante ha ottenuto un buon numero di informazioni.
Adesso si andrà ad effettuare una ricerca sulla riga 25, sempre tramite un HTTP Stream.



La query inserita dall'attaccante rileverà una grande quantità di informazioni, ovvero tutte le tabelle presenti sul database, contenenti tutti gli username e tutti gli altri campi come password, email ecc.
La prossima riga che verrà analizzata sarà la 28, che sarà anche quella conclusiva di questo attacco SQL Injection.



La query immessa, questa volta, specificherà il campo *password,* le password che verranno visualizzate saranno criptate in codice hash md5, un dato che probabilmente condurrà ad un attacco bruted force alle password.

6. Conclusioni

In questa esercitazione, abbiamo esplorato diverse tecniche e strumenti utili per l'analisi del traffico di rete e la gestione delle operazioni di sicurezza all'interno di un Security Operations Center (SOC).
Il laboratorio su PowerShell ci ha permesso di comprendere le potenzialità di questo strumento per la gestione dei processi, l'automazione delle attività e il controllo della configurazione del sistema operativo. Attraverso i comandi di rete e la gestione dei file, abbiamo imparato come eseguire operazioni avanzate di amministrazione.
L'analisi del traffico HTTP e HTTPS ha evidenziato l'importanza della crittografia nella protezione dei dati trasmessi tra client e server web. Mentre il protocollo HTTP trasmette le informazioni in chiaro, rendendo vulnerabili le credenziali di accesso, l'uso del protocollo HTTPS protegge efficacemente i dati attraverso la crittografia SSL/TLS.
Nel laboratorio dedicato a Nmap, abbiamo esaminato la struttura di rete e le porte aperte sui dispositivi, dimostrando come l'analisi delle porte possa rivelare informazioni critiche sui servizi attivi in un ambiente di rete. Le scansioni di rete ci hanno fornito preziose informazioni sulle porte aperte e sui potenziali punti di vulnerabilità.

Infine, l'attacco SQL Injection ha mostrato quanto sia importante proteggere le applicazioni web da input non convalidati. Attraverso la manipolazione di query SQL non sicure, l'attaccante è stato in grado di ottenere informazioni sensibili dal database, come nomi utente e password, mettendo a rischio l'integrità del sistema. Questa serie di esercitazioni ha sottolineato l'importanza di una protezione solida e di una continua vigilanza da parte dei team di sicurezza per prevenire e mitigare attacchi informatici. La comprensione di questi strumenti e tecniche è cruciale per chiunque operi nel settore della sicurezza informatica.

Progetto a cura di

Sonia Laterza