

S11L5



Data: 13/12/24

INFORMAZIONI PRINCIPALI

Laboratorio - Utilizzo di Windows PowerShell

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell.

<https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html>

Laboratorio - Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

In questo laboratorio, completa i seguenti obiettivi:

- Catturare e visualizzare il traffico HTTP
- Catturare e visualizzare il traffico HTTPS

<https://itexamanswers.net/10-6-7-lab-using-wireshark-to-examine-http-and-https-traffic-answers.html>

Bonus 1 Laboratorio - Esplorazione di Nmap

La scansione delle porte è solitamente parte di un attacco di ricognizione.

Esistono diversi metodi di scansione delle porte che possono essere utilizzati.

<https://itexamanswers.net/9-3-8-lab-exploring-nmap-answers.html>

Bonus 2 Attacco a un Database MySQL

In questo laboratorio, completa il seguente obiettivo:

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

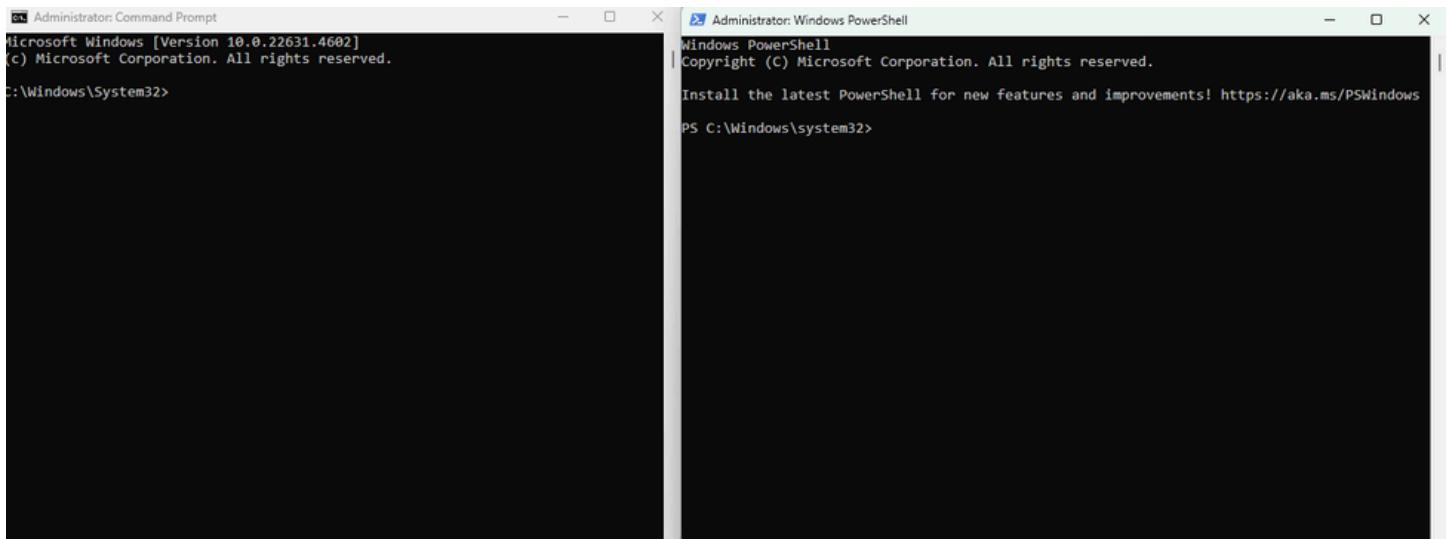
<https://itexamanswers.net/17-2-6-lab-attacking-a-mysql-database-answers.html>

INDICE

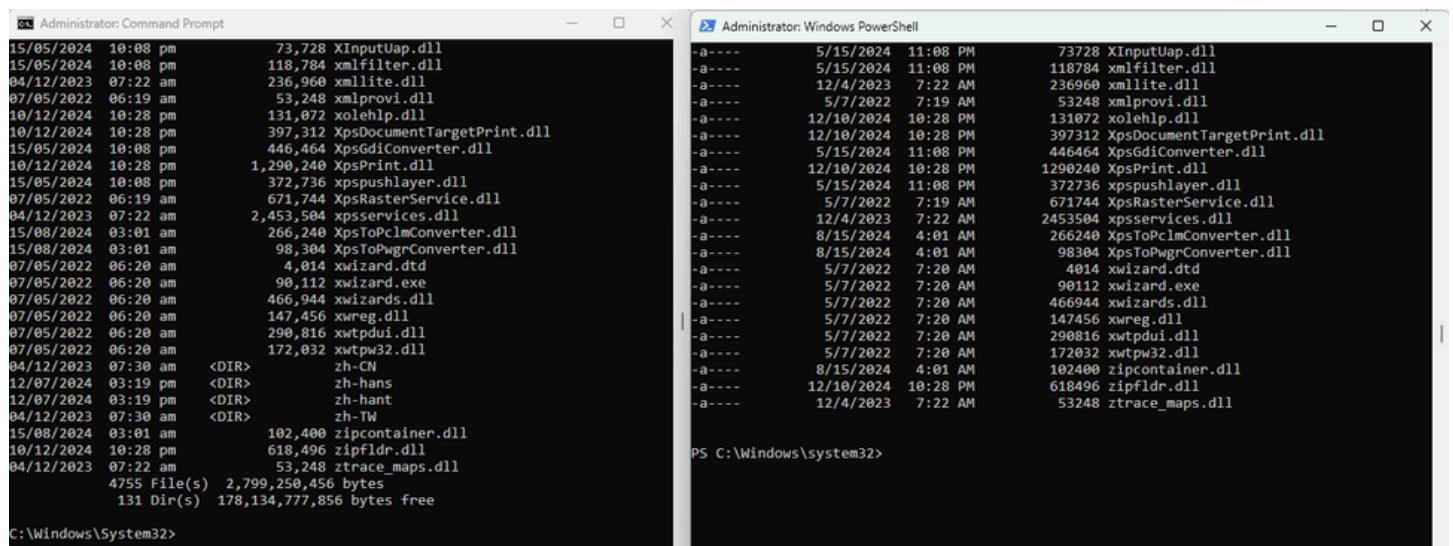
1. Windows PowerShell.....	pag. 3
2. Riflessioni PowerShell.....	pag. 9
3. Analisi Wireshark.....	pag. 10
4. Riflessioni Wireshark	pag. 14
5. Bonus 1 Nmap.....	pag. 15
6. Riflessioni Bonus 1	pag. 20
7. Bonus 2 Sqli.....	Pag. 21
8. Riflessioni Bonus 2.....	Pag. 25

WINDOWS POWERSHELL & CMD

Apriamo Powershell e Command Prompt (CMD), possiamo tramite “start” e cercandoli entrambi o possiamo tramite win+r scrivendo cmd e powershell (Warning, doing so tought will open powershell and cmd with your USER rights and not as SYSTEM) Aperti con administrator rights, (not necessary for this exercise) procediamo con l'esercizio.



Usiamo il comando dir e su entrambi ci mostrerà una lista di sudirectories,file e le informazioni associate ad essi. tipo la grandezza, la data in cui è stato modificato. Su powershell abbiamo la grandezza e l'ultima modifica ma non abbiamo il totale dei file e il numero delle directory ma abbiamo le proprietà del file (RWX di linux basically, cosa l'utente può fare con quel file)



Proviamo con Ping,Cd e Ipconfig. Il risultato è identico.

The screenshot shows two side-by-side Command Prompt windows. The left window is titled 'Administrator: Command Prompt' and the right one is 'Administrator: Windows PowerShell'. Both windows show the results of running 'ping 192.168.1.1', 'ipconfig', and 'cd /' commands. The output is identical between the two environments, demonstrating the consistency of command execution across them.

```
c:\Windows\System32>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

c:\Windows\System32>ipconfig
Windows IP Configuration

Wireless LAN adapter Connessione alla rete locale (LAN)* 1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Connessione alla rete locale (LAN)* 10:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

PS C:\Windows\system32> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

PS C:\Windows\system32> ipconfig
Windows IP Configuration

Wireless LAN adapter Connessione alla rete locale (LAN)* 1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Connessione alla rete locale (LAN)* 10:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

PS C:\Windows\system32> cd /
PS C:\>
```

Procediamo su powershell con “Get-Alias” per avere il comando tradotto da CMD o “l’alias”. Se usiamo “dir” su powershell, funzionerà comunque allo stesso identico modo. è solo per far capire la “shortcut” o riconvinta di powershell. l’alias è Get-ChildItem e Powershell utilizzerà questo.

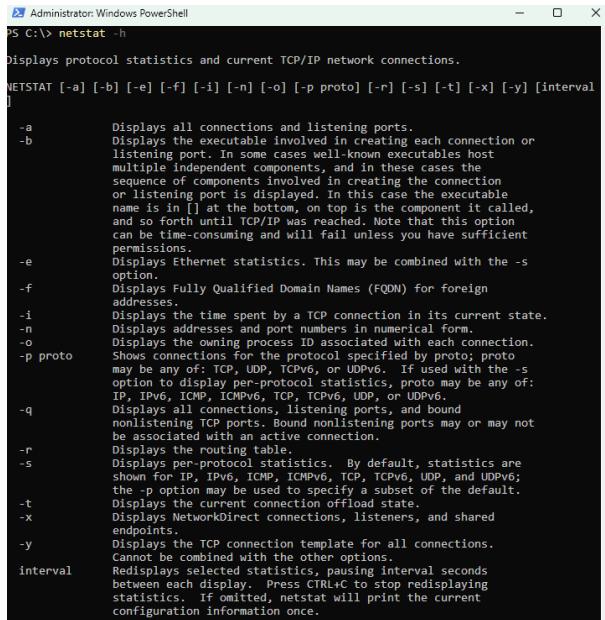
The screenshot shows a single Windows PowerShell window. It displays the output of the 'Get-Alias dir' command. The output shows that the alias 'dir' is mapped to the cmdlet 'Get-ChildItem'. This demonstrates how PowerShell uses aliases to map common commands from the command-line interface to its own cmdlets.

```
PS C:\> Get-Alias dir
 CommandType      Name          Version   Source
 -----          --          --          --
 Alias           dir -> Get-ChildItem

PS C:\>
```

I cmdlet di PowerShell sono piccoli comandi che ti permettono di fare cose specifiche come vedere file, cambiare impostazioni o controllare il sistema, con nomi facili tipo "Prendi-File" (Get-File)

Procediamo con netstat -h (help che funziona con il 99% dei comandi) per mostrarcvi una lista di flag utilizzabili con una descrizione accurata per ognuno.

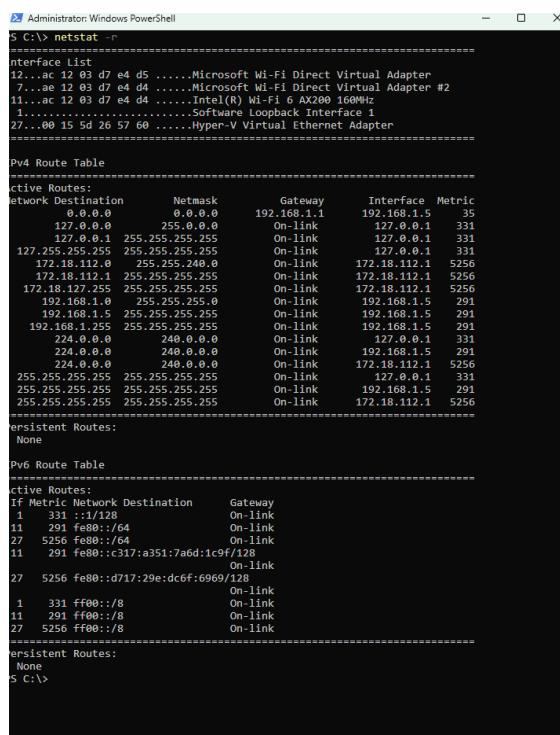


```
Administrator: Windows PowerShell
PS C:\> netstat -h
Displays protocol statistics and current TCP/IP network connections.

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

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
listening port. In some cases well-known executables host
multiple independent components, and in these cases the
sequence of components involved in creating the connection
or listening port is displayed. In this case the executable
name is in [] at the bottom, on top is the component it called,
and so forth until TCP/IP was reached. Note that this option
can be time-consuming and will fail unless you have sufficient
permissions.
-e          Displays Ethernet statistics. This may be combined with the -s
option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
addresses.
-i          Displays the time spent by a TCP connection in its current state.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
may be any of: TCP, UDP, TCPIP, ICMP, ICMPV6, TCP, TCPV6, UDP, or UDPV6.
-q          Displays all connections, listening ports, and bound
nonlistening TCP ports. Bound nonlistening ports may or may not
be associated with an active connection.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
shown for IP, IPv6, ICMP, ICMPV6, TCP, TCPV6, UDP, and UDPV6;
the -p option may be used to specify a subset of the default.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
endpoints.
-y          Displays the TCP connection template for all connections.
Cannot be combined with the other options.
interval   Redisplay selected statistics, pausing interval seconds
between each display. Press Ctrl+C to stop redisplaying
statistics. If omitted, netstat will print the current
configuration information once.
```

Con netstat -r mostriamo la routing table, le destinazioni delle comunicazioni di rete e come i pacchetti vengono instradati attraverso la rete (sia per le connessioni locali che quelle esterne). Il gateway che stiamo usando è 1.1. on-link significa che non ha bisogno di uscire all'esterno e che è raggiungibile localmente (falls in the ip range, no need for a gateway to be used)



```
Administrator: Windows PowerShell
PS C:\> netstat -r
=====
Interface List
12...ac 12 03 d7 e4 d5 .....Microsoft Wi-Fi Direct Virtual Adapter
7...ae 12 03 d7 e4 d4 .....Microsoft Wi-Fi Direct Virtual Adapter #2
11...ac 12 03 d7 e4 d4 .....Intel(R) Wi-Fi 6 AX200 160MHz
1.....Software Loopback Interface 1
27...00 15 5d 26 57 60 .....Hyper-V Virtual Ethernet Adapter
=====

Pv4 Route Table
=====
Active Routes:
Network Destination     Netmask      Gateway       Interface Metric
0.0.0.0                 0.0.0.0       192.168.1.1   192.168.1.5   35
127.0.0.1               255.0.0.0     On-link        127.0.0.1    331
127.255.255.255         255.255.255.255  On-link        127.0.0.1    331
127.255.255.255.255    255.255.255.255  On-link        127.0.0.1    331
172.18.112.0             255.255.240.0   On-link        172.18.112.1  5256
172.18.112.1             255.255.255.255  On-link        172.18.112.1  5256
172.18.127.255           255.255.255.255  On-link        172.18.112.1  5256
192.168.1.0              255.255.255.0   On-link        192.168.1.5   291
192.168.1.5              255.255.255.255  On-link        192.168.1.5   291
192.168.1.255            255.255.255.255  On-link        192.168.1.5   291
224.0.0.0                240.0.0.0     On-link        127.0.0.1    331
224.0.0.1                240.0.0.1     On-link        192.168.1.5   291
254.0.0.0                255.255.255.255  On-link        172.18.112.1  5256
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        192.168.1.5   291
255.255.255.255          255.255.255.255  On-link        172.18.112.1  5256
=====
Persistent Routes:
None
=====
Pv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1     331 ::1/128                 On-link
11    291 fe80::/64                On-link
27    5256 fe80::/64                On-link
11    291 fe80::c317:a351:7a6d:1c9f128
27    5256 fe80::d717:29e:dc6f:6969/128
1     331 ff00::/8                 On-link
11    291 ff00::/8                 On-link
27    5256 ff00::/8                 On-link
=====
Persistent Routes:
None
PS C:\>
```

Con netstat -abno ci mostra le connessioni attualmente attive TCP E UDP

```
PS Select Administrator: Windows PowerShell
11    291 fe80::c317:a351:7a6d:1c9f/128
                                         On-link
27    5256 fe80::d717:29e:dc6f:6969/128
                                         On-link
 1    331 ff00::/8
11    291 ff00::/8
27    5256 ff00::/8
=====
Persistent Routes:
  None
PS C:\> netstat -abno

Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    0.0.0.0:135           0.0.0.0:0            LISTENING  1896
  RpcEptMapper
[svchost.exe]
  TCP    0.0.0.0:445           0.0.0.0:0            LISTENING   4
Can not obtain ownership information
  TCP    0.0.0.0:2179          0.0.0.0:0            LISTENING  2512
[vmms.exe]
  TCP    0.0.0.0:5040          0.0.0.0:0            LISTENING  9788
  CDPSvc
[svchost.exe]
  TCP    0.0.0.0:7680          0.0.0.0:0            LISTENING  4320
Can not obtain ownership information
  TCP    0.0.0.0:49664         0.0.0.0:0            LISTENING  1576
[lsass.exe]
  TCP    0.0.0.0:49665         0.0.0.0:0            LISTENING  1468
Can not obtain ownership information
  TCP    0.0.0.0:49666         0.0.0.0:0            LISTENING  2448
  Schedule
[svchost.exe]
  TCP    0.0.0.0:49667         0.0.0.0:0            LISTENING  3032
  EventLog
[svchost.exe]
  TCP    0.0.0.0:49668         0.0.0.0:0            LISTENING  4984
[spoolsv.exe]
  TCP    0.0.0.0:49669         0.0.0.0:0            LISTENING  1544
Can not obtain ownership information
  TCP    127.0.0.1:6463        0.0.0.0:0            LISTENING  13268
[Discord.exe]
  TCP    127.0.0.1:9080        0.0.0.0:0            LISTENING  5492
[NahimicService.exe]
  TCP    127.0.0.1:50284       127.0.0.1:50285      ESTABLISHED 17696
[CiscoCollabHost.exe]
  TCP    127.0.0.1:50285       127.0.0.1:50284      ESTABLISHED 17696
[CiscoCollabHost.exe]
  TCP    127.0.0.1:50286       127.0.0.1:50287      ESTABLISHED 17696
[CiscoCollabHost.exe]
  TCP    127.0.0.1:50287       127.0.0.1:50286      ESTABLISHED 17696
[CiscoCollabHost.exe]
  TCP    127.0.0.1:50288       127.0.0.1:50289      ESTABLISHED 17696
[CiscoCollabHost.exe]
  TCP    127.0.0.1:50289       127.0.0.1:50288      ESTABLISHED 17696
=====

  UDP    127.0.0.1:1900        *:*                  8676
  SSDPSRV
[svchost.exe]
  UDP    127.0.0.1:49664       127.0.0.1:49664      4316
  iphlpsvc
[svchost.exe]
  UDP    127.0.0.1:56575       *:*                  8676
  SSDPSRV
[svchost.exe]
  UDP    127.0.0.1:63472       *:*                  8576
[nvcontainer.exe]
  UDP    172.18.112.1:67        *:*                  3536
  SharedAccess
[svchost.exe]
  UDP    172.18.112.1:68        *:*                  2526
```

Cerchiamo ora il PID 1896 su task manager. nella tabella processes possiamo vedere i servizi associati “attivi” mentre su details vediamo che il processo svchost.exe è associata al PID. Vediamo lo stato “running” username o utente del processo “SERVIZIO DI RETE” (l’utente che lo sta eseguendo) la cpu usata la memoria in uso, il tipo di archettura e una descrizione breve ma accurata.

Processo host per i servizi di windows. (Host process for Windows Services)

The screenshot shows the Windows Task Manager with the 'Processes' tab selected. A search bar at the top right contains the number '1896'. The main table has columns for Name, CPU, Status, Memory, Network, and Disk. The row for PID 1896, 'Service Host: Remote Procedure Call (2)', is highlighted in blue. This row contains three sub-items: 'Remote Procedure Call (RPC)', 'RPC Endpoint Mapper', and 'RPC'. The 'RPC' item is also highlighted in blue. The 'CPU' column shows 9% usage, while 'Memory' shows 36% usage (6.6 MB). The 'Status' column indicates the process is running.

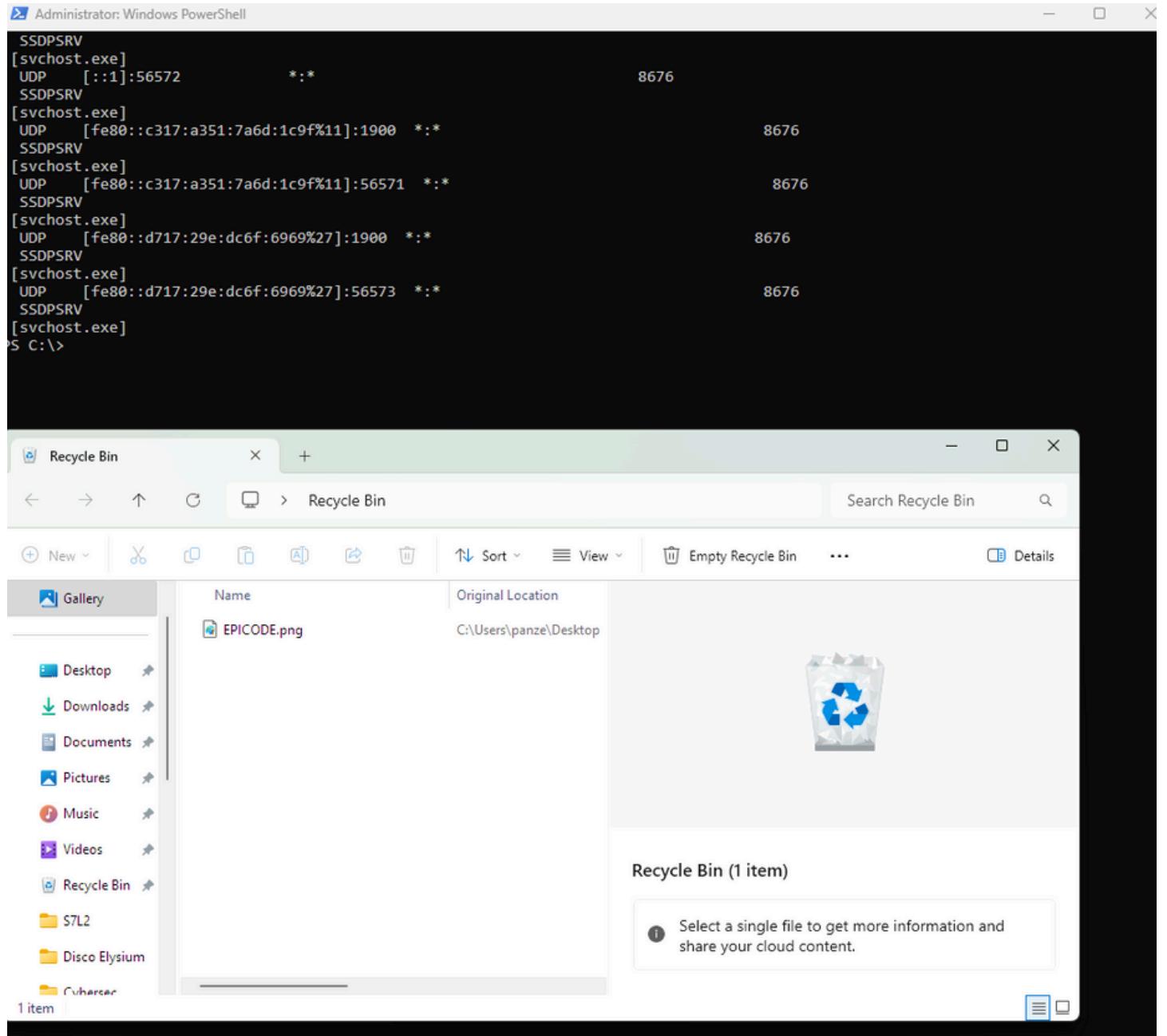
Name	CPU	Status	Memory	Network	Disk
Service Host: Remote Procedure Call (2)	9%	Running	36% 6.6 MB	0 Mbps	0 MB/s
Remote Procedure Call (RPC)		Efficiency...			
RPC Endpoint Mapper		Efficiency...			

Sta usando 6,688k di memoria ram o 6,6MB (poco, i pc moderni di oggi hanno almeno 16GB per essere “fluidi” 8GB a volte possono comunque essere sufficienti, more is always better)

The screenshot shows the Windows Task Manager with the 'Details' tab selected. A search bar at the top right contains the number '1896'. The table has columns for Name, PID, Status, Username, CPU, Memory, Architecture, and Description. The row for PID 1896, 'svchost.exe', is highlighted in blue. The 'Description' column shows 'Host Process for Windows Services'. The 'Status' column shows 'Running', and the 'Username' column shows 'SERVIZIO DI RETE'.

Name	PID	Status	Username	CPU	Memory (active private...)	Architecture	Description
svchost.exe	1896	Running	SERVIZIO DI RETE	00	6,688 K	x64	Host Process for Windows Services

E finiamo con pulire il cestino tramite Powershell per completare la prima parte dell'esercizio con Clear-Recyclebin (pulisci il cestino, letteralmente)

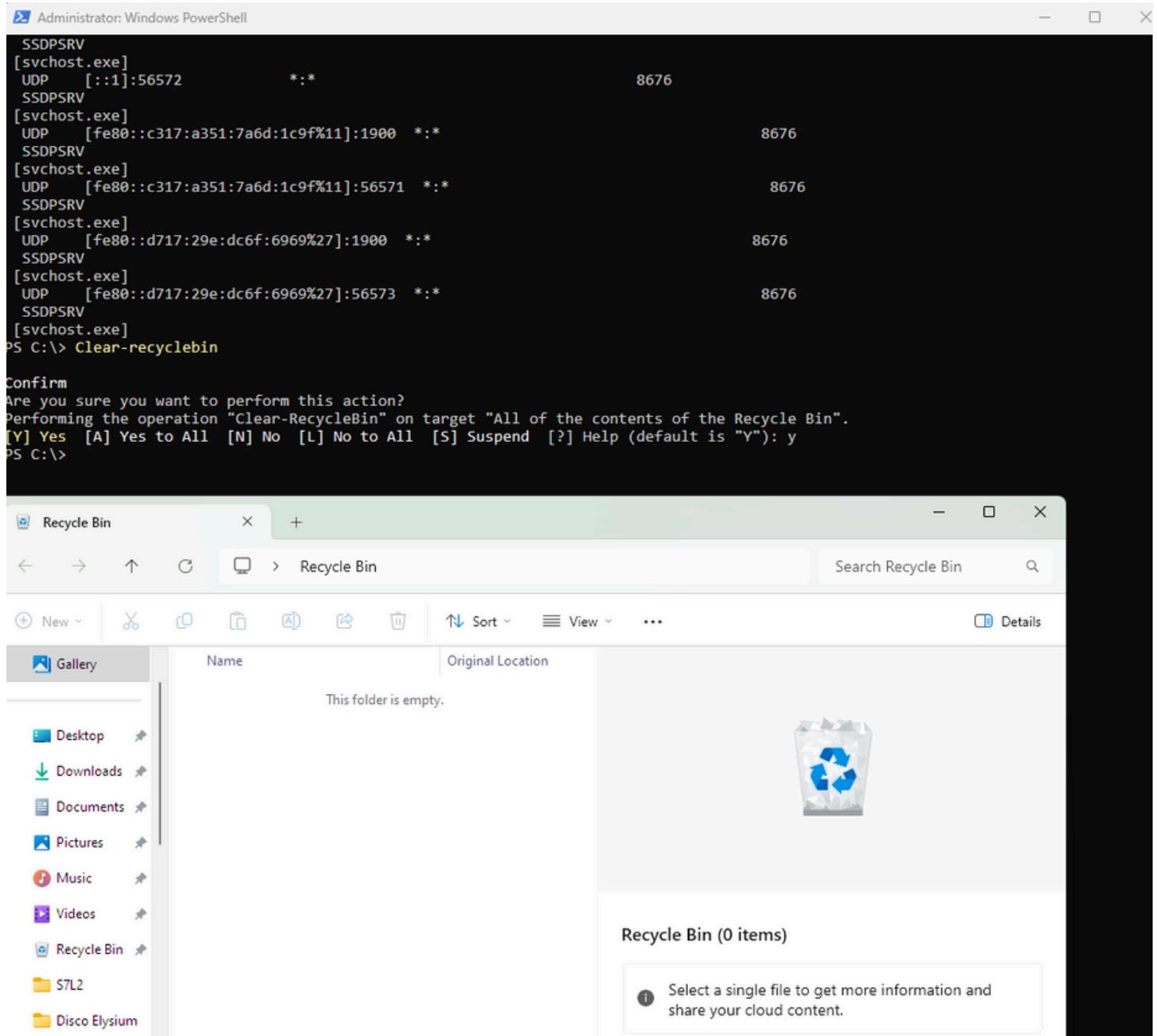


The screenshot shows two windows side-by-side. On the left is a Windows PowerShell window titled 'Administrator: Windows PowerShell' with the following command history:

```
SSDPSRV
[svchost.exe]
  UDP  [::1]:56572      *:*
  SSDPSRV
[svchost.exe]
  UDP  [fe80::c317:a351:7a6d:1c9f%11]:1900  *:*
  SSDPSRV
[svchost.exe]
  UDP  [fe80::c317:a351:7a6d:1c9f%11]:56571  *:*
  SSDPSRV
[svchost.exe]
  UDP  [fe80::d717:29e:dc6f:6969%27]:1900  *:*
  SSDPSRV
[svchost.exe]
  UDP  [fe80::d717:29e:dc6f:6969%27]:56573  *:*
  SSDPSRV
[svchost.exe]
'S C:\>
```

On the right is the Windows Recycle Bin window, which displays one item: 'EPICODE.png' from 'C:\Users\panze\Desktop'. The Recycle Bin icon is shown.

Con questo comando e se gli diamo lo yes to all, i file verrano eliminati tutti.
Very “Poetry-like” As it is our last Exam.



```

Administrator: Windows PowerShell
PS C:\> Get-NetTCPConnection | Where-Object { $_.State -eq "Established" } | Select-Object LocalAddress, LocalPort, RemoteAddress, RemotePort, State, ProcessId
LocalAddress LocalPort RemoteAddress RemotePort State ProcessId
: : : : : :
PS C:\> Get-EventLog -LogName Application | Where-Object { $_.Source -eq "Windows Security" } | Select-Object TimeGenerated, Source, Message
TimeGenerated Source Message
: : :
PS C:\> Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Run" | Select-Object Name, Value
Name Value
: :
PS C:\> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
PS C:\> Get-ExecutionPolicy
ExecutionPolicy
RemoteSigned
PS C:\> Get-Process | Where-Object { $_.Name -eq "svchost.exe" } | Select-Object Name, CPU, Handles, Id, MemoryUsage, ProcessName, Threads, WorkingSet
Name CPU Handles Id MemoryUsage ProcessName Threads WorkingSet
svchost.exe 8676 8676 8676 8676 8676 8676 8676
PS C:\> Clear-recyclebin
Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\>

```

Recycle Bin

Name Original Location

This folder is empty.

Gallery

Desktop Downloads Documents Pictures Music Videos Recycle Bin S7L2 Disco Elysium

Sort View Details

Recycle Bin (0 items)

Select a single file to get more information and share your cloud content.

RIFLESSIONI

PowerShell offre diversi comandi che possono semplificare il lavoro di un analista della sicurezza. Ad esempio, Get-Process aiuta a monitorare i processi attivi per rilevare comportamenti sospetti, mentre Get-NetTCPConnection identifica le porte TCP aperte e le connessioni attive. Il comando Get-EventLog permette di esaminare i log degli eventi, essenziale per la risposta cyber-threats. Inoltre, Get-ItemProperty è utile per verificare le versioni dei software installati, mentre Set-ExecutionPolicy consente di impostare politiche di esecuzione sicure per prevenire l'esecuzione di script dannosi. Questi strumenti, migliorano la sicurezza del nostro sistema.

CYBEROPS WORKSTATION PART 2

Proseguiamo con la parte 2, apriamo la workstation effettuiamo il login e aperto il terminale eseguiamo un TCP dump su la nostra interfaccia attualmente in uso (per collegarsi ad internet 1.29 interface enp0s3) sudo per i permessi, tcpdump per effettuare il dump -i per specificare l'interfaccia> enp0s3, -s su 0 (per non dare nessuna lunghezza min-max salvata del nostro pacchetto e -w per scrivere su un file (write) il risultato.

```
[analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C1102 packets captured
1123 packets received by filter
0 packets dropped by kernel
[analyst@secOps Desktop]$
```

Mentre è in ascolto andiamo su questo sito non protetto in http (non crypted) che ci avverrà con il lucchetto in alto ma anche quando premiamo su username o password. procediamo a mettere Admin Admin (mentre il tcp dump è in corso) e premiamo login. Procediamo nel chiudere il nostro dump con cntrl+c e andiamo ad analizzare il nostro file.

The screenshot shows a Mozilla Firefox window with the title "Altoro Mutual - Mozilla Firefox". The address bar displays "oro Mutual" and the URL "www.altoromutual.com/login.jsp". The page content includes the Altoro Mutual logo, navigation links for "Sign In", "Contact Us", "Feedback", and "Search", and a "DEMO SITE ONLY" banner. On the left sidebar, there are links for "ONLINE BANKING LOGIN", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The main content area features an "Online Banking Login" form with fields for "Username" (containing "Admin") and "Password" (containing "....."). A "Login" button is located below the password field.

Lo apriamo o andando su wireshark>file e lo apriamo. o possiamo anche cliccarlo due volte.



Una volta dentro filtriamo per solo il protocollo HTTP e cerchiamo il messaggio POST, espandiamo HTML FORM URL ENCODEED: che ci mostrerà username, password e il form che abbiamo utilizzato per questi dati (li abbiamo messi nel Login)

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
420	25.377032	65.61.137.117	192.168.1.29	HTTP	8871	HTTP/1.1 200 OK (text/html)
439	25.457181	192.168.1.29	65.61.137.117	HTTP	421	GET /style.css HTTP/1.1
439	25.602618	65.61.137.117	192.168.1.29	HTTP	176	HTTP/1.1 200 OK (text/css)
441	25.603345	192.168.1.29	65.61.137.117	HTTP	412	GET /images/logo.gif HTTP/1.1
442	25.603609	192.168.1.29	65.61.137.117	HTTP	418	GET /images/header_pic.jpg HTTP/1.1
448	25.748363	65.61.137.117	192.168.1.29	HTTP	1179	HTTP/1.1 200 OK (GIF89a)
460	25.755938	192.168.1.29	65.61.137.117	HTTP	415	GET /images/pf_lock.gif HTTP/1.1
461	25.756301	192.168.1.29	65.61.137.117	HTTP	416	GET /images/gradient.jpg HTTP/1.1
466	25.896501	65.61.137.117	192.168.1.29	HTTP	666	HTTP/1.1 200 OK (JPEG/JFIF image)
466	25.907088	65.61.137.117	192.168.1.29	HTTP	366	HTTP/1.1 200 OK (GIF89a)
470	25.908428	65.61.137.117	192.168.1.29	HTTP	1187	HTTP/1.1 200 OK (JPEG/JFIF image)
474	25.935330	192.168.1.29	65.61.137.117	HTTP	420	GET /favicon.ico HTTP/1.1
485	26.042413	192.168.1.29	65.61.137.117	HTTP	360	GET /favicon.ico HTTP/1.1
486	26.084693	65.61.137.117	192.168.1.29	HTTP	7180	HTTP/1.1 404 Not Found (text/html)
495	26.195536	65.61.137.117	192.168.1.29	HTTP	3076	HTTP/1.1 404 Not Found (text/html)
792	67.864620	192.168.1.29	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
798	68.048806	65.61.137.117	192.168.1.29	HTTP	318	HTTP/1.1 302 Found
800	68.056581	192.168.1.29	65.61.137.117	HTTP	609	GET /bank/main.jsp HTTP/1.1
810	68.239908	65.61.137.117	192.168.1.29	HTTP	6514	HTTP/1.1 200 OK (text/html)

Frame 792: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)
Ethernet II, Src: PcsCompu_andCf0 (08:00:27:a0:c0:f0), Dst: 14:14:59:27:51:60 (14:14:59:27:51:60)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 44222, 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"
0000 14:14:59:27:51:60 00:08:00 27 aa 0c f0 08 00 45 00 .YY'...E
0010 02 4b 16 c3 40 00 00 06 95 72 0a 80 01 d4 13 00 K.@@.r..A
0020 39 75 ac be 00 50 b5 45 f2 7f 62 d6 56 2c 80 18 u.P.E.b.V.
0030 2e 58 e5 00 00 01 01 08 0a 36 0f 6f 4d 00 00 6.M

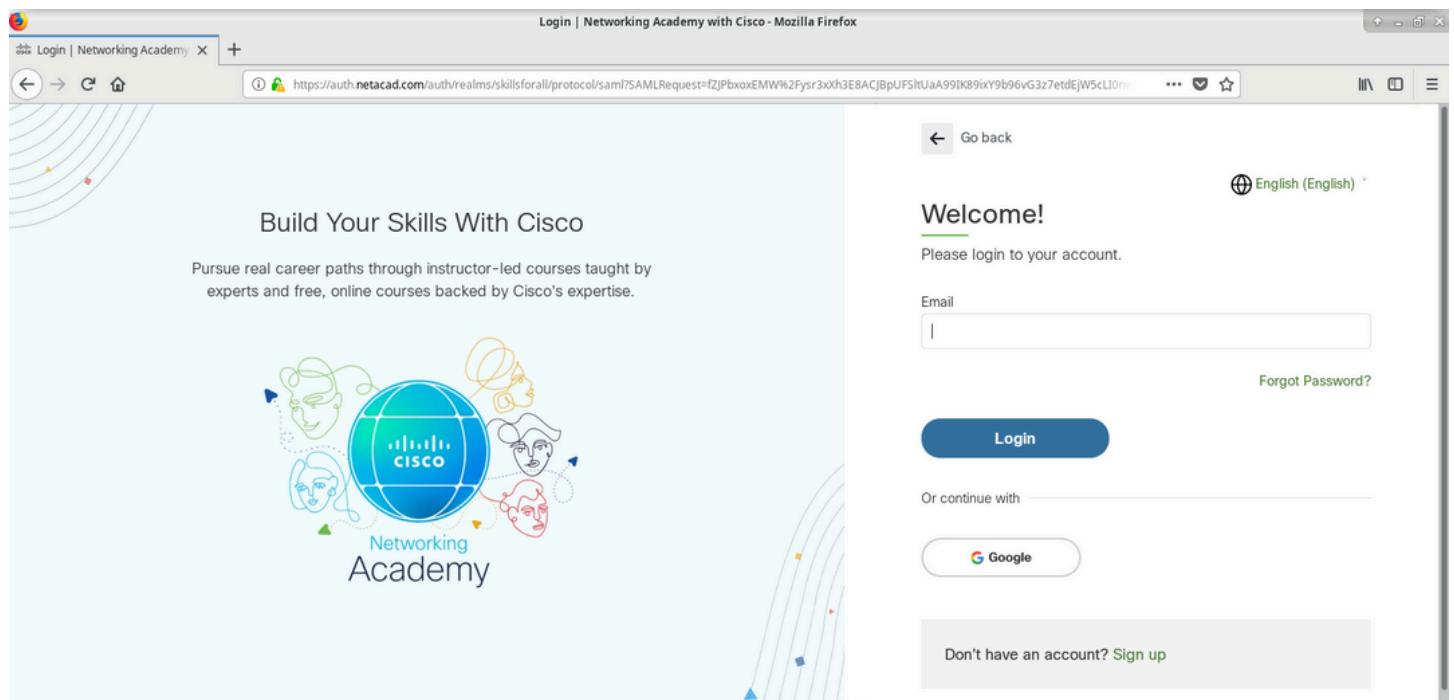
Frame (frame), 601 bytes Profile: Default

Adesso la stessa cosa ma con il traffico HTTPS (sempre tramite TCP DUMP)

```
[analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Ci colleghiamo a netacad che per connettersi tramite browser dobbiamo però prima cambiare la data sudo date -s "12 MAY 2020 21:38:20"

E comunque ci avverrà del certificato "expired" and "not safe" e non avremo il lucchetto blu che conferma una connessione sicura, il certificato che abbiamo ricevuto "non era valido" ma aggiunta una eccezione potremo comunque andare avanti.



Inseriamo l'email (il sito è cambiato, non è più come mostrato nella guida) e torniamo di là e fermiamo il Dump. Procediamo nell'analizzarlo.

Aperto wireshark e il dump tcp, cerchiamo Application Data e notiamo che in fondo non ha più (nei dettagli) la sezione HTTP ma SSL con ENCRYPTED APPLICATION DATA. IL payload è criptato usando TLS V1.2 e non può essere letto.

httpsdump.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
49	14.993652	192.168.1.29	34.120.5.221	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
50	15.012522	34.120.5.221	192.168.1.29	TLSv1.2	377	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
51	15.012534	192.168.1.29	34.120.5.221	TCP	66	60152 → 443 [ACK] Seq=296 Ack=3300 Win=40448 Len=0 TSval=305202527 TSecr=2353041037
52	15.012939	34.120.5.221	192.168.1.29	TLSv1.2	141	Application Data

Frame 52: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)
Ethernet II, Src: 14:14:59:27:51:60 (14:14:59:27:51:60), Dst: PcsCompu_aa:0c:f0 (08:00:27:aa:0c:f0)
Internet Protocol Version 4, Src: 34.120.5.221, Dst: 192.168.1.29
Transmission Control Protocol, Src Port: 443, Dst Port: 60152, Seq: 3300, Ack: 296, Len: 75
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http2
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 70
Encrypted Application Data: 000000000000000017ea4f1e4819984806960112daf496632...

0040 05 49 17 03 03 00 46 00 00 00 00 00 00 00 01 7e 1,...F
0050 a4 f1 e4 81 99 84 80 69 60 11 2d af 49 66 32 18l`.-.lf2.
0060 db 23 c4 be 29 00 8a 9c 2f d0 82 f4 30 c3 80 b3 1.#...).../.0...
0070 db be 39 5c 81 64 18 af 89 5e 85 a9 68 a0 53 de 1.9..d..^..h.S

Payload is encrypted application data ... Packets: 3918 · Displayed: 2179 (55.6%) · Load time: 0:00.025

Completando la prima parte.

RIFLESSIONI PART 2

Utilizzare HTTPS anziché HTTP comporta diversi vantaggi. Il traffico tra browser e sito è protetto grazie alla crittografia mediante il protocollo SSL/TLS. Questo permette di proteggersi da attacchi in cui l'hacker vuole intercettare dati personali, come la password ad esempio, senza però riuscire decifrare il contenuto del messaggio. HTTPS garantisce che il sito web che stai visitando risulta essere esattamente quello previsto (usually) ed evita che informazioni sensibili come password vengano intercettate. Gli attacchi di tipo "man-in-the-middle" non possono sfruttare una connessione HTTPS, e qualsiasi tipo di avviso nell'accedere o usare un sito HTTP (NON PROTETTO) dovrebbe essere difficile da ignorare anche per un utente medio.

Tuttavia, questo non è sufficiente. In molti casi infatti, è stato studiato che il protocollo viene usato dai siti web per recuperare e trafugare ogni tipo di dato utente, dalle password alle credenziali di accesso. Motivo per cui, non è sufficiente affermare che "il sito è sicuro perché è in HTTPS", anche se comunque è necessario per la sicurezza della propria connessione con il sito Internet. Inoltre i "malintenzionati" possono comunque utilizzare HTTPS mentre ti stanno prendendo i dati (fake site, fake certificate). Per concludere, anche se un sito Internet è in HTTPS, è sempre bene non abbassare la guardia: purtroppo, oggi giorno si può rimanere vittima di phishing anche se il sito usa tale protocollo.

BONUS 1

Apriamo un terminale su CyberopsWorkstation e mettiamo il comando “man nmap” che ci aprira la guida/manuale. e ci spiegherà l'utilizzo il what is di nmap.

Nmap non è altro che un tool (strumento) per l'esplorazione del network scanner di sicurezza (vuln) e porte e determina gli host e i servizi “offerti” sul network. Con nmap possiamo fare anche “host discovery”, port scanning (like we said before) e capire il tipo di sistema operativo messo in uso da un host (nmap -O) e troverà vulnerabilità sul network, con la possibilità di sapere le versioni dei servizi (in depth scan nmap -sV per la versione e --script vuln per avere le vulnerabilità)

```
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.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    Manual page nmap(1) line 1 (press h for help or q to quit)
```

Per l'esercizio cerchiamo “/example” e il comando usato per questo esempio è nmap -A -T4 (con questo comando non ci si preoccupa o meno di fare “rumore” è aggressivo T4 piuttosto veloce, ed è un buon compromesso tra velocità e detecting, mentre con -A vediamo tutto versione sistema operativo, versione dei servizi, traceroute

A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are **-A**, to enable OS and version detection, script scanning, and traceroute; **-T4** for faster execution; and then the hostname.

Example 1. A representative Nmap scan

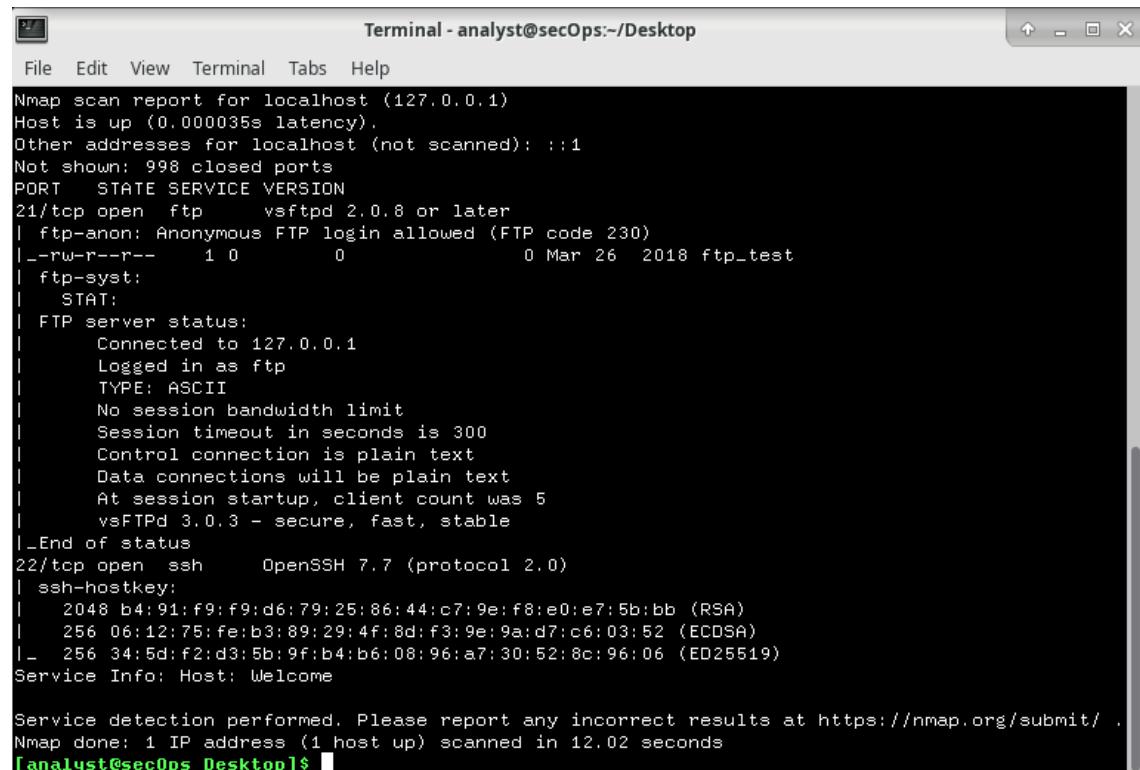
```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open     http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldp
1720/tcp  filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

Chiudiamo la guida e procediamo ad uno scan su localhost con

nmap -A -T4 localhost e troviamo la porta 21 e la porta 22 aperta entrambe tcp

Ftp utilizza vsftpd 2.0.8 (or later) e ssh utilizza OpenSSH 7.7(prot 2.0)



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/Desktop". The window contains the output of an Nmap scan on the local host (127.0.0.1). The output shows two open TCP ports: port 21 (FTP) and port 22 (SSH). The FTP service is identified as vsftpd 2.0.8 or later, and the SSH service is identified as OpenSSH 7.7 (protocol 2.0). The Nmap command used was "nmap -A -T4 localhost". The terminal prompt at the bottom is "[analyst@secOps Desktop]\$".

```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000035s 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 5
|     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 12.02 seconds
[analyst@secOps Desktop]$
```

Procediamo con uno scan sul nostro network, ma prima individuiamo il nostro IP e verifichiamo a quale "network" appartiene (ad esempio, 192.168.1.0/24 con subnet mask 255.255.255.0). Il subnetting della rete domestica è lo stesso, dato che la configurazione è attualmente su modalità "bridge". Confermiamo che apparteniamo allo stesso subnetting con un ping

```
[analyst@secOps Desktop]$ 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
    inetc6 ::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:aa:0c:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.29/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 77385sec preferred_lft 77385sec
    inetc6 fe80::a00:27ff:fea:cf0/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$
```

Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\panze>ping 192.168.1.29

Pinging 192.168.1.29 with 32 bytes of data:
Reply from 192.168.1.29: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.29:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\panze>

```
[analyst@secOps Desktop]$ 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
    inetc6 ::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:aa:0c:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.29/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 77385sec preferred_lft 77385sec
    inetc6 fe80::a00:27ff:fea:cf0/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$
```

Eseguiamo uno scan adesso sul nostro network totale con nmap -A -T4 192.168.1.0/24 e abbiamo 3 host totali "up". gli indirizzi ip di questi host sono 192.168.1.1 (vodafone router) 192.168.1.29 (se stessa) e 1.28 (un cellulare connesso al wifi) Non ha potuto trovare a me sul network 1.5 perché bloccato ^^ (rimossa individuazione sul network, totale. regole di firewall, modalità stealth, disabilitato icmp, etc.)

```
service detection performed. Please report any incorrect results at http://nmap.org/submit/
map done: 256 IP addresses (3 hosts up) scanned in 194.52 seconds
```

1.28 ha tutte le porte chiuse 1.29 ha ftp e ssh come prima.

Passiamo ad 1.1 (vodafone)

```
Nmap scan report for Redmi-Note-13.station (192.168.1.28)
Host is up (0.0076s latency).
All 1000 scanned ports on Redmi-Note-13.station (192.168.1.28) are closed

Nmap scan report for secOps.station (192.168.1.29)
Host is up (0.00033s 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 192.168.1.29
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:
```

abbiamo le classiche porte aperte, niente da approfondire. (http?) perchè non riconosce la versione/nonostante abbia avuto una risposta di versione etc. (fingerprint missing, please upload the fingerprint to nmap etc.*) Le altre sono napster su ssl,ftps e blackice-icecap. (others are irrelevant)

```
Not shown: 988 closed ports
PORT      STATE SERVICE           VERSION
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open     domain          dnsmasq 2.84
| dns-nsid:
|_ bind.version: dnsmasq-2.84
80/tcp    open     http?
| fingerprint-strings:
```

E adesso eseguiamo uno scan esterno su scanme.nmap.org

With nmap -A -T4 scanme.nmap.org

Terminal - analyst@secOps:~/Desktop

File Edit View Terminal Tabs Help

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-13 00:28 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 00:28 (0:00:00 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 34.55% done; ETC: 00:28 (0:00:04 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 100.00% done; ETC: 00:28 (0:00:00 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 00:29 (0:00:02 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: 995 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)
53/tcp      open      domain      dnsmasq 2.84
| dns-nsid:
|_ bind.version: dnsmasq-2.84
80/tcp      filtered http
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 18.81 seconds
[analyst@secOps Desktop]$
```

Come vediamo le porte aperte con protocollo e servizio associato sono la 22/tcp:ssh, 53/tcp:dnsmasq, 80/tcp:http, 9929/tcp:nping-echo e 31337/tcp:tcpwrapped e abbiamo come “filtered” solo la porta 80 con servizio http. L’indirizzo ipv4 del server è 45.33.32.167 e 2600:3c01::f03c:91ff:fe18:bb2f come ipv6. (not scanned) e Ubuntu Linux è il sistema operativo.

RIFLESSIONI

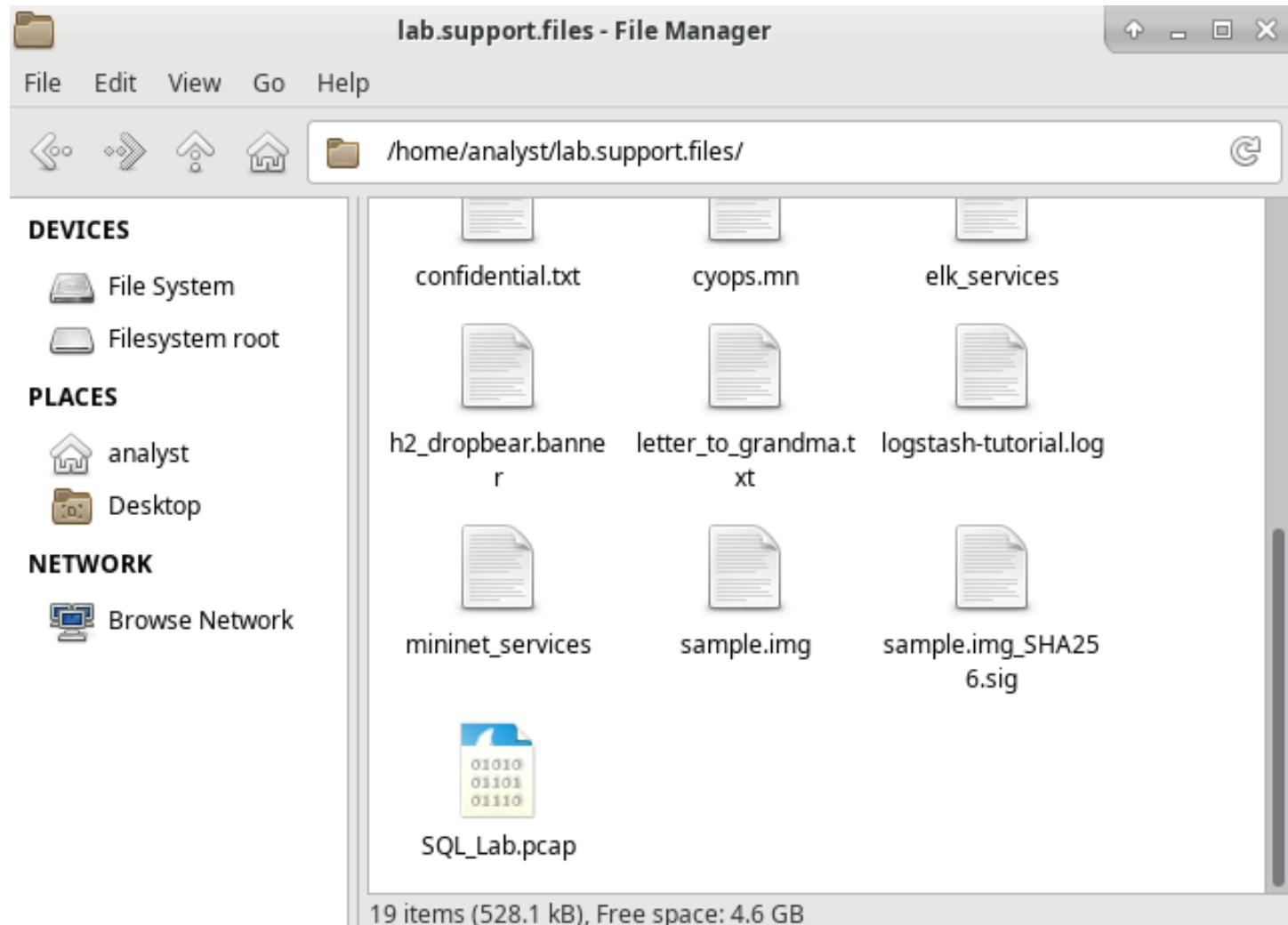
Nmap è uno tool molto potente per l'esplorazione e la gestione delle reti.

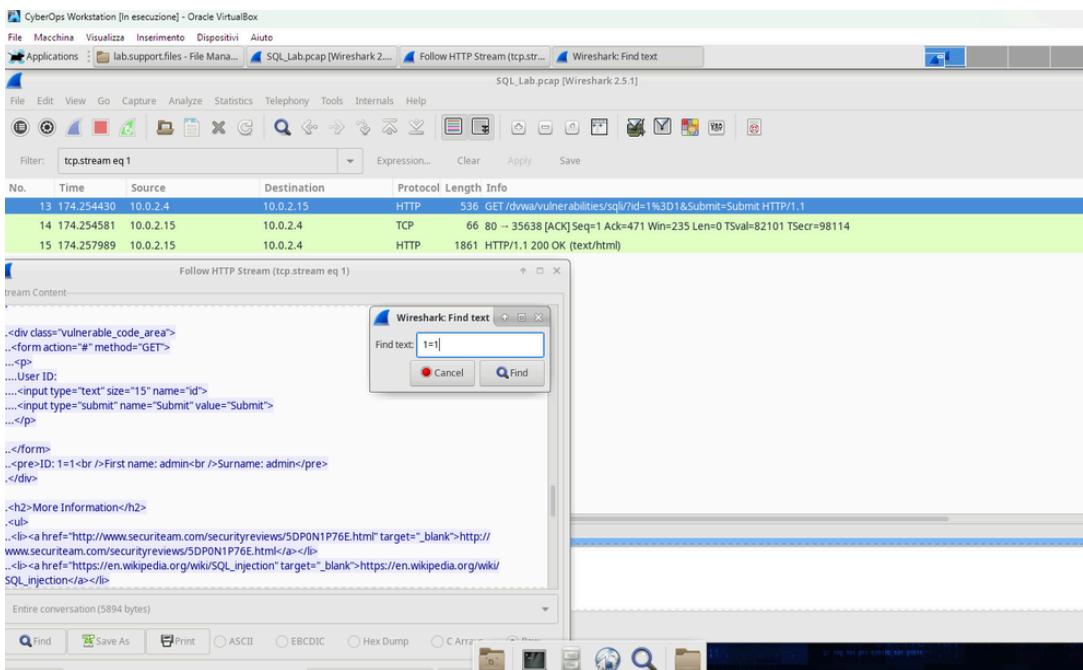
From one side, Nmap può essere utilizzato per analizzare una rete interna alla ricerca di porte aperte specifiche e non , in modo da trovare ed identificare possibili vulnerabilità. Può anche essere impiegato per eseguire un “inventario della rete”, verificando che tutti i sistemi siano adeguatamente aggiornati e protetti contro vulnerabilità note.

From the other, Nmap può essere usato per scopi di ricognizione da parte di un attore malintenzionato, consentendo di individuare porte aperte e raccogliere informazioni sensibili sulla rete, che potrebbero essere sfruttate per attacchi successivi.

BONUS 2 SQLI

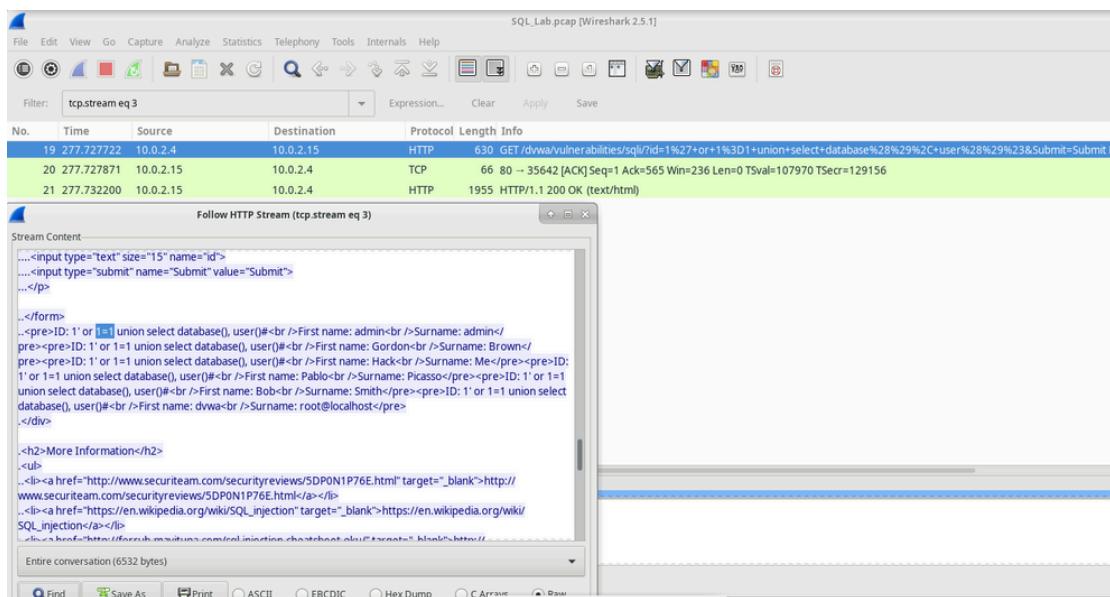
Analizzeremo un attacco SQLI e una volta aperto il file log con wireshark procediamo con l'analisi. Il file è l'intera durata dell'attacco, 441 Secondi c.ca) e i due indirizzi ip coinvolti sono 10.0.2.4 and 10.0.2.15





Seguiamo con il tasto destro lo “stream” HTTP e cerchiamo le query dell’attaccante. notiamo invece che restituigli errore (input sanitization) gli ha risposto con un record del database. L’attaccante ha confermato che può fare SQL injection.

leviamo il filtro e andiamo alla riga 19 eseguendo la stessa cosa per seguire i suoi passi e cerchiamo sempre 1=1 (input inserito da l’attaccante) per vedere che cosa è riuscito ad ottenere. L’attaccante ha inserito una query (1' or 1=1 union select database(), user()#) nella casella di ricerca dell’ID utente sul target 10.0.2.15. Invece di rispondere con un messaggio di errore di login, l’applicazione ha restituito le seguenti informazioni



Il nome del database è dvwa e l’utente del database root@localhost. inoltre ci sono altri account in mostra. e seguendo la nostra traccia nel prossimo get alla linea 22 vediamo che l’attaccante ha inserito una query (1' or 1=1 union select null, version()#) nella casella di ricerca dell’ID utente sul target 10.0.2.15 per individuare la versione

The screenshot shows the Wireshark interface with a filter applied to show only stream 4. The main pane displays three captured packets, with the third one selected. A detailed view of the selected packet's content is shown in a modal window titled "Follow HTTP Stream (tcp.stream eq 4)".

Stream Content:

```
<div class="vulnerable_code_area">
<form action="#" method="GET">
<p>
...User ID:<br/>
<input type="text" size="15" name="id">
<input type="submit" name="Submit" value="Submit">
</p>

</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: 5.7.12-0ubuntu1.1</pre>
</div>

<h2>More Information</h2>
```

Transmission Control Panel:

Index	Time	Source	Destination	Protocol	Length	Info
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+null%2C+version+%28%29%23&Submit=
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	313.712141	10.0.2.15	10.0.2.4	HTTP	1054	HTTP/1.1 200 OK (text/html)

Nel prossimo GET alla linea 25 ha inserito una query (1'or 1=1 union select null, table_name from information_schema.tables#) nella casella di ricerca dell'ID utente sul target 10.0.2.15 per visualizzare tutte le tabelle presenti nel database. Questa operazione ha generato un output ampiissimo contenente numerose tabelle, l'attaccante non ha specificato il valore "null" senza ulteriori filtri o specifiche.

Se l'attaccante avesse usato (1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users')

Il database avrebbe risposto con un output molto più breve, filtrato in base alla presenza della parola "users".

Proseguendo con la linea 28 (o prossimo GET) seguiamo lo stream e cerchiamo 1=1 identifichiamo i dati che l'attaccante è riuscito a estrarre sfruttando il nostro input non sanitizzato. con (1'or 1=1 union select user, password from users#) nel nostro userID (o searchbox) l'attaccante è riuscito ad ottenere tutti gli hash delle nostre password e nomi utente/username associati.

The screenshot shows the Wireshark interface with a packet list and a detailed view of an HTTP stream. The packet list shows three relevant packets:

No.	Time	Source	Destination	Protocol	Length	Info
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sql/?id=1%27+or+1%3D1+union+select+user%2C+password+from+users%23&Submit=Submit
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TStamp=148990 TSecr=178379
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

The details pane shows the HTTP response body, which contains a large amount of sensitive data extracted via SQL injection. The Stream Content pane displays the raw HTML output, including user names, last names, and their corresponding MD5 hashes. The transmission pane on the left shows the sequence of transmitted bytes.

User 1337 ha come hash 8d353... e la sua password è charley. (cracked, this is bad. it took me 2 seconds.) Completando e finendo anche il Bonus 2.

RIFLESSIONI BONUS 2

Molti applicativi e siti web collegati a database utilizzano il linguaggio SQL per l'accesso e l'interrogazione alle informazioni, questo rappresenta una delle principali cause di vulnerabilità ad attacchi di tipo SQL injection. La severità delle iniezioni SQL dipende dal livello di iniezione riuscito all'attaccante.

Attraverso una SQL injection, un potenziale attaccante può trasmettere codice SQL indesiderato, e può compromettere la sicurezza dei database di back-end. Le iniezioni possono consentire ad un avversario di eludere i meccanismi di autenticazione e di prelievo di utenti.

Per prevenire attacchi SQL Injection:

1. Filtrare ogni utente dell'input
2. Usare parametri con procedure memorizzate (stored procedures) o query preparate (prepared queries)
3. Implementare controlli di input condivisioni obbligatorie
4. Utilizzare un Web Application Firewall
5. Catturare e registrare le query SQL generate dalle applicazioni
6. Disattivare le funzioni pericolose e non utilizzate, come l'esecuzione diretta di comandi di sistema

Ringrazio tutto il Team Epicode, ma soprattutto i miei Professori. Mentor nello studio ma anche di vita. Grazie Manuel & Niko