

Progetto S11/L5

Filippo Giorgio Rondò

13 Dicembre 2024

Indice

- [Windows Powershell](#) 1
- [Cattura HTTP e HTTPS](#) 15
- [Esplorare Nmap](#) 21
- [Ringraziamento](#) 26

Windows Powershell

Obiettivi

- Esplorare funzioni cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

Breve accenno teorico

Ping serve per verificare la connettività tra due dispositivi collegati alla medesima rete

Ipconfig dà informazioni sulla configurazione di rete del computer: IP, subnet, i gateway e altro

Dir elenca i contenuti della directory corrente

Cd cambia la directory di lavoro

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> dir

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r---             09/07/2024   16:37             Contacts
d-r---             22/07/2024   12:10             Desktop
d-r---             09/07/2024   18:05             Documents
d-r---             09/07/2024   16:37             Downloads
d-r---             09/07/2024   16:37             Favorites
d-r---             09/07/2024   16:37             Links
d-r---             09/07/2024   16:37             Music
d-r---             09/07/2024   16:40             OneDrive
d-r---             09/07/2024   16:39             Pictures
d-r---             09/07/2024   16:37             Saved Games
d-r---             09/07/2024   16:39             Searches
d-r---             09/07/2024   16:37             Videos
```

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>dir
Il volume nell'unit  C non ha etichetta.
Numero di serie del volume: B068-65A2

Directory di C:\Users\user

13/12/2024  10:16    <DIR>          .
13/12/2024  10:16    <DIR>          ..
09/07/2024  15:37    <DIR>          Contacts
22/07/2024  11:10    <DIR>          Desktop
09/07/2024  17:05    <DIR>          Documents
09/07/2024  15:37    <DIR>          Downloads
09/07/2024  15:37    <DIR>          Favorites
09/07/2024  15:37    <DIR>          Links
09/07/2024  15:37    <DIR>          Music
09/07/2024  15:40    <DIR>          OneDrive
09/07/2024  15:39    <DIR>          Pictures
09/07/2024  15:37    <DIR>          Saved Games
09/07/2024  15:39    <DIR>          Searches
09/07/2024  15:37    <DIR>          Videos
                 File                  byte
              14 Directory  19.627.417.600 byte disponibili
```

Una volta avviati powershell e prompt dei comandi possiamo digitare il comando ‘dir’ e analizzare i loro comportamenti. Come si pu  notare le informazioni fornite sono quasi identiche, ad eccezione del fatto che powershell fornisce in aggiunta indicazioni sugli attributi/modalit 

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ping 192.168.1.102

Esecuzione di Ping 192.168.1.102 con 32 byte di dati:
Risposta da 192.168.1.102: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.102: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.102: byte=32 durata=1ms TTL=128
Risposta da 192.168.1.102: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.1.102:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 1ms, Medio = 0ms
```

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::c594:42e6:2365:b1ae%4
    Indirizzo IPv4. . . . . : 192.168.1.106
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:2087:8022:92cb:a256
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2087:8022:92cb:a256%5
    Gateway predefinito . . . . . : ::
```

```
Windows PowerShell
PS C:\Users\user> ping 192.168.1.102

Esecuzione di Ping 192.168.1.102 con 32 byte di dati:
Risposta da 192.168.1.102: byte=32 durata=6ms TTL=128
Risposta da 192.168.1.102: byte=32 durata=1ms TTL=128
Risposta da 192.168.1.102: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.102: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.1.102:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 6ms, Medio = 1ms
PS C:\Users\user>
```

```
Windows PowerShell
PS C:\Users\user> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::c594:42e6:2365:b1ae%4
    Indirizzo IPv4. . . . . : 192.168.1.106
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

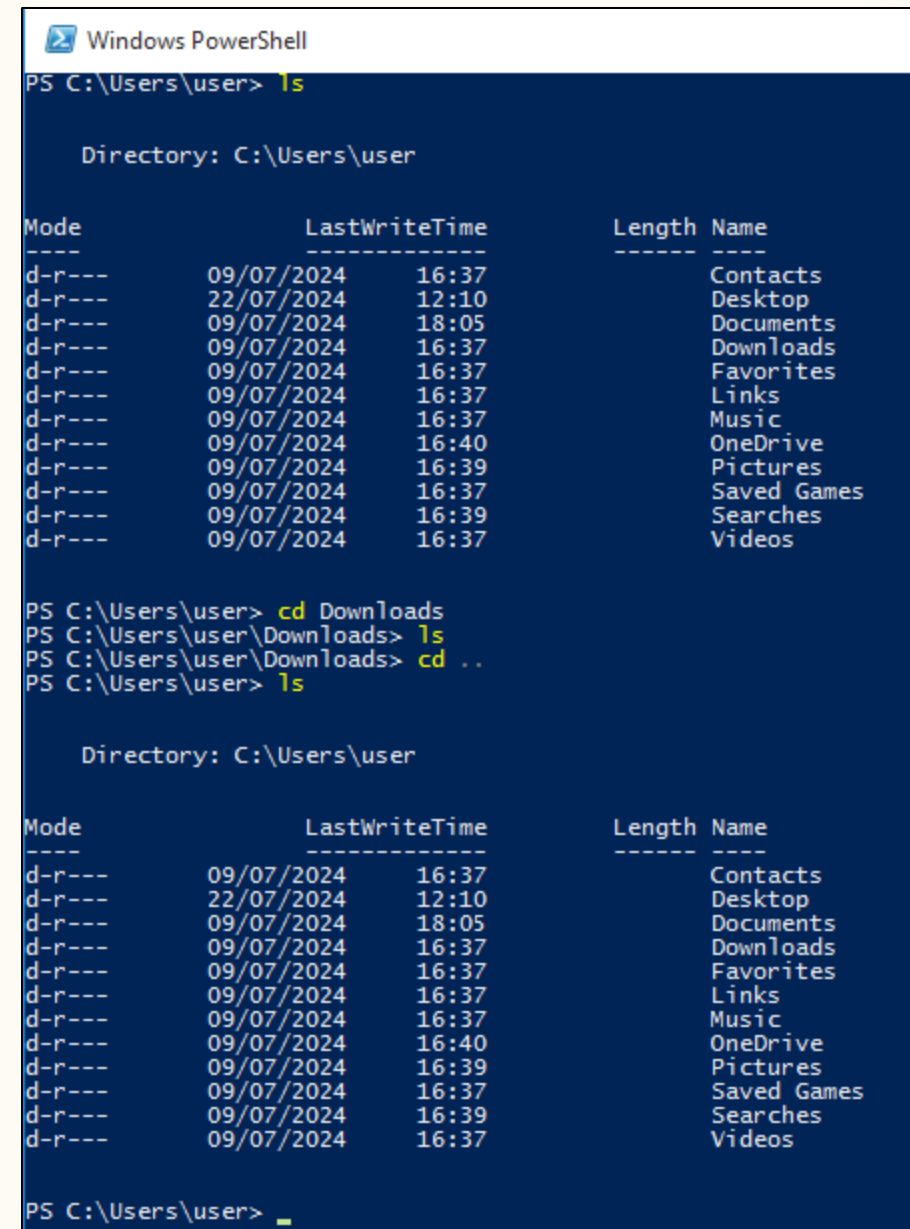
    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:2087:8022:92cb:a256
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2087:8022:92cb:a256%5
    Gateway predefinito . . . . . : ::
PS C:\Users\user>
```

Noteremo che le risposte ottenute sono simili anche utilizzando comandi come **'ping'**, **'ipconfig'** o **'cd'**

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell



```
Windows PowerShell
PS C:\Users\user> ls

Directory: C:\Users\user

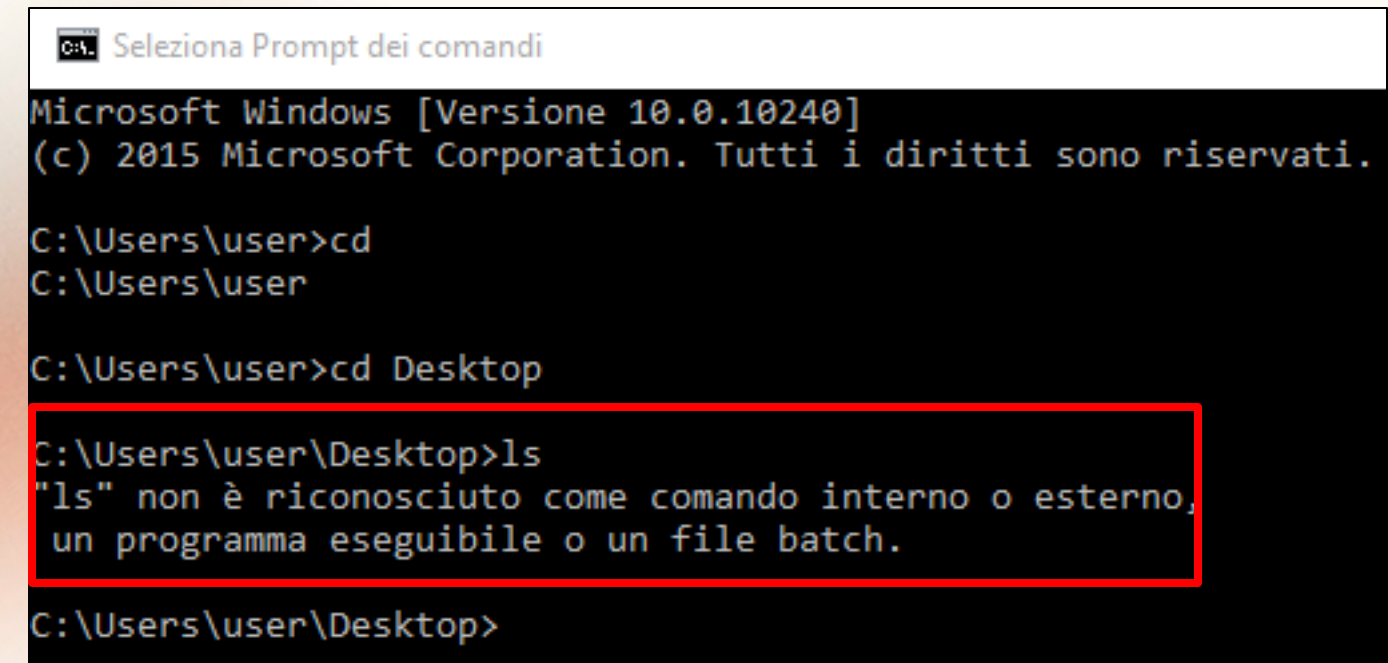
Mode                LastWriteTime         Length Name
----                -
d-r---          09/07/2024   16:37             Contacts
d-r---          22/07/2024   12:10             Desktop
d-r---          09/07/2024   18:05             Documents
d-r---          09/07/2024   16:37             Downloads
d-r---          09/07/2024   16:37             Favorites
d-r---          09/07/2024   16:37             Links
d-r---          09/07/2024   16:37             Music
d-r---          09/07/2024   16:40             OneDrive
d-r---          09/07/2024   16:39             Pictures
d-r---          09/07/2024   16:37             Saved Games
d-r---          09/07/2024   16:39             Searches
d-r---          09/07/2024   16:37             Videos

PS C:\Users\user> cd Downloads
PS C:\Users\user\Downloads> ls
PS C:\Users\user\Downloads> cd ..
PS C:\Users\user> ls

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r---          09/07/2024   16:37             Contacts
d-r---          22/07/2024   12:10             Desktop
d-r---          09/07/2024   18:05             Documents
d-r---          09/07/2024   16:37             Downloads
d-r---          09/07/2024   16:37             Favorites
d-r---          09/07/2024   16:37             Links
d-r---          09/07/2024   16:37             Music
d-r---          09/07/2024   16:40             OneDrive
d-r---          09/07/2024   16:39             Pictures
d-r---          09/07/2024   16:37             Saved Games
d-r---          09/07/2024   16:37             Searches
d-r---          09/07/2024   16:39             Videos

PS C:\Users\user>
```



```
Seleziona Prompt dei comandi

Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>cd
C:\Users\user

C:\Users\user>cd Desktop

C:\Users\user\Desktop>ls
"ls" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.

C:\Users\user\Desktop>
```

Un confronto interessante è che il prompt dei comandi non riconosce il comando **'ls'**. Ossia il comando che mostra file e cartelle presenti nella directory corrente

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

Breve accenno teorico

Un **cmdlet** è un comando speciale usato in **PowerShell**. Cmdlet sono simili ai comandi eseguiti nel **Prompt dei comandi (CMD)**, ma sono molto più potenti e flessibili. Ogni cmdlet è progettato per svolgere un compito specifico e restituisce **oggetti**, non solo testo, che possono essere manipolati ulteriormente.

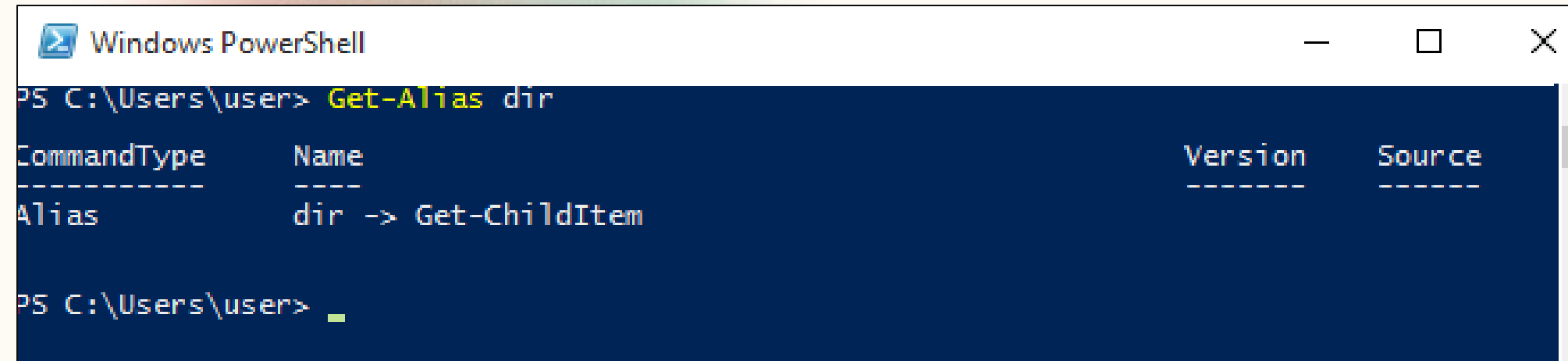
Alias è un nome abbreviato che può essere utilizzato al posto di un cmdlet o di un comando. In altre parole, un alias è un **nickname** per un comando più lungo. L'uso degli alias rende più facile e veloce l'esecuzione di comandi, soprattutto se si usano spesso.

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

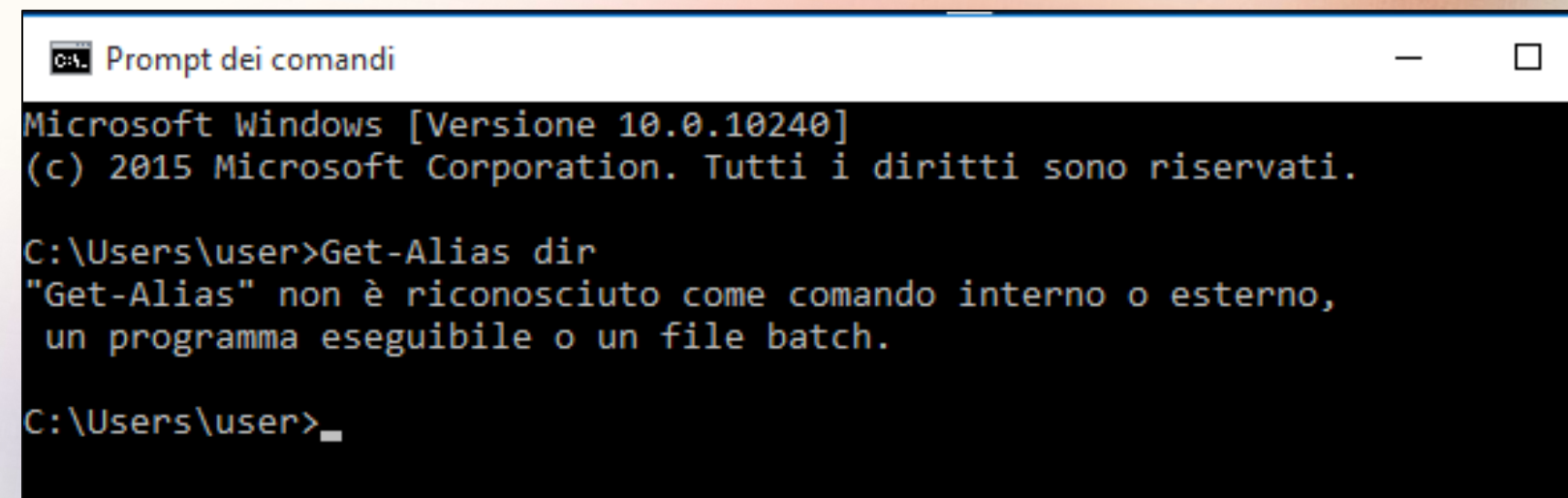
Il comando '**Get-Alias**', in powershell, restituisce l'alias di un determinato comando, in questo caso del comando '**dir**'. Infatti 'dir' non fa altro che emulare il comando '**Get-ChildItem**'. In sintesi, il comando dir sostituisce il comando Get-ChildItem



```
Windows PowerShell
PS C:\Users\user> Get-Alias dir

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

PS C:\Users\user> _
```



```
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>Get-Alias dir
"Get-Alias" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.

C:\Users\user> _
```

Notiamo anche come il Prompt dei Comandi non supporta il cmdlet, infatti, come si nota dalla foto, non viene riconosciuto come comando

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

Breve accenno teorico

Netstat, l'abbreviazione di network statistics, è un comando di rete che fornisce informazioni di dettaglio sulle connessioni di rete attive, sulle porte in ascolto, i router e le interfacce di rete. In powershell può essere dunque utilizzato come comando per diagnosticare le connessioni di rete del proprio computer, anche quelle di dominio

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

```
Windows PowerShell
PS C:\Users\user> netstat -h

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

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [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.
-n Visualizza indirizzi e numeri di porta in forma numerica.
-o Visualizza l'ID del processo proprietario associato a ogni
  connessione.
-p proto Visualizza le connessioni relative al protocollo specificato
  da "proto", che può essere TCP, UDP, TCPv6 o UDPv6.
  Se utilizzato insieme all'opzione -s per le statistiche per
  protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP,
  TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e le porte
  TCP non di ascolto associate. Le porte non di ascolto associate
  possono essere associate o meno a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione
  predefinita, vengono visualizzate le statistiche per IP,
  IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare
  un sottoinsieme dei valori predefiniti, è possibile
  utilizzare l'opzione -p.
-t Visualizza lo stato di offload della connessione corrente.
-x Visualizza le connessioni, i listener e gli endpoint
  condivisi.
-y Visualizza il modello di connessione TCP per tutte le
  connessioni. Non può essere utilizzata in combinazione con le
```

Il comando ‘**netstat -h**’ mostra una guida con le opzioni e i parametri disponibili da poter utilizzare con netstat, offrendo anche una breve spiegazione del parametro

Il comando ‘**netstat -r**’ permette di visualizzare la propria tabella di routing.

```
Windows PowerShell
PS C:\Users\user> netstat -r

=====
Elenco interfacce
4...08 00 27 07 bd 0f .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
6...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
5...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask      Gateway    Interfaccia Metrica
-----
0.0.0.0             0.0.0.0    192.168.1.1 192.168.1.106 10
127.0.0.0           255.0.0.0    On-link     127.0.0.1     306
127.0.0.1           255.255.255.255 On-link     127.0.0.1     306
127.255.255.255     255.255.255.255 On-link     127.0.0.1     306
192.168.1.0         255.255.255.0 On-link     192.168.1.106 266
192.168.1.106       255.255.255.255 On-link     192.168.1.106 266
192.168.1.255       255.255.255.255 On-link     192.168.1.106 266
224.0.0.0           240.0.0.0    On-link     127.0.0.1     306
224.0.0.0           240.0.0.0    On-link     192.168.1.106 266
255.255.255.255     255.255.255.255 On-link     127.0.0.1     306
255.255.255.255     255.255.255.255 On-link     192.168.1.106 266
=====

Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione Gateway
-----
5 306 ::/0 On-link
1 306 ::1/128 On-link
5 306 2001::/32 On-link
5 306 2001:0:2851:782c:2087:8022:92cb:a256/128 On-link
4 266 fe80::/64 On-link
5 306 fe80::/64 On-link
5 306 fe80::2087:8022:92cb:a256/128 On-link
4 266 fe80::c594:42e6:2365:b1ae/128 On-link
1 306 ff00::/8 On-link
4 266 ff00::/8 On-link
5 306 ff00::/8 On-link
=====

Route permanenti:
Nessuna
PS C:\Users\user>
```

Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

```
Windows PowerShell
PS C:\Users\user> netstat -abno
Per eseguire l'operazione richiesta è necessaria l'esecuzione con privilegi elevati.
PS C:\Users\user>
```

Il comando **'netstat -abno'**:

- a serve a visualizzare le connessioni sui protocolli TCP attivi
- b serve ad elencare i processi
- n mostra gli indizzi ip e le porte, evita dal risoluzione del DNS
- o aggiunge il PID ossia il valore numerico di un determinato processo

```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
PS C:\Windows\system32> netstat -abno

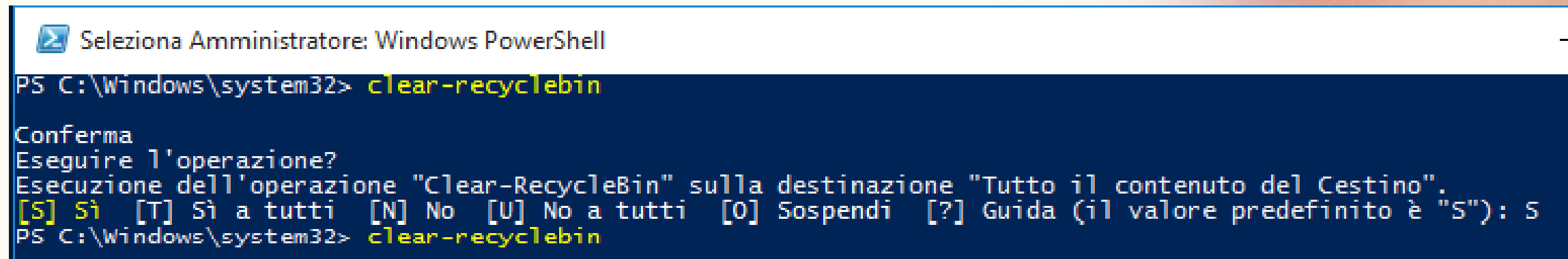
Connessioni attive

Proto Indirizzo locale      Indirizzo esterno  Stato  PID
-----
TCP    0.0.0.0:7                0.0.0.0:0          LISTENING 2064
[tcpvcs.exe]
TCP    0.0.0.0:9                0.0.0.0:0          LISTENING 2064
[tcpvcs.exe]
TCP    0.0.0.0:13               0.0.0.0:0          LISTENING 2064
[tcpvcs.exe]
TCP    0.0.0.0:17               0.0.0.0:0          LISTENING 2064
[tcpvcs.exe]
TCP    0.0.0.0:19               0.0.0.0:0          LISTENING 2064
[tcpvcs.exe]
TCP    0.0.0.0:80               0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:135              0.0.0.0:0          LISTENING 760
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:1801             0.0.0.0:0          LISTENING 1480
[mqsvc.exe]
TCP    0.0.0.0:2103             0.0.0.0:0          LISTENING 1480
[mqsvc.exe]
TCP    0.0.0.0:2105             0.0.0.0:0          LISTENING 1480
[mqsvc.exe]
TCP    0.0.0.0:2107             0.0.0.0:0          LISTENING 1480
[mqsvc.exe]
TCP    0.0.0.0:2869             0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:3389             0.0.0.0:0          LISTENING 920
TermService
[svchost.exe]
TCP    0.0.0.0:5357             0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5432             0.0.0.0:0          LISTENING 2724
[postgres.exe]
TCP    0.0.0.0:8009             0.0.0.0:0          LISTENING 2288
[tomcat7.exe]
TCP    0.0.0.0:8080             0.0.0.0:0          LISTENING 2288
[tomcat7.exe]
TCP    0.0.0.0:8443             0.0.0.0:0          LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49408            0.0.0.0:0          LISTENING 472
Impossibile ottenere informazioni sulla proprietà
```


Windows Powershell

Obiettivi

- Esplorare alcune funzioni di cmd e di powershell.
- Esplorare cmdlet.
- Esplorare netstat.
- Svuotare il cestito da powershell

A screenshot of a Windows PowerShell console window titled "Seleziona Amministratore: Windows PowerShell". The prompt is "PS C:\Windows\system32> clear-recyclebin". Below the command, a confirmation dialog is displayed: "Conferma", "Eseguire l'operazione?", "Esecuzione dell'operazione 'Clear-RecycleBin' sulla destinazione 'Tutto il contenuto del Cestino'." followed by options "[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è 'S'):". The user has entered 'S', and the prompt returns to "PS C:\Windows\system32> clear-recyclebin".

```
Seleziona Amministratore: Windows PowerShell
PS C:\Windows\system32> clear-recyclebin
Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S
PS C:\Windows\system32> clear-recyclebin
```

Grazie a powershell, è possibile eseguire comandi per gestire una vasta rete. Può risultare molto più rapido poiché si evitano tutti gli interventi di interfaccia grafica. Un comando molto utile è '**clear-recyclebin**'. Questo è in grado di eliminare definitivamente tutti gli elementi presenti nel cestino

Windows Powershell

Scenario pratico

Immaginiamo di voler analizzare l'integrità dei nostri processi attivi, ad esempio su Tomcat7.exe che ha stabilito diverse connessioni su porte diverse

Step 1: utilizzo del comando **netstat -abno** per vedere i processi attivi su TCP

TCP	127.0.0.1:8005	0.0.0.0:0	LISTENING	2288
[tomcat7.exe]				
TCP	127.0.0.1:49415	127.0.0.1:49416	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49416	127.0.0.1:49415	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49417	127.0.0.1:49418	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49418	127.0.0.1:49417	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49419	127.0.0.1:49420	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49420	127.0.0.1:49419	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49421	127.0.0.1:49422	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49422	127.0.0.1:49421	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49423	127.0.0.1:49424	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49424	127.0.0.1:49423	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49425	127.0.0.1:49426	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49426	127.0.0.1:49425	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49427	127.0.0.1:49428	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49428	127.0.0.1:49427	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49429	127.0.0.1:49430	ESTABLISHED	2288
[tomcat7.exe]				
TCP	127.0.0.1:49430	127.0.0.1:49429	ESTABLISHED	2288

Step 2: Utilizzare il PID ottenuto e cercarlo nel task manager. Da qui possiamo notare le risorse di sistema utilizzate: non anomale

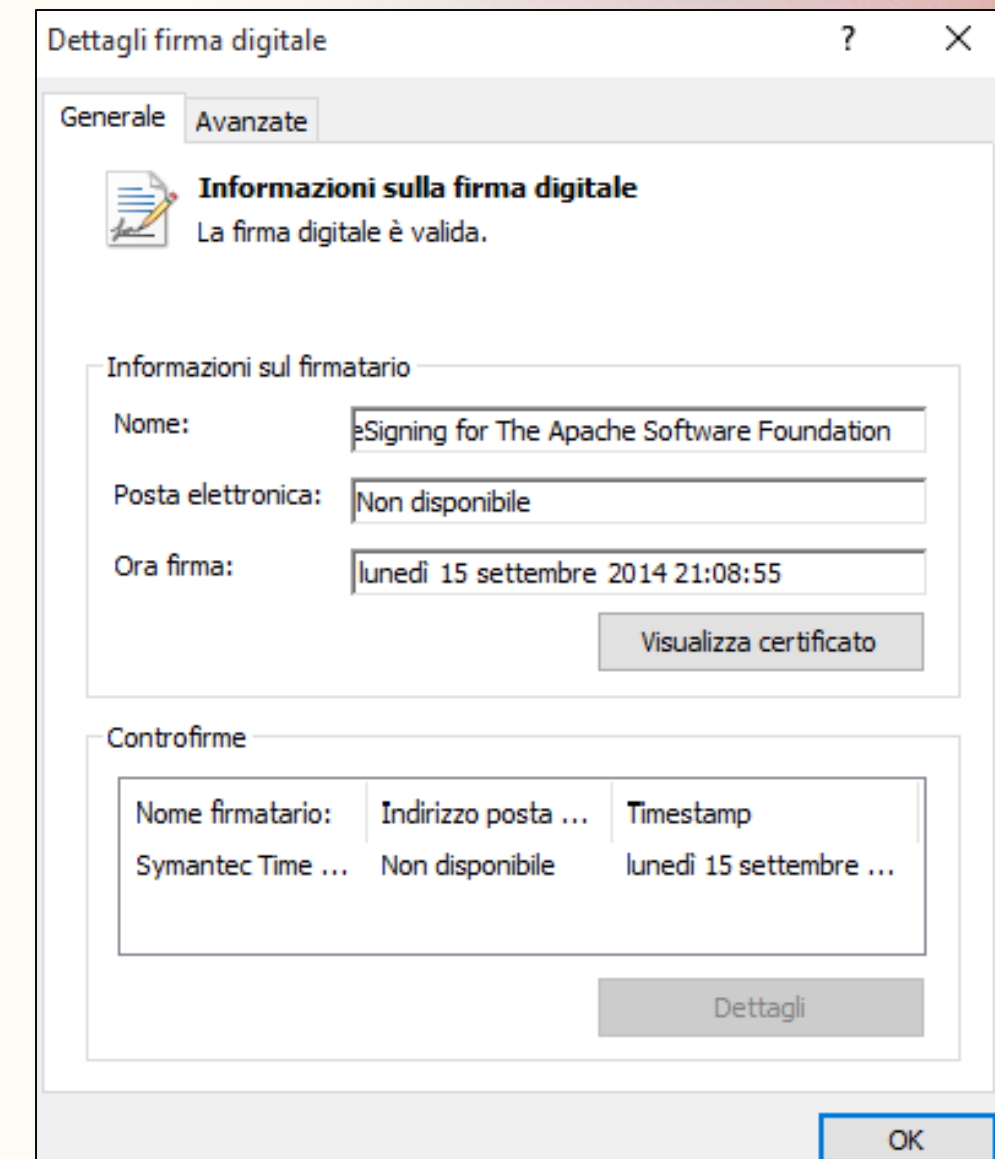
Processi	Prestazioni	Cronologia applicazioni	Avvio	Utenti	Dettagli	Servizi
Nome	Stato	PID	2% CPU	41% Memoria	0% Disco	0% Rete
> Host servizio: Servizio helper ho...		1940	0%	0,8 MB	0 MB/s	0 Mbps
> utcsvc		1948	0%	2,6 MB	0 MB/s	0 Mbps
> Host servizio: servizio di rete (co...		1964	0%	0,4 MB	0 MB/s	0 Mbps
> ipripsvc		2032	0%	0,3 MB	0 MB/s	0 Mbps
> TCP/IP Services Application		2064	0%	0,3 MB	0 MB/s	0 Mbps
> Servizio SNMP		2072	0%	0,7 MB	0 MB/s	0 Mbps
> appmodel (2)		2200	0%	2,5 MB	0 MB/s	0 Mbps
Runtime Broker		2248	0%	4,7 MB	0 MB/s	0 Mbps
Host servizio: Internet Informati...		2268	0%	0,8 MB	0 MB/s	0 Mbps
Servizio Attivazione processo ...						
Servizio Pubblicazione sul Web						
Commons Daemon Service Run...		2288	0%	62,4 MB	0 MB/s	0 Mbps
Apache Tomcat 7.0 Tomcat7						
Console Window Host		2424	0%	0,1 MB	0 MB/s	0 Mbps
PostgreSQL Server		2724	0%	0,9 MB	0 MB/s	0 Mbps
Host servizio: gruppo servizi Uni...		2744	0%	1,0 MB	0 MB/s	0 Mbps
Console Window Host		2788	0%	0,3 MB	0 MB/s	0 Mbps
PostgreSQL Server		2956	0%	0,1 MB	0 MB/s	0 Mbps
PostgreSQL Server		3188	0%	0,2 MB	0 MB/s	0 Mbps

Windows Powershell

Scenario pratico

Immaginiamo di voler analizzare l'integrità dei nostri processi attivi, ad esempio su Tomcat7.exe che ha stabilito diverse connessioni su porte diverse

Step 3: analizzare il processo.
Dalle proprietà e i dettagli forniti ricaviamo che Tomcat7.exe è un demone ossia un processo attivo in background. Per quanto riguarda la firma digitale, è originale e non ha subito mai modifiche. Anche importante è il percorso file, in questo caso non risulta anomalo



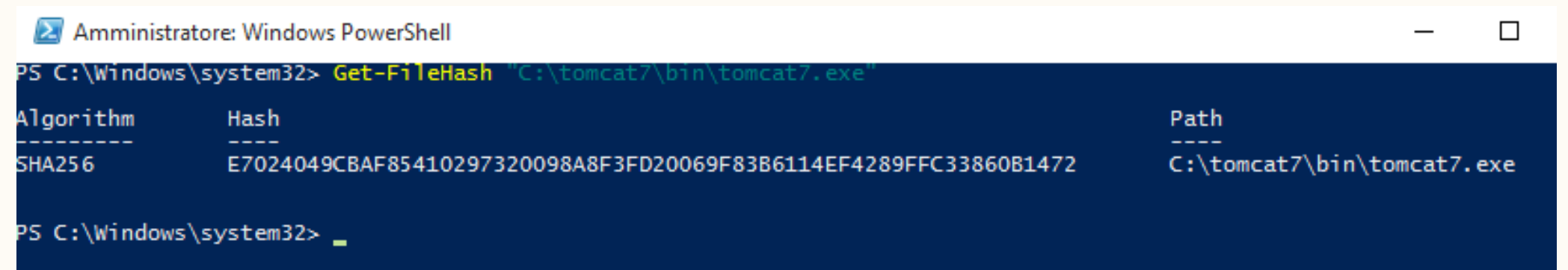
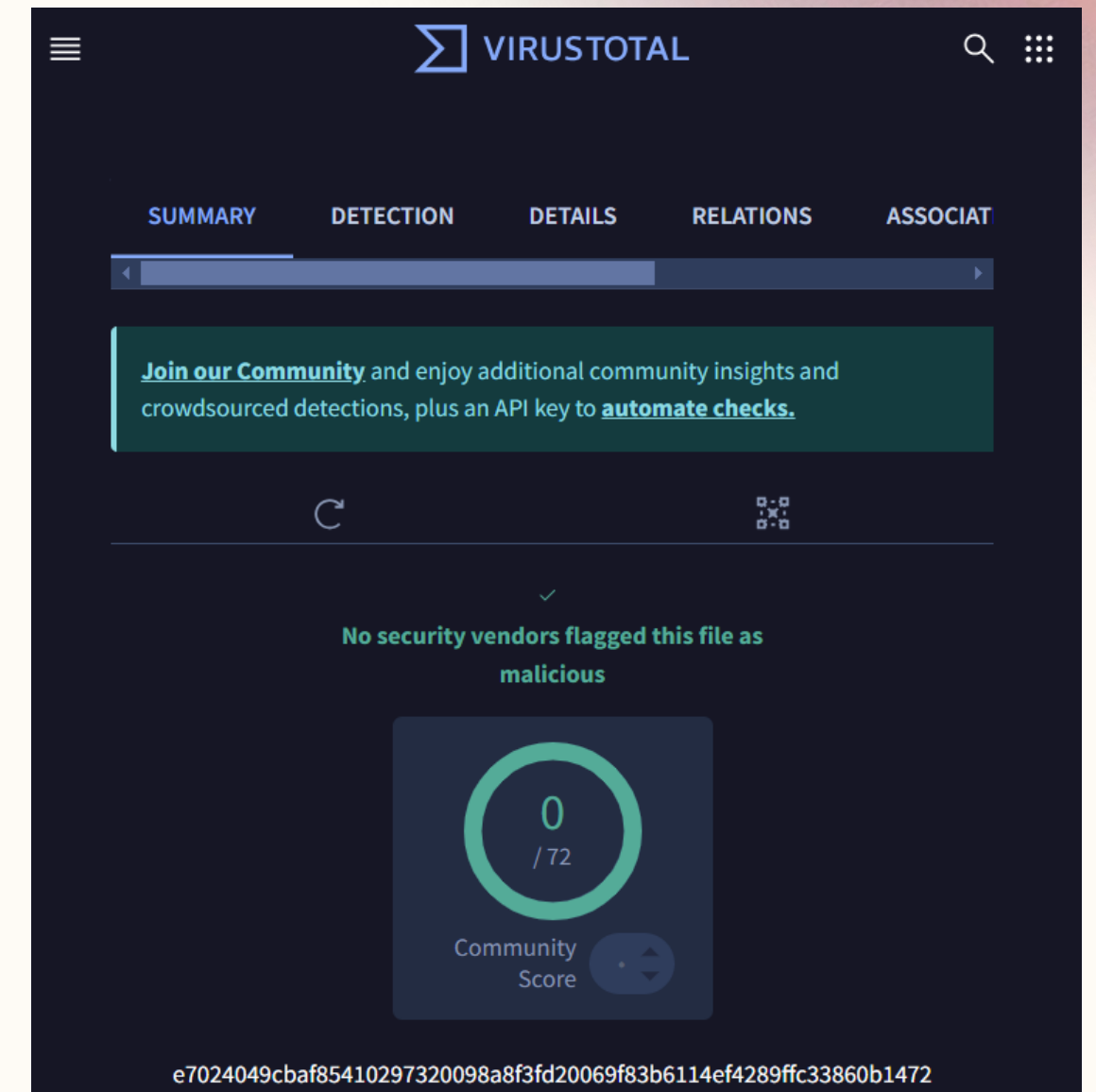
 tomcat7.exe	2288	In esecuzione	SYSTEM	00	8.560 K	Commons Daemon Service Runner
---	------	---------------	--------	----	---------	-------------------------------

Windows Powershell

Scenario pratico

Immaginiamo di voler analizzare l'integrità dei nostri processi attivi, ad esempio su Tomcat7.exe che ha stabilito diverse connessioni su porte diverse

Step 4: ricavare l'hash del processo e verificarlo online.
Grazie al comando '**Get-FileHash**' seguito dal Path del file



Cattura HTTP e HTTPS –wireshark

Obiettivi

- Catturare e analizzare il traffico HTTP
- Catturare e analizzare il traffico HTTPS

Cattura HTTP e HTTPS

Obiettivi

- Catturare e analizzare il traffico HTTP
- Catturare e analizzare il traffico HTTPS

REQUISITI

VM: cyberops workspace

Impostazioni di rete: Scheda con bridge e connessione ad internet

CREDENZIALI UTENTE

Username: analyst

Password: cyberops

Step 1: Avviare il prompt dei comandi, verificare l'indirizzo ip ed eseguire il comando `'sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap'`

```
[analyst@sec0ps ~]$ 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 08:00:27:69:ff:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.108/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 85913sec preferred_lft 85913sec
    inet6 fe80::a00:27ff:fe69:ff67/64 scope link
        valid_lft forever preferred_lft forever
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Il comando avvierà tcpdump e registrerà il traffico di rete sull'interfaccia enp0s3.

-i specifica l'interfaccia

-s specifica la dimensione della cattura

-w permette di salvare il file come formato pcap con il nome specificato

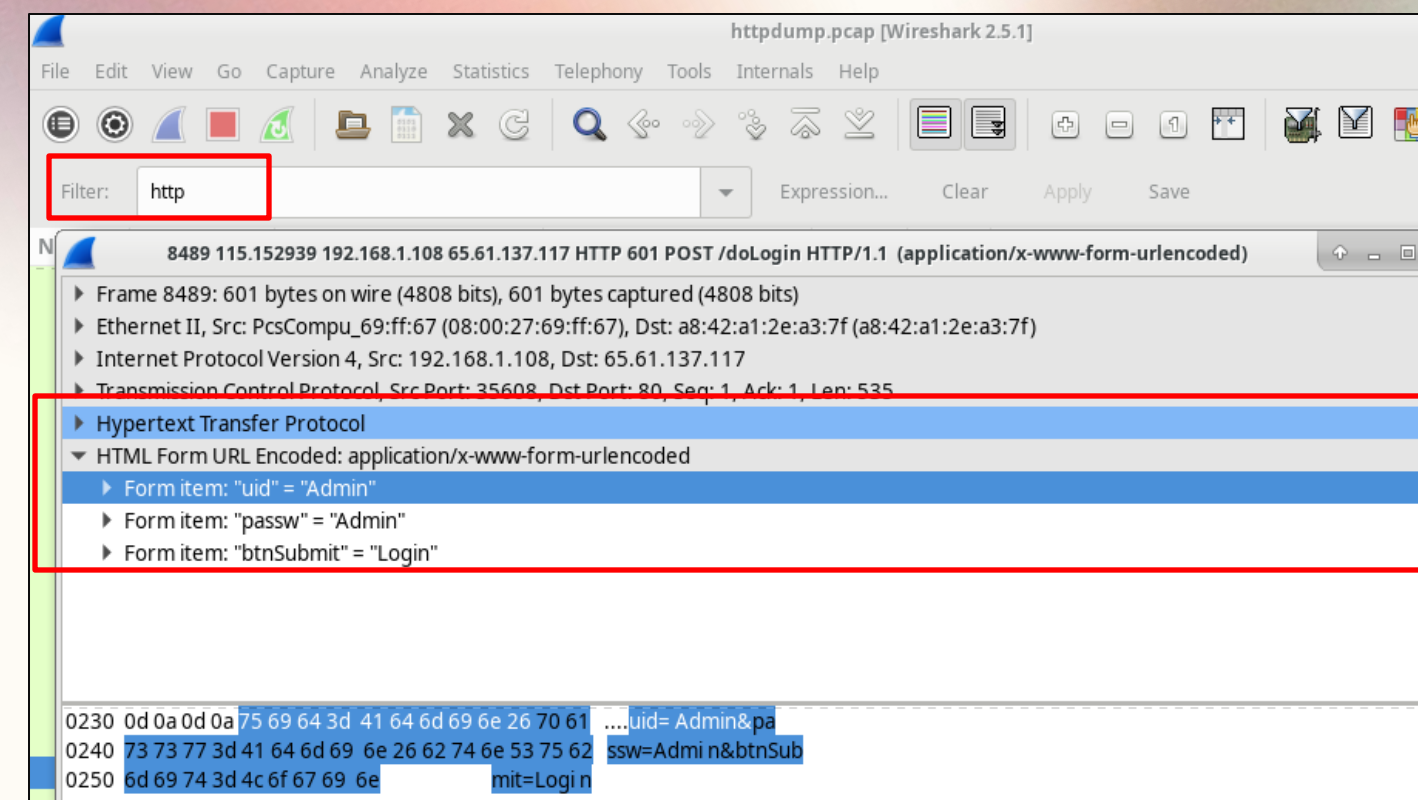
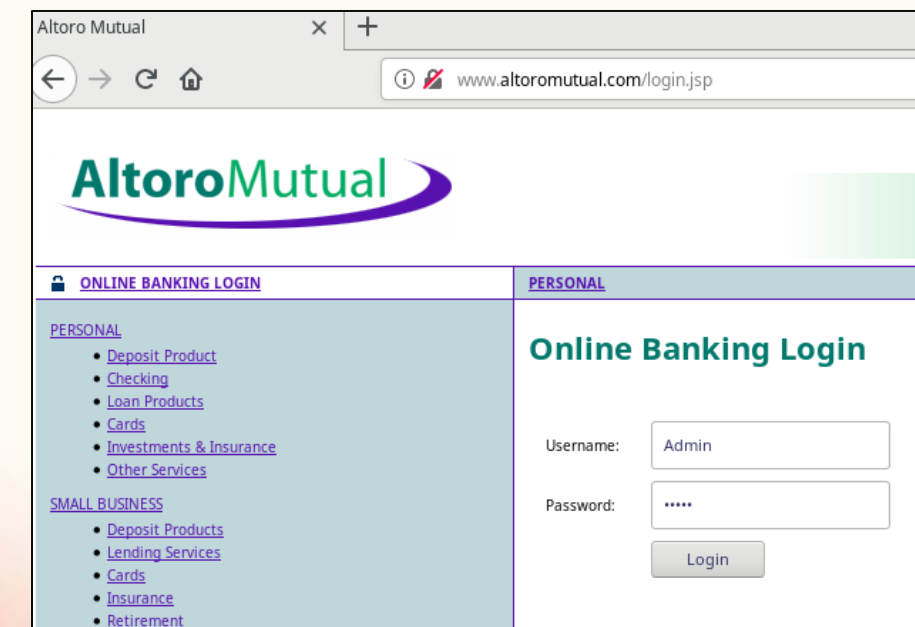
Cattura HTTP e HTTPS

Obiettivi

- Catturare e analizzare il traffico HTTP
- Catturare e analizzare il traffico HTTPS

Step 2: Visitare un sito web non protetto da crittografia e registrarsi nel login, inserendo 'Admin' nei campi username e password. Una volta che uscirà il popup potremo chiudere la pagina web e arrestare il comando avviato in precedenza con Ctrl + C

Step 2: Aprire con Wireshark la cattura salvata nei file e filtrare solo catture HTTP. In particolare noteremo una richiesta POST, ossia quella dove abbiamo inserito le credenziali. Indagando nell'HTML Form URL possiamo vedere in chiaro le credenziali che abbiamo inserito

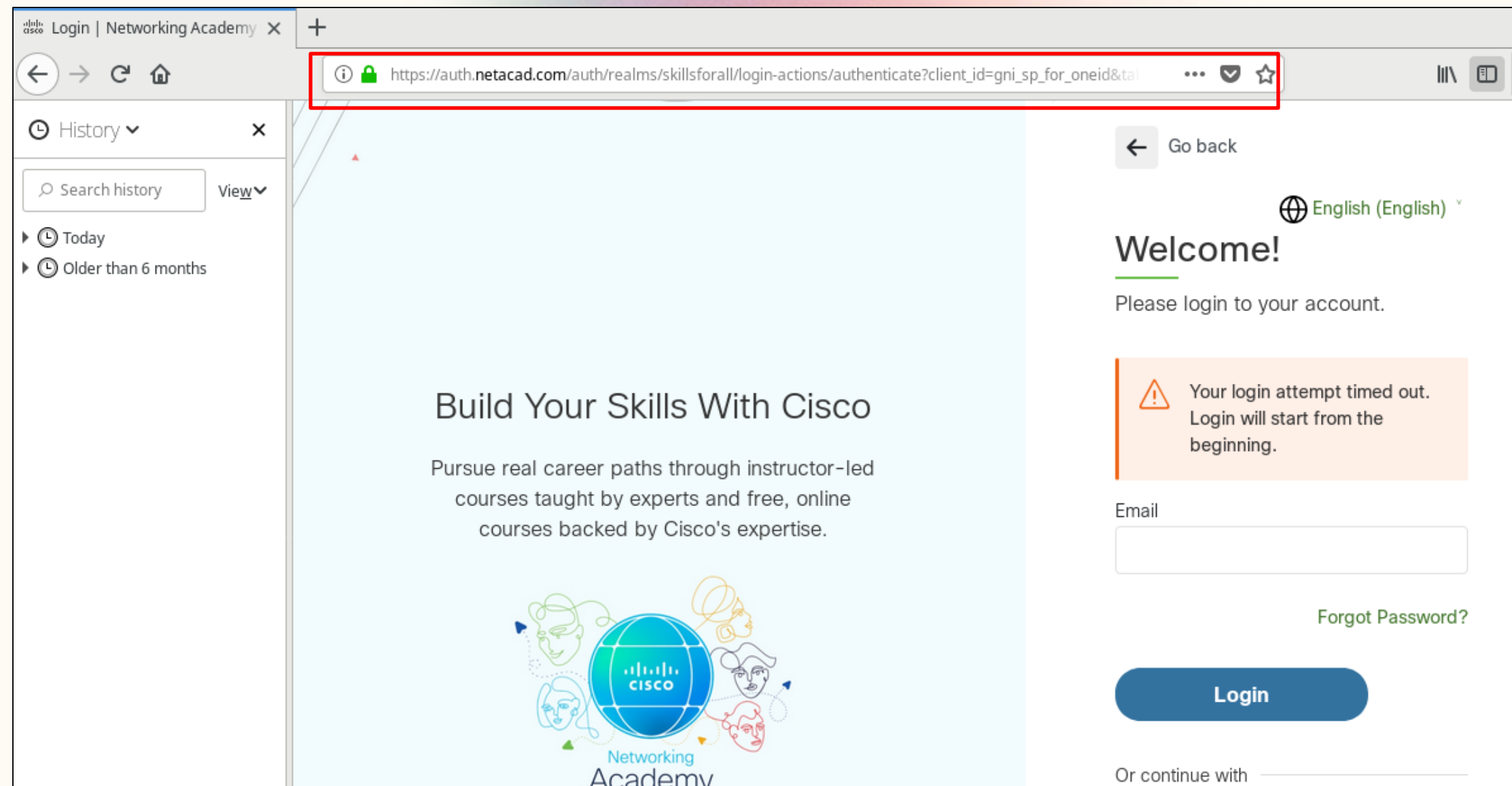


Cattura HTTP e HTTPS

Obiettivi

- Catturare e analizzare il traffico HTTP
- Catturare e analizzare il traffico HTTPS

Per quanto riguarda la cattura HTTPS il processo è identico: avviare tcpdump (modificando il nome di salvataggio del file) e registrarsi al sito. La differenza è che la registrazione verrà effettuata in un sito protetto da crittografia. Oltre al fatto che utilizza il protocollo HTTPS è facilmente riconoscibile dal lucchetto verde vicino l'URL; quello non protetto aveva un lucchetto sbarrato in rosso



Cattura HTTP e HTTPS

Obiettivi

- Catturare e analizzare il traffico HTTP
- Catturare e analizzare il traffico HTTPS

Questa volta, una volta aperta la cattura, filtrare il traffico sulla porta 443 e selezionare il frame che riguarda Application Data. Nella sezione Secure Sockets Layer noteremo una voce 'Encrypted Application Data' che non è altro che la sezione di credenziali fornite ma cifrate

Filter: tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
54	7.648337	192.168.1.108	35.190.72.216	TCP	74	40296 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2
55	7.649061	192.168.1.108	34.120.237.76	TLSv1.2	243	Application Data
56	7.649230	192.168.1.108	34.120.237.76	TLSv1.2	374	Application Data

▶ Frame 55: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)

▶ Ethernet II, Src: PcsCompu_69:ff:67 (08:00:27:69:ff:67), Dst: a8:42:a1:2e:a3:7f (a8:42:a1:2e:a3:7f)

▶ Internet Protocol Version 4, Src: 192.168.1.108, Dst: 34.120.237.76

▶ Transmission Control Protocol, Src Port: 55620, Dst Port: 443, Seq: 569, Ack: 157, Len: 177

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: http2

Content Type: Application Data (23)

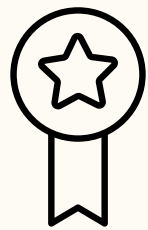
Version: TLS 1.2 (0x0303)

Length: 172

Encrypted Application Data: 000000000000000013b0737bdcda9e8295aaa2f9113c823a5...

Evitare furto di credenziali

[Torna all'indice](#)



HTTPS > HTTP

Grazie a questo protocollo i nostri dati sono al sicuro da attacchi come il MITM



Sito sicuro

Prima di inserire le credenziali verificare l'attendibilità e la sicurezza del sito



Credenziali diverse

Utilizzare account diversi per la registrazione ai siti e modificare la password con frequenza

Esplorare Nmap

Obiettivi

- Capire come utilizzare nmap e fare scansioni semplici

Esplorare Nmap

Obiettivi

- Capire come utilizzare nmap e fare scansioni semplici

RISORSE RICHIESTE

MV: Cyberops Workspace

Configurazione di rete: scheda con bridge e connessione ad internet

Accenno teorico

Un attaccante prima di mettersi in gioco ha bisogno di conoscere la topologia della rete e avere più informazioni sui servizi e le versioni, sui sistemi operativi e sulle porte. Questa, anche definita come fase di enumerazione, prevede l'utilizzo di tool come nmap. Inoltre, questo tool non effettua solo scansioni ma è dotato anche di alcuni script (**nmap --script-**) per testare le vulnerabilità anche se il suo utilizzo principale è la scansione.

Esplorare Nmap

Obiettivi

- Capire come utilizzare nmap e fare scansioni semplici

Il comando **man** [programma | *utilità* | *funzione*] visualizza le pagine di manuale associate agli argomenti. Le pagine di manuale sono i manuali di riferimento presenti sui sistemi operativi Unix e Linux. Eseguendo **man nmap** è possibile visionare il manuale. Se necessario si possono ricercare parole specifiche all'interno di esso utilizzando **'/paroladacercare'** o il **'?'** se si tratta di frasi. Il manuale propone anche un esempio di comando, il più classico

```
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: 1186-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
```

Il comando `'nmap -A -T4 scanme.nmap.org'` effettua una scansione aggressiva e invasiva, restituendo il sistema operativo, servizi, versioni, delle porte e avvia alcuni script. Queste informazioni sono date dal parametro `-a`. Invece il parametro `-T4` indica la velocità con cui deve essere effettuata la scansione. Considerando che questo parametro va da 0 a 5, `-T4` sarà relativamente veloce, diminuendo il tempo a discapito della precisione

Esplorare Nmap

Obiettivi

- Capire come utilizzare nmap e fare scansioni semplici

E' possibile effettuare una scansione sul dispositivo in uso tramite il comando **nmap -A -T4 localhost (oppure ip corrente)**

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 11:23 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00082s 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 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.16 seconds
[analyst@secOps ~]$
```

In breve, da questa scansione si ottengono le porte aperte ftp ed ssh con le corrispettive versioni. Inoltre vi sono informazioni aggiuntive, ad esempio la registrazione come anonimo al protocollo ftp e le ssh-hostkey.

Esplorare Nmap

Obiettivi

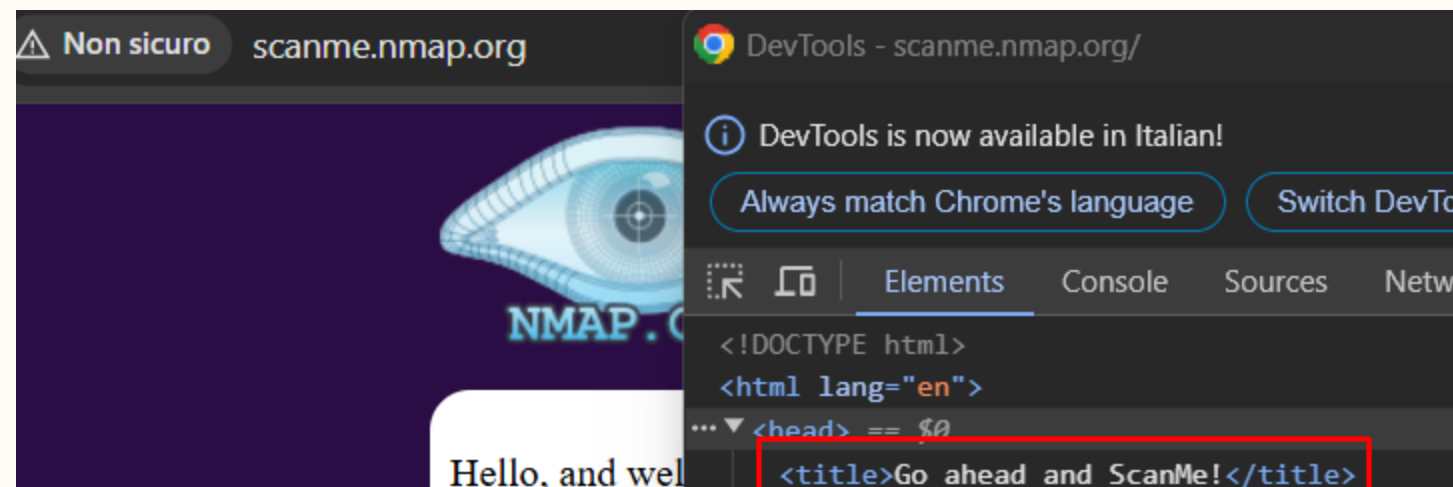
- Capire come utilizzare nmap e fare scansioni semplici

Nmap -A -T4 <indirizzo del server>

```
[analyst@sec0ps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-13 11:30 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s 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 33.77 seconds
[analyst@sec0ps ~]$
```

Da questo scan si ottengono informazioni sui servizi, porte e informazioni consuete e in aggiunta informazioni che si trovano negli header e il titolo della pagina



Grazie dell'attenzione

Filippo Giorgio Rondò

13 Dicembre 2024