Cyber Security & Ethical Hacking Progetto

Esercizio 1 ↵ Usare Windows PowerShell

Obiettivi

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- *Parte 1 ↵ Accedere alla console PowerShell.*
- *Parte 2 ↵ Esplorare i comandi del Prompt dei Comandi e di PowerShell.*
- *Parte 3 ↵ Esplorare i cmdlet.*
- *Parte 4 ↵ Esplorare il comando netstat usando PowerShell.*
- *Parte 5 ↵ Svuotare il cestino usando PowerShell.*

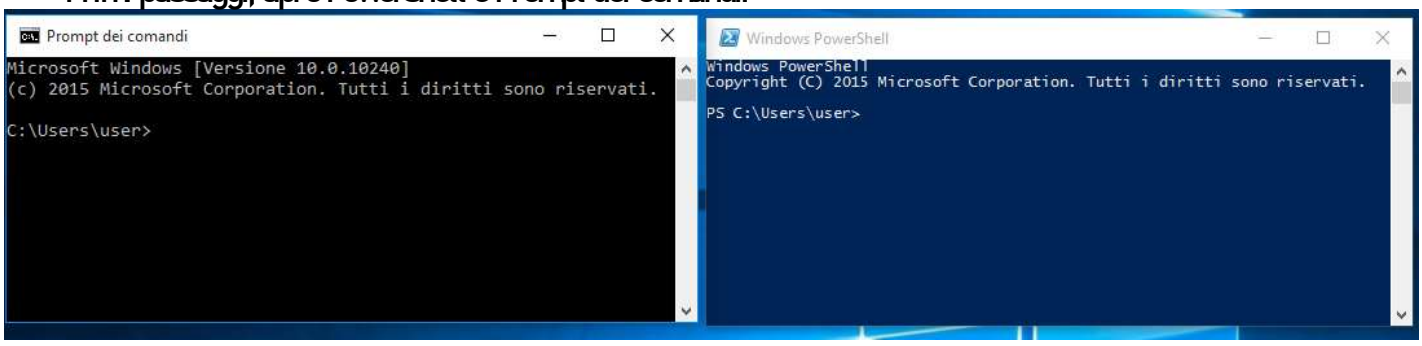
Contesto / Scenario

PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo laboratorio, userai la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell ha anche funzioni che possono creare script per automatizzare compiti e lavorare insieme al Sistema Operativo Windows.

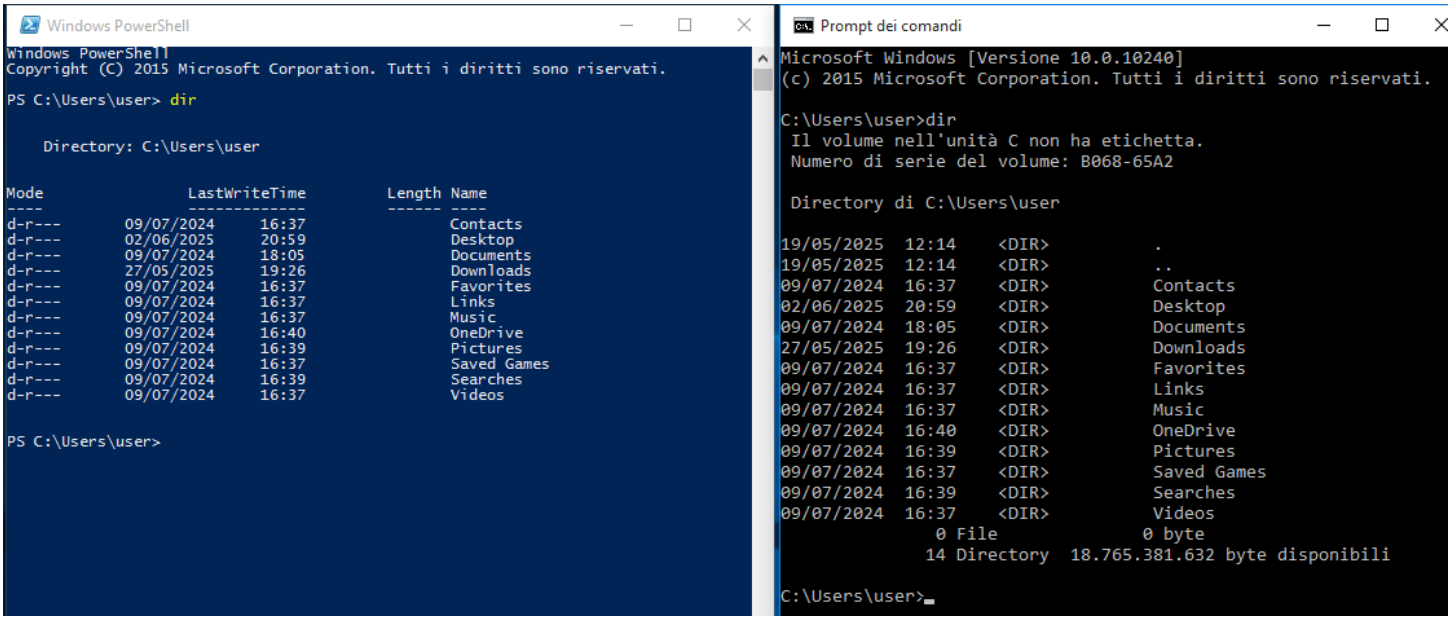
Risorse Richieste

- *1 PC Windows con PowerShell installato e accesso a internet*

Primi passaggi, apro Powershell e Prompt dei comandi.



Inserisco dir a entrambe le finestre.



QUALI SONO GLI OUTPUT DEL COMANDO DIR?

L'output del comando dir, sia in PowerShell che nel Prompt dei comandi, mi mostra un elenco dei file e directory presenti nella directory corrente. Ci sono informazioni come nome del file e directory, la data e l'ora dell'ultima modifica e la dimensione del file. In realta la differenza è minima con piccole differenze nel formato di visualizzazione tra PowerShell e il Prompt dei comandi, ma le informazioni sono le stesse.

Ho usato altri comandi, nel prompt, come c.. ipconfig e ping (in questo caso ho pingato 8.8.8.8)

```
C:\Users>ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione: homenet.telecomitalia.it
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::3125:a4a1:415d:a0f8%8
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.21
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.1.1

Scheda Tunnel isatap.homenet.telecomitalia.it:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: homenet.telecomitalia.it

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 . . . . . . . . . . . . . . . . . . . . : 2001:0:2851:782c:1422:3084:a8fe:2dab
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::1422:3084:a8fe:2dab%10
   Gateway predefinito . . . . . . . . . : ::
```

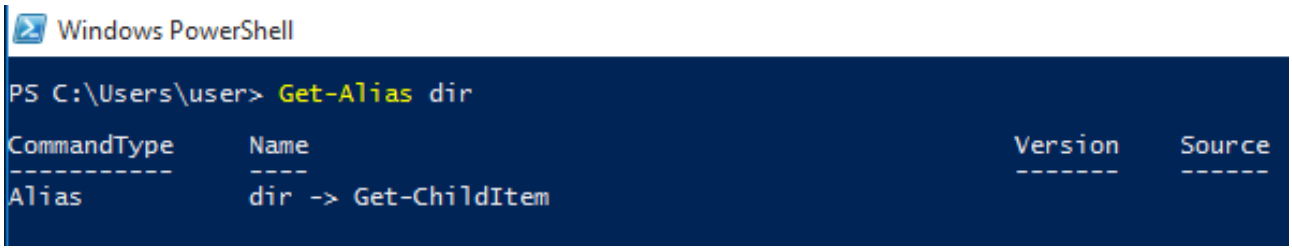
```
C:\Users\user>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=29ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=41ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=35ms TTL=114
Risposta da 8.8.8.8: byte=32 durata=28ms TTL=114

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 28ms, Massimo =  41ms, Medio =  33ms
```

```
C:\Users\user>cd ..

C:\Users>ipconfig
```

QUALI SONO I RISULTATI?

Con il ping 8.8.8.8, stavo controllando se la mia macchina riusciva a comunicare con un server di Google. Da qui mi mostra che ho ricevuto quattro risposte dal server. Significa che la mia connessione a internet funziona bene e sono riuscito a raggiungere il server di Google.
Ho digitato cd .. , mostra la mia posizione è cambiata. Prima ero in C:\Users\user e adesso C:\Users.
Infine ho eseguito con ipconfig, ho chiesto al mio computer di mostrarmi tutte le informazioni sulla sua configurazione di rete, vedendo i dettagli sulla mia connessione di rete, mostrandomi il mio indirizzo IP e l'indirizzo del mio router, il suffisso DNS specifico per connessione.

Vado su powershell e eseguo il comando Get-Alias dir

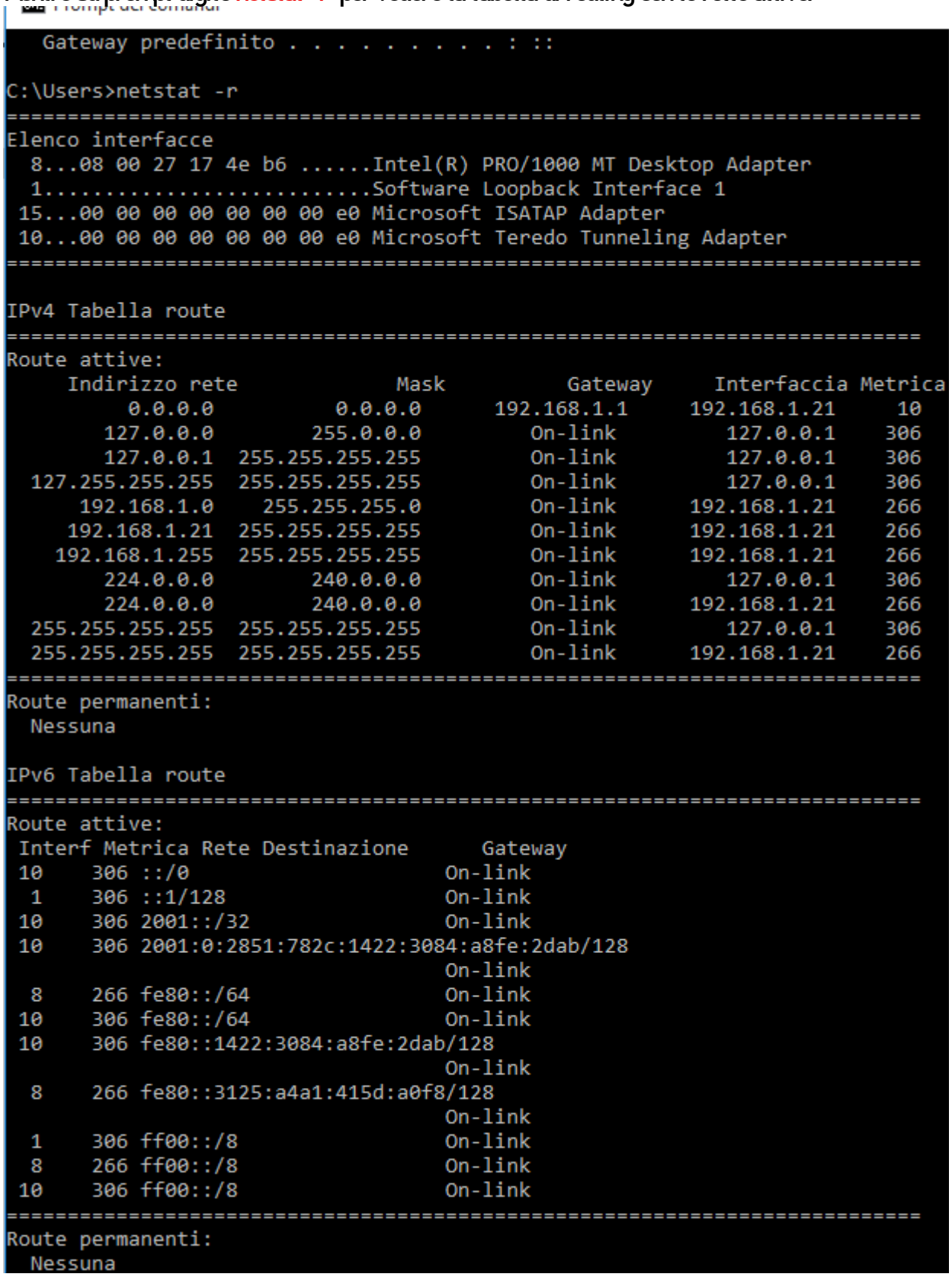


QUAL È IL COMANDO POWERSHELL PER DIR?

Get-ChildItem

Su PowerShell, inserisco netstat -h per vedere le opzioni disponibili per il comando netstat.

Mentre su prompt digito netstat –r per vedere la tabella di routing con le rotte attive.

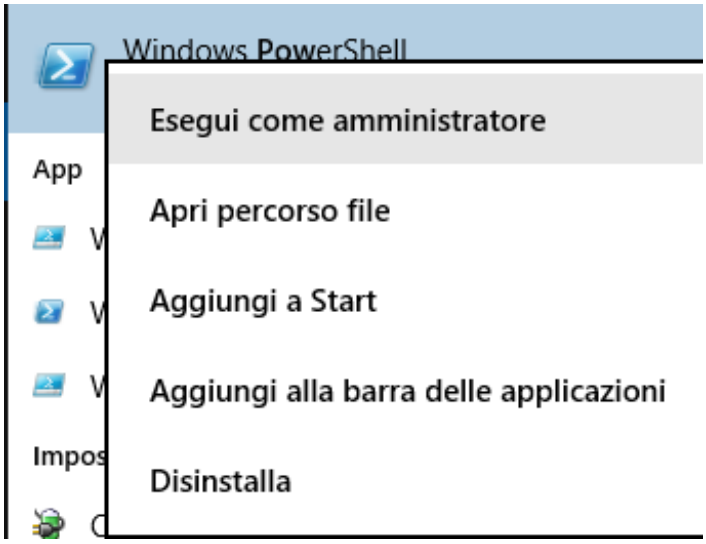


```
   Gateway predefinito . . . . . . . . . : ::

C:\Users>netstat -r
===========================================================================
Elenco interfacce
  8...08 00 27 17 4e b6 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
 15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 10...00 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     192.168.1.21     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      192.168.1.21    266
     192.168.1.21  255.255.255.255         On-link      192.168.1.21    266
    192.168.1.255  255.255.255.255         On-link      192.168.1.21    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      192.168.1.21    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      192.168.1.21    266
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
 10     306 ::/0                     On-link
  1     306 ::1/128                  On-link
 10     306 2001::/32                On-link
 10     306 2001:0:2851:782c:1422:3084:a8fe:2dab/128
                                     On-link
  8     266 fe80::/64                On-link
 10     306 fe80::/64                On-link
 10     306 fe80::1422:3084:a8fe:2dab/128
                                     On-link
  8     266 fe80::3125:a4a1:415d:a0f8/128
                                     On-link
  1     306 ff00::/8                 On-link
  8     266 ff00::/8                 On-link
 10     306 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
```

QUAL È IL GATEWAY IPv4?

Indirizzo rete di 0.0.0.0 e una Mask di 0.0.0.0. Questa riga rappresenta il default gateway. Nella colonna Gateway di quella riga, ho trovato il mio gateway IPv4 è 192.168.1.1.

Apro una seconda Powershell, questa volta eseguo come amministratore.



Ho eseguito prima con il comando netstat -abno , dopodichè, Gestione Attività, navigo alla scheda Dettagli. Faccio clic sull'intestazione PID in modo che i PID siano in ordine. In questo caso il PID è 1436.

```
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       1436
 [tcpsvcs.exe]
  TCP    0.0.0.0:9              0.0.0.0:0              LISTENING       1436
 [tcpsvcs.exe]
  TCP    0.0.0.0:13             0.0.0.0:0              LISTENING       1436
 [tcpsvcs.exe]
  TCP    0.0.0.0:17             0.0.0.0:0              LISTENING       1436
 [tcpsvcs.exe]
  TCP    0.0.0.0:19             0.0.0.0:0              LISTENING       1436
 [tcpsvcs.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       692
  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       1988
 [mqsvc.exe]
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       1988
 [mqsvc.exe]
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       1988
 [mqsvc.exe]
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       1988
 [mqsvc.exe]
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       872
  TermService
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
```

Gestione attività

File Opzioni Visualizza

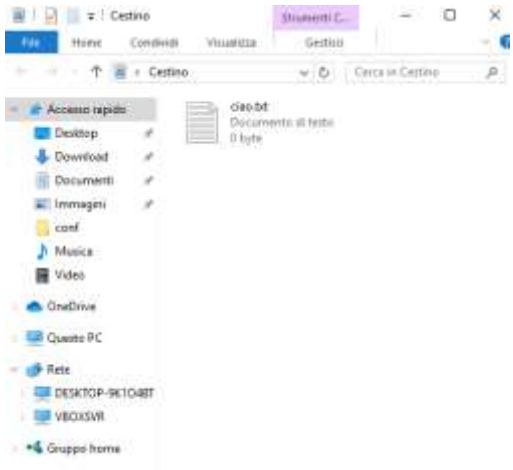
Processi | Prestazioni | Cronologia applicazioni | Avvio | Utenti | Dettagli | Servizi

Nome	PID	Stato	Nome ute...	CPU	Memoria (...	Descrizione
Taskmgr.exe	460	In esecuzione	user	00	8.704 K	Gestione attività
winlogon.exe	508	In esecuzione	SYSTEM	00	484 K	Applicazione Accesso a Windows
services.exe	548	In esecuzione	SYSTEM	00	2.040 K	App Servizi e Controller
lsass.exe	556	In esecuzione	SYSTEM	00	2.220 K	Local Security Authority Process
svchost.exe	612	In esecuzione	SERVIZIO L...	00	5.424 K	Processo host per servizi di Wind
svchost.exe	636	In esecuzione	SYSTEM	00	2.920 K	Processo host per servizi di Wind
svchost.exe	692	In esecuzione	SERVIZIO ...	00	2.552 K	Processo host per servizi di Wind
svchost.exe	872	In esecuzione	SERVIZIO ...	00	4.732 K	Processo host per servizi di Wind
dwm.exe	880	In esecuzione	DWM-1	00	32.560 K	Gestione finestre desktop
svchost.exe	888	In esecuzione	SYSTEM	00	10.872 K	Processo host per servizi di Wind
svchost.exe	940	In esecuzione	SERVIZIO L...	00	1.768 K	Processo host per servizi di Wind
svchost.exe	960	In esecuzione	SERVIZIO L...	00	8.392 K	Processo host per servizi di Wind
conhost.exe	1100	In esecuzione	user	00	2.596 K	Console Window Host
powershell.exe	1136	In esecuzione	user	00	47.380 K	Windows PowerShell
pg_ctl.exe	1244	In esecuzione	SERVIZIO ...	00	444 K	pg_ctl - starts/stops/restarts the P
WmsSvc.exe	1356	In esecuzione	SYSTEM	00	1.320 K	WmsService
WmsSelfHealingSvc....	1364	In esecuzione	SYSTEM	00	440 K	WmsRepairService
svchost.exe	1416	In esecuzione	user	00	748 K	Processo host per servizi di Wind
TCPSVCS.EXE	1436	In esecuzione	SERVIZIO L...	00	320 K	TCP/IP Services Application
spoolsv.exe	1568	In esecuzione	SYSTEM	00	1.068 K	Applicazione sottosistema spoole
svchost.exe	1676	In esecuzione	SERVIZIO L...	00	4.360 K	Processo host per servizi di Wind
svchost.exe	1732	In esecuzione	SYSTEM	00	792 K	Processo host per servizi di Wind
svchost.exe	1760	In esecuzione	SYSTEM	00	3.332 K	Processo host per servizi di Wind

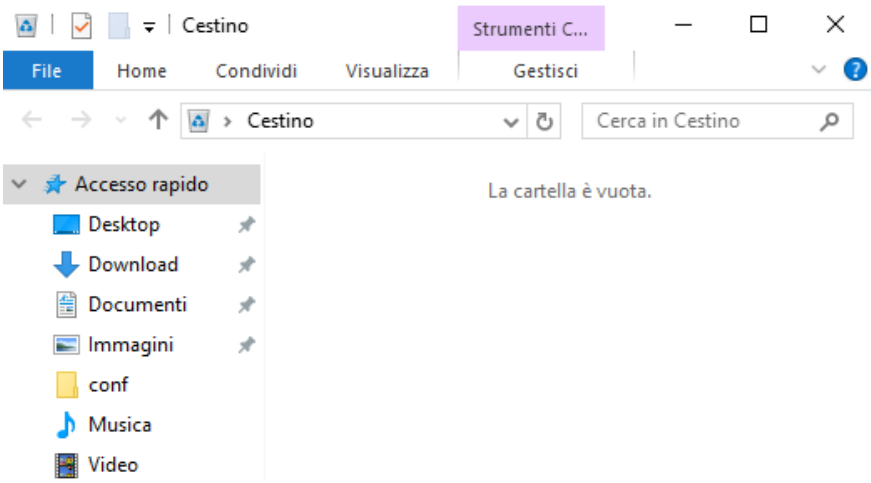
QUALI INFORMAZIONI PUOI OTTENERE DALLA SCHEDA DETTAGLI E DALLA FINESTRA DI DIALOGO PROPRIETÀ PER IL PID SELEZIONATO?

Aprendo la finestra proprietà ho trovato diverse informazioni utili, specialmente nella scheda "Dettagli". C'è il nome del processo, è un file eseguibile, mi dice a cosa serve quel processo, in questo caso è un'applicazione legata ai servizi TCP IP, il percorso è importante per capire se è sospetto o meno, le dimensioni, l'orario, le modifiche, ultimo accesso al file. Praticamente come la nostra Carta d'identità.

Creo un file di testo chiamato "ciao.txt" e lo sposto nel cestino



In una console PowerShell, inserisco clear-recyclebin al prompt. Metto "Si" e la cartella è vuota



COSA È SUCCESSO AI FILE NEL CESTINO?

Il file ciao.txt nel Cestino è stato eliminato

Domanda di Riflessione

PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.

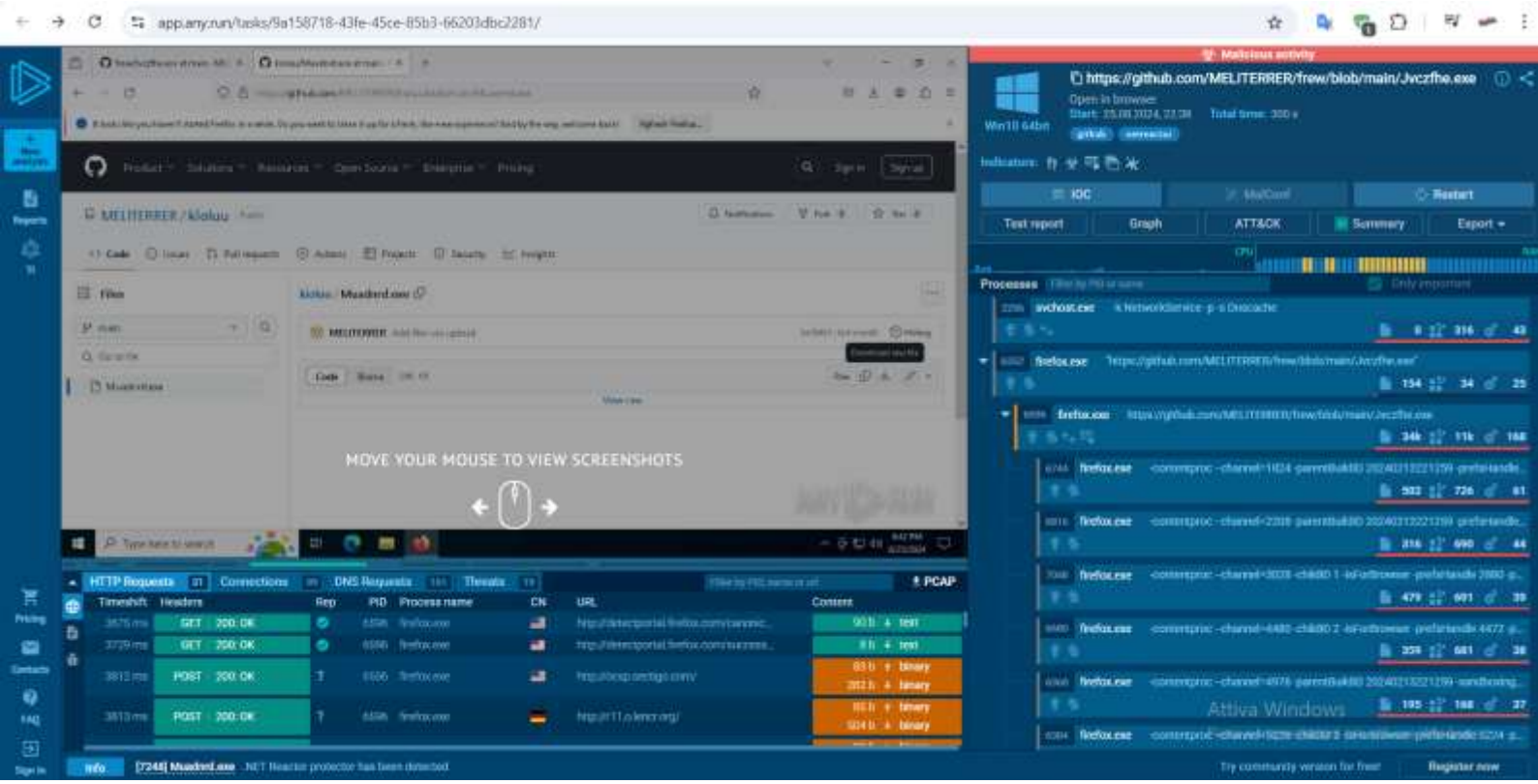
Cercando alcuni comandi su internet ho trovato:

- Get-Process : Per trovare processi che consumano troppa CPU
- Get-NetTCPConnection: Per vedere le connessioni di rete attive verso l'esterno
- Get-WinEvent: Per analizzare i log di sicurezza e trovare tentativi di accesso falliti
- Get-Service: mostra tutti i servizi
- Start-MpScan: Per avviare una scansione antivirus con Windows Defender.

Esercizio 2: Studio Ioc

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.
https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

Accedo al link fornito dalla traccia.



SPIEGAZIONE: Innanzitutto, Cos'è ANYRUN? E' come un laboratorio virtuale dove posso eseguire programmi o aprire file sospetti senza far danni al mio vero computer. Mi permette di vedere cosa fa il programma, se crea nuovi file, se cerca di rubare informazioni ecc. È uno strumento usato per analizzare il malware in un ambiente controllato e piu' sicuro.
Le Minacce: Ho analizzato quindi il report di Anyrun relativo al link che mi ha fornito la traccia.
Il file chiamato MELITTERER/freew/main/xcxftt.exe vedo che proviene da ghitub. Questo è già un sospetto perché i malware la maggior parte delle volte si nascondono in file eseguibili scaricati da altri siti. Un altro campanello è stato vedre il processo principale ovvero Firefox.exe, e sembra che stia cercando di connettersi a vari indirizzi. Vedo anche connessioni a vari indirizzi che potrebbero essere usati per mascherare attività malevole.
Poi vedo anche il file xcxftt.exe è stato scaricato e sta usando Firefox per comunicare con server esterni ,e questo è molto sospetto perché potrebbero raccogliere informazioni o prendere il controllo.

Bonus 1: Esplorazione di Nmap

Obiettivi

- *Parte 1 ↵ Esplorazione di Nmap*
- *Parte 2 ↵ Scansione delle Porte*

Aperte Contesto / Scenario

La scansione delle porte fa solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte utilizzabili. Esploreremo come usare l'utility Nmap. Nmap è una potente utility di rete usata per la scoperta della rete e l'audit di sicurezza.

Risorse Richieste

- *Macchina virtuale CyberOps Workstation*
- *Accesso a Internet*

Eseguiamo con i passaggi, apro Cyberops workstations e avvio il terminale, nel terminale digito man nmap

```
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
       information is the "interesting ports table".  That table lists the
       port number and protocol, service name, and state. The state is either
       open, filtered, closed, or unfiltered.  Open means that an application
       on the target machine is listening for connections/packets on that
       port.  Filtered means that a firewall, filter, or other network
       obstacle is blocking the port so that Nmap cannot tell whether it is
       open or closed.  Closed ports have no application listening on them,
       though they could open up at any time. Ports are classified as
       unfiltered when they are responsive to Nmap's probes, but Nmap cannot
       determine whether they are open or closed. Nmap reports the state
       combinations open|filtered and closed|filtered when it cannot determine
       which of the two states describe a port. The port table may also
       include software version details when version detection has been
       requested. When an IP protocol scan is requested (-sO), Nmap provides
       information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further
       information on targets, including reverse DNS names, operating system
       guesses, device types, and MAC addresses.

       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.
```

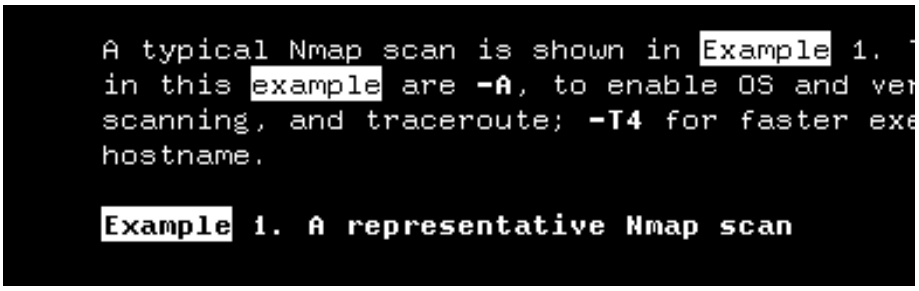
COS'È NMAP?

Nmap è un software libero creato per effettuare port scanning, è uno strumento open source ed esplora delle reti per la sicurezza.

PER COSA VIENE USATO NMAP?

In sostanza usiamo nmap principalmente per mappare una rete, scoprire i dispositivi attivi, capire quali servizi offrono e identificare punti deboli per la sicurezza.

Dopodichè digito /example nel file e mi evidenzia tutte le parole "example"
Esempio:



QUAL È IL COMANDO NMAP USATO?

nmap -A -T4 scanme.nmap.org

COSA FA L'OPZIONE -A?

esegue diverse scansioni, cercando informazioni ho visto che sta per scansione aggressiva con una sola volta

COSA FA L'OPZIONE -T4?

Ho cercato nelle pagine di manuale e una ricerca su internet. Ho capito che -T controlla la velocità della scansione, 4 indica il livello di velocità.

Andando avanti, sempre sul terminale, nmap -A -T4 localhost, avendo una scansione

```
[analyst@secOps ~]$  nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:22 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000023s 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)
| 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/ .
```

QUALI PORTE E SERVIZI SONO APERTI?

La porta 21(FTP) e il servizio è vsftpd, inoltre, FTP risulta consentito, quindi dovremmo configurarla e fare molta attenzione

inserisco ip address per determinare l' IP e la subnet mask per questo host.

```
[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:b1:cd:51 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 84217sec preferred_lft 84217sec
    inet6 fd00::a00:27ff:feb1:cd51/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 85902sec preferred_lft 13902sec
    inet6 fe80::a00:27ff:feb1:cd51/64 scope link
       valid_lft forever preferred_lft forever
```

A QUALE RETE APPARTIENE LA TUA VM?

appartiene alla rete 10.0.2.0 togliendo .15

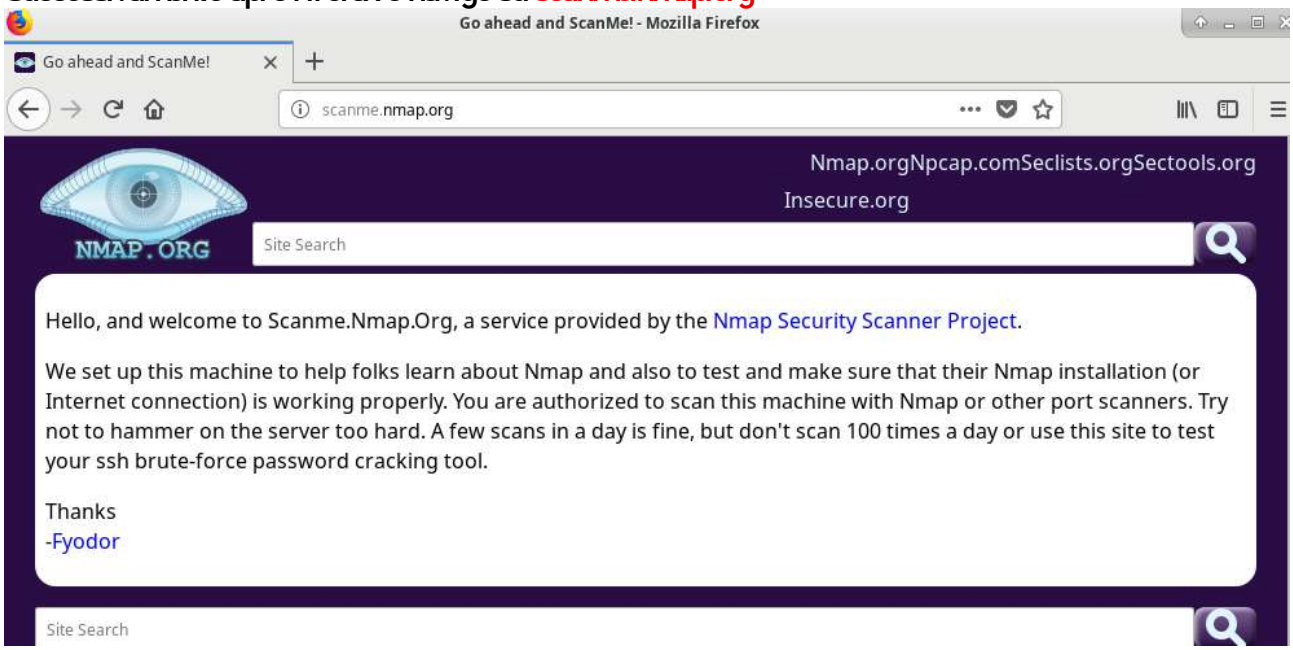
Seguendo la traccia inserisco nmap -A -T4 indirizzo_rete/prefisso. In questo caso 10.0.2.0/24

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:37 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00013s 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 10.0.2.15
|      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: 256 IP addresses (1 host up) scanned in 21.65 seconds
[analyst@secOps ~]$
```

QUANTI HOST SONO ATTIVI?

ha rilevato 1 host attivo. L'host attivo è la VM su cui sto lavorando (10.0.2.15).

Successivamente apro Firefox e navigo su scanme.nmap.org



QUAL È LO SCOPO DI QUESTO SITO?

Questo sito è stato creato dal Nmap Security Scanner Project per aiutare le persone a imparare Nmap e la seguente installazione in modo da far funzionare correttamente. Si puo' fare pratica senza rischiare nulla.

Al prompt inserisco nmap -A -T4 scanme.nmap.org

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:49 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered 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 39.06 seconds
[analyst@secOps ~]$
```

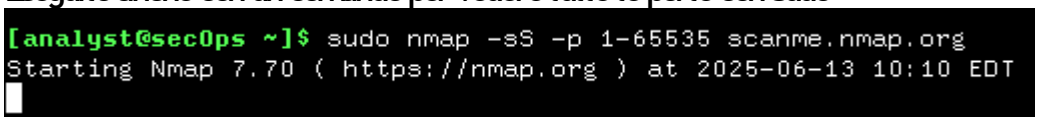
QUALI PORTE E SERVIZI SONO APERTI?

Porta 22/tcp Servizio ssh, Porta 80/tcp Servizio http, Porta 9929/tcp Servizio nping-echo, Porta 31337/tcp Servizio tcpwrapped

QUALI PORTE E SERVIZI SONO FILTRATI?

25/tcp filtered smtp , 139/tcp filtered netbios-ssn, 445/tcp filtered microsoft-ds, 593/tcp: filtered http-rpc-epmap

Eseguito anche con un comando per vedere tutte le porte con sudo



QUAL È L'INDIRIZZO IP DEL SERVER?

45.33.32.156

QUAL È IL SISTEMA OPERATIVO?

Linux

DOMANDA DI RIFLESSIONE

Nmap è uno strumento potente per l'esplorazione e la gestione della rete.

Come può Nmap aiutare con la sicurezza della rete?

Mi aiuta a trovare quali porte sono aperte, se servizi sono attivi e se ci sono versioni di software insicure sulla mia rete così posso chiudere le porte che non servono e aggiorno i servizi per proteggere meglio il sistema

Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Con Nmap lo puo' usare anche l'attaccante per spiare la rete cercando le stesse informazioni, quindi, porte aperte, i servizi ecc.. trovando punti deboli.

Bonus 2 ↵ Attacco a un database MySQL

Obiettivi

In questo laboratorio, visualizzerai un file PCAP di un attacco precedente contro un database SQL.

- Parte 1 ↵ Aprire Wireshark e caricare il file PCAP.
- Parte 2 ↵ Visualizzare l'attacco di SQL Injection.
- Parte 3 ↵ L'attacco di SQL Injection continua...
- Parte 4 ↵ L'attacco di SQL Injection fornisce informazioni di sistema.
- Parte 5 ↵ L'attacco di SQL Injection e le informazioni sulle tabelle
- Parte 6 ↵ L'attacco di SQL Injection si conclude.

Contesto / Scenario

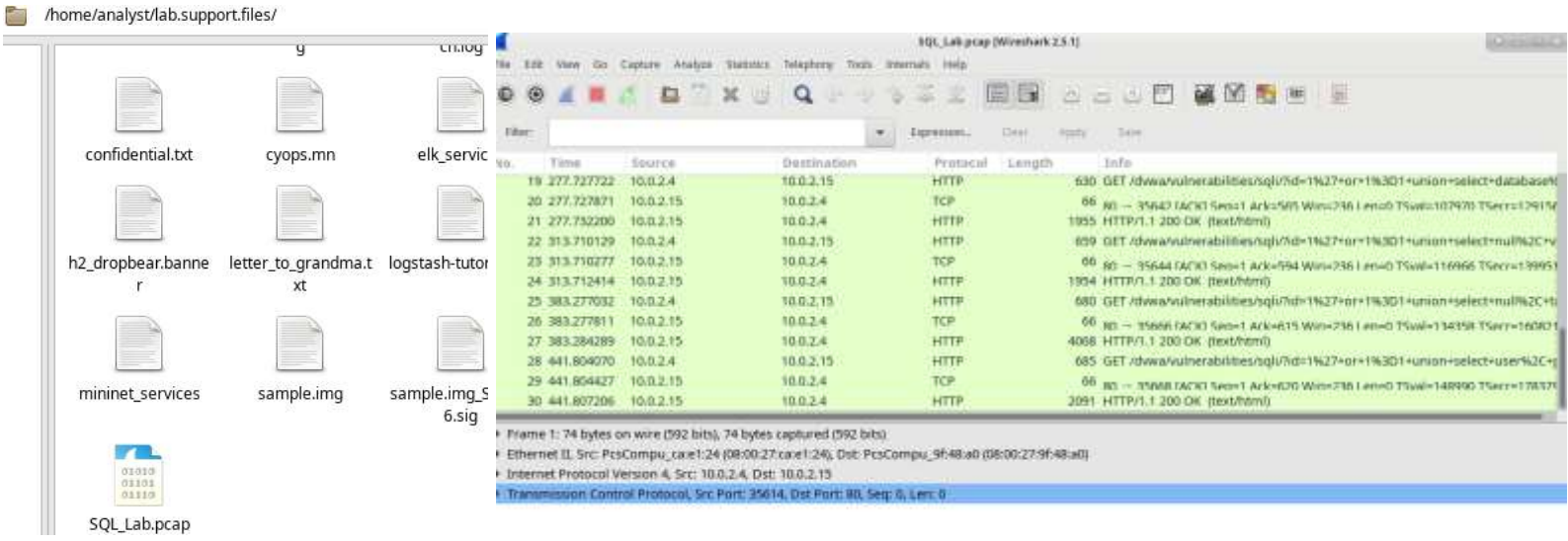
Gli attacchi di SQL injection consentono agli hacker malintenzionati di digitare istruzioni SQL in un sito web e ricevere una risposta dal database. Ciò permette agli aggressori di manomettere i dati correnti nel database, falsificare identità e compiere varie azioni dannose. È stato creato un file PCAP per consentirti di visualizzare un attacco precedente contro un database SQL. In questo laboratorio, visualizzerai gli attacchi al database SQL e risponderai alle domande.

Risorse Richieste

- Macchina virtuale CyberOps Workstation

Iniziamo!!

clic su Applicazioni > CyberOPS > Wireshark > cerco lab.support.files > apro il file SQL_Lab.pcap.

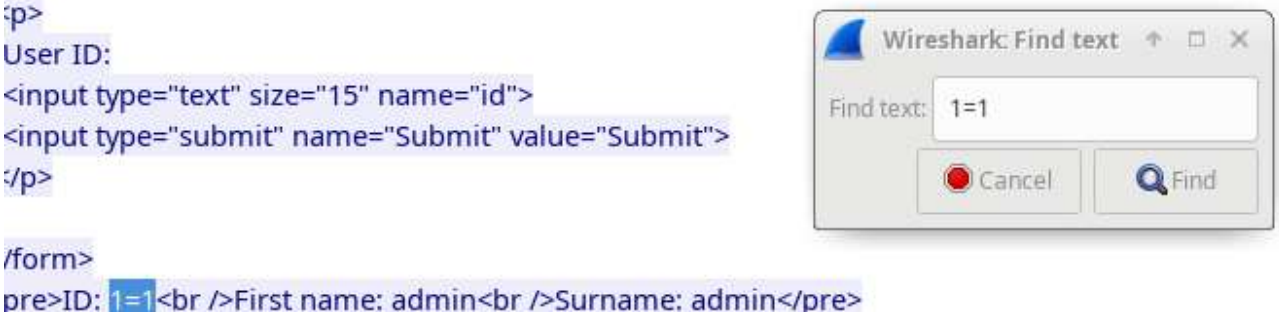


QUALI SONO I DUE INDIRIZZI IP COINVOLTI IN QUESTO ATTACCO DI SQL INJECTION IN BASE ALLE INFORMAZIONI VISUALIZZATE?

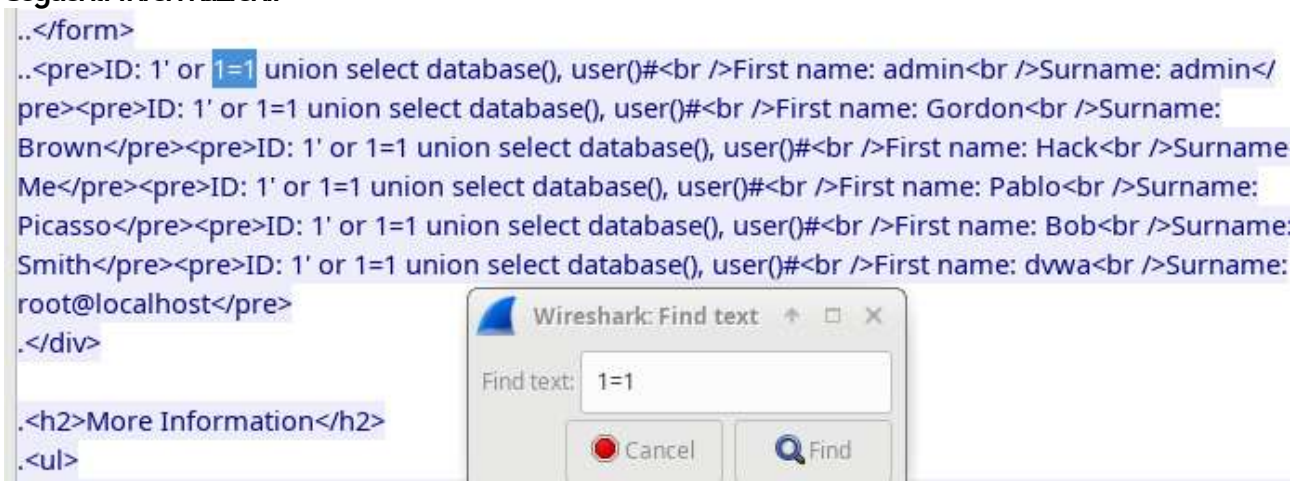
10.0.2.15 (l'attaccante) , 10.0.2.4 (bersaglio)

In Wireshark, faccio clic con il pulsante destro del mouse sulla riga 13 e seleziono Seguo Flusso http stream, utile per seguire il flusso di dati.
Il traffico sorgente è mostrato in rosso. La sorgente ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

Cerco 1=1



Chiudo il flusso che ho aperto prima e apro uno nuovo sulla riga 19, l'applicazione ha risposto con le seguenti informazioni:



*Il nome del database è dvwa e l'utente del database è root@localhost. Vengono visualizzati anche più account utente.

Stessa cosa su riga 22

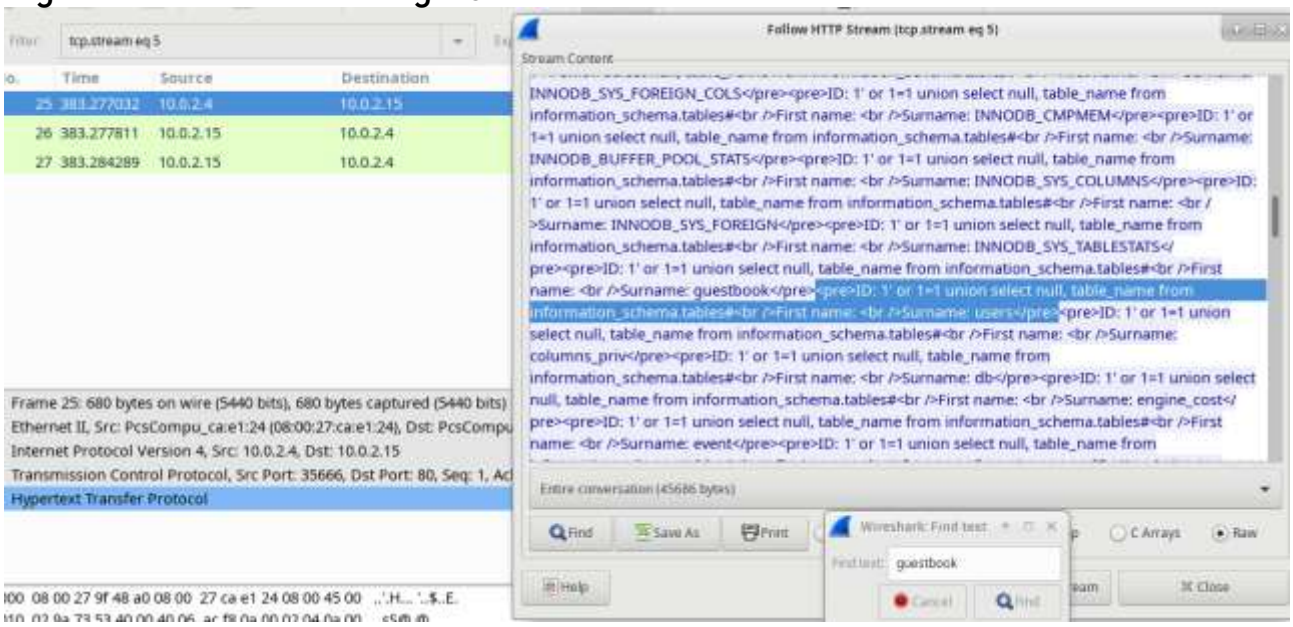
..<pre>ID: 1' or 1=1 union select null, version ()#
First name: admin
Surname: admin</
pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Gordon
Surname: Brown</
pre><pre>ID: 1' or 1=1 union select null, version ()#
First name: Hack
Surname: Me</
pre><pre>ID: 1' or 1=1 union select null,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

.<h2>More Information</h2>
.
..
<a href="http://www.securitear E.html" target="_blank">http://
www.securiteam.com/securityrevie

QUAL È LA VERSIONE?

La versione è 5.7.12-0Ubuntu1.1

Seguendo la traccia vado sulla riga 25



Riga 28, stesso procedimento

QUALE UTENTE HA L'HASH DELLA PASSWORD DI 8D3533D75AE2C3966D7E0D4FCC69216B?

1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b</ ID: 1337.

QUAL è LA PASSWORD IN CHIARO?

Ho usato sito crackstation.net e di incollare l'hash della password ovvero 8d3533d75ae2c3966d7e0d4fcc69216b. La password è "charley"

DOMANDE DI RIFLESSIONE

1. Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?

   I siti web sono comunemente basati su database e utilizzano il linguaggio SQL. La gravità di un attacco di SQL injection dipende dall'aggressore.

2. Naviga in internet ed esegui una ricerca per "prevenire attacchi di SQL injection". Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

   Le risposte varieranno, ma dovrebbero includere: filtrare l'input dell'utente, implementare un firewall per applicazioni web, disabilitare funzionalità/capacità non necessarie del database, monitorare le istruzioni SQL, utilizzare parametri con stored procedure e utilizzare parametri con SQL dinamico.

1 Il rischio è che se un sito non controlla bene quello che scrivo, inganno il database con comandi SQL nascosti per rubare dati sensibili. Quindi il mio input lo tarsformo in un comando pericoloso. Quindi il sito web deve controllare sempre tutto ciò che l'utente, scrive nei testi.

2 Prevenire la SQL Injection significa combinare su tanti starti come la cipolla, 2 metodi, sicuramente, WAF(firewall): È un filtro esterno che blocca gli attacchi SQL Injection prima di arrivare all'applicazione, analizzando il traffico.

Minimi privilegi: L'applicazione deve usare un account con solo i permessi necessari. Meno permessi hai e meno danni avrai da parte dell' Attaccante.

GRAZIE PER L'ATTENZIONE

Mattia Di Turo