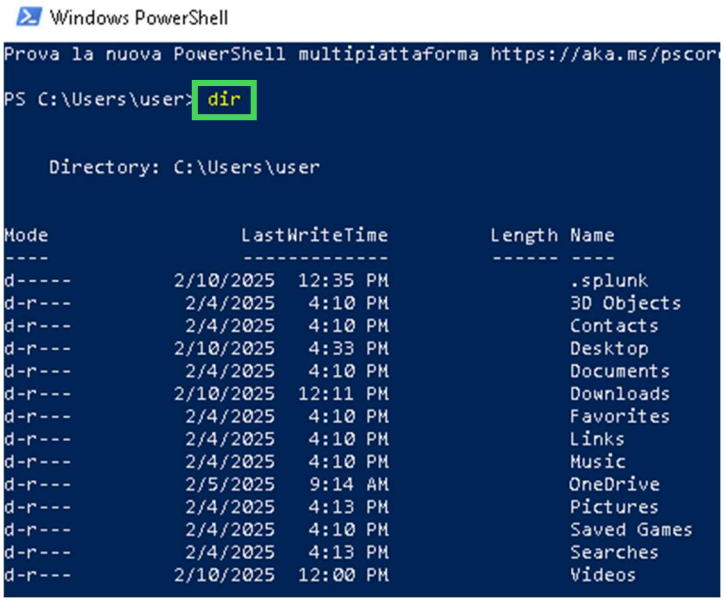
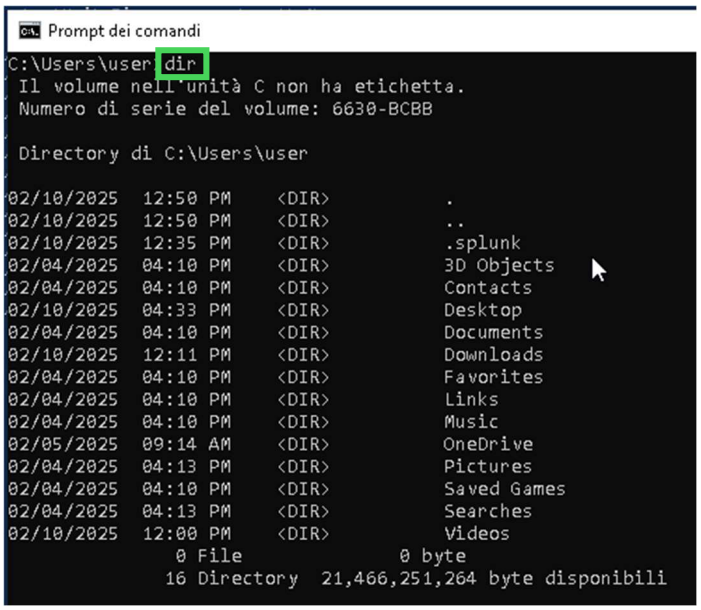
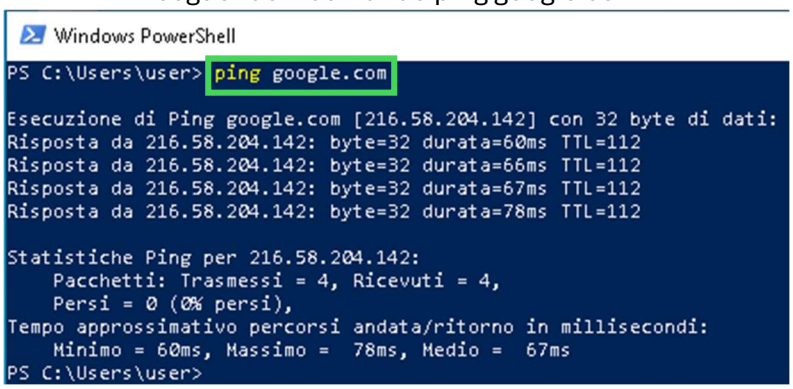
Esercizio 1

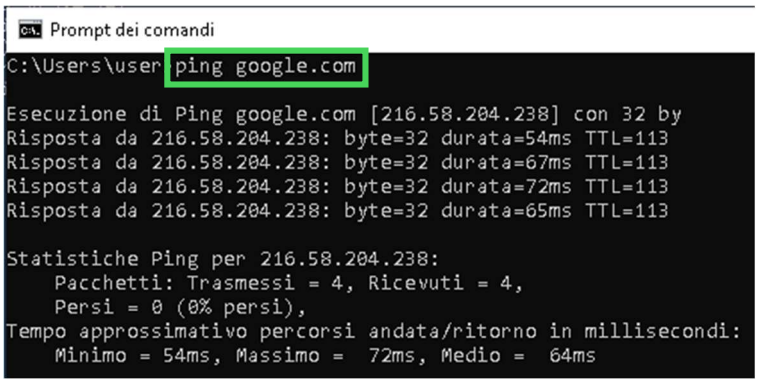




Sia PowerShell che CMD mostrano un elenco delle directory presenti nell'attuale percorso di esecuzione (C:\Users\user).

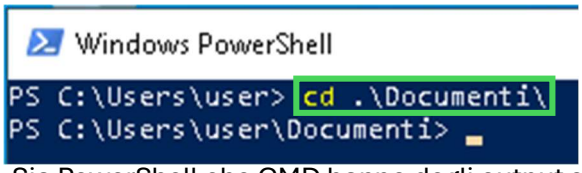
Eseguendo il comando ping google.com:

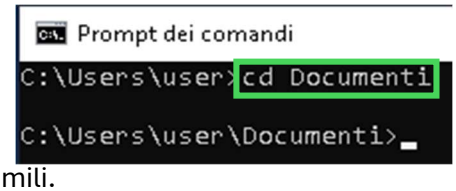




Sia PowerShell che CMD hanno degli output simili.

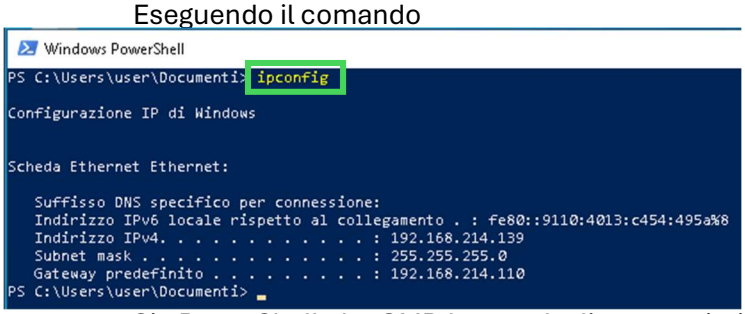
Eseguendo il comando cd Documenti:

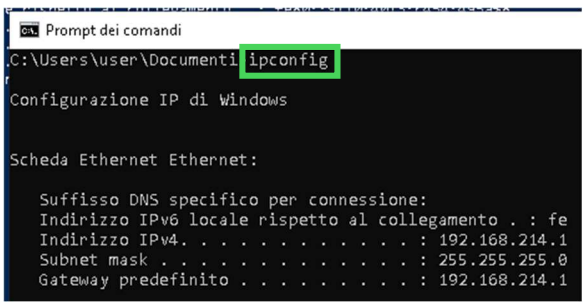




Sia PowerShell che CMD hanno degli output simili.

Eseguendo il comando





Sia PowerShell che CMD hanno degli output simili.

usando il comando Get-alias dir serve per verificare a quale comando effettivo corrisponde l'alias dir in PowerShell:

```
PS C:\Users\user\Documenti> Get-alias dir

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

il che sta ad indicare che dir è un alias in PowerShell, non un comando nativo.

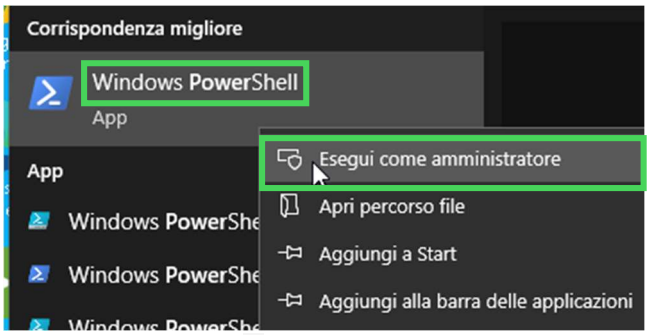
Usando poi il comando netstat -h possiamo visualizzare tutte le opzioni utilizzabili con il comando netstat:

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

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

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

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -b            Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
                porta di ascolto. In alcuni casi, host di eseguibili noti
                più componenti indipendenti e in questi casi il
                sequenza di componenti coinvolti nella creazione della connessione
                o la porta in ascolto. In questo caso, l'eseguibile
                il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
                e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
                può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
                autorizzazioni.
  -e visualizza le statistiche Ethernet. È possibile combinare
                opzione.
  -f Visualizza nomi di dominio completi (FQDN) per stranieri
                indirizzi.
  -n Visualizza indirizzi e numeri di porta in formato numerico.
  -o Visualizza l'ID del processo proprietario associato a ogni connessione.
  -p proto Mostra le connessioni per il protocollo specificato da proto; proto
                può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6.  Se usato con-s
                opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  -q            Visualizza tutte le connessioni, le porte di ascolto e i binding
                non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
                essere associato a una connessione attiva.
  -r            Visualizza la tabella di routing.
  -s            Visualizza le statistiche per protocollo.  Per impostazione predefinita, le statistiche vengono
                visualizzata per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
                l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
  -t            Visualizza lo stato corrente di offload della connessione.
  -x            Visualizza connessioni NetworkDirect, listener e condivisi
                endpoint.
  -y            Visualizza il modello di connessione TCP per tutte le connessioni.
                Non può essere combinato con le altre opzioni.
  intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
                tra ogni schermo.  Premere CTRL+C per interrompere la rivisualizzazione
                Statistiche.  Se viene omesso, netstat stamperà il
                informazioni di configurazione una volta.
```

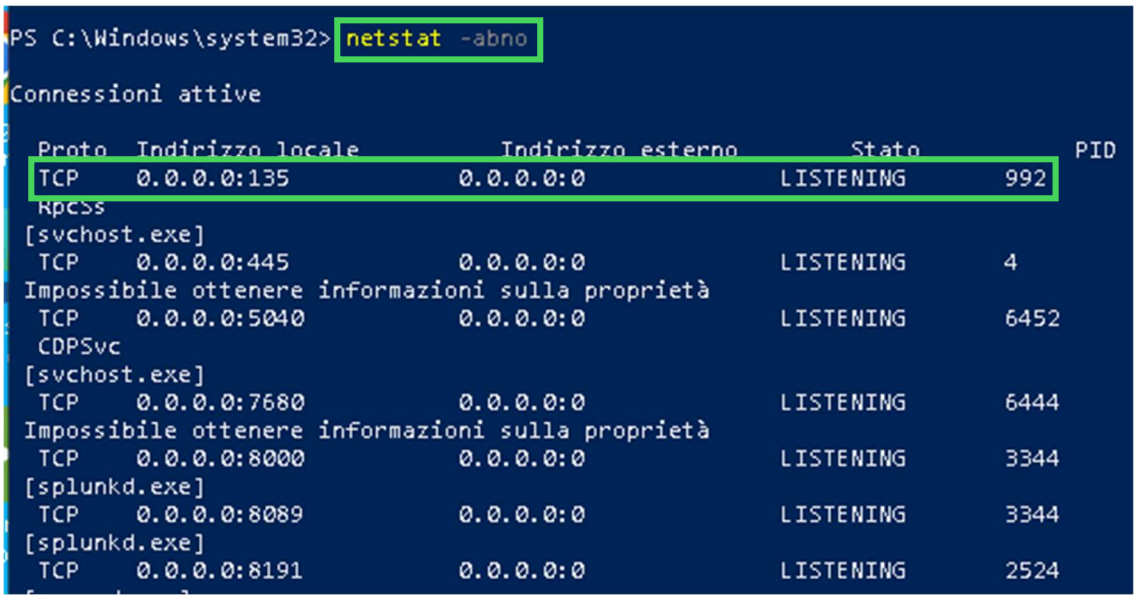
Quindi, per poter visualizzare la tabella di routing basta digitare il comando netstat -r:

```
PS C:\Users\user\Documenti> netstat -r
===========================================================================
Elenco interfacce
  8...08 00 27 fb 69 f8 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete             Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0  192.168.214.110  192.168.214.139     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.214.0    255.255.255.0         On-link   192.168.214.139    281
  192.168.214.139  255.255.255.255         On-link   192.168.214.139    281
  192.168.214.255  255.255.255.255         On-link   192.168.214.139    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.214.139    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.214.139    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  1    331 ::1/128                  On-link
  8    281 fe80::/64                On-link
  8    281 fe80::9110:4013:c454:495a/128
                                    On-link
  1    331 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
```

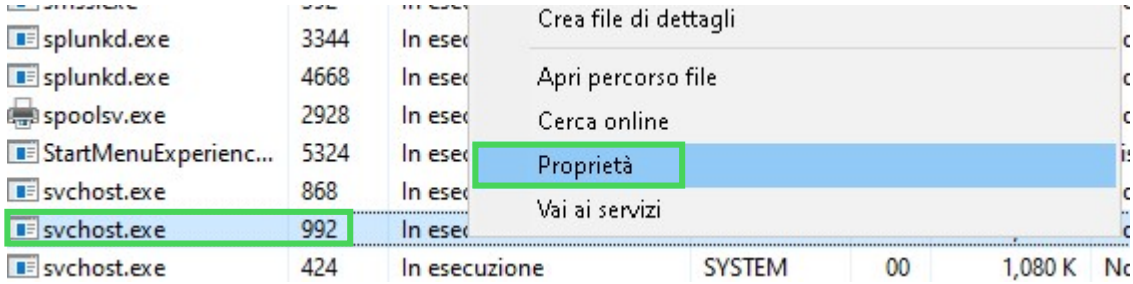
Adesso apro un secondo PowerShell con diritti di amministratore:



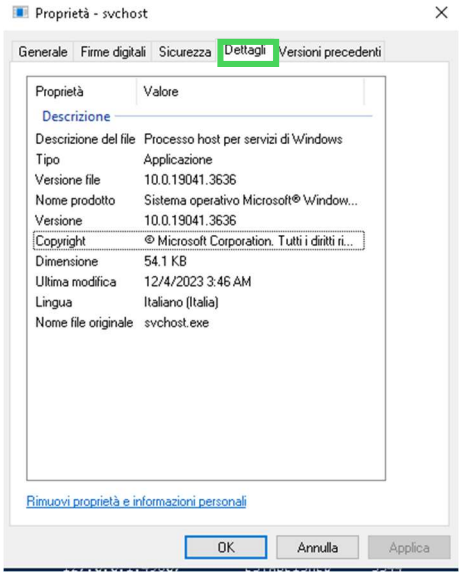
e digito il comando netstat -abno che serve per visualizzare i processi associati alle connessioni TCP attive:



E, aprendo il task manager con la sequenza di tasti ctrl+shift+esc, cerco e seleziono il primo processo con PID 992 e cliccando col tasto destro, vado su proprietà :

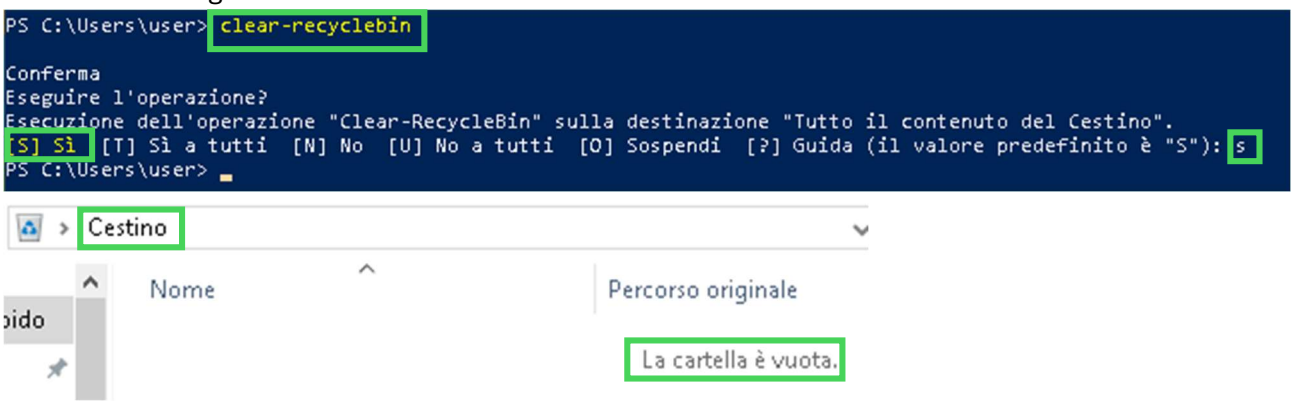


È possibile visualizzare una scheda con alcuni dettagli riguardante il processo preso in considerazione:



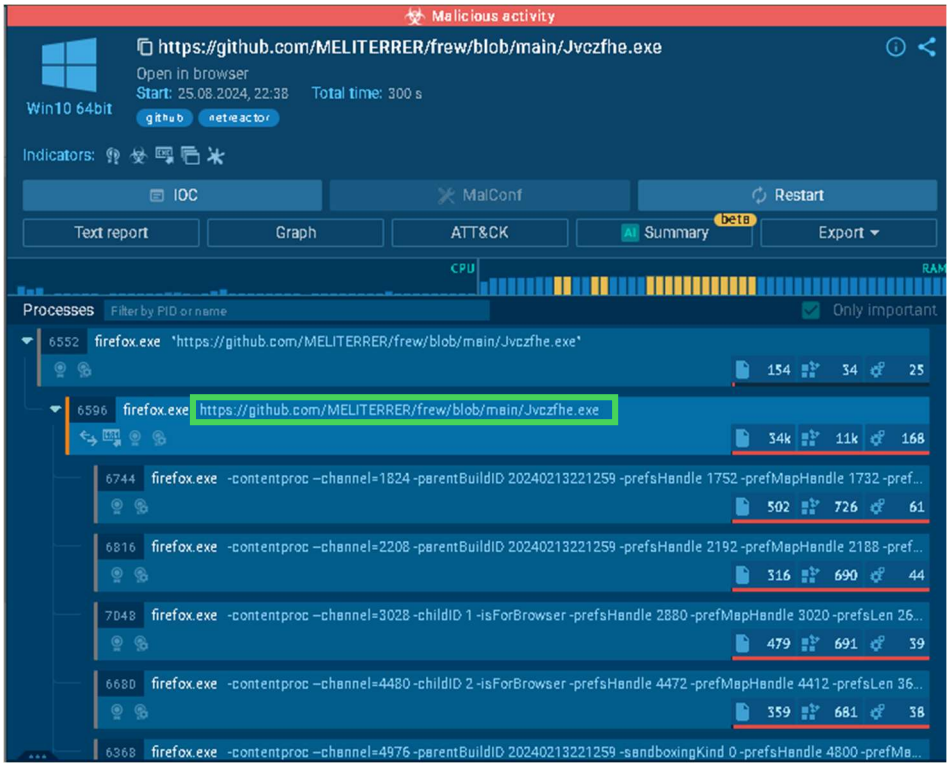
il passaggio finale della guida è la possibilità di eliminare elementi contenuti nel cestino usando PowerShell; quindi, creo degli elementi da poter inserire nel cestino:

e successivamente, usando PowerShell, digito il comando clear-recyclebin per eliminare definitivamente gli elementi all'interno del cestino:

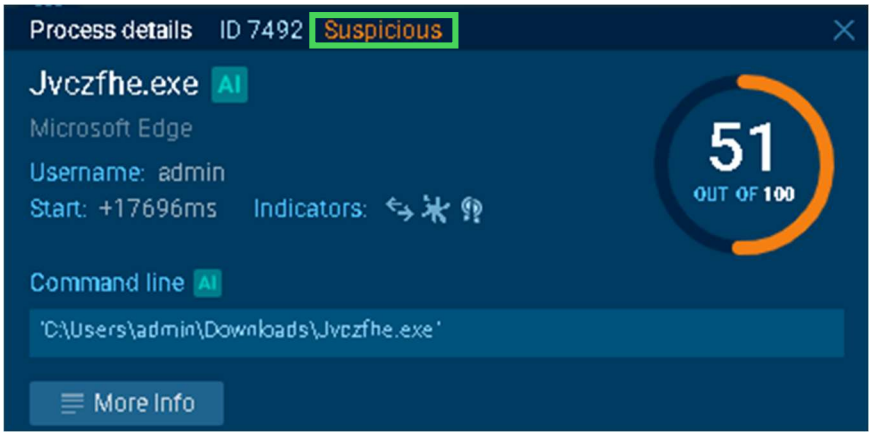


Esercizio 2

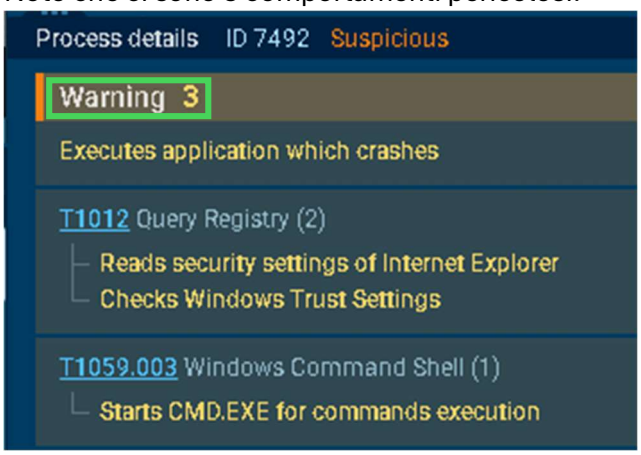
La prima operazione eseguita da questo malware è quella di aprire una pagina web che punta ad una repository di GitHub contenente due file e scarica il file chiamato “Jvczfhe.exe”:



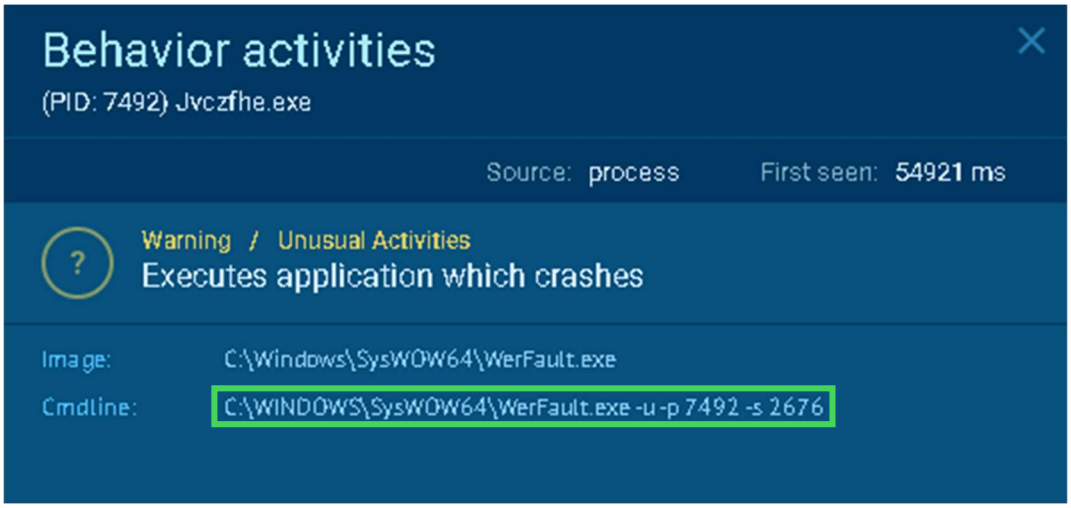
E andando ad analizzare il file:



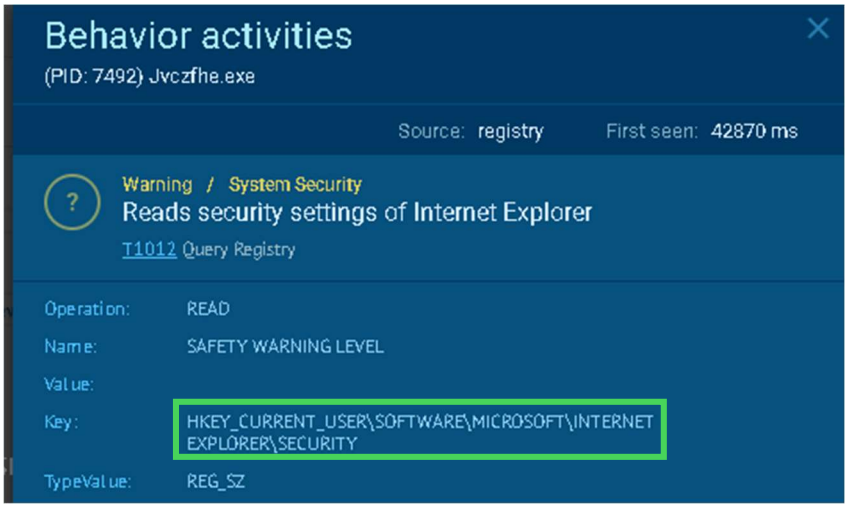
Noto che ci sono 3 comportamenti pericolosi:



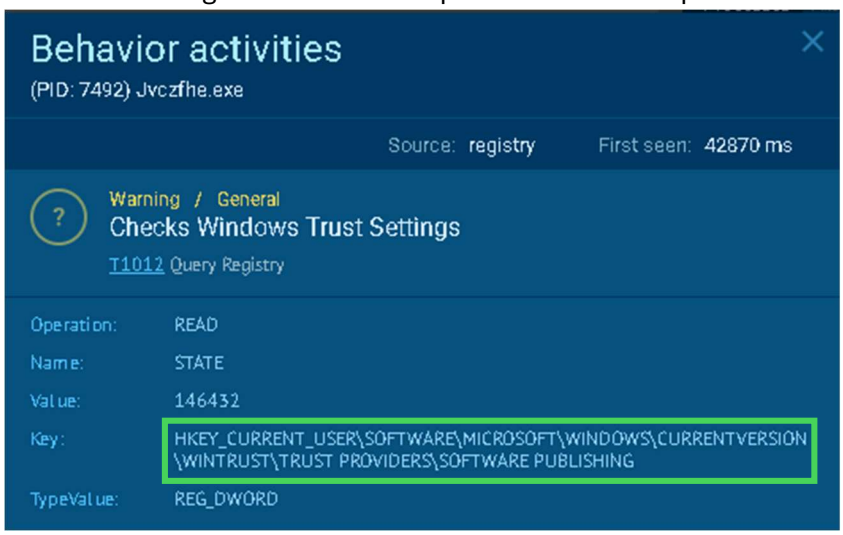
Il primo manda in crash l'applicazione WerFault.exe che è progettata per raccogliere informazioni su errori e crash di applicazioni e se un'applicazione o un processo causa un crash, si attiva per raccogliere informazioni diagnostiche e inviarle a Microsoft.
Il file Jvczfhe.exe potrebbe voler disattivare WerFault.exe per non essere rilevato.



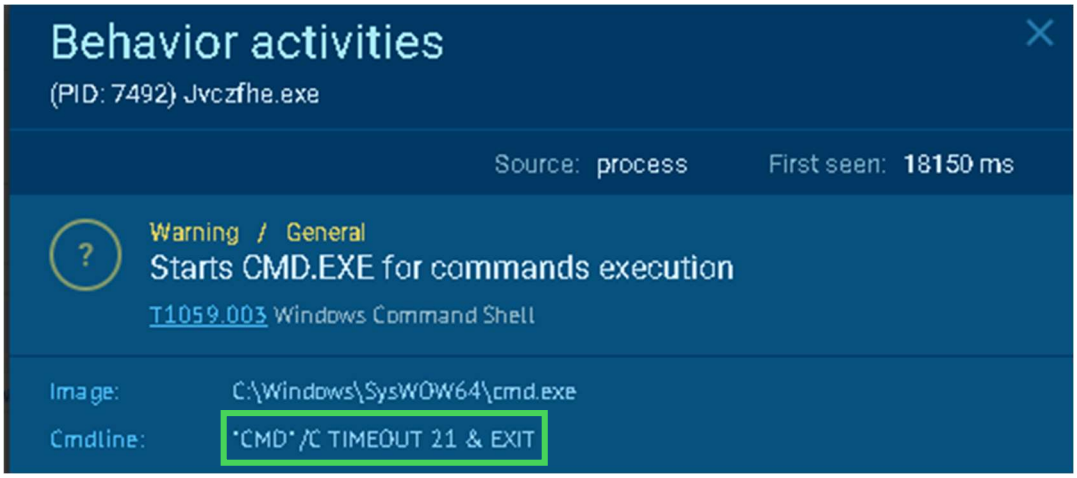
Successivamente legge le informazioni di sicurezza su Internet Explorer.



E legge lo stato della chiave associata a Windows Trust Settings utilizzata per verificare la legittimità dei software e il grado di fiducia da parte del sistema operativo.

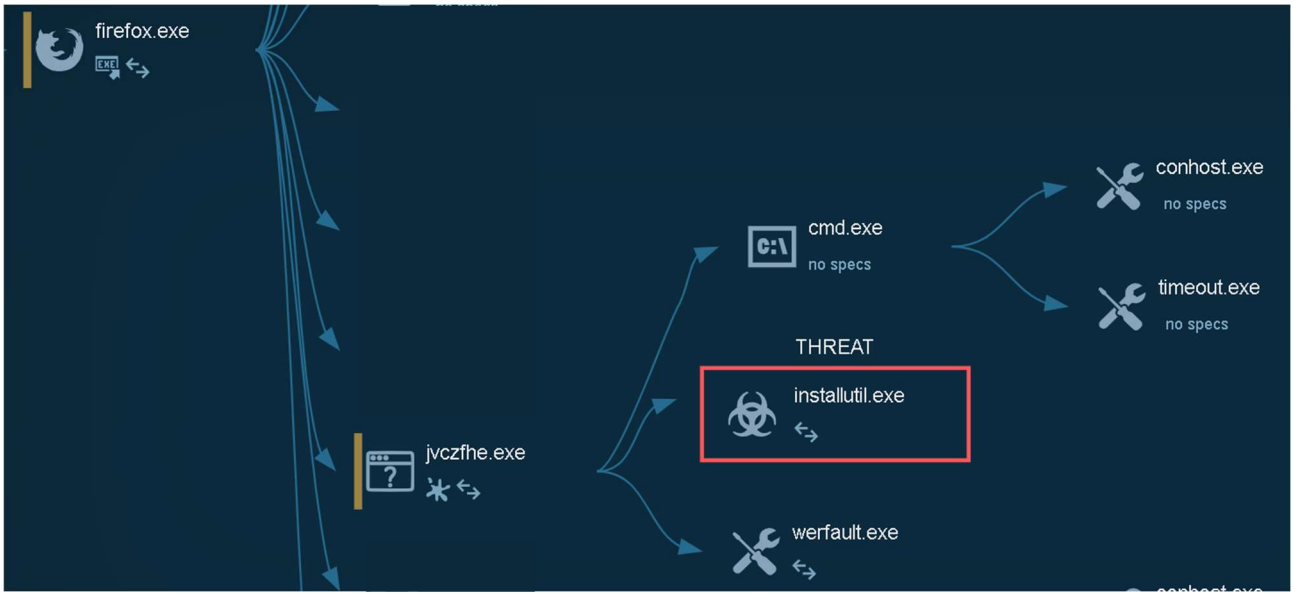


E infine mette in attesa il Promt dei comandi (CMD) per 21 secondi per poi chiuderlo (EXIT).

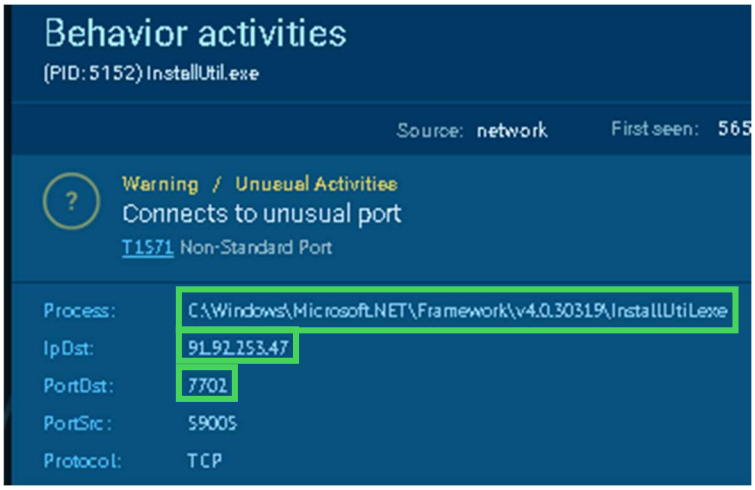


Quindi, il file Jvczfhe.exe quando eseguito legge le impostazioni di fiducia di windows e rallenta il rilevamento da parte del sistema operativo.

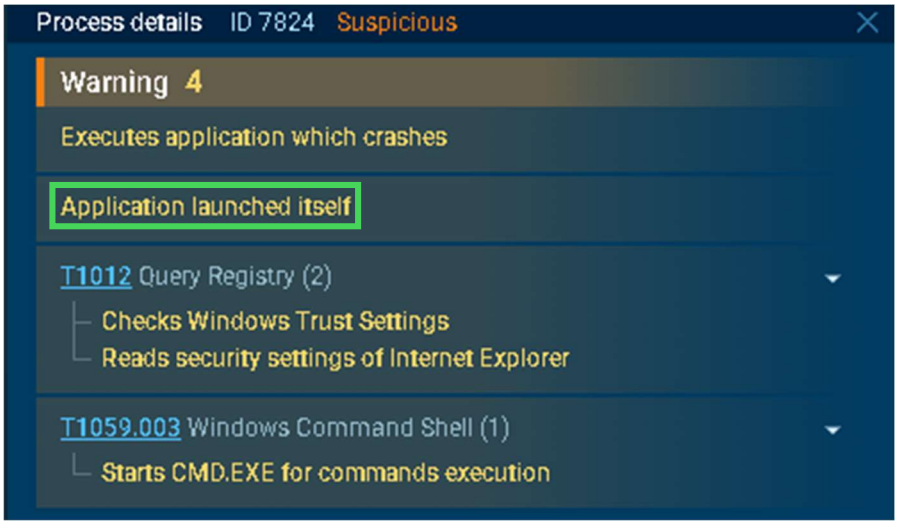
Andando a visionare il grafico:



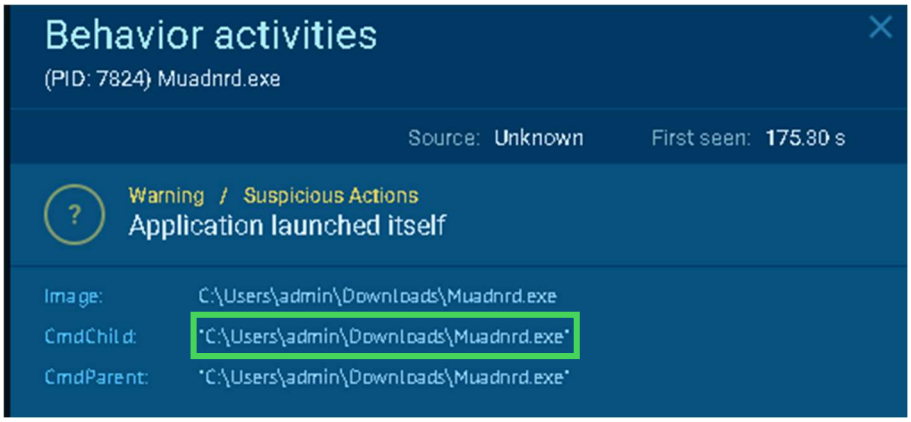
Viene evidenziato in rosso “installutil.exe” che è un programma legittimo di Windows utilizzata per l'installazione di componenti del framework .NET che viene usata da malintenzionati per comunicare con un server di comando e controllo (C&C) (in questo caso un server con indirizzo 91.92.253.47 alla porta 7702) o per eseguire esfiltrazione di dati o esecuzione di payload malevoli.



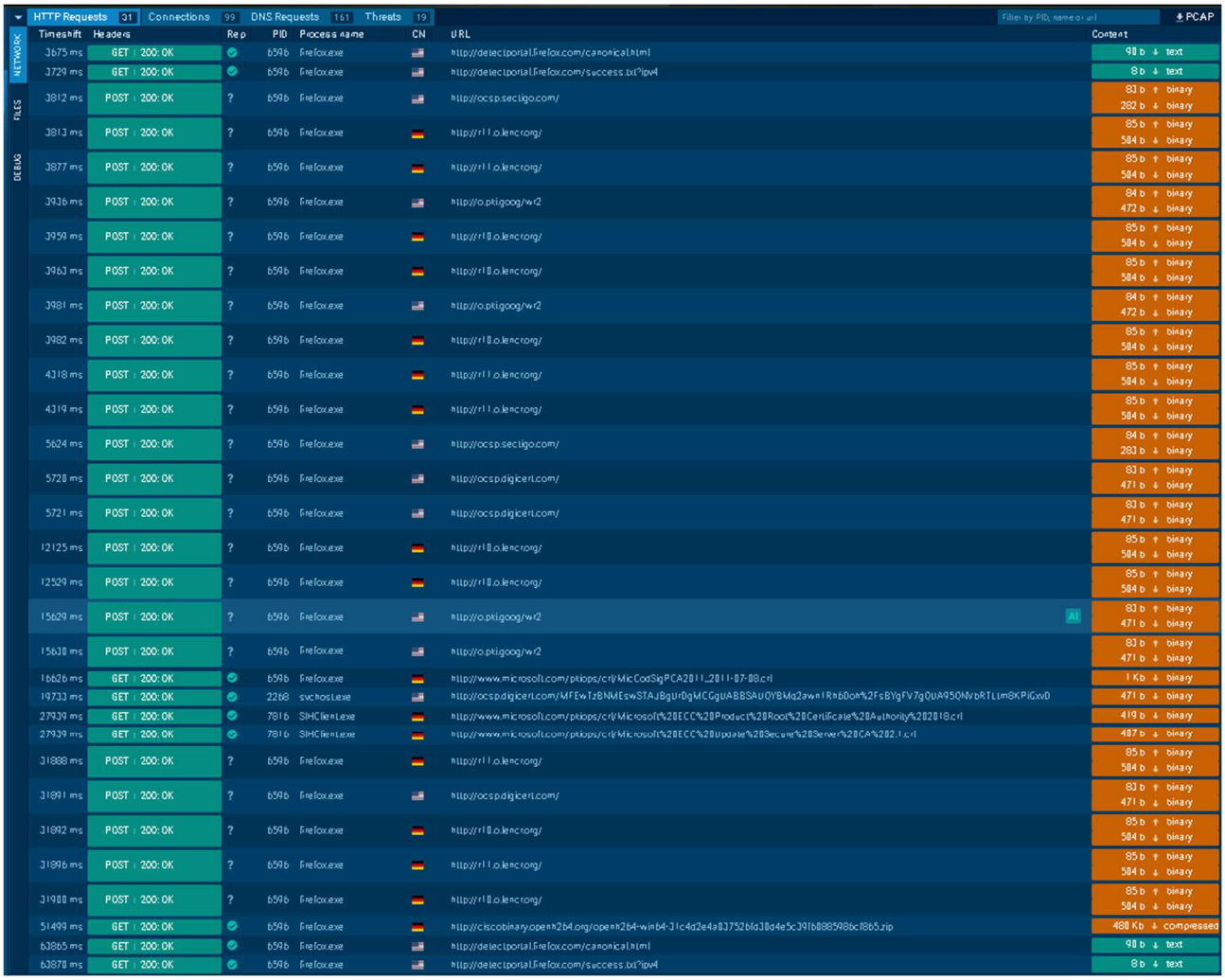
Successivamente, il file “firefox.exe” esegue poi un download di Muadrnd.exe, sempre tramite una pagina di GitHub, che ha dei comportamenti rilevati sospetti molto simili a quelli del precedente file Jvczfhe.exe analizzato:



Dove però è presente un comportamento dove Muadrnd.exe avvia sé stesso. Questo comportamento è un comportamento tipico di malware che si auto-esegue, spesso come parte di una tecnica per mantenere la persistenza sul sistema ed evitare la rimozione.



Infine, andando a visualizzare il traffico di rete:

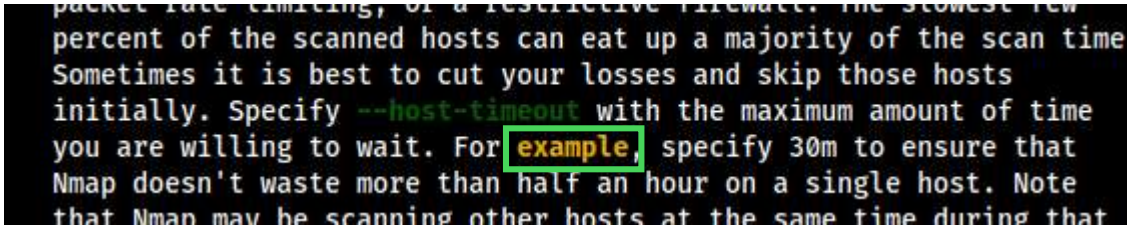


Possiamo notare con vengono fatte tante richieste POST e GET verso dei server relativi agli indirizzi "ilc.org", "ospeciico.com" il che mi fa pensare che si tratti di due server di Comando e Controllo che inviano dati in binario, tramite richiesto POST, contenenti payload malevoli e ricevono informazioni tramite richieste POST di dati sempre in binario.

Concludendo, mi sembra si tratti di un malware che avvia in autorun una pagina di Firefox per installare da GitHub due file Jvczfhe.exe e Muadrnd.exe che cercano di rallentare il rilevamento dai sistemi di sicurezza del sistema operativo e mantengono la persistenza sul sistema tramite Muadrnd.exe che fa varie chiamate a sé stesso e utilizza Jvczfhe.exe per avviare installutil.exe e installare altri payload malevoli.
Il malware poi è controllato da due server C&C ilc.org e ospeciico.com che ricevono informazioni sul sistema target e inviano payload malevoli.

Bonus 1

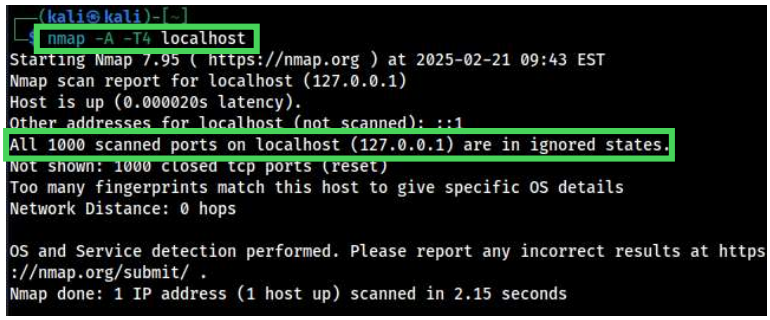
Il bonus spiega alcuni passaggi su come utilizzare nmap.
Il primo passo è quello di aprire il manuale usando il comando man nmap.
All'interno del manuale ci si sposta con le frecce direzionali, mentre con la barra spaziatrice si scorre una pagina avanti. Viene anche spiegato che, se si volesse cercare una parola basta premere / oppure ?. la barra consente di cercare avanti nel documento, mentre il punto interrogativo consente di cercare indietro nel documento.
Digitando infatti /example, verrà cercata la parola example all'interno del manuale di nmap:



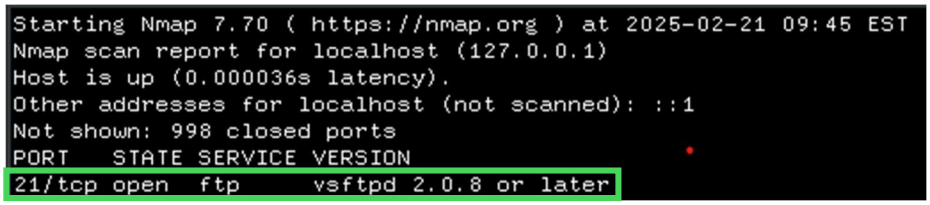
Vengono infatti evidenziate in giallo tutte le parole example contenute all'interno del manuale.
Per passare alla corrispondenza successiva, basta premere "n" e per uscire basta premere "q".

Dop aver visionato il manuale, possiamo dire che il comando "nmap -A -T4 scanme.nmap.org serve per effettuare una scansione verso il sito nmap.org, lo switch -A abilita il rilevamento del sistema operativo, lo switch -T4 serve per eseguire rapidamente la scansione.

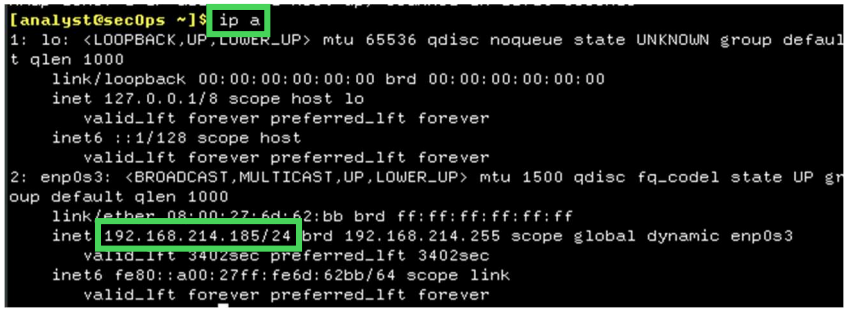
Con nmap è possibile effettuare una scansione al proprio localhost usando il comando
nmap -A -T4 localhost



Nella macchina kali linux su cui ho effettuato la scansione non è risultata nessuna porta aperta, mentre usando la macchina CyberOps Workstation indicata nella guida:

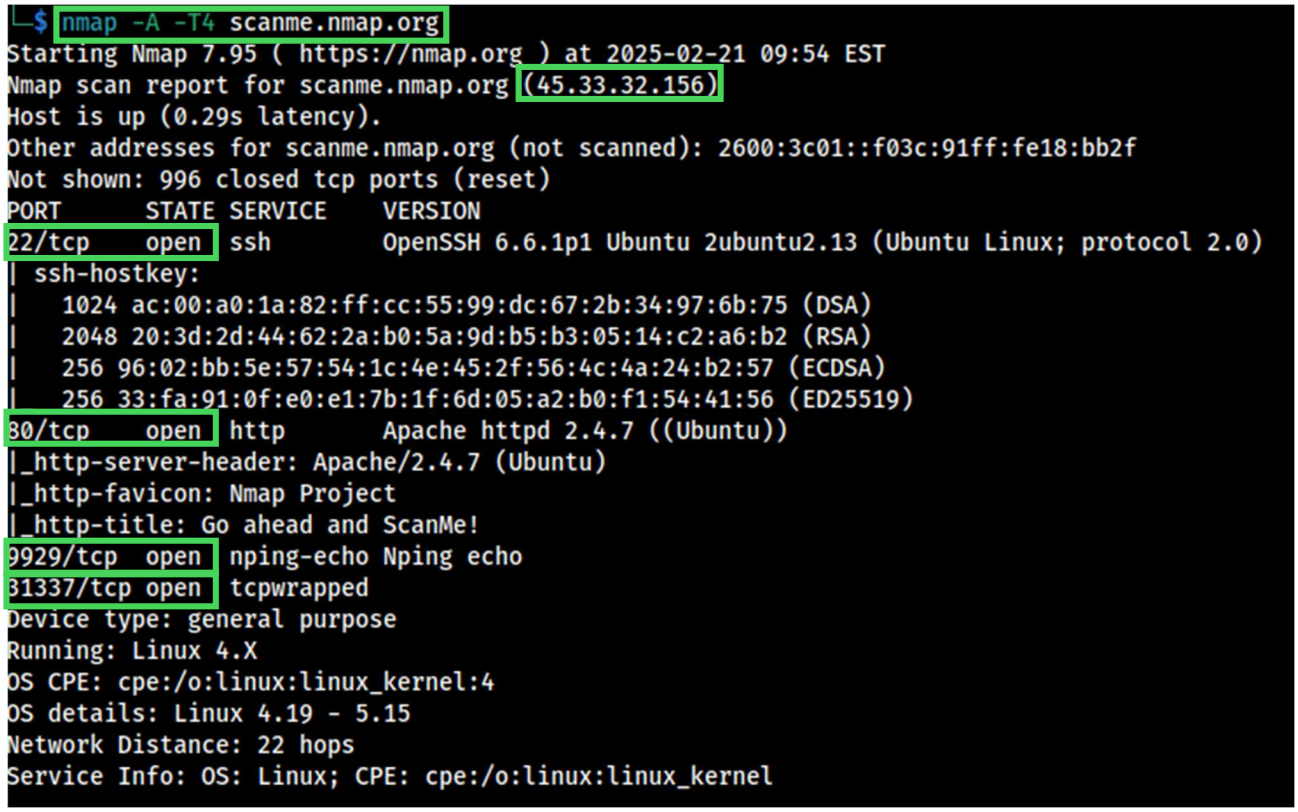


Viene visualizzata la porta 21 aperta.
Successivamente, tramite il comando "ip a" possiamo visualizzare informazioni sul network dell'host corrente:



E per visualizzare altri dispositivi presenti all'interno della stessa rete, basta mettere l'indirizzo IP della rete attuale seguito da \24 che sta ad indicare la Subnet mask.

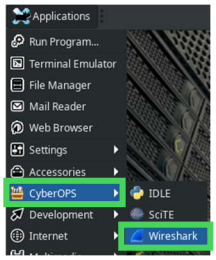
Ora effettuo una scansione sul server remoto scanme.nmap.org:



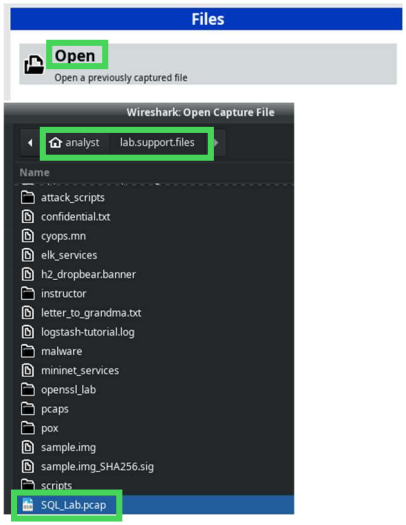
E possiamo vedere che le porte aperte sono 4 e sono le porte 22 tcp, 80 tcp:http, 9929 tcp, 31337 tcp. Viene visualizzato anche l'indirizzo IP del server che è il 45.33.32.156 e ha Ubuntu Linux come sistema operativo.

Bonus 2

Per il bonus numero 2 viene chiesto di aprire Wireshark sulla macchina virtuale CyberOps Workstation

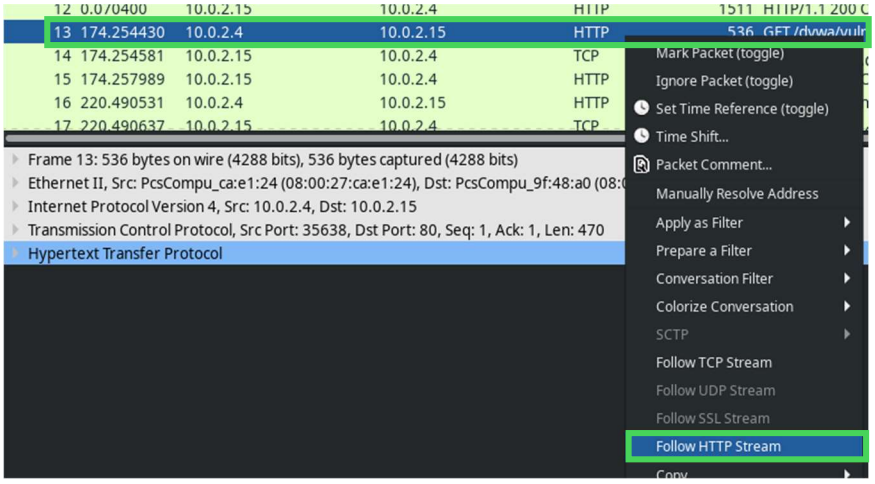


Successivamente, tramite il pulsante Open, aprire il file SQL_Lab.pcap al path /home/analystlab.support.files:

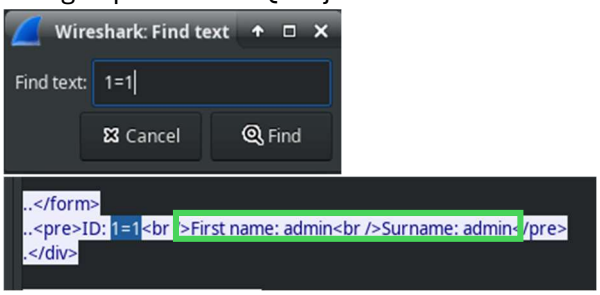


All'interno di questa cattura, gli indirizzi IP coinvolti sono 10.0.2.4 e 10.0.2.15.

Successivamente viene indicato di cliccare col tasto destro del mouse la riga 13 e successivamente su Follow HTTP Stream:

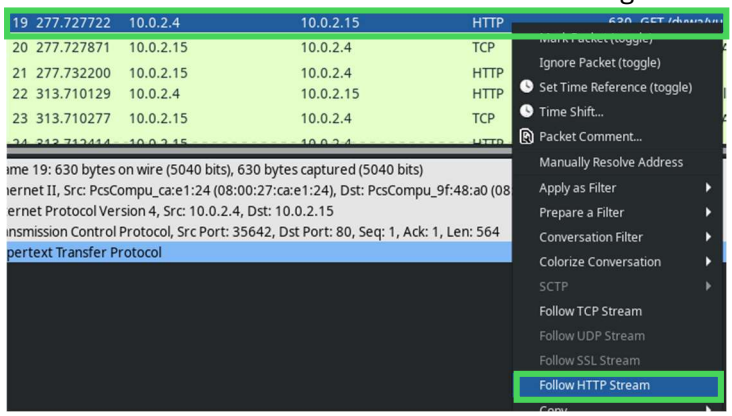


Allinterno di questa finestra possiamo vedere come viene rappresentata una richiesta GET, evidenziata in rosso, effettuata dalla macchina con indirizzo IP10.0.2.15 verso la macchina con indirizzo IP 10.0.1.4 che ha risposto con il codice HTTP evidenziato in blu.
Per visualizzare la stringa della SQL Injection basta cliccare sul tasto Find e cercare “1=1” che è una stringa tipica delle SQL injection:

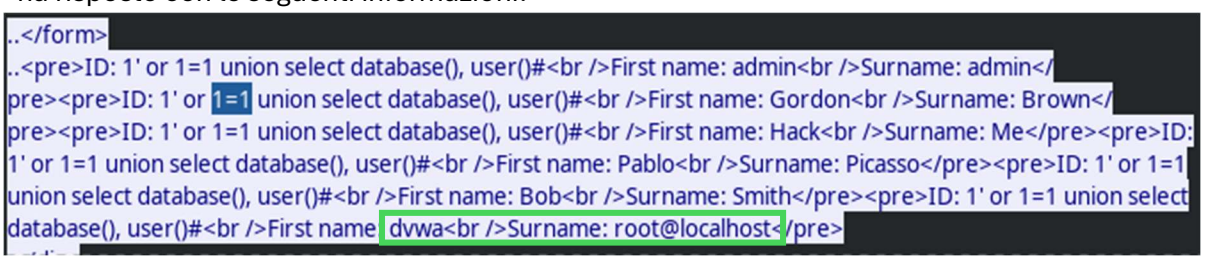


E possiamo vedere come nella risposta è presente un record da un database e non un messaggio di errore.

Successivamente viene chiesto di analizzare la riga 19 usando il tasto destro del mouse:

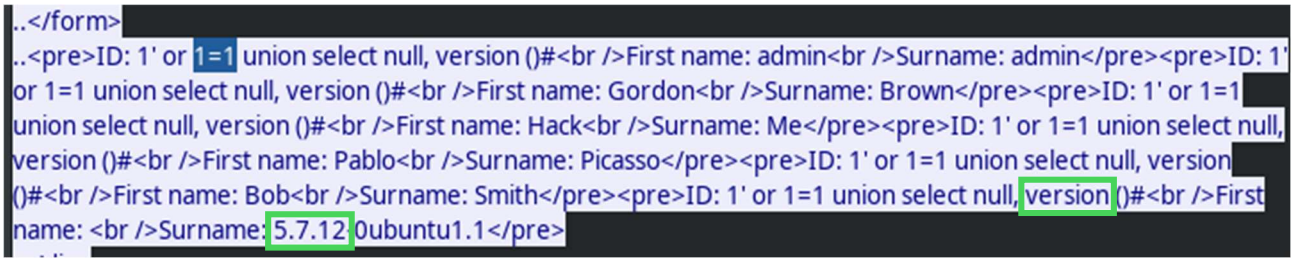


Usiamo lo stesso metodo usato precedentemente per cercare la stringa della SQL Injection e troviamo che l'attaccante ha inserito una query (1' o 1=1 union select database(), user()#) in una casella di ricerca sulla destinazione 10.0.2.15 che, invece di rispondere con un messaggio di errore di accesso, ha risposto con le seguenti informazioni:



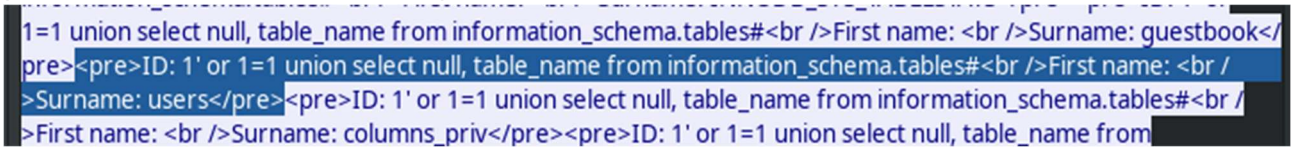
Dove viene specificato il nome del database che è dvwa, l'utente del database root@localhost e altri account utente.

Ci viene adesso chiesto di visualizzare i dettagli presenti alla riga 22 e usando gli stessi passaggi fatti precedentemente:



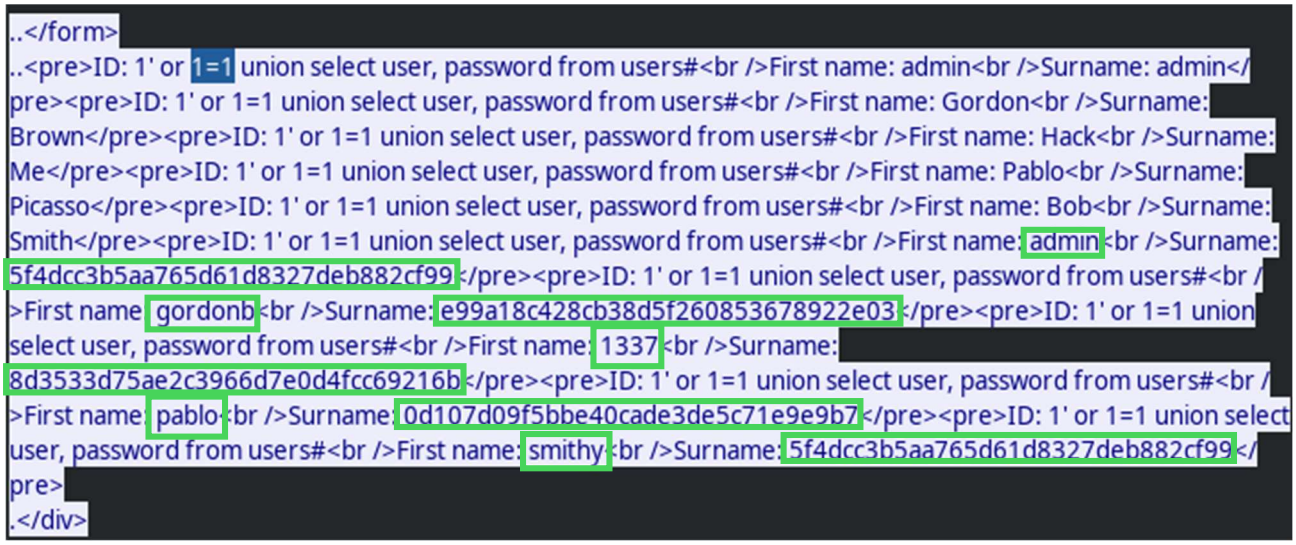
Che l'attaccante ha inserito la query (1' o 1=1 union select null, version ()#) in una casella di ricerca sul target 10.0.2.15 per individuare l'identificativo della versione che si trova alla fine.

Viene successivamente richiesto di analizzare la riga 25 usando gli stessi procedimenti fatti precedentemente ma cercando la parola chiave users:



E possiamo notare come l'attaccante abbia inserito la query (1'or 1=1 union select null, table_name from information_schema.tables#) per visualizzare tutte le tabelle all'interno del database.

Viene infine chiesto di analizzare la riga 28 seguendo gli stessi procedimenti fatti precedentemente:



E possiamo notare come l'aggressore abbia inserito la query (1'or 1=1 union select user, password from users#) per estrarre nomi utente e hash delle password