RDP Brute Force Detection and Active Response using Wazuh

Introduction

Remote Desktop Protocol (RDP) is widely used to remotely access Windows systems for administration and support purposes. Because RDP provides direct system access, it is often targeted by attackers using brute force techniques to guess usernames and passwords.

In this implementation, Wazuh is used to monitor RDP login activity on a Windows system, detect brute force attempts, generate alerts, and automatically block the attacker's IP address using Active Response.

Objective

The main objectives of this implementation are:

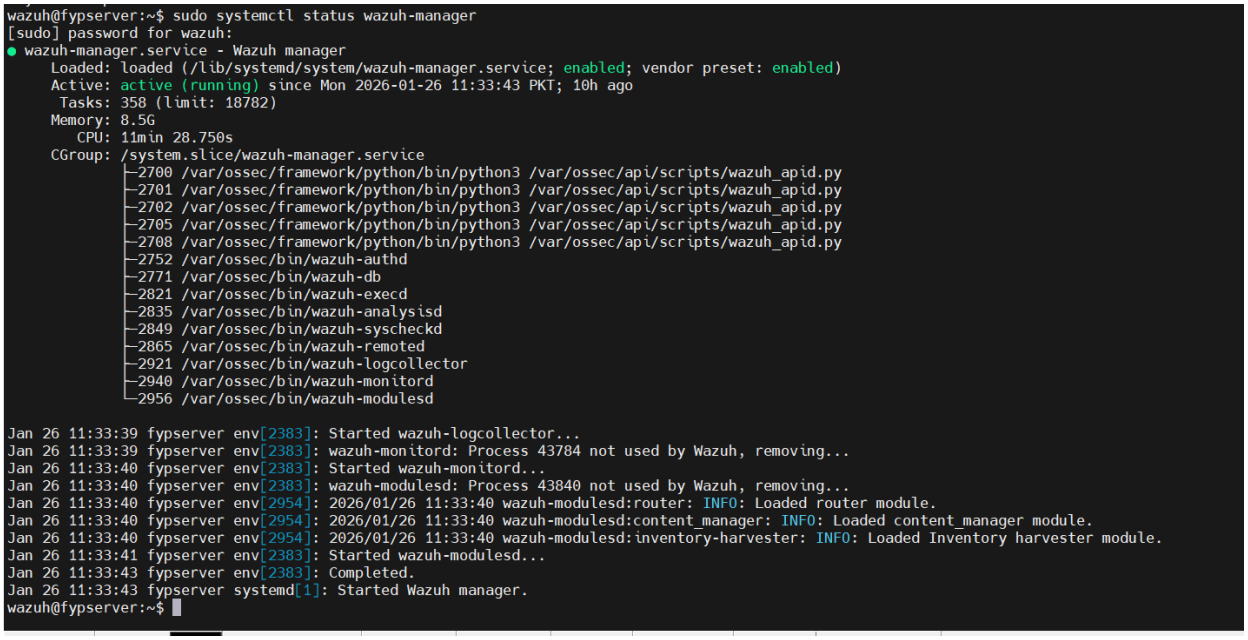
- Enable Remote Desktop (RDP) on a Windows system
- Monitor RDP login attempts using Wazuh
- Detect RDP brute force attacks based on failed login attempts
- Automatically block attacker IP addresses using Active Response
- Display alerts and responses on the Wazuh Dashboard

Step-by-Step Methodology

Verify Wazuh Manager Status

Ensure the Wazuh Manager is running properly.

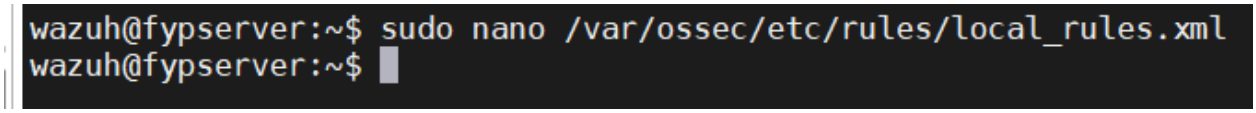
```
sudo systemctl status wazuh-manager
```



Step 2: Configure RDP Detection Rules on Wazuh Manager

Edit the custom rules file:

```
sudo nano /var/ossec/etc/rules/local_rules.xml
```



Add the following rules:

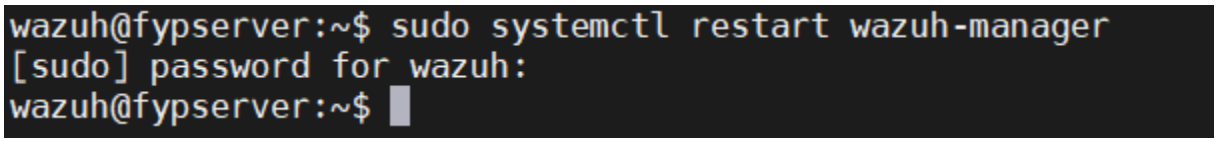
```
<group name="rdp">
  <rule id="60122" level="0">
    <decoded_as>eventchannel</decoded_as>
    <field name="event_id">4625</field>
    <field name="logon_type">10</field>
    <description>RDP Failed Login (for correlation
only)</description>
    <options>no_full_log</options>
  </rule>
</group>

<group name="rdp">
```

```
  <rule id="100111" level="10" frequency="3" timeframe="120">
    <if_matched_sid>60122</if_matched_sid>
    <description>RDP Bruteforce Attack Detected</description>
  </rule>
</group>
```

Save and exit the file.

Restart the Wazuh Manager:

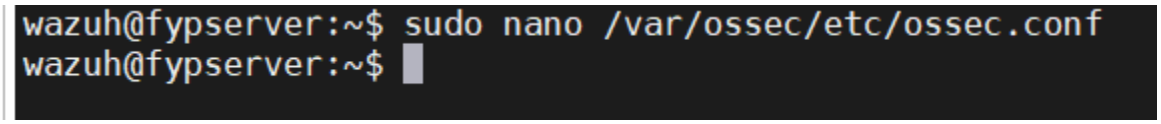
```
sudo systemctl restart wazuh-manager
```



Step 3: Register Active Response Command on Manager

Edit the Wazuh Manager configuration file:

```
sudo nano /var/ossec/etc/ossec.conf
```



Add the following command:

```
<command>
  <name>netsh</name>
  <executable>netsh.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
```

```
</command>
```

```
GNU nano 6.2                                                /var/ossec/etc/ossec.conf *

<command>
   <name>netsh</name>
   <executable>netsh.exe</executable>
   <timeout_allowed>yes</timeout_allowed>
</command>
```

Step 4: Configure Active Response Trigger on Manager

In the same file, add:

```
<active-response>
  <disabled>no</disabled>
  <command>netsh</command>
  <location>local</location>
  <rules_id>100111</rules_id>
  <timeout>86400</timeout>
</active-response>
```

```
GNU nano 6.2                                                /var/ossec/etc/ossec.conf *
<command>
   <name>netsh</name>
   <executable>netsh.exe</executable>
   <timeout_allowed>yes</timeout_allowed>
</command>
<active-response>
  <disabled>no</disabled>
  <command>netsh</command>
  <location>local</location>
  <rules_id>100111</rules_id>
  <timeout>86400</timeout>
</active-response>
```

Save the file and restart the manager:

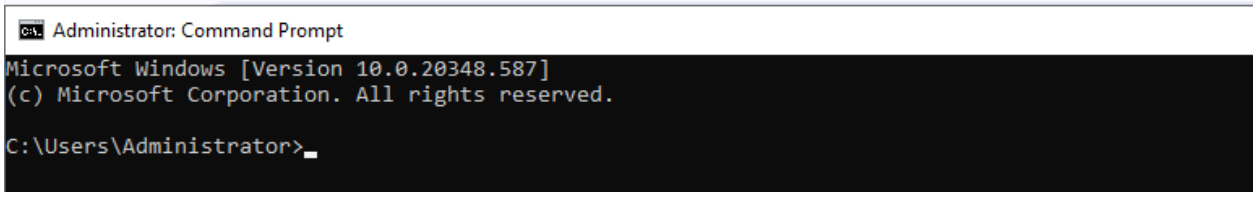
```
sudo systemctl restart wazuh-manager
```

```
wazuh@fypserver:~$ sudo systemctl restart wazuh-manager
wazuh@fypserver:~$
```

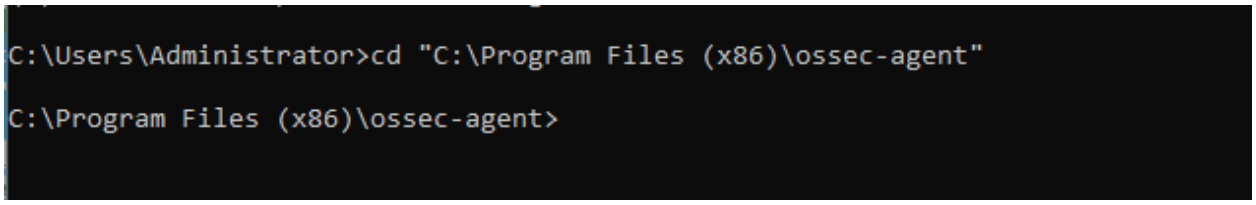
Step 5: Configure Wazuh Agent on Windows System

Open Command Prompt as Administrator.

Navigate to the agent directory:

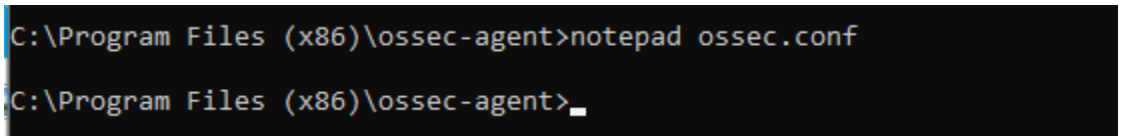



```
cd "C:\Program Files (x86)\ossec-agent"
```



Edit the agent configuration file:

```
notepad ossec.conf
```



Add the following configuration:

```
<active-response>
  <disabled>no</disabled>
  <command>netsh</command>
  <rules_id>100111</rules_id>
  <timeout>86400</timeout>
</active-response>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
</localfile>
```

*ossec - Notepad

File Edit Format View Help

```
<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <bin_path>C:\Program Files\osquery\osqueryd</bin_path>
  <log_path>C:\Program Files\osquery\log\osqueryd.results.log</log_path>
  <config_path>C:\Program Files\osquery\osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>
<active-response>
  <disabled>no</disabled>
  <command>netsh</command>
  <rules_id>100111</rules_id>
  <timeout>86400</timeout>
</active-response>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Save the file.

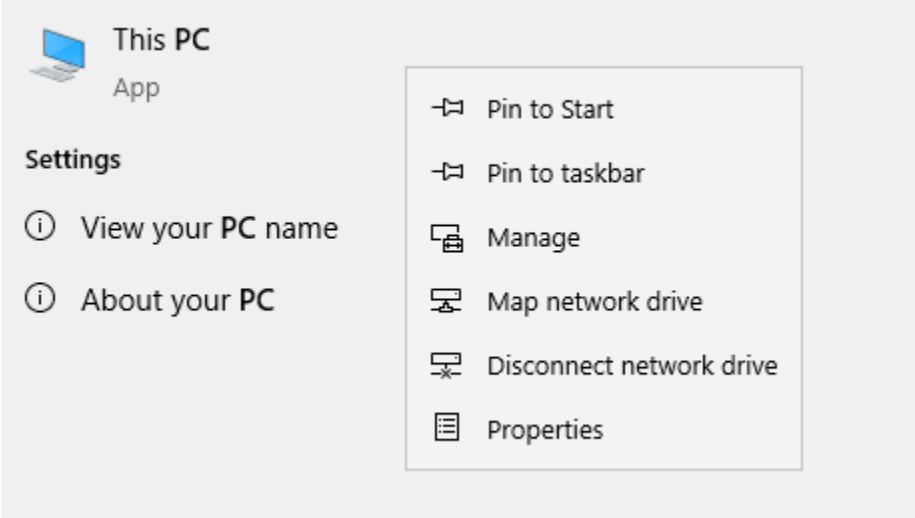
Restart the Wazuh Agent:

```
Restart-Service -Name wazuh
```

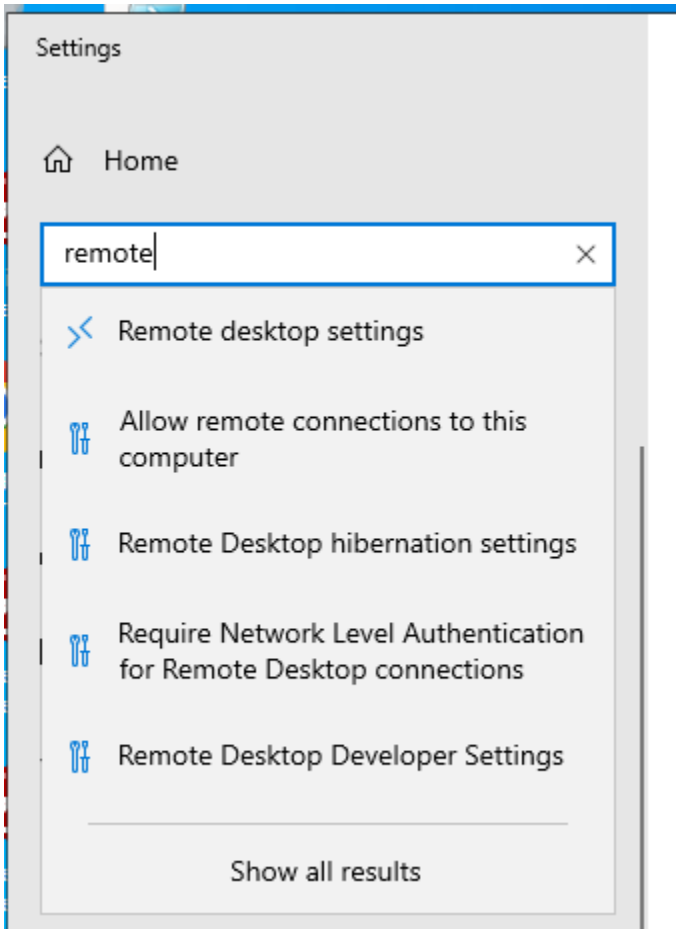
```
PS C:\Users\Administrator> Restart-Service -Name wazuh
PS C:\Users\Administrator>
```

Step 6: Enable Remote Desktop (RDP) on Windows

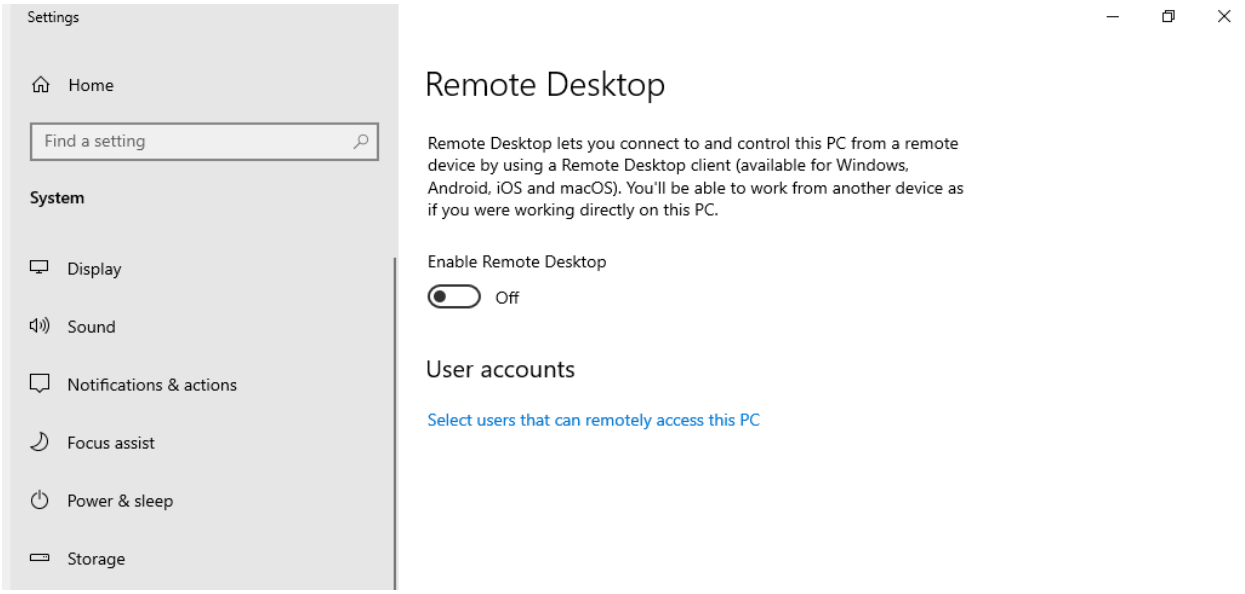
1. Right-click This PC → Properties



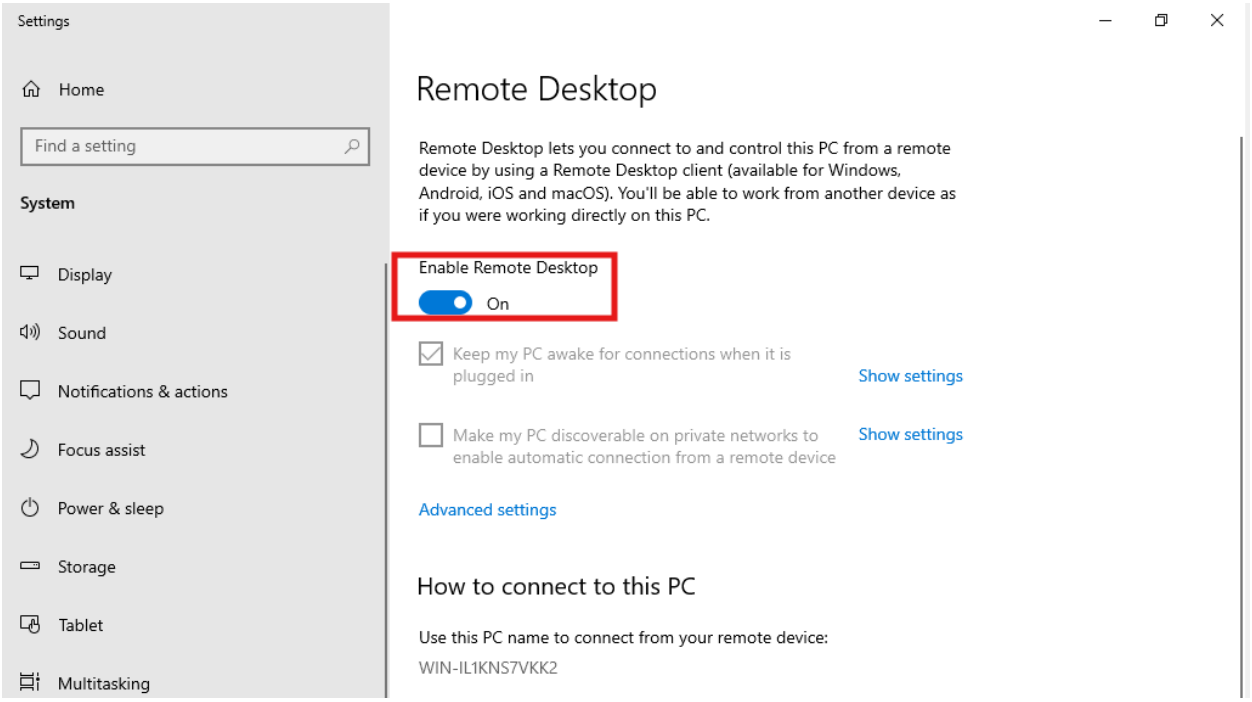
2. In the left-hand menu, open Remote Desktop settings.



3. Open Remote Desktop settings



4. Turn ON Remote Desktop



(Optional for testing)
Disable Network Level Authentication if required.

Step 7: Prepare Attacker Machine

Install Hydra on a Linux system:

```
sudo apt update
```

```
wazuh@fypserver:~$ sudo apt update
[sudo] password for wazuh:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 https://packages.wazuh.com/4.x/apt stable InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [112 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/restricted i386 Packages [52.7 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [5,110 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [958 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 DEP-11 Metadata [212 B]
Get:11 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [359 kB]
Get:12 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [59.0 kB]
Get:13 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse i386 Packages [8,984 B]
Get:14 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [13.5 kB]
Get:15 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:16 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [7,296 B]
Get:17 http://archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 DEP-11 Metadata [212 B]
Get:18 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [10.2 kB]
Get:19 http://archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 DEP-11 Metadata [212 B]
Get:20 http://archive.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [54.5 kB]
Get:21 http://archive.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Get:22 http://archive.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [125 kB]
Get:23 http://archive.ubuntu.com/ubuntu jammy-security/multiverse amd64 DEP-11 Metadata [208 B]
Fetched 7,257 kB in 14s (502 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
18 packages can be upgraded. Run 'apt list --upgradable' to see them.
wazuh@fypserver:~$
```

```
sudo apt install hydra
```

```
wazuh@fypserver:~$ sudo apt install hydra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.2-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 18 not upgraded.
wazuh@fypserver:~$
```

Create username and password files:

```
echo "administrator" > user.txt
echo "123456" > pass.txt
echo "password" >> pass.txt
```

```
wazuh@fypserver:~$ sudo su
root@fypserver:/home/wazuh# echo "administrator" > user.txt
echo "123456" > pass.txt
echo "password" >> pass.txt
root@fypserver:/home/wazuh#
```

Step 8: Perform RDP Brute Force Attack

Run the attack command:

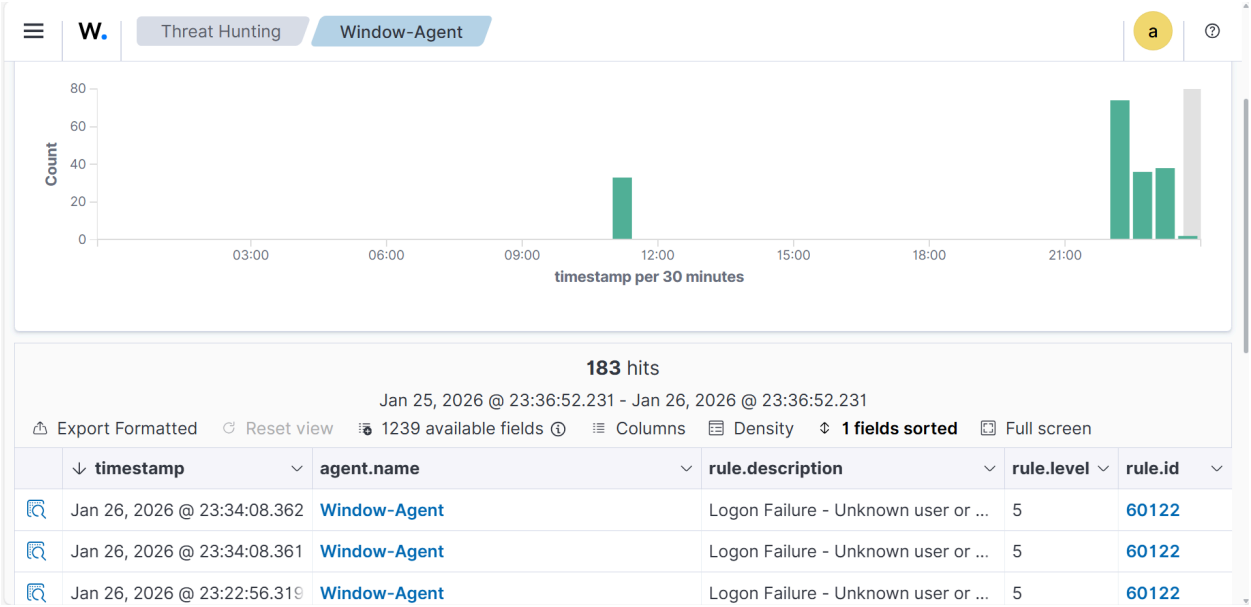
```
hydra -L user.txt -P pass.txt -t 1 rdp://<WINDOWS_IP>
hydra -L user.txt -P pass.txt -t 1 rdp://10.10.10.241
```

```
root@fypserver:/home/wazuh# hydra -L user.txt -P pass.txt -t 1 rdp://10.10.10.241
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-26 23:22:54
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 2 login tries (l:1/p:2), ~2 tries per task
[DATA] attacking rdp://10.10.10.241:3389/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-26 23:22:55
root@fypserver:/home/wazuh#
```

Step 9: Monitor Alerts on Wazuh Dashboard

1. Open Wazuh Dashboard
2. Go to Threat Hunting / Security Events

At first I tried from the attacker machine only with one user name and password and so only one failed login alert came in the dashboard and no active response trigger.



Details:

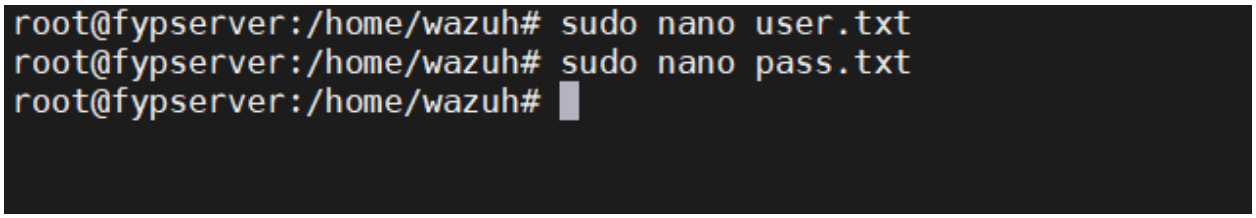
Table JSON

@timestamp	Jan 26, 2026 @ 23:34:08.361
_index	wazuh-alerts-4.x-2026.01.26
agent.id	001
agent.ip	10.10.10.241
agent.name	Window-Agent
data.win.eventdata.authenticationPackageName	NTLM
data.win.eventdata.failureReason	%%2313
data.win.eventdata.ipAddress	10.10.10.240
data.win.eventdata.ipPort	0
data.win.eventdata.keyLength	0
data.win.eventdata.logonProcessName	NtLmSsp
data.win.eventdata.logonType	3
data.win.eventdata.targetUserName	administrator
data.win.eventdata.targetUserSid	S-1-0-0
data.win.eventdata.workstationName	fypserver
data.win.system.channel	Security
data.win.system.computer	WIN-IL1KNS7VKK2
data.win.system.eventID	4625
data.win.system.eventRecordID	27133
data.win.system.keywords	0x8010000000000000
data.win.system.level	0
data.win.system.message	"An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0

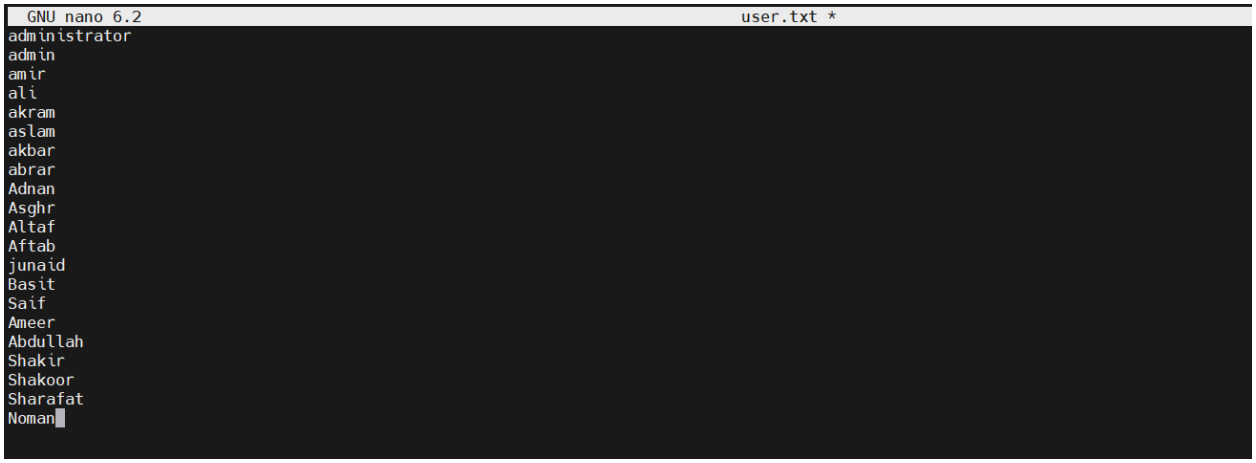
t	data.win.system.providerName	Microsoft-Windows-Security-Auditing
t	data.win.system.severityValue	AUDIT_FAILURE
t	data.win.system.systemTime	2026-01-27T07:34:04.7987116Z
t	data.win.system.task	12544
t	data.win.system.threadID	5716
t	data.win.system.version	0
t	decoder.name	windows_eventchannel
t	id	1769452448.20667486
t	input.type	log
t	location	EventChannel
t	manager.name	fypserver
t	rule.description	Logon Failure - Unknown user or bad password
#	rule.firedtimes	3
t	rule.gdpr	IV_35.7.d, IV_32.2

Now I try with many user name and password for triggering the active response:

First I create the user list on attacker machine:

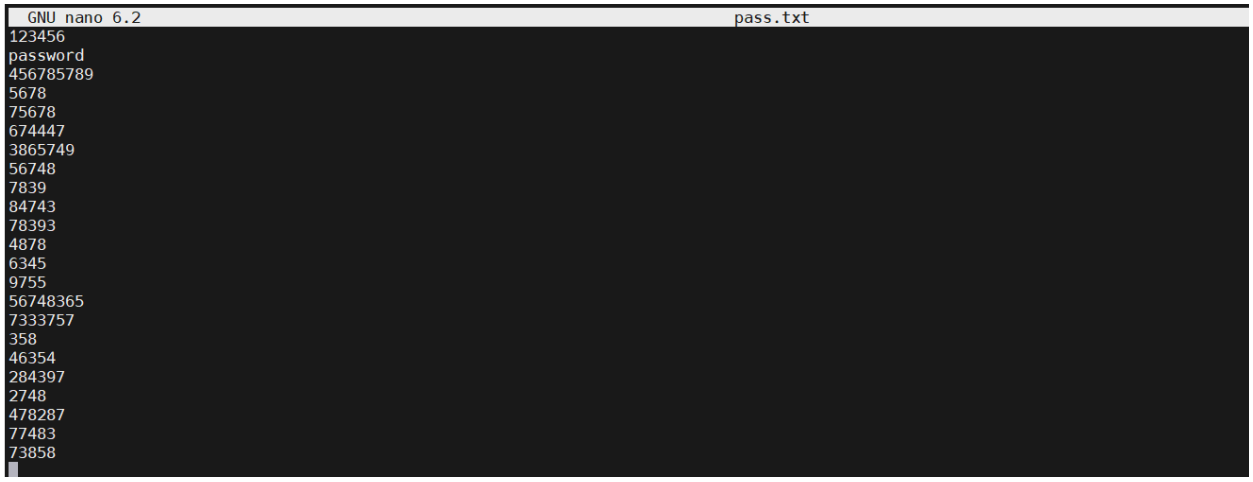


sudo nano user.txt



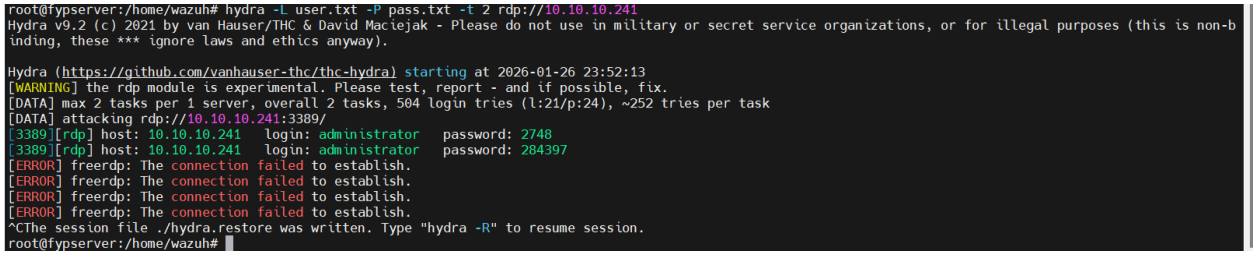
Then I create the password list:

sudo nano pass.txt



Now again tried the attack on Agent machine:

hydra -L user.txt -P pass.txt -t 2 rdp://10.10.10.241



Now I launched an RDP brute-force attack using Hydra with two parallel attempts (-t 2). After two failed login attempts, Wazuh generated alerts and immediately triggered Active Response, which blocked the attacker IP.
Once the IP was blocked, Hydra started showing “connection failed to establish” errors because the Windows firewall denied further RDP connections.

Step 10: Verify IP Blocking on Windows Agent

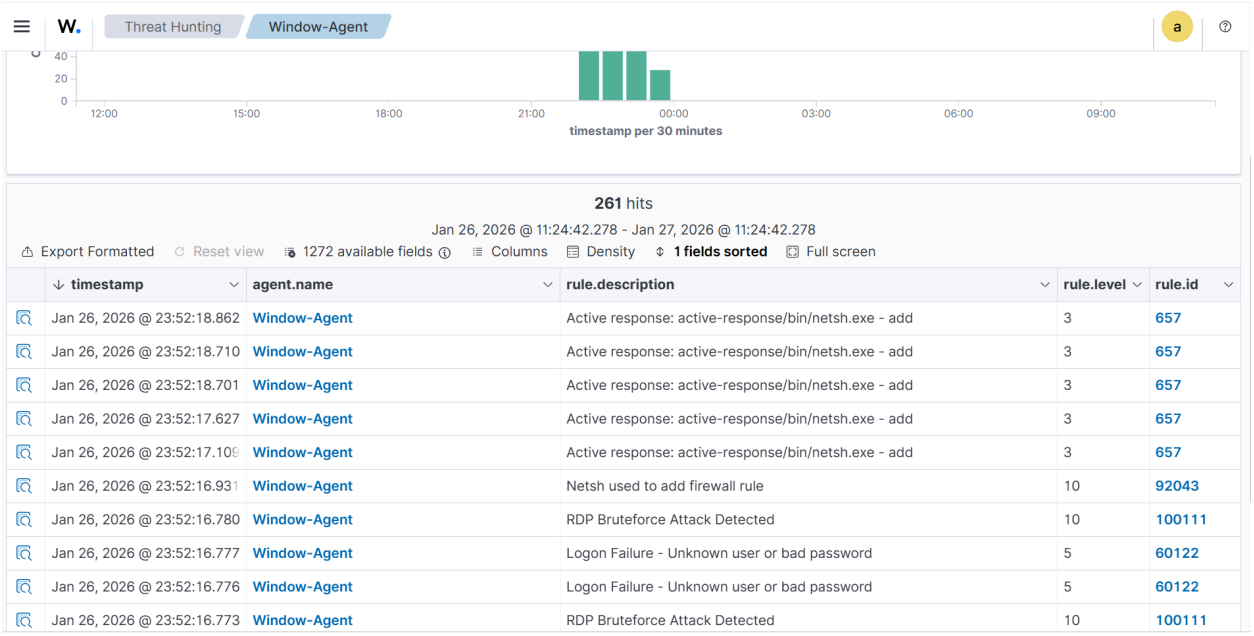
Check firewall rules:

netsh advfirewall firewall show rule name=all | findstr 10.10.10.240

```
C:\Users\Administrator>

C:\Users\Administrator>netsh advfirewall firewall show rule name=all | findstr 10.10.10.240
RemoteIP:                             10.10.10.240/32

C:\Users\Administrator>
```

Confirm that the attacker IP is blocked.

Now we see the alerts in the Wazuh Dashboard:



timestamp	agent.name	rule.description	rule.level	rule.id
Jan 26, 2026 @ 23:52:18.862	Window-Agent	Active response: active-response/bin/netsh.exe - add	3	657
Jan 26, 2026 @ 23:52:18.710	Window-Agent	Active response: active-response/bin/netsh.exe - add	3	657
Jan 26, 2026 @ 23:52:18.701	Window-Agent	Active response: active-response/bin/netsh.exe - add	3	657
Jan 26, 2026 @ 23:52:17.627	Window-Agent	Active response: active-response/bin/netsh.exe - add	3	657
Jan 26, 2026 @ 23:52:17.109	Window-Agent	Active response: active-response/bin/netsh.exe - add	3	657
Jan 26, 2026 @ 23:52:16.931	Window-Agent	Netsh used to add firewall rule	10	92043
Jan 26, 2026 @ 23:52:16.780	Window-Agent	RDP Bruteforce Attack Detected	10	100111
Jan 26, 2026 @ 23:52:16.777	Window-Agent	Logon Failure - Unknown user or bad password	5	60122
Jan 26, 2026 @ 23:52:16.776	Window-Agent	Logon Failure - Unknown user or bad password	5	60122
Jan 26, 2026 @ 23:52:16.773	Window-Agent	RDP Bruteforce Attack Detected	10	100111

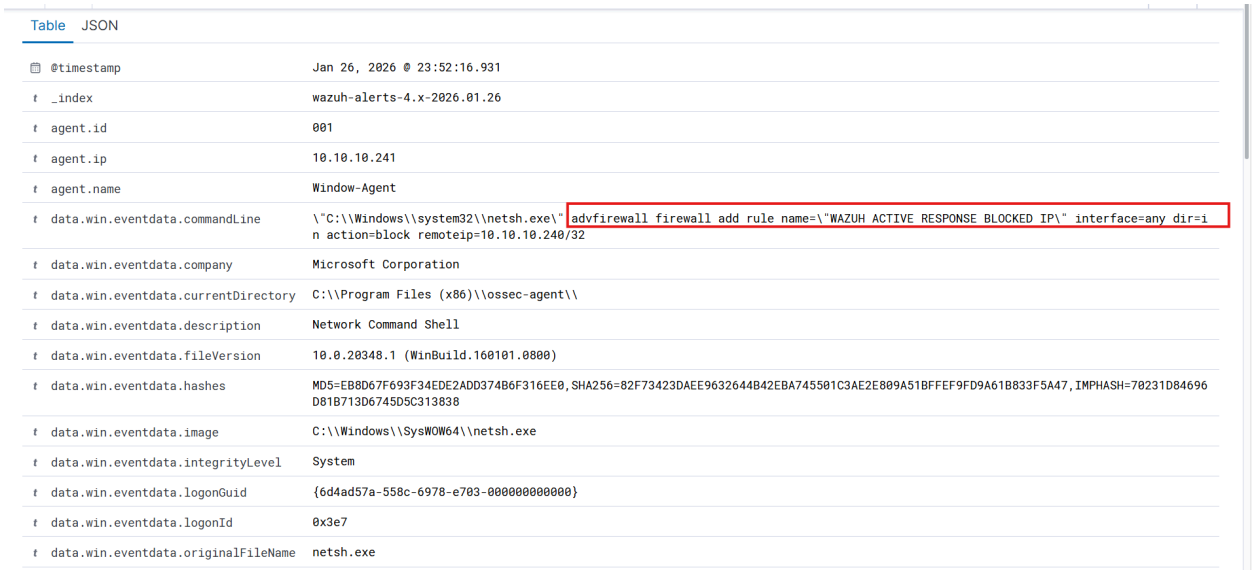


Table JSON

@timestamp	Jan 26, 2026 @ 23:52:16.931
_index	wazuh-alerts-4.x-2026.01.26
agent.id	001
agent.ip	10.10.10.241
agent.name	Window-Agent
data.win.eventdata.commandLine	\"C:\\Windows\\system32\\netsh.exe\" advfirewall firewall add rule name=\"WAZUH ACTIVE RESPONSE BLOCKED IP\" interface=any dir=in action=block remoteip=10.10.10.240/32
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\Program Files (x86)\\ossec-agent\\
data.win.eventdata.description	Network Command Shell
data.win.eventdata.fileVersion	10.0.20348.1 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=EB8D67F693F34EDE2ADD374B6F316EE0,SHA256=82F73423DAEE9632644B42EBA745501C3AE2E809A51BFFEF9FD9A61B833F5A47,IMPHASH=70231D84696D81B713D6745D5C313838
data.win.eventdata.image	C:\\Windows\\SysWOW64\\netsh.exe
data.win.eventdata.integrityLevel	System
data.win.eventdata.logonGuid	{6d4ad57a-558c-6978-e703-000000000000}
data.win.eventdata.logonId	0x3e7
data.win.eventdata.originalFileName	netsh.exe

Details of alerts:

Table JSON

@timestamp	Jan 26, 2026 @ 23:52:18.862
_index	wazuh-alerts-4.x-2026.01.26
agent.id	001
agent.ip	10.10.10.241
agent.name	Window-Agent
data.command	add
data.origin.module	wazuh-execd
data.origin.name	node01
data.parameters.alert.agent.id	001
data.parameters.alert.agent.ip	10.10.10.241
data.parameters.alert.agent.name	Window-Agent
data.parameters.alert.data.win.eventdata.authenticationPackageName	NTLM
data.parameters.alert.data.win.eventdata.failureReason	%%2313
data.parameters.alert.data.win.eventdata.ipAddress	10.10.10.240
data.parameters.alert.data.win.eventdata.ipPort	0
data.parameters.alert.data.win.eventdata.keyLength	0
data.parameters.alert.data.win.eventdata.logonProcessName	NtLmSsp

t data.parameters.alert.data.win.eventdata.subjectUserSid	S-1-0-0
t data.parameters.alert.data.win.eventdata.targetUserName	administrator
t data.parameters.alert.data.win.eventdata.targetUserSid	S-1-0-0
t data.parameters.alert.data.win.eventdata.workstationName	fypserver
t data.parameters.alert.data.win.system.channel	Security
t data.parameters.alert.data.win.system.computer	WIN-IL1KNS7VKK2
t data.parameters.alert.data.win.system.eventID	4625
t data.parameters.alert.data.win.system.eventRecordID	27158
t data.parameters.alert.data.win.system.keywords	0x8010000000000000
t data.parameters.alert.data.win.system.level	0
t data.parameters.alert.data.win.system.message	› "An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0
t data.parameters.alert.data.win.system.opcode	0
t data.parameters.alert.data.win.system.processID	684

t data.parameters.alert.data.win.system.providerGuid	{54849625-5478-4994-a5ba-3e3b0328c30d}
t data.parameters.alert.data.win.system.providerName	Microsoft-Windows-Security-Auditing
t data.parameters.alert.data.win.system.severityValue	AUDIT_FAILURE
t data.parameters.alert.data.win.system.systemTime	2026-01-27T07:52:13.8589007Z
t data.parameters.alert.data.win.system.task	12544
t data.parameters.alert.data.win.system.threadID	5000
t data.parameters.alert.data.win.system.version	0
t data.parameters.alert.decoder.name	windows_eventchannel
t data.parameters.alert.full_log	› {"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4625","version":"0","level":"0","task":"12544","opcode":"0","keywords":"0x8010000000000000","systemTime":"2026-01-27T07:52:13.8589007Z","eventRecordID":"27158","processID":"684","threadID":"5000","channel":"Security","computer":"WIN-IL1KNS7VKK2","severityValue":"AUDIT_FAILURE","message":"\"An account failed to log on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nLogon Type:\t\t\t3\r\n\r\nAccount For Which Logon Failed:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\t
t data.parameters.alert.id	1769453536.20840989
t data.parameters.alert.location	EventChannel
t data.parameters.alert.manager.name	fypserver

t data.parameters.alert.previous_output	{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4625","version":"0","level":"0","task":"12544","opcode":"0","keywords":"0x8010000000000000","systemTime":"2026-01-27T07:52:13.8578315Z","eventRecordID":"27157","processID":"684","threadID":"5000","channel":"Security","computer":"WIN-IL1KNS7VKK2","severityValue":"AUDIT_FAILURE","message":"\"An account failed to log on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nLogon Type:\t\t\t3\r\n\r\nAccount For Which Logon Failed:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\t
t data.parameters.alert.rule.description	RDP Bruteforce Attack Detected
t data.parameters.alert.rule.firedtimes	6
t data.parameters.alert.rule.frequency	3
t data.parameters.alert.rule.groups	rdp
t data.parameters.alert.rule.id	100111
t data.parameters.alert.rule.level	10
t data.parameters.alert.rule.mail	false
t data.parameters.alert.timestamp	2026-01-26T23:52:16.780+0500
t data.parameters.extra_args	
t data.parameters.program	active-response/bin/netsh.exe
t data.srcip	10.10.10.240
t data.version	1

t full_log	2026/01/26 23:52:16 active-response/bin/netsh.exe: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2026-01-26T23:52:16.780+0500","rule":{"level":10,"description":"RDP Bruteforce Attack Detected","id":"100111","frequency":3,"firedtimes":6,"mail":false,"groups":["rdp"]},"agent":{"id":"001","name":"Window-Agent","ip":"10.10.10.241"},"manager":{"name":"fypserver"},"id":"1769453536.20840989","previous_output":"{\"win\":{\"system\":{\"providerName\":\"Microsoft-Windows-Security-Auditing\",\"providerGuid\":\"{54849625-5478-4994-a5ba-3e3b0328c30d}\",\"eventID\":\"4625\",\"version\":\"0\",\"level
t id	1769453538.20962825
t input.type	log
t location	active-response\active-responses.log
t manager.name	fypserver
t rule.description	Active response: active-response/bin/netsh.exe - add
# rule.firedtimes	6
t rule.gdpr	IV_35.7.d
t rule.groups	ossec, active_response
t rule.id	657
# rule.level	3
rule.mail	false
t rule.nist_800_53	SI.4
t rule.pci_dss	11.4
t rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3, CC7.4

RDP Brute Force Detection and Blocking Wazuh Flow

- When someone tries to log in to a Windows system using RDP, Windows records this activity in the Security Event Logs.
- Every failed RDP login attempt generates a log with Event ID 4625. This log includes the username, source IP address, time, and logon type.
- Logon type 10 indicates that the login attempt was made through Remote Desktop (RDP).

- The Wazuh Agent installed on the Windows system continuously monitors these Security Event Logs in real time.

- The agent reads failed login events and extracts important details such as IP address, username, and timestamp.

- After collecting the log information, the Wazuh Agent securely sends it to the Wazuh Manager.

- The Wazuh Manager receives logs from all agents and applies detection rules to analyze the events.

- A base rule detects each failed RDP login attempt using Event ID 4625.

- To avoid false alerts, Wazuh uses correlation rules instead of acting on a single failed attempt.

- If multiple failed RDP login attempts are detected from the same IP address within a short time, Wazuh identifies it as a brute force attack.

- Once the brute force condition is met, Wazuh generates a high-severity alert.

- This alert is displayed on the Wazuh Dashboard with full details such as attacker IP, number of attempts, and time window.

- After the alert is generated, the Active Response feature is triggered automatically.

- Active Response runs a firewall command on the Windows system and blocks the attacker’s IP address.

- The blocked IP is prevented from making further RDP login attempts.

- The IP block remains active for a defined time period and is removed automatically after the timeout.

- All block and unblock actions are logged for auditing and verification purposes.

- This process allows Wazuh to detect and stop RDP brute force attacks automatically without manual intervention.

Summary:

In this project, I implemented RDP brute force attack detection and prevention using Wazuh and its Active Response feature. When an attacker repeatedly tries different usernames and passwords on the Remote Desktop Protocol (RDP) service, these failed login attempts are recorded in the Windows Security Event Logs on the target machine. The Wazuh agent installed on the Windows system continuously monitors these logs and sends the collected events to the Wazuh manager.

The Wazuh manager analyzes the received logs using custom detection and correlation rules. When the number of failed RDP login attempts from the same IP address exceeds a defined limit within a short time, Wazuh identifies this behavior as an RDP brute force attack. At this point, a security alert is generated and displayed on the Wazuh dashboard, showing details such as the attacker IP, time, and severity.

After the brute force attack is detected, the Active Response mechanism is automatically triggered. The Wazuh manager sends a response command to the Wazuh agent running on the Windows machine. The agent then executes the Windows firewall command (netsh) locally, which creates a firewall rule to block the attacker's IP address.

Once the IP address is blocked, the attacker can no longer establish an RDP connection to the system. Any further login attempts from the same IP fail immediately due to the firewall restriction. The successful execution of the Active Response is also logged and visible on the Wazuh dashboard, confirming that the attacker's IP has been blocked.

This project demonstrates that Wazuh can effectively detect and prevent RDP brute force attacks in real time without manual intervention. By combining log monitoring, rule-based detection, and automated Active Response, the system enhances Windows security and protects Remote Desktop services from unauthorized access.