Wazuh – RDP Brute Force Attack

ACTIVE RESPONSE

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Wazuh is an open-source security platform that provides comprehensive security monitoring and threat detection capabilities. One of its features is active response, which enables automated responses to detected threats, such as blocking IP addresses involved in brute force attacks. Here, we will focus on how Wazuh can be configured to block RDP (Remote Desktop Protocol) brute force attacks.

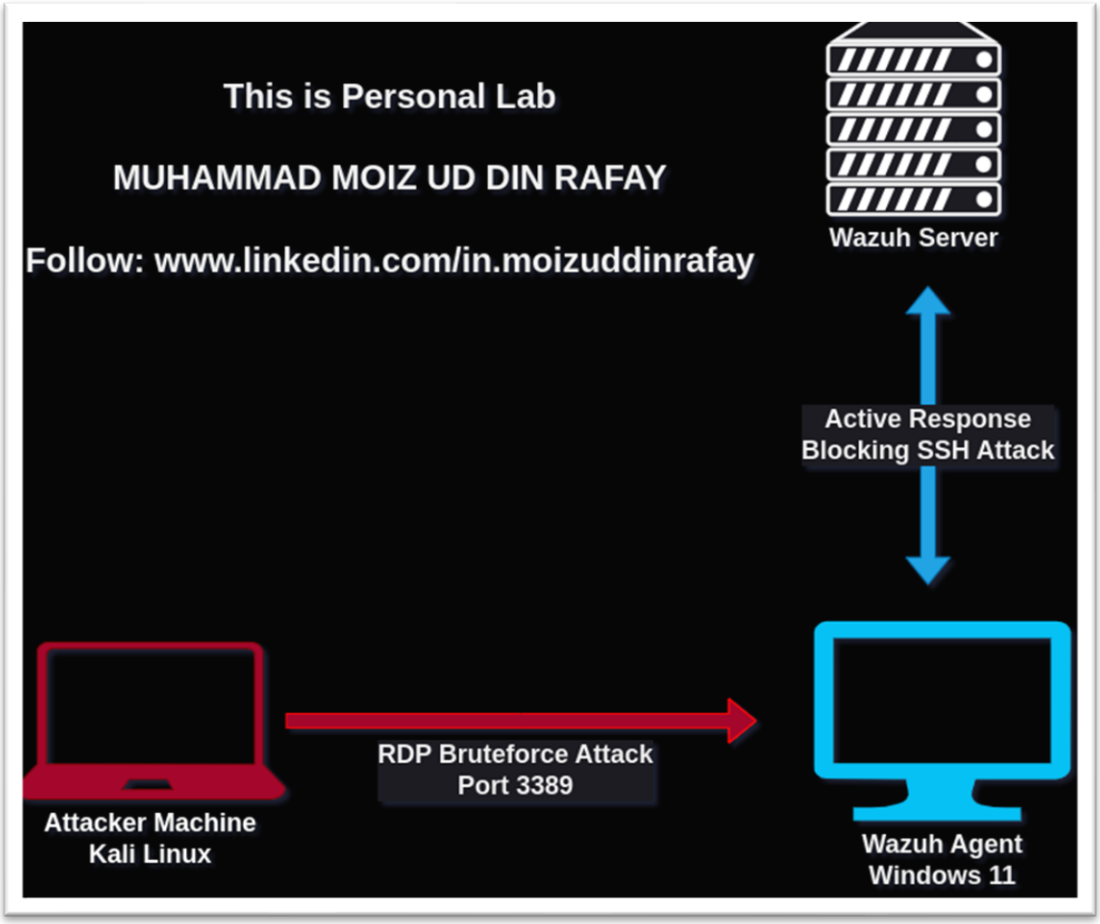
RDP Brute Force Attacks

RDP brute force attacks involve attackers systematically trying various username and password combinations to gain unauthorized access to a system via RDP. These attacks can compromise the security of a network, leading to data breaches and other malicious activities.

Wazuh Active Response

Wazuh's active response feature can be configured to detect and mitigate such attacks. Here's how it works:

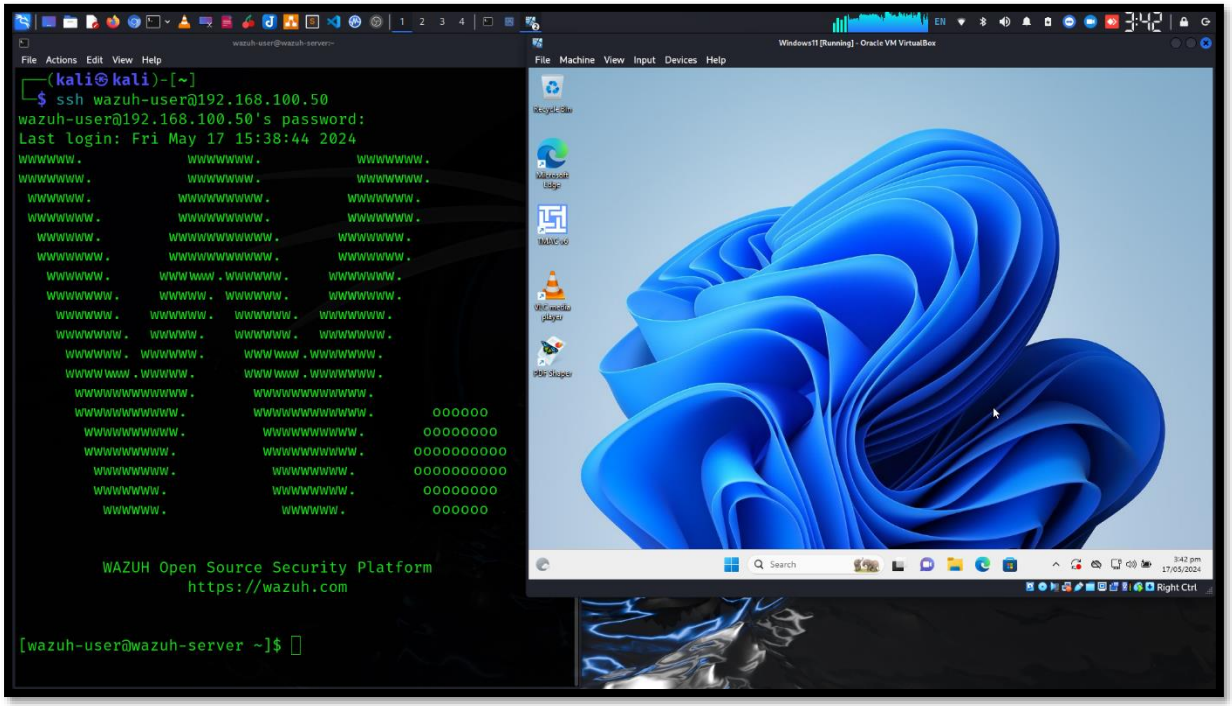
1. **Detection Rules**: Wazuh uses detection rules to identify suspicious activities. For RDP brute force attacks, rules can be set to monitor failed login attempts. If a certain threshold of failed attempts is reached within a specific time period, it triggers an alert.
2. **Triggering Alerts**: When the threshold for failed login attempts is reached, Wazuh generates an alert. These alerts can include details like the source IP address, the targeted system, and the time of the attempts.
3. **Active Response Configuration**: Wazuh's active response mechanism can be configured to automatically execute predefined actions in response to specific alerts. For RDP brute force attacks, the response might include adding the attacking IP address to a block list.
4. **Blocking the Attacker**: Upon triggering the active response, Wazuh can use various methods to block the attacker. One common method is modifying the firewall rules to block traffic from the offending IP address. This can be done using tools like iptables on Linux or the Windows Firewall.



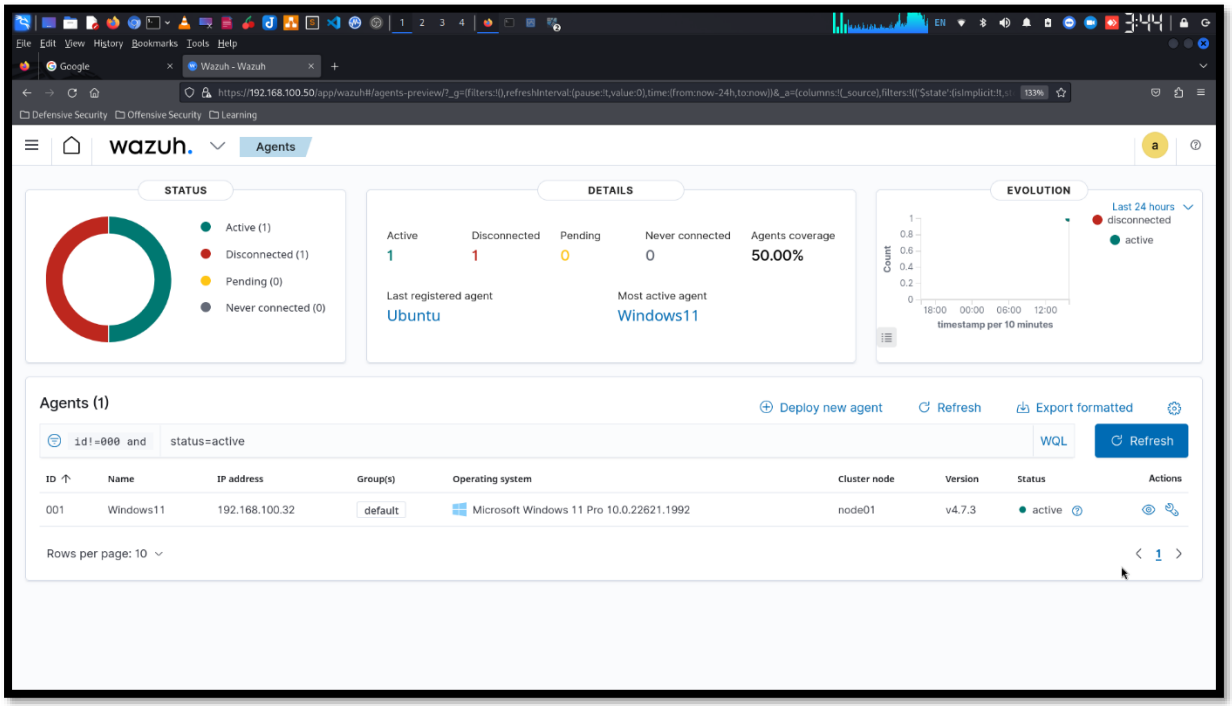
Implementation Steps

1. **Install and Configure Wazuh**: Ensure Wazuh is installed and configured on the systems you wish to protect. The Wazuh agent should be installed on endpoints to monitor local events.
2. **Define Detection Rules**: Customize or use predefined Wazuh rules to detect multiple failed RDP login attempts. These rules are often based on log analysis, such as monitoring Windows Event Logs for specific event IDs that indicate failed logins.
3. **Set Up Active Response**: Configure active response policies in Wazuh to specify the actions taken when certain rules are triggered. This involves creating a response command, such as a script that updates firewall rules to block the attacker's IP.
4. **Deploy and Monitor**: Deploy the configured Wazuh agents and active response policies across your network. Regularly monitor the Wazuh dashboard to ensure that the responses are correctly triggered and that attackers are being blocked effectively.

Here is Wazuh Server running on my lab environment. I access Wazuh console via SSH connection.



Wazuh Dashboard is running and Active-agent Windows11



Now we have to configure “local rules” for detecting and blocking RDP Brute Force Attack.

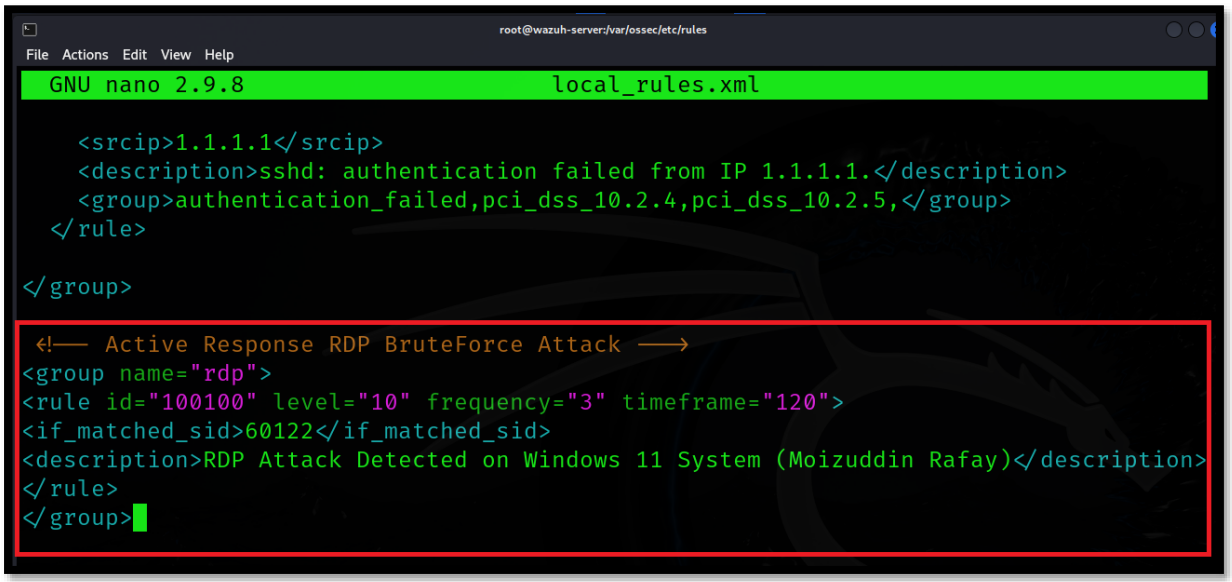
```
root@wazuh-server:/var/ossec/etc/rules
File  Actions  Edit  View  Help
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /var/ossec/etc/rules
[root@wazuh-server rules]# ls
local_rules.xml
[root@wazuh-server rules]# nano local_rules.xml
```

Here is “local_rules.xml” file now edit configuration.

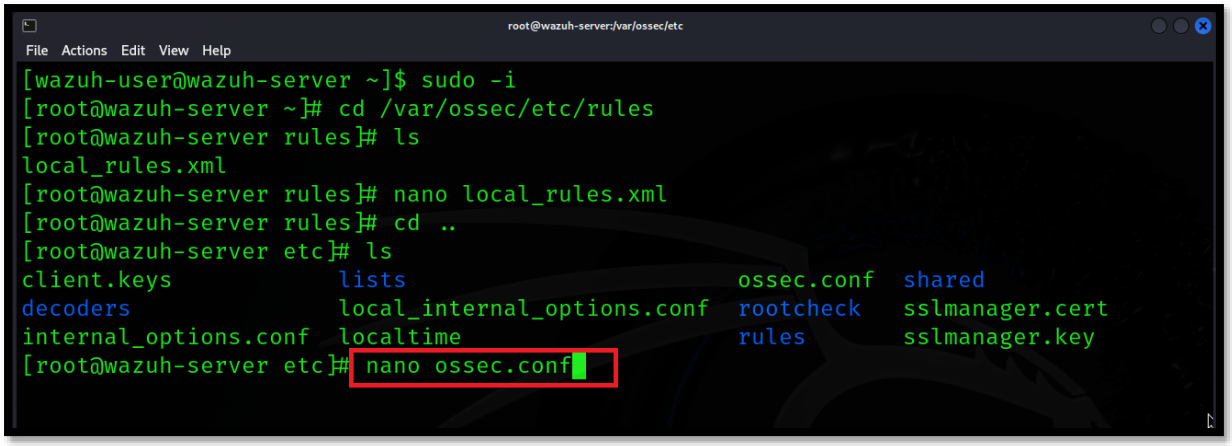
```
root@wazuh-server:/var/ossec/etc/rules
File  Actions  Edit  View  Help
  GNU nano 2.9.8                    local_rules.xml                    Modified

<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 $
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Edit these lines in “local_rules.xml” configuration.

```
<group name=”rdp”>
<rule id=”100100” level=”10” frequency=”3” timeframe=”120”>
<if_matched_sid>60122</if_matched_sid>
<description> RDP Attack Detected </description>
</rule>
</group>
```



Now we have to edit configuration in “ossec.conf” file



Scroll down to “Active Response”

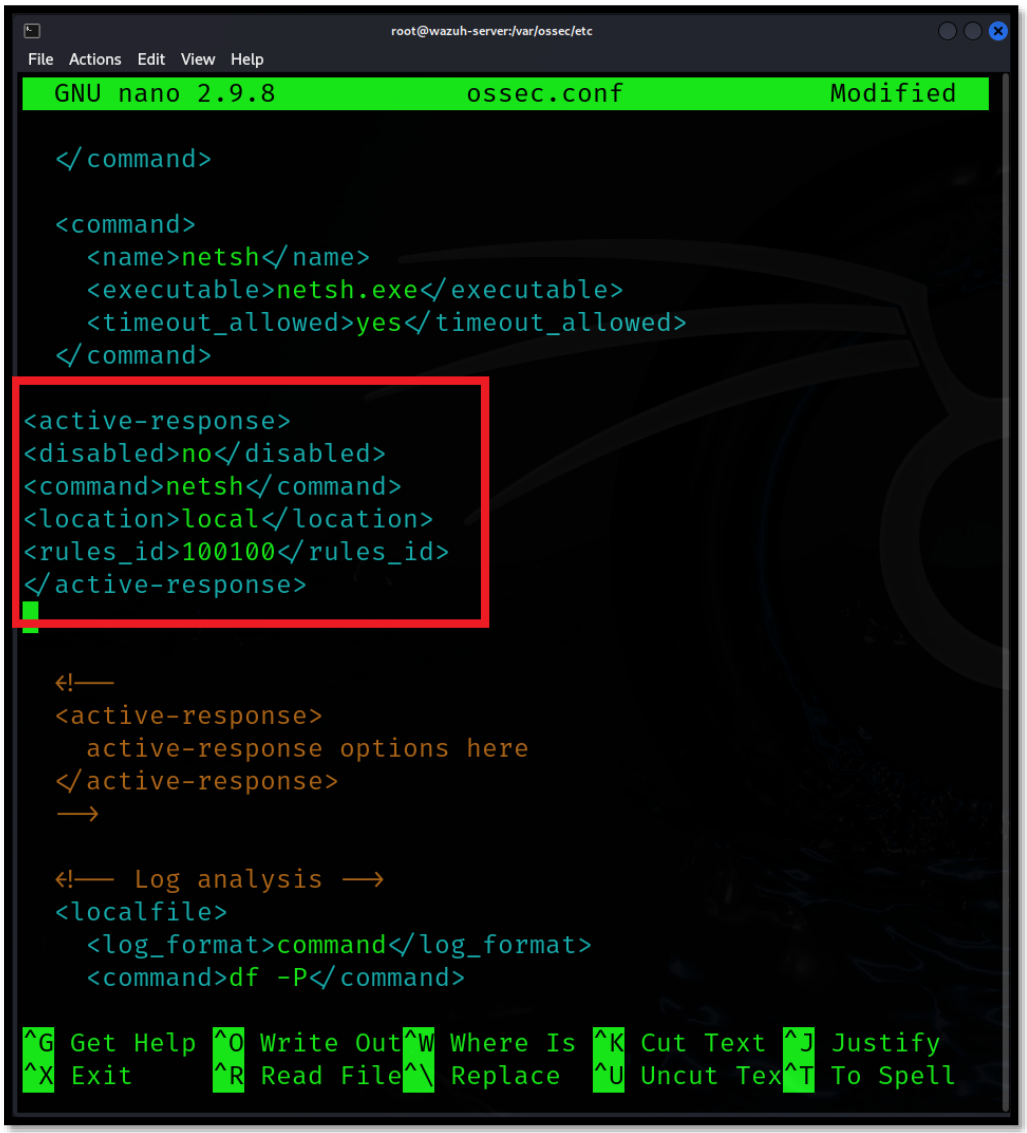
```
root@wazuh-server:/var/ossec/etc
File  Actions  Edit  View  Help
  GNU nano 2.9.8                    ossec.conf

    <process_priority>10</process_priority>

    <!-- Maximum output throughput -->
    <max_eps>50</max_eps>

    <!-- Database synchronization settings -->
    <synchronization>
      <enabled>yes</enabled>
      <interval>5m</interval>
      <max_eps>10</max_eps>
    </synchronization>
  </syscheck>

  <!-- Active response -->
  <global>
    <white_list>127.0.0.1</white_list>
    <white_list>^localhost.localdomain$</white_list>
    <white_list>172.31.0.2</white_list>
  </global>

  <command>
    <name>host-deny</name>
    <executable>host-deny.sh</executable>
    <expect>srcip</expect>
  </command>
  <command>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Here we have to edit configuration.

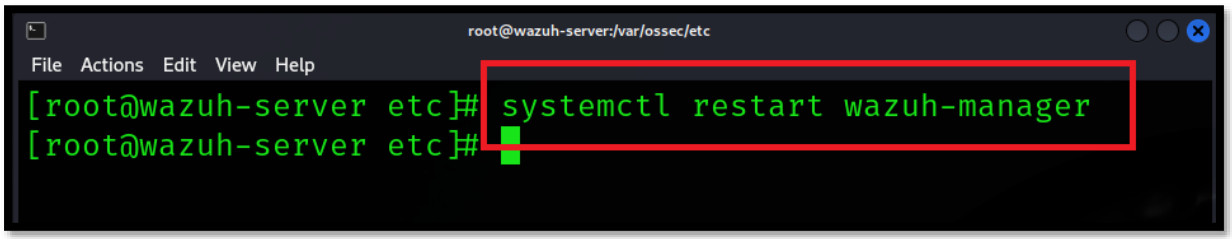
```
root@wazuh-server:/var/ossec/etc
File  Actions  Edit  View  Help
  GNU nano 2.9.8                    ossec.conf                    Modified


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


  <!--
  <active-response>
    active-response options here
  </active-response>
  -->

  <!-- Log analysis -->
  <localfile>
    <log_format>command</log_format>
    <command>df -P</command>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:$

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Edit these lines here:

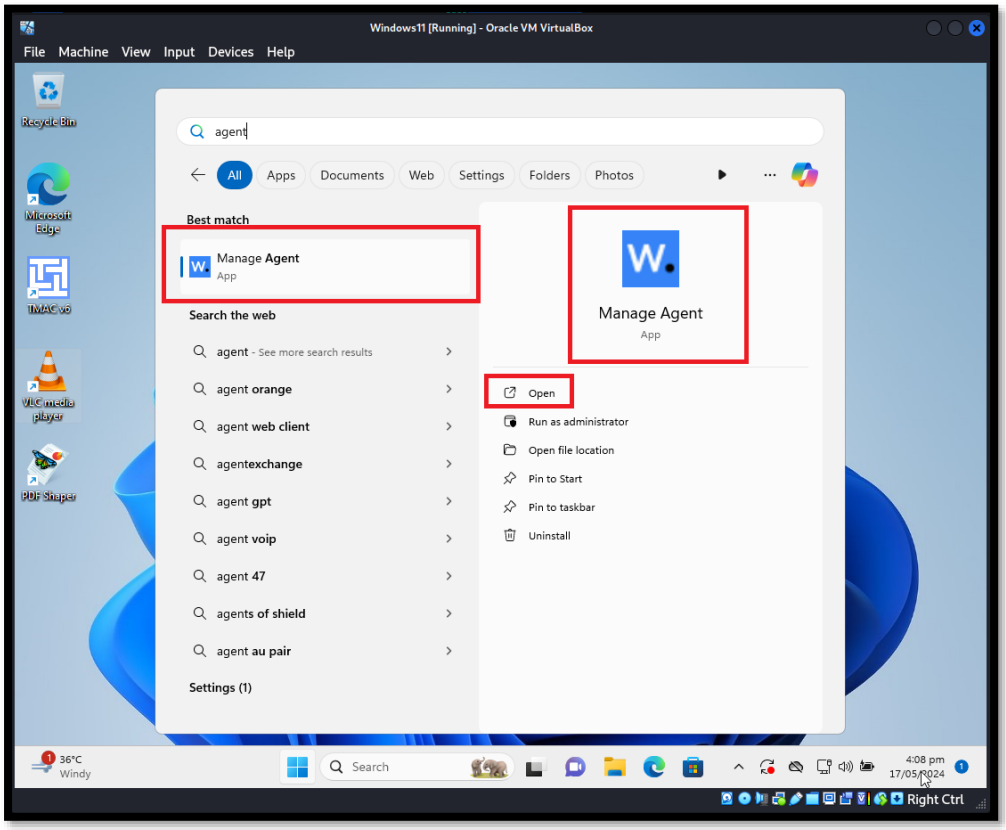
```
<active-response>
<disabled>no</disabled>
<command>netsh</command>
<location>local</local>
<rules_id>100100</rules_id>
</active-response>
```



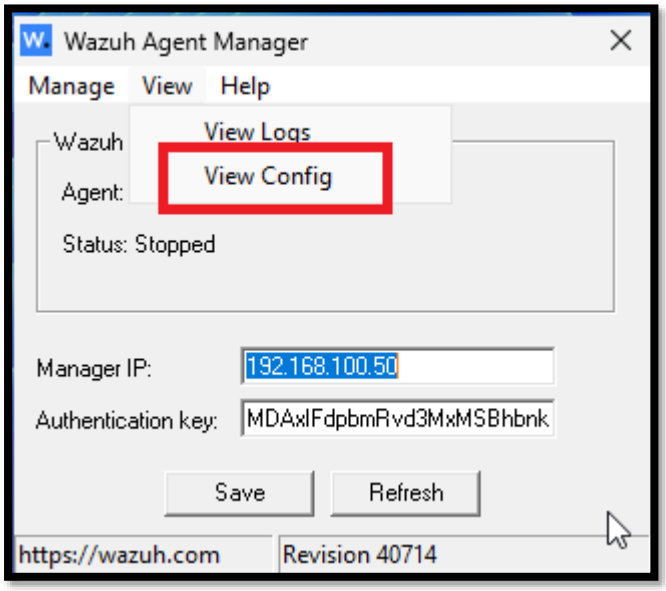
Save the configuration and restart “Wazuh-manager”



Now in “Windows11” go to “Manage Agent”



Go to “View Config”



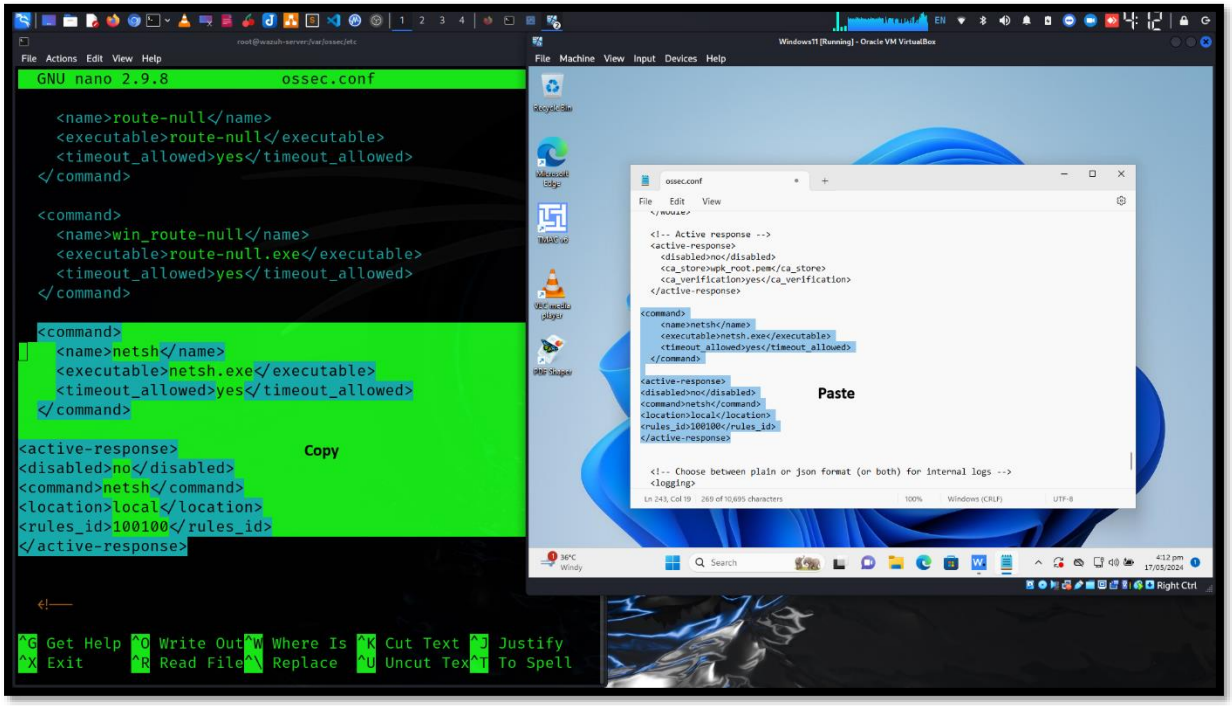
Here is “ossec.conf” file in windows11-agent

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.100.50</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <enrollment>
      <enabled>yes</enabled>
      <manager_address>192.168.100.50</manager_address>
      <agent_name>Windows11</agent_name>
```

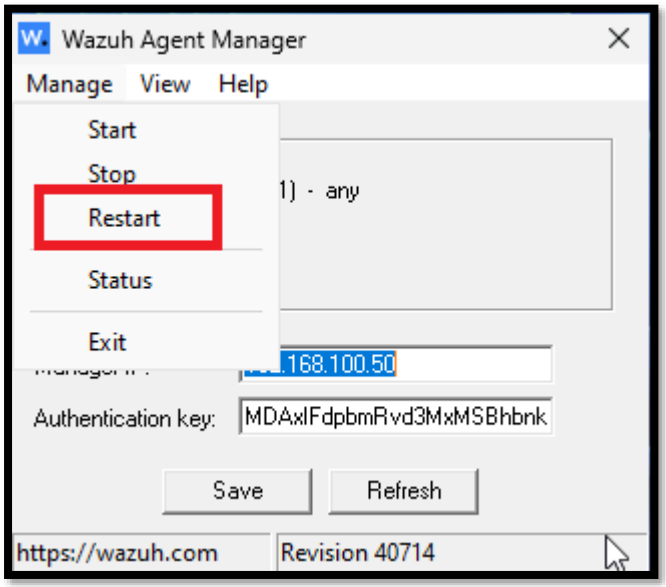
Scroll down and here we have to edit configuration under “Active response”

```
    <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 -->
  <active-response>
    <disabled>no</disabled>
    <ca_store>wpk_root.pem</ca_store>
    <ca_verification>yes</ca_verification>
  </active-response>

  <!-- Choose between plain or json format (or both) for internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

</ossec_config>

<!-- END of Default Configuration. -->
```

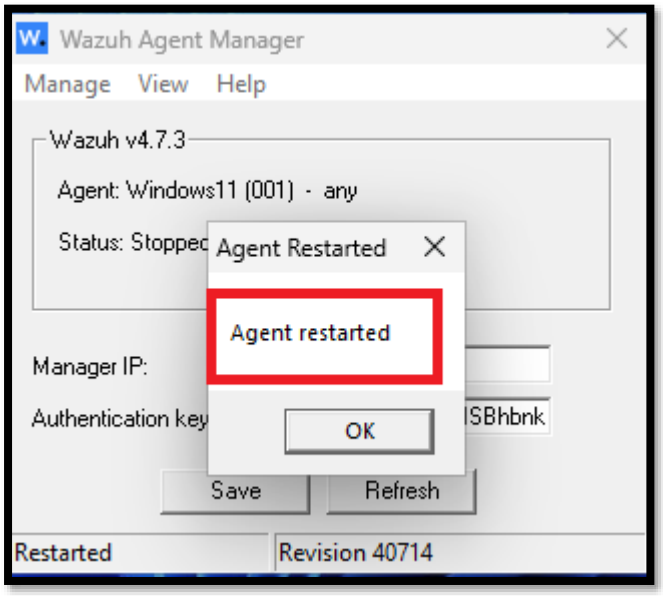
Now have a look here we have to edit same configuration in both “ossec.conf” file, Wazuh Server and Wazuh Agent



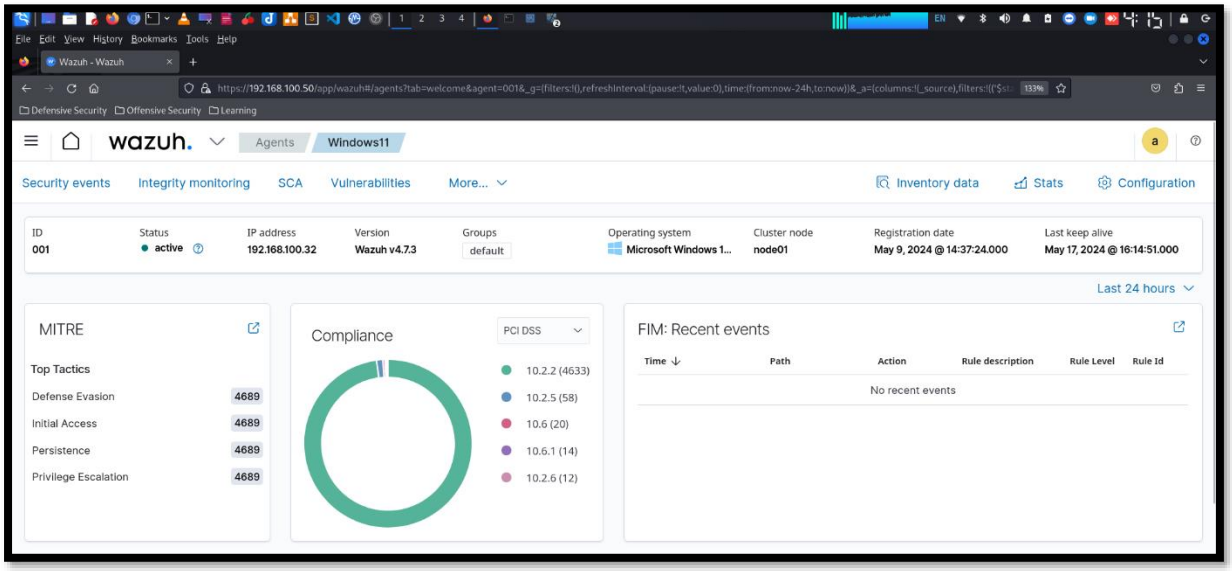
After saving the configuration we have to restart wazuh-agent manager



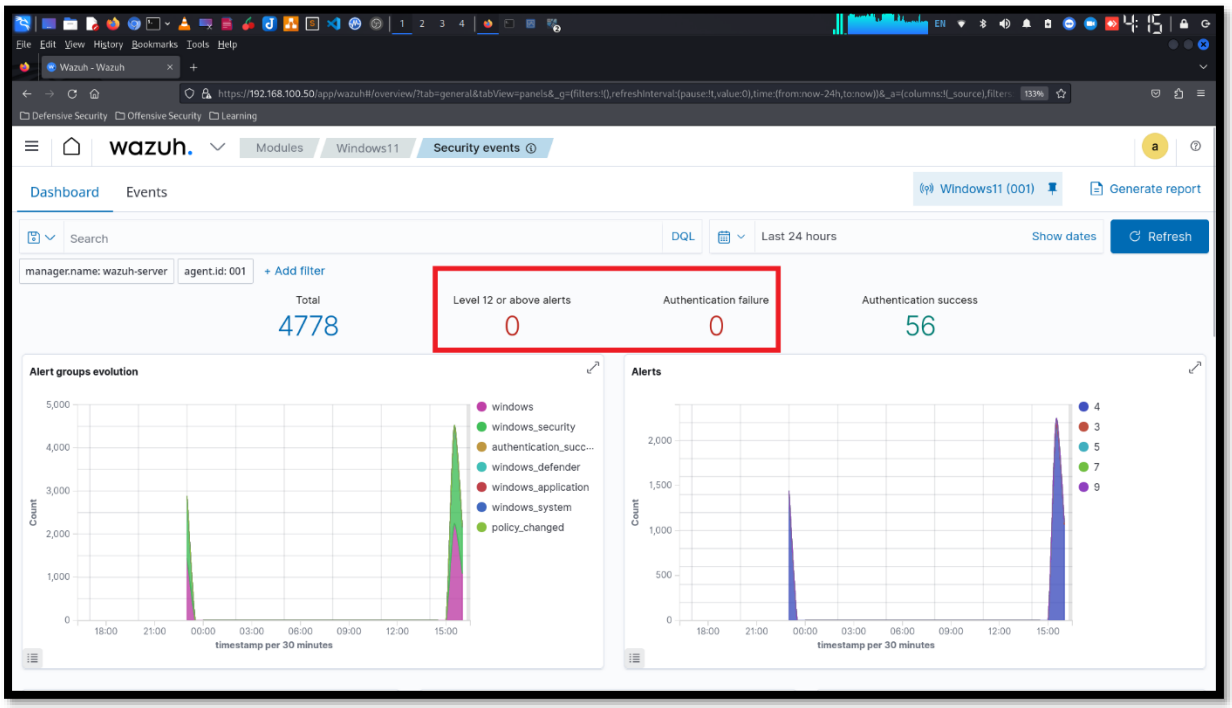
Wazuh Agent Restarted



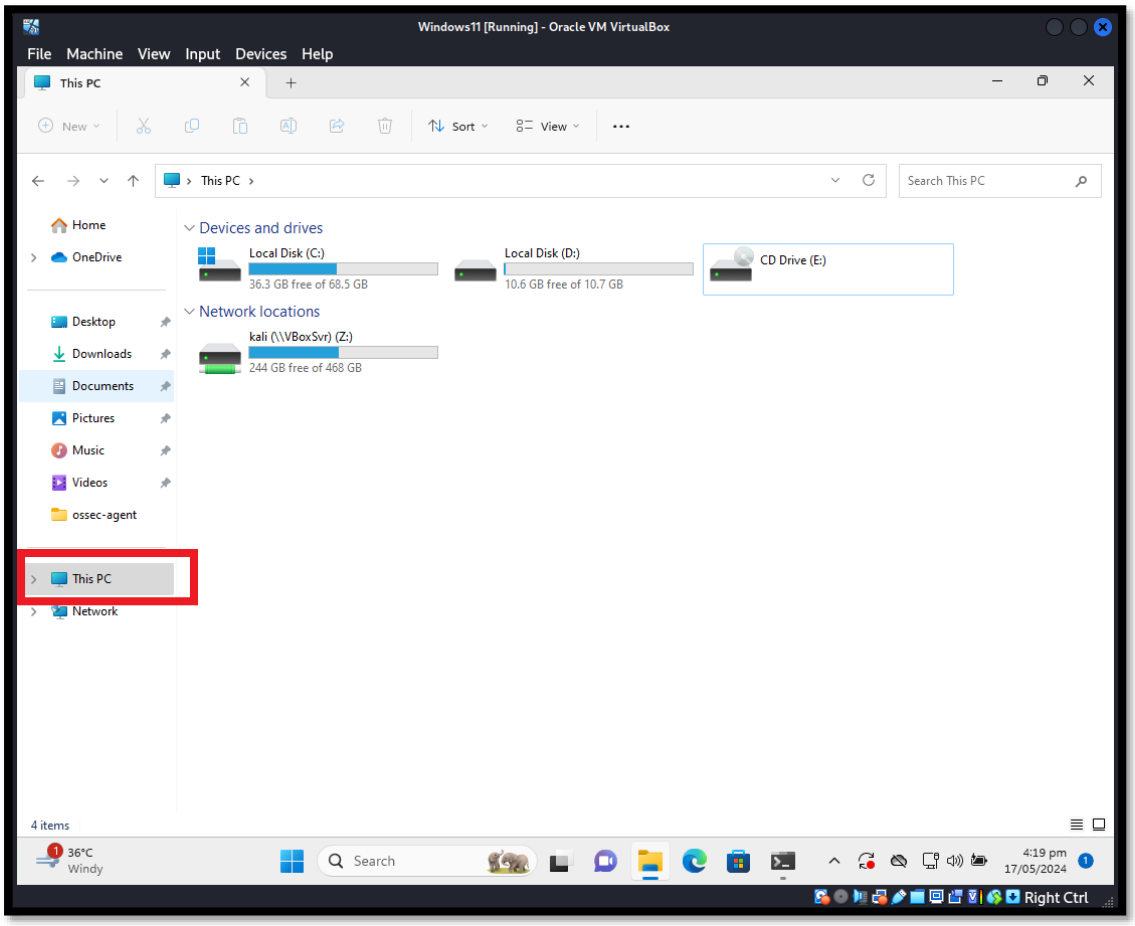
Here is “Windows11” agent in Wazuh Dashboard.



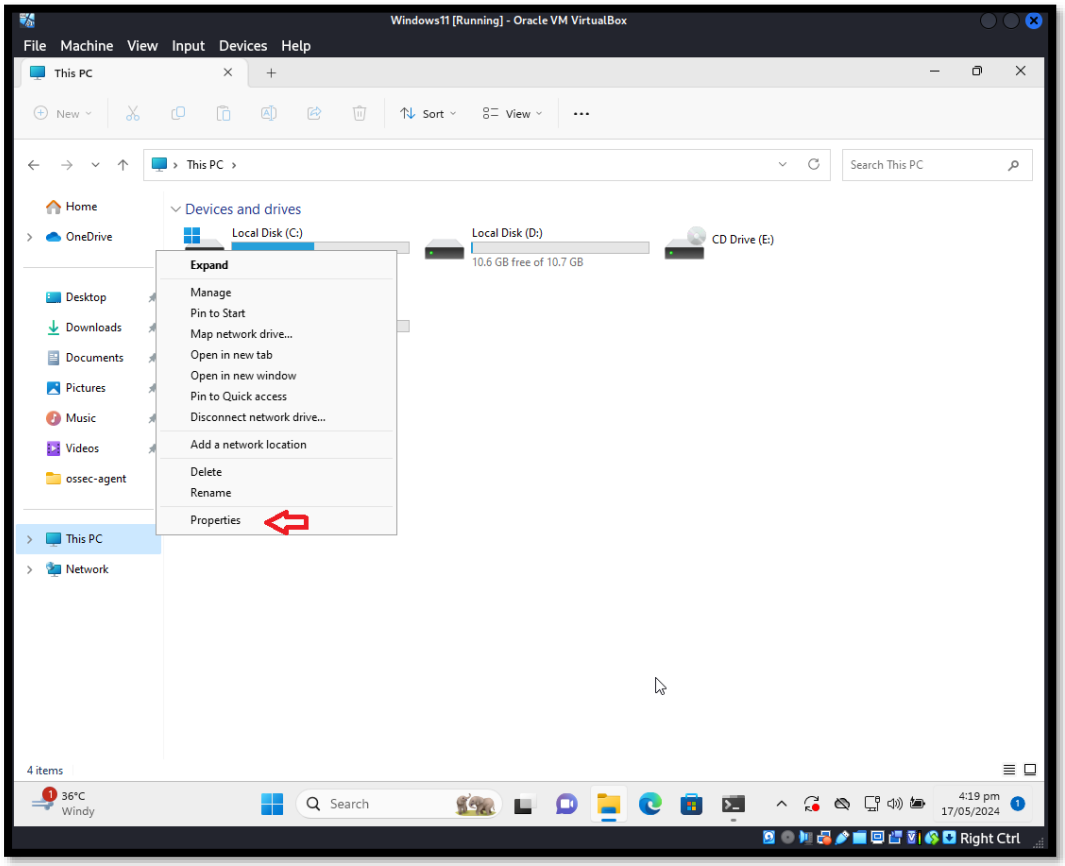
Have a look there is no result for now.

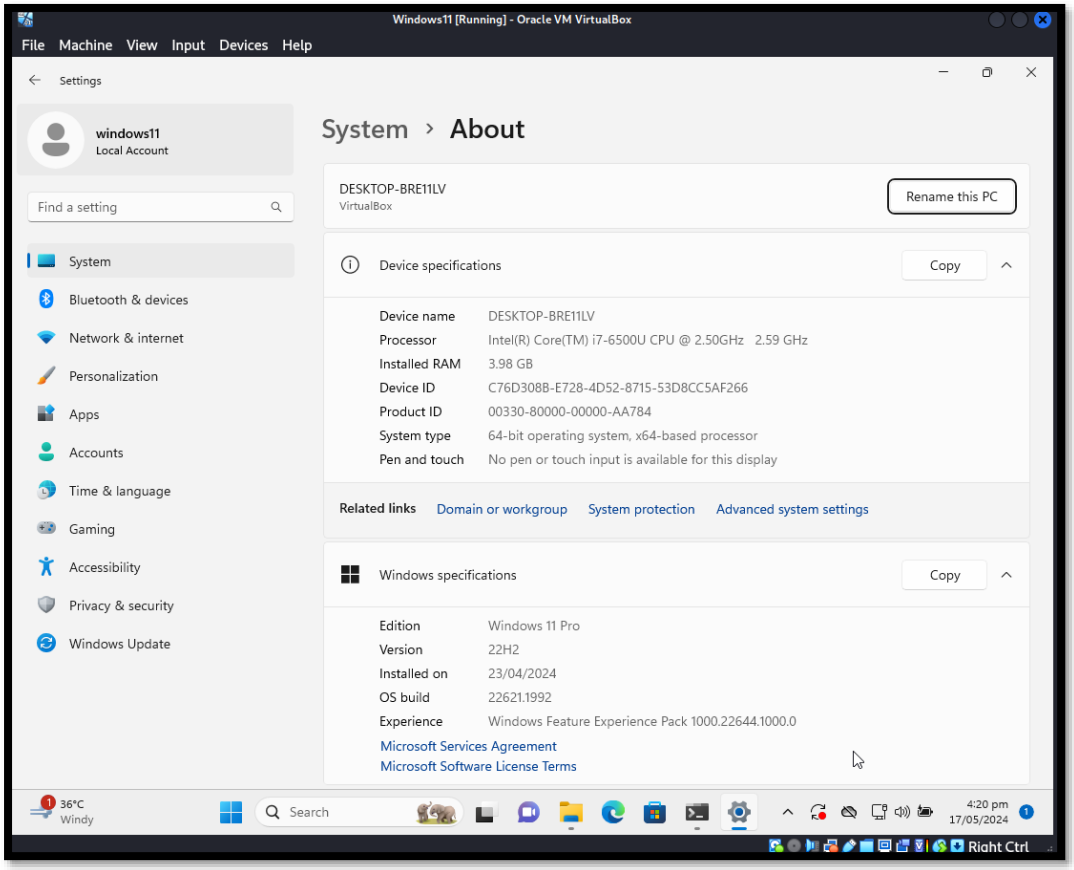


So before going farther we have to enable RDP – Remote Desktop in Windows11. Follow same shown in figures.

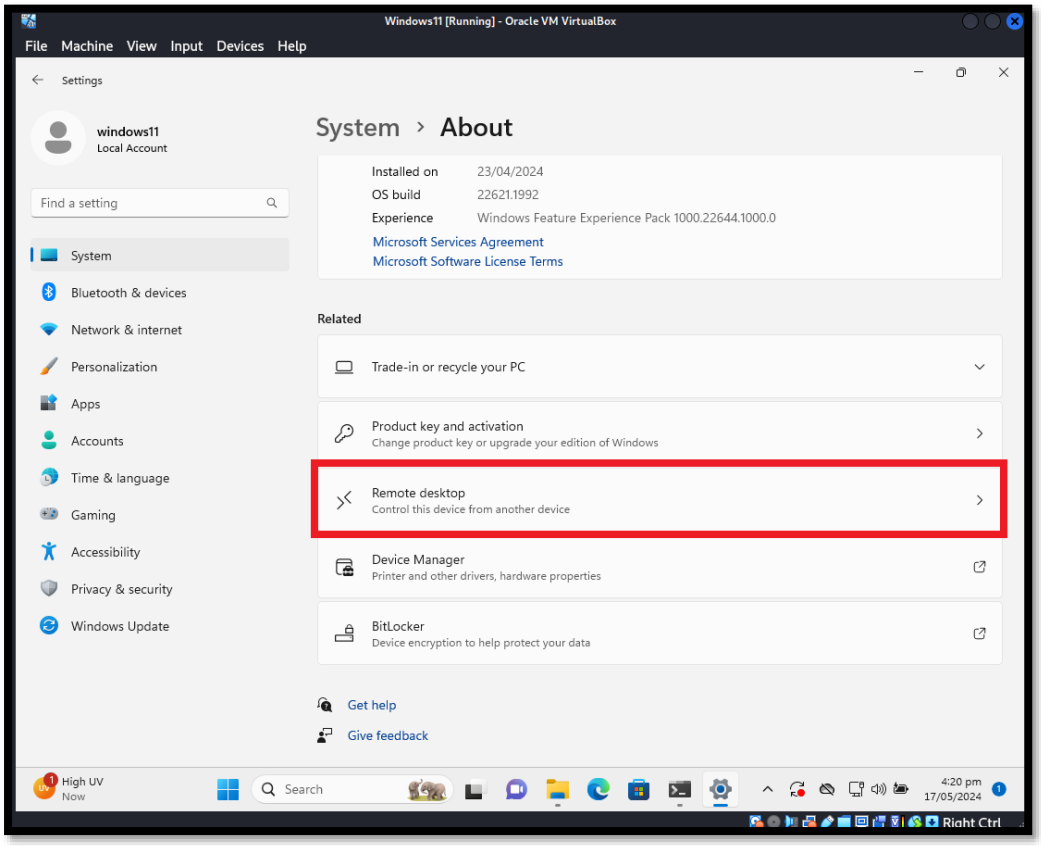


Go to “This PC” Properties

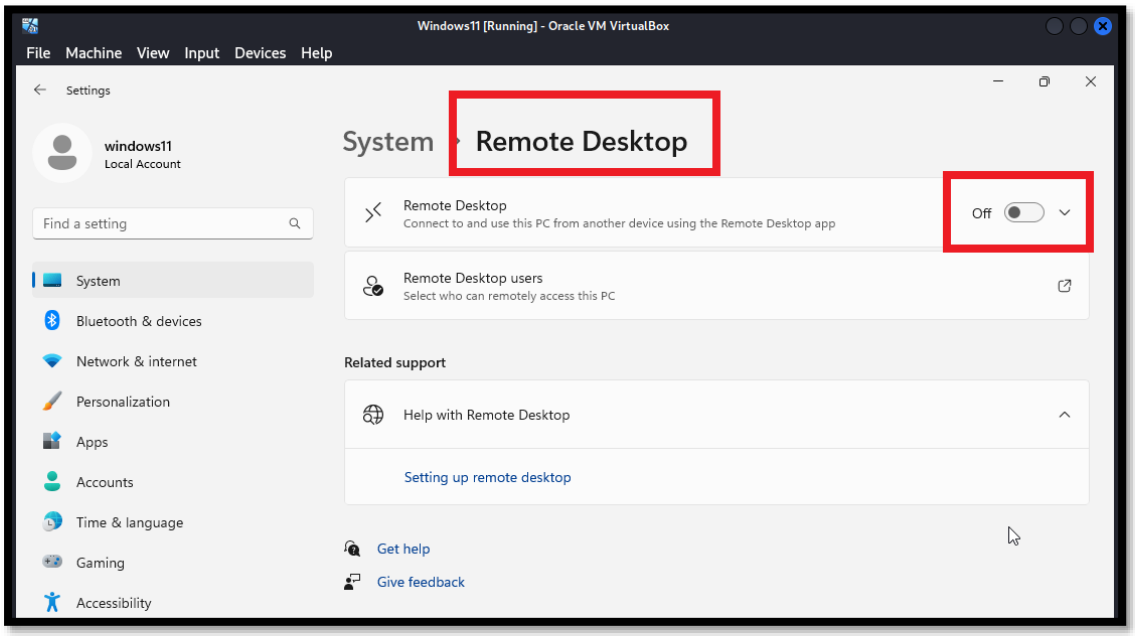




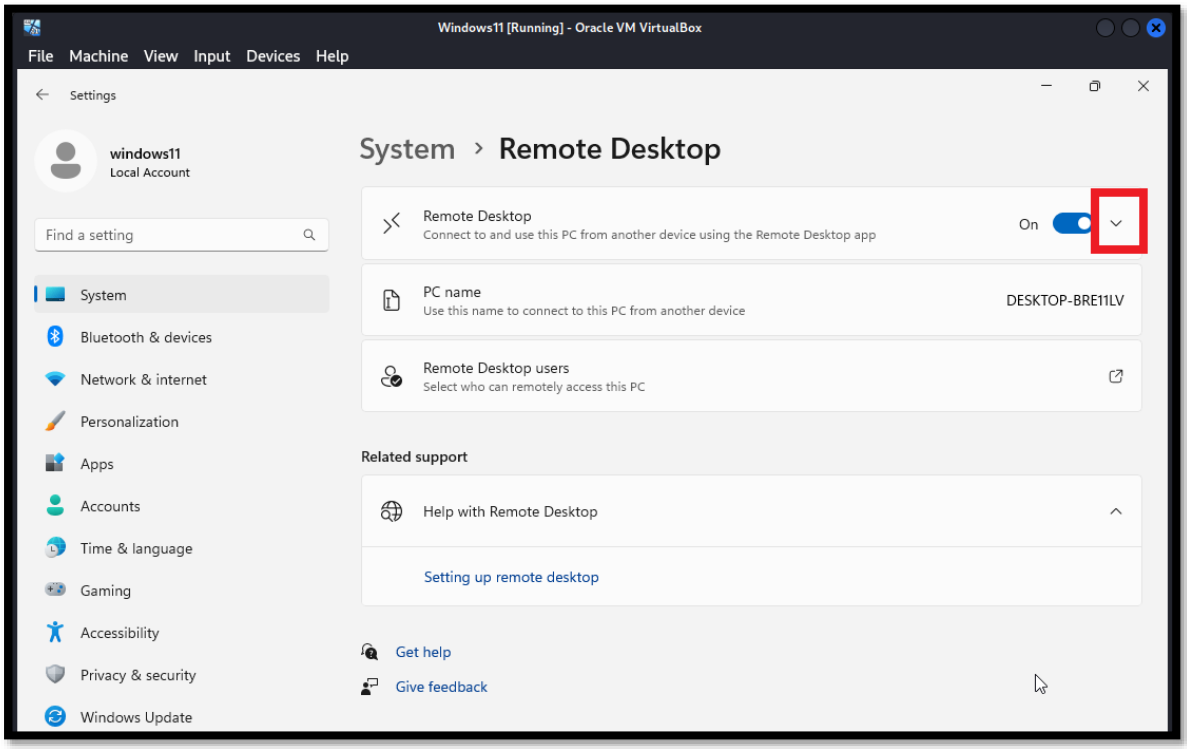
Scroll down and go to “Remote desktop”



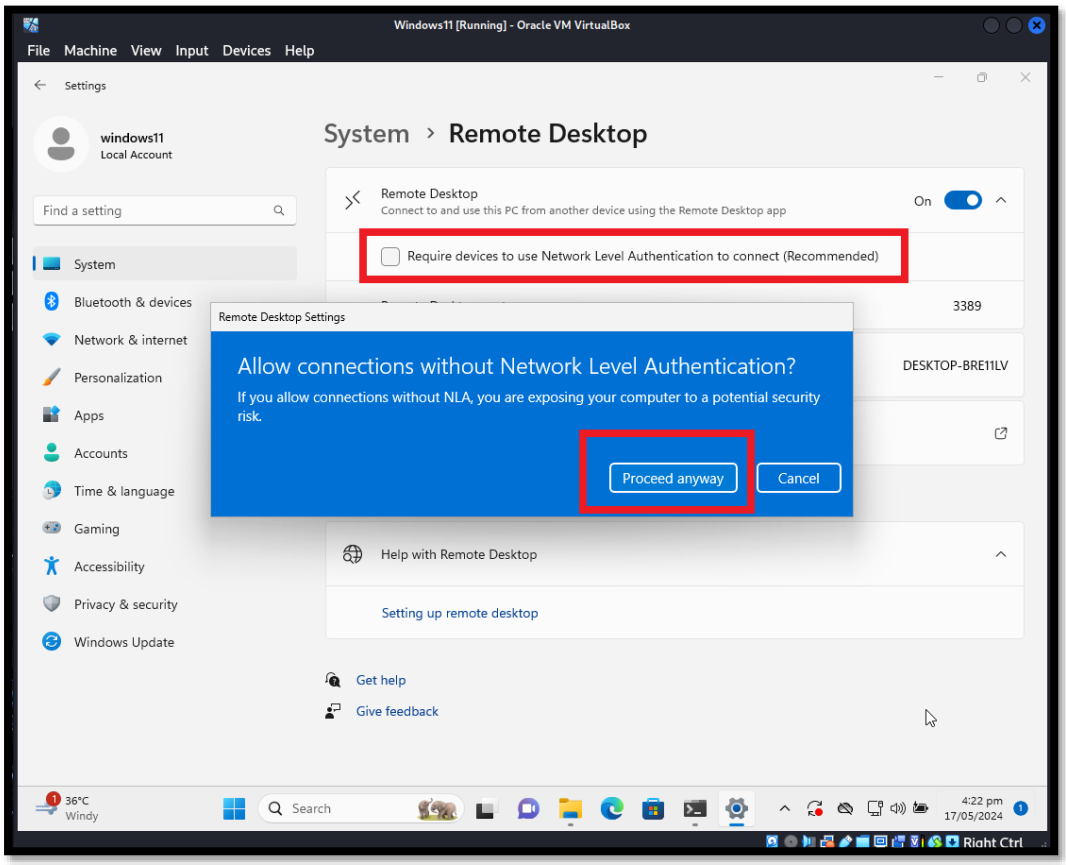
Turn this “ON”



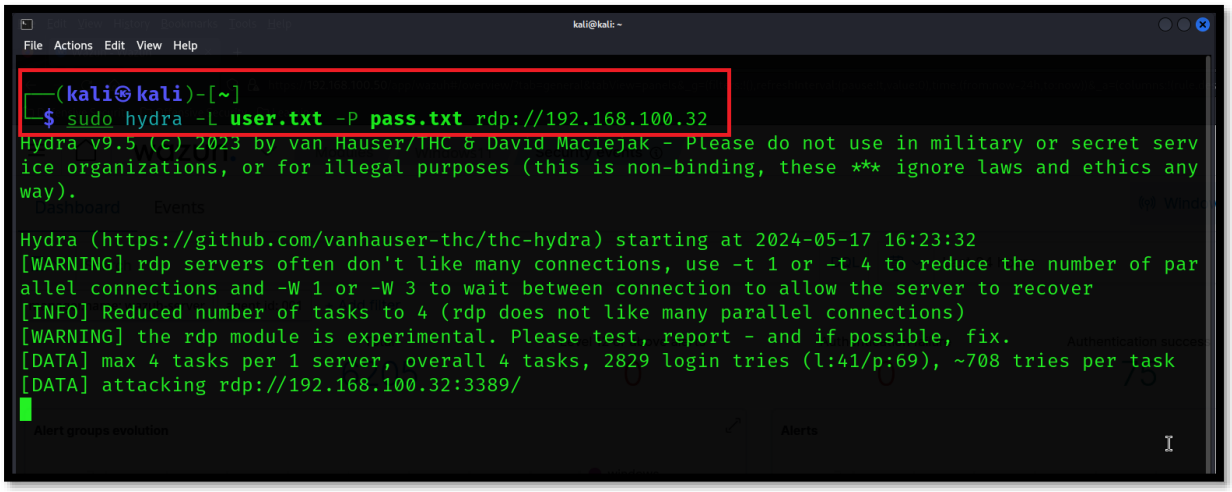
Now click on drop down button.



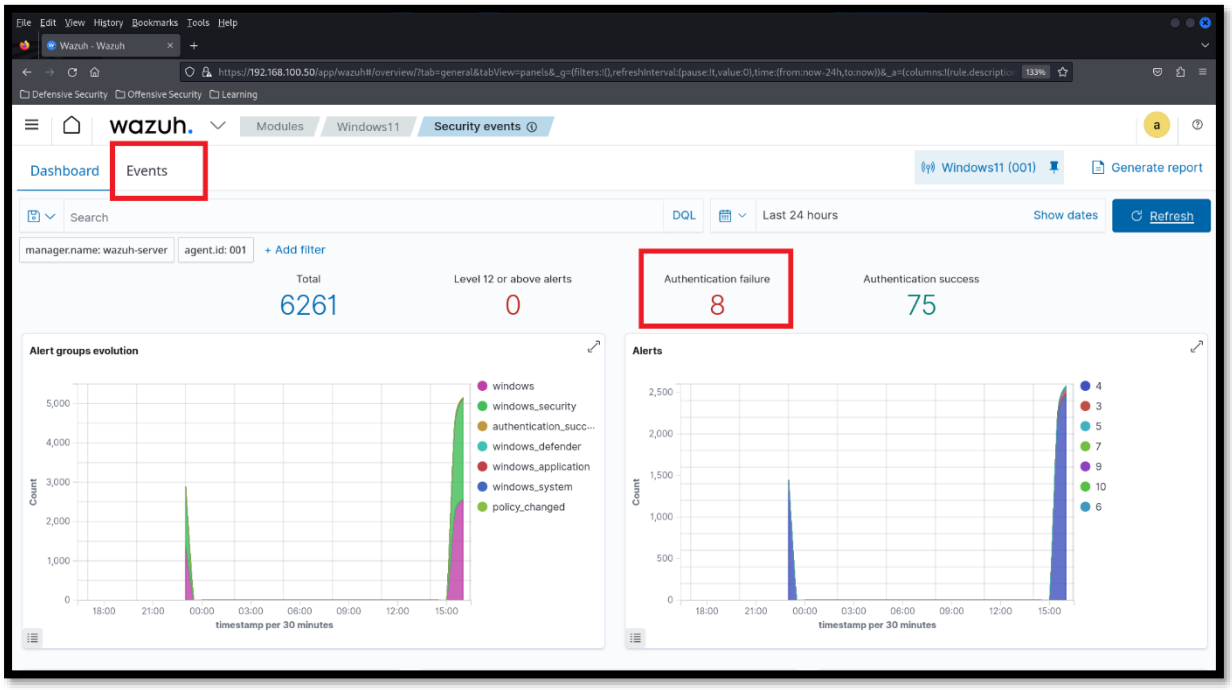
Uncheck “Require devices to use Network Level Authentication”, Click on “Proceed anyway” button.



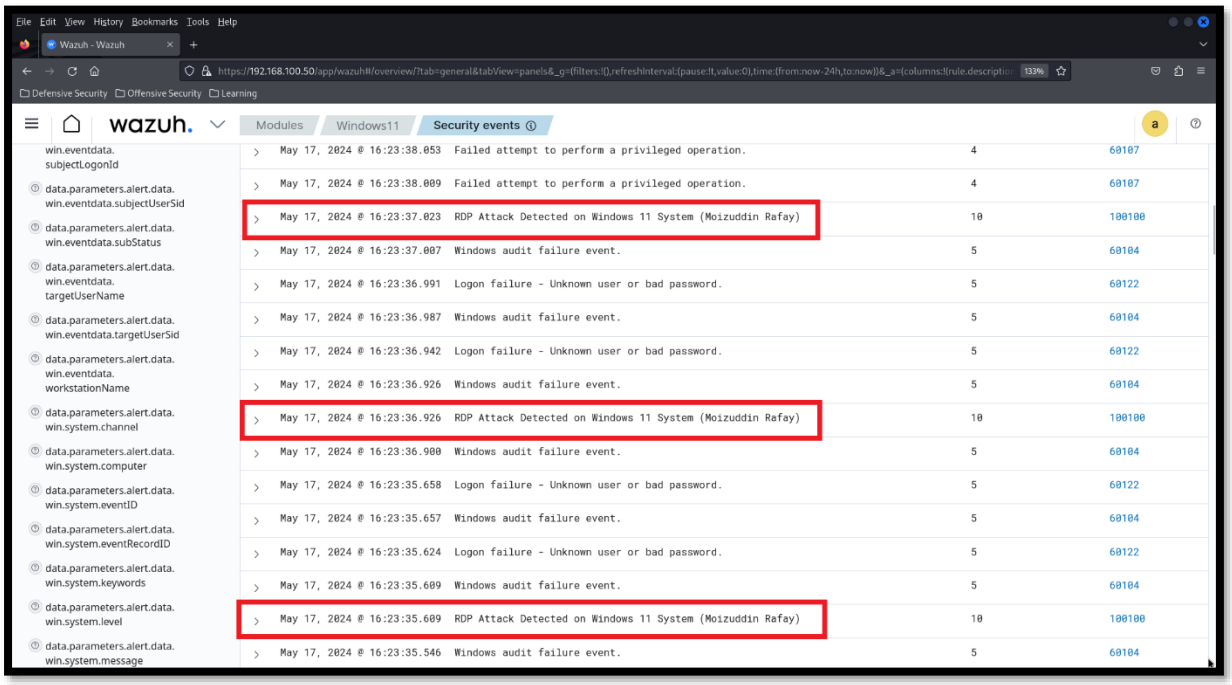
Now we have to launch RDP Brute Force Attack with “Hydra” tool.
Command: sudo hydra -L user.txt -P pass.txt rdp://192.168.100.32
Explain:
hydra = tool it self
-L for username dictionary
-P for passwords dictionary
rdp://192.168.100.32 (Protocol with IP address)

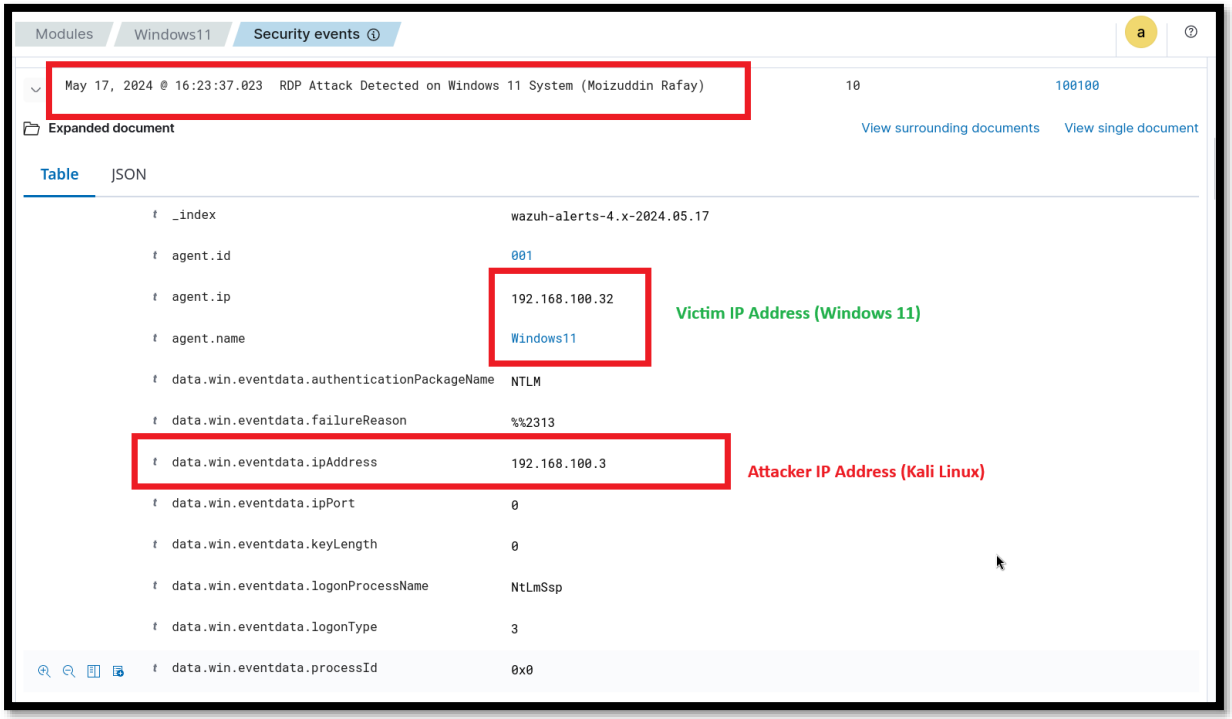


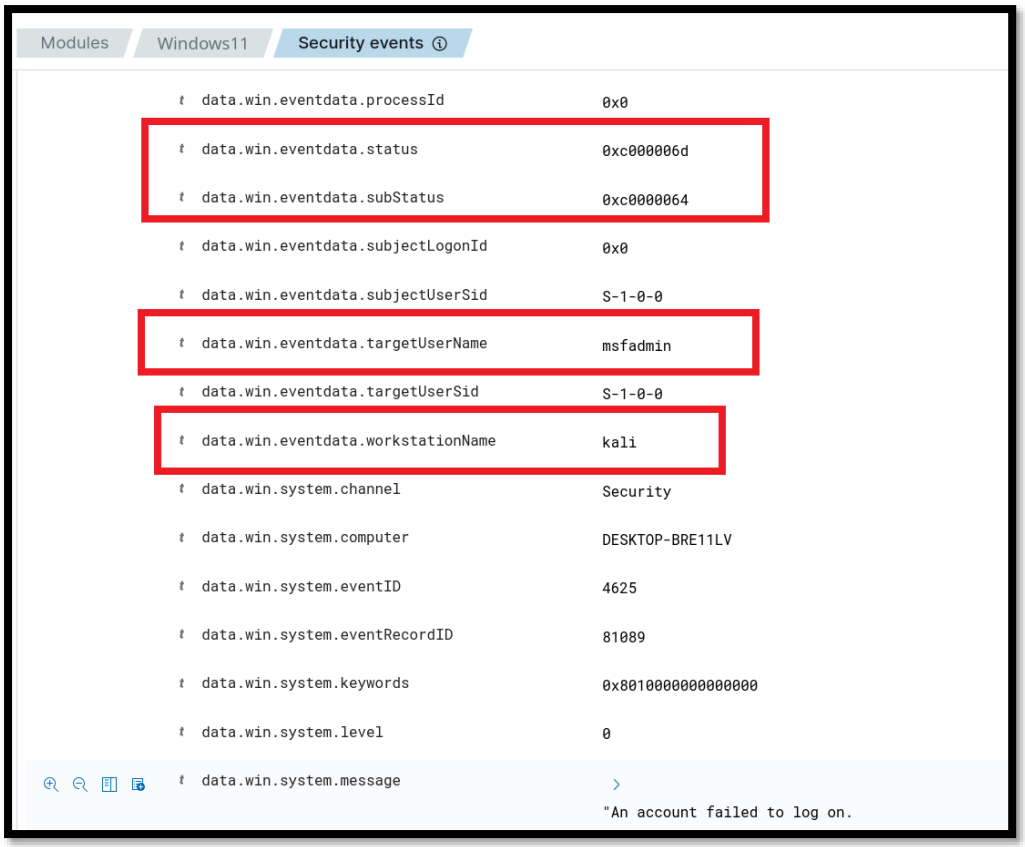
Now we have to observe Events, you can see “Authentication Failure” now go to “Events” tab.



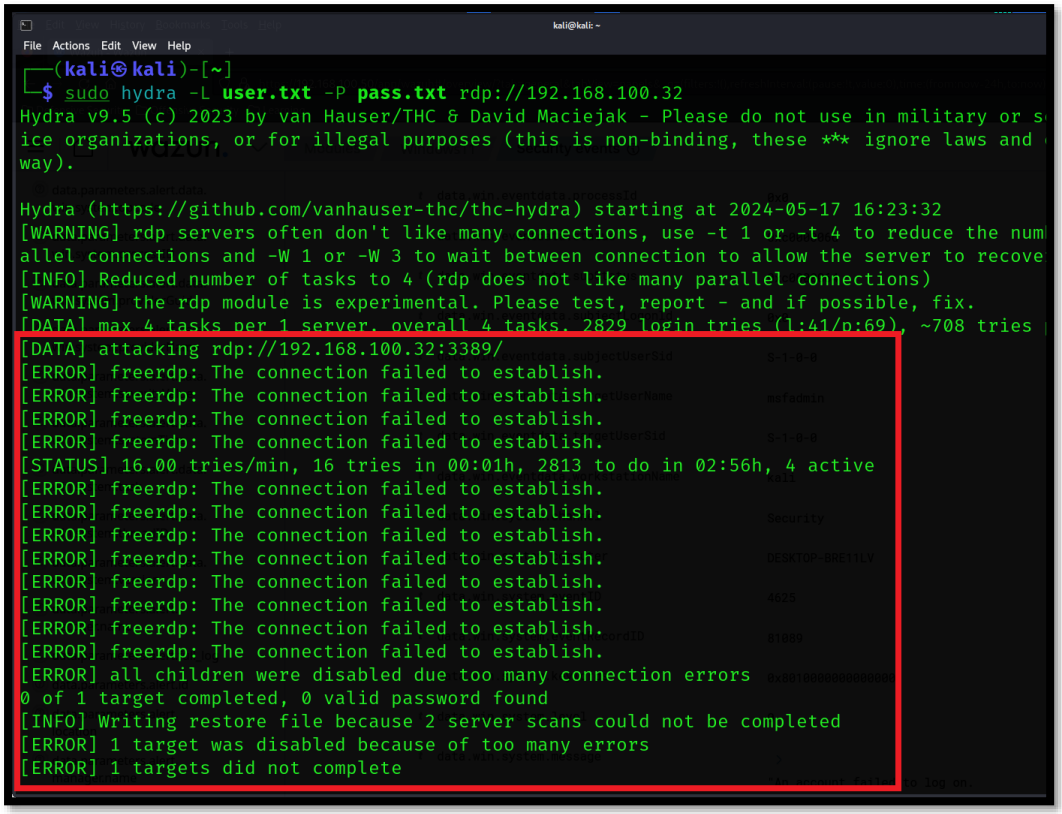
Let’s do Event Analysis







During the events and logs analysis you can see “Brute Force Attack” is failed because Wazuh is performing “Active Response”

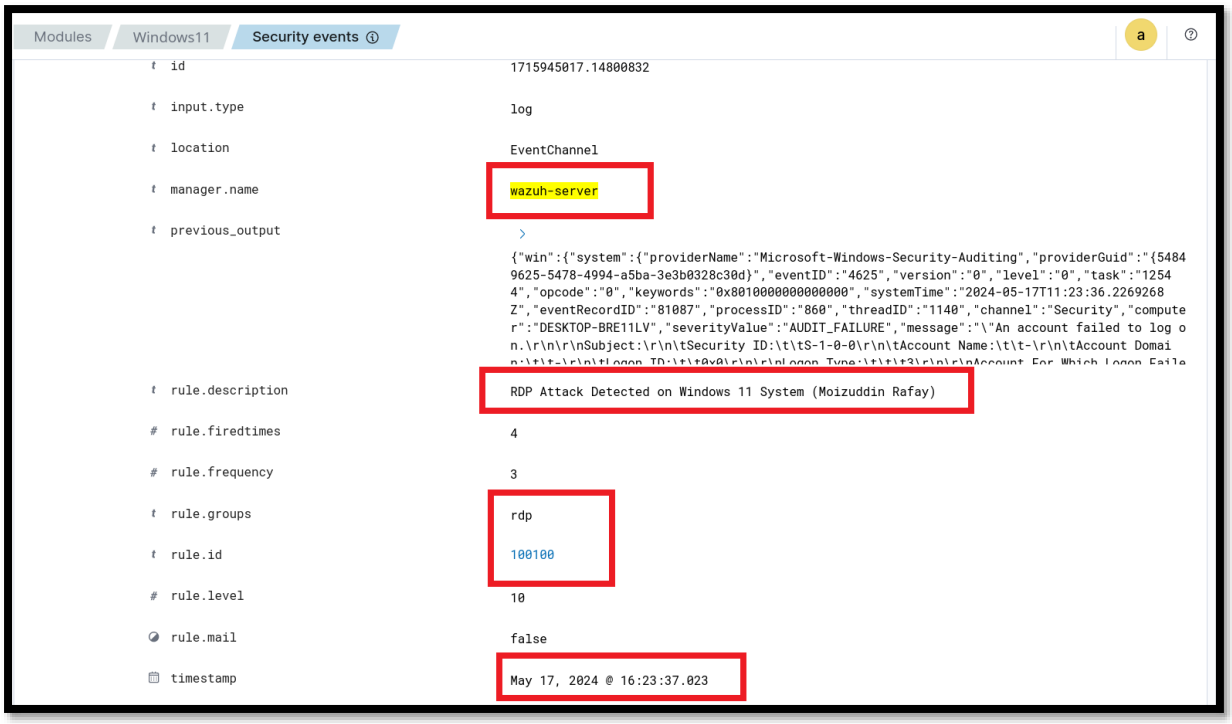


```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-17 16:23:32
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of par
allel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2829 login tries (l:41/p:69), ~708 tries per task
[DATA] attacking rdp://192.168.100.32:3389/
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 2813 to do in 02:56h, 4 active
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-17 16:25:14

┌──(kali㉿kali)-[~]
└─$
```

Now continue to events and logs analysis.

Modules | Windows11 | Security events

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
data.win.system.opcode	0
data.win.system.processID	860
data.win.system.providerGuid	{54849625-5478-4994-a5ba-3e3b0328c30d}
data.win.system.providerName	Microsoft-Windows-Security-Auditing
data.win.system.severityValue	AUDIT_FAILURE
data.win.system.systemTime	2024-05-17T11:23:36.2347703Z
data.win.system.task	12544
data.win.system.threadID	1448
data.win.system.version	0
decoder.name	windows_eventchannel
full_log	



SUMMARY

In summary, Wazuh's active response capability is a powerful tool to automatically mitigate RDP brute force attacks by blocking malicious IP addresses. By setting up appropriate detection rules and response actions, organizations can protect their systems from unauthorized access and enhance their overall security posture. Regular monitoring and updates to these configurations ensure ongoing protection against evolving threats.