Wazuh SIEM Project

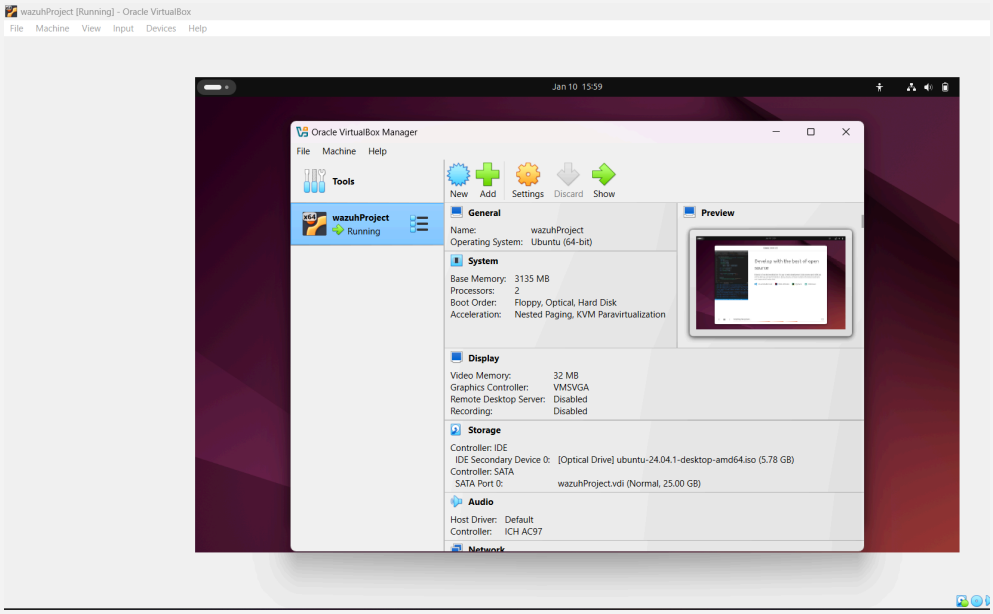
Jaleel Calhoun

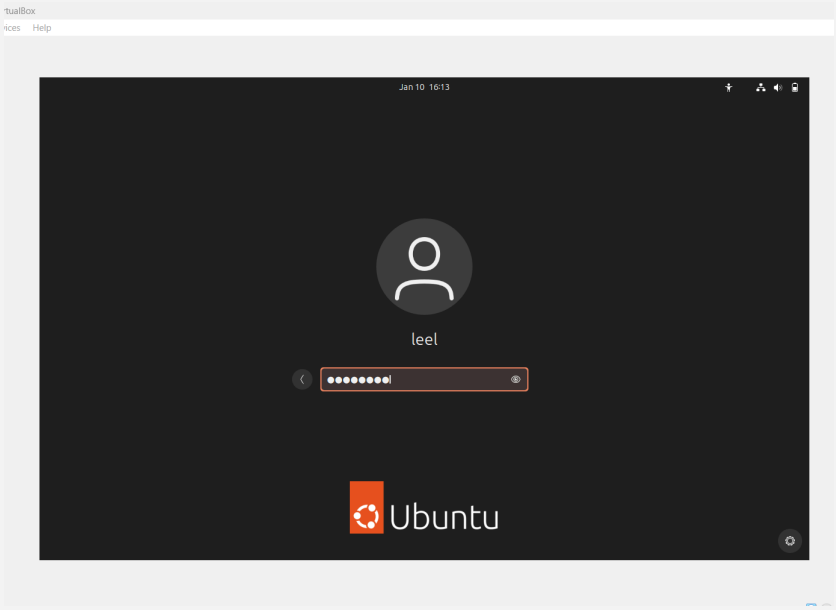
Objective:

- Install free SIEM platform “Wazuh” hosting on a linux VM to analyze endpoint device(s) and explore additional Wazuh capabilities. To then configure and utilize Wazuh to harden endpoint security/remediate vulnerabilities from added devices.

Setting up Virtual Machine and Wazuh

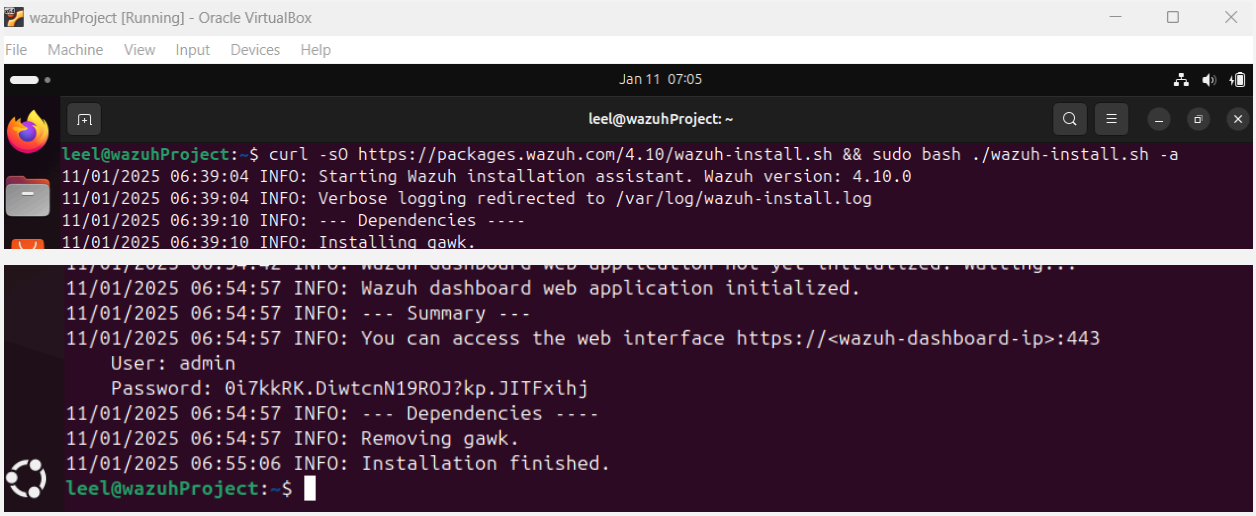
Installed Oracle VM and Ubuntu linux to set up a linux VM:



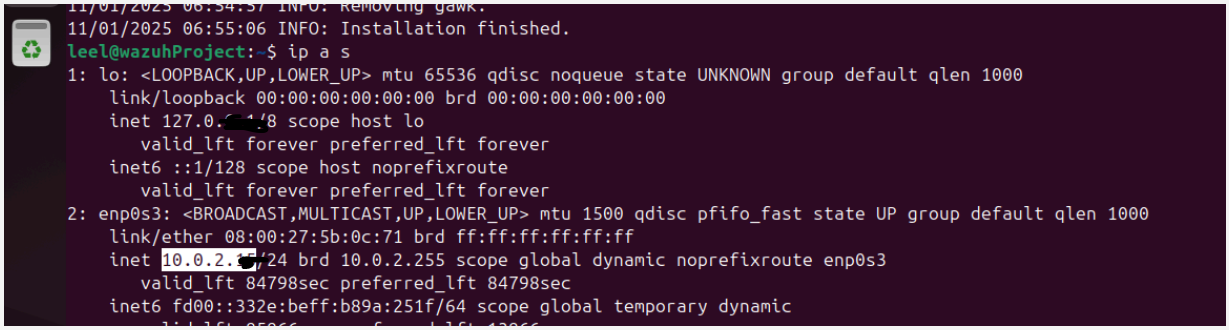


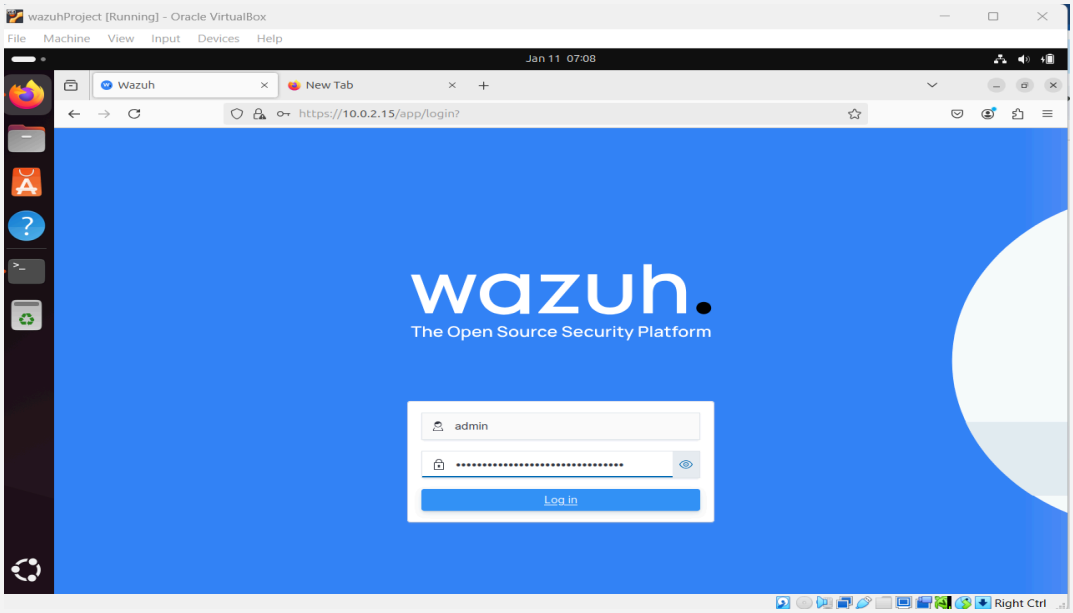
Installed Wazuh in the linux terminal once logged into Ubuntu. Ensured **hardware requirements** were met to install Wazuh.

- **Received log in credentials and instructions during installation**

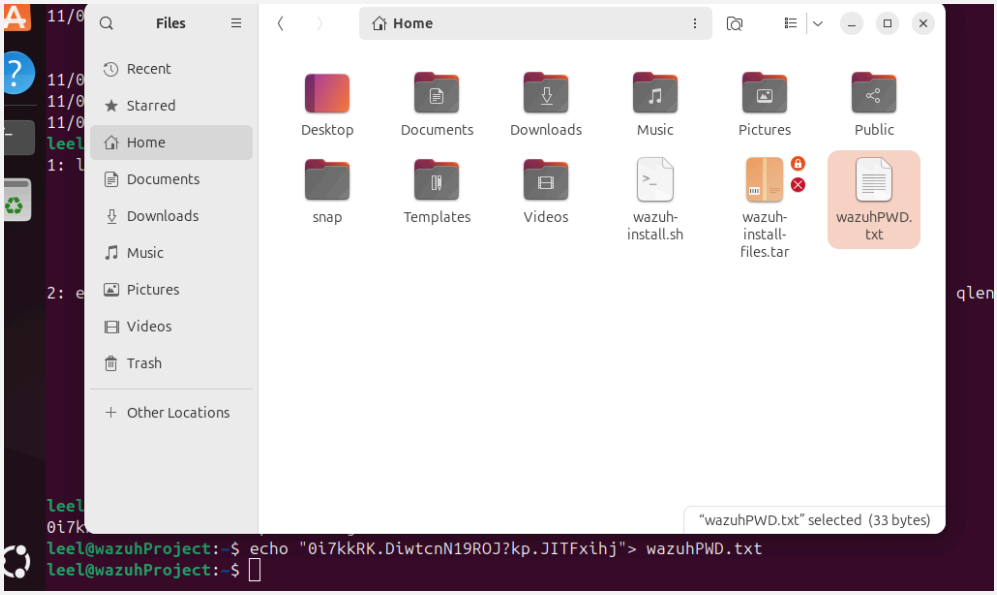


- Used “ip a s” command to receive the ip address of the VM to be able to access the Wazuh interface/dashboard in the browser.



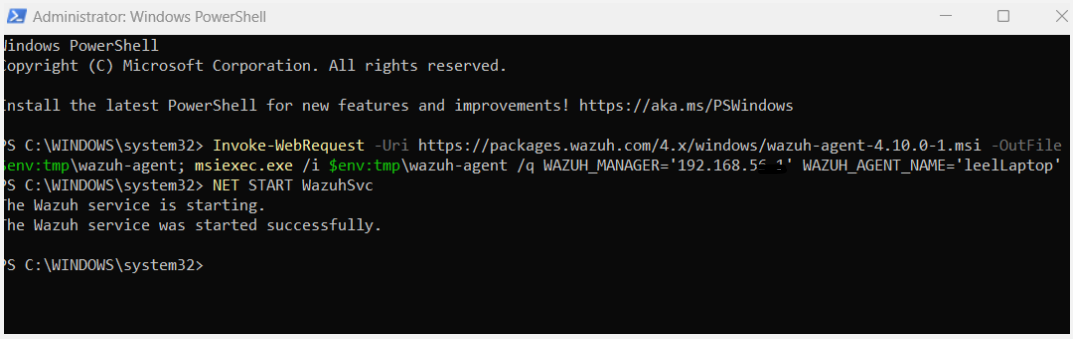


- Used command (echo “provided_password_txt”> file_Name.txt) to place the provided password in a text file for future use.



Add endpoint device to Wazuh once able to log in to the platform

- Utilizing Windows device and used the following commands to connect device to Wazuh server
- Used Windows Powershell as admin

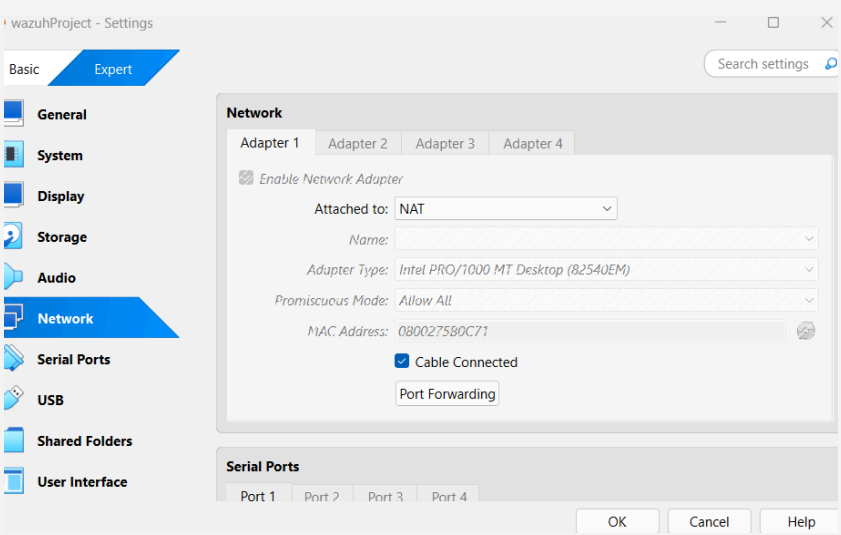


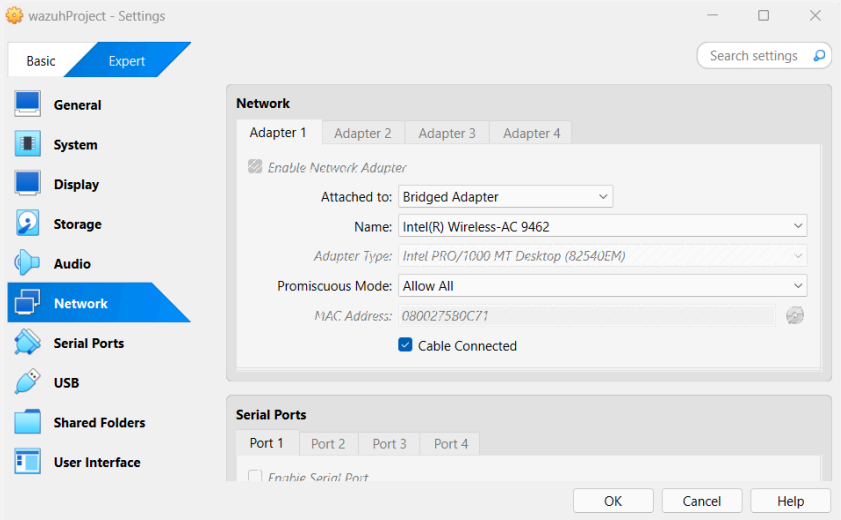
Obstacles

Troubleshooting process I had endured:

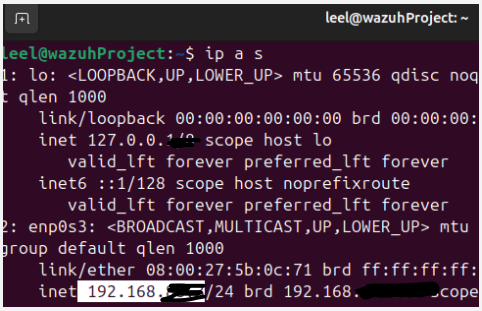
- After running the commands above to add a Windows device to Wazuh, I noticed the device did not add properly.
- Tested the network connection of the VM to Windows device, and the status failed.
- Confirmed the ip addresses of both machines were accurate and analyzed the VM's network settings.
- Found a solution of switching the network adapter from NAT to bridged to enable a shared network.
- Tested the network connection of the two machines and it was successful. Enabling myself to add the Windows machine properly.
- Would have analyzed if the necessary ports were open and view if there were any network security such as firewalls preventing access

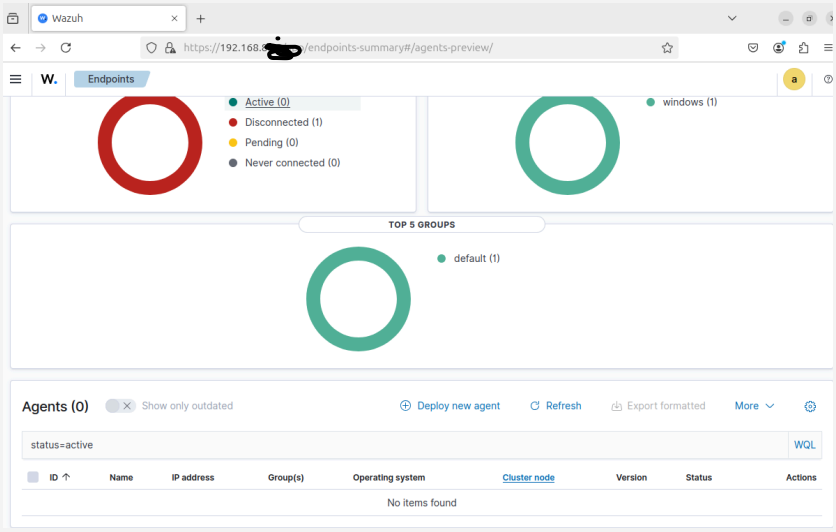
```
PS C:\Program Files (x86)\ossec-agent> Test-NetConnection -ComputerName 10.0.2.15 -Port 1515
WARNING: TCP connect to (10.0.2.15 : 1515) failed
WARNING: Ping to 10.0.2.15 failed with status: TimedOut


ComputerName            : 10.0.2.15
RemoteAddress           : 10.0.2.15
RemotePort              : 1515
InterfaceAlias          : Wi-Fi
SourceAddress           : 192.168.88.9
PingSucceeded           : False
PingReplyDetails (RTT)  : 0 ms
TcpTestSucceeded        : False



PS C:\Program Files (x86)\ossec-agent> Test-NetConnection -ComputerName 192.168.88.5 -Port 1515


ComputerName     : 192.168.88.5
RemoteAddress    : 192.168.88.5
RemotePort       : 1515
InterfaceAlias   : Wi-Fi
SourceAddress    : 192.168.88.9
TcpTestSucceeded : True
```



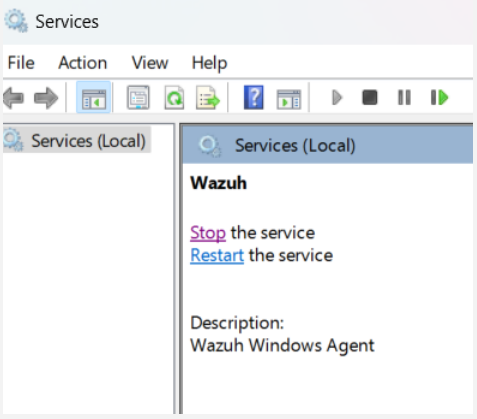


Reconnecting Windows machine to Wazuh server

- Continued this project on a new day and was unable to load up Wazuh log in page due to a VM ip address change
- Obtained current ip address from VM to use for Wazuh's login page
- 

- 

- As presented above, the Window machine disconnected
- So I stopped the current Wazuh server connection on Window machine



  - Updated Wazuh's configuration file on the windows machine and modified the updated ip address into the <Address> tag
  - Saved the "Ossec.conf" file

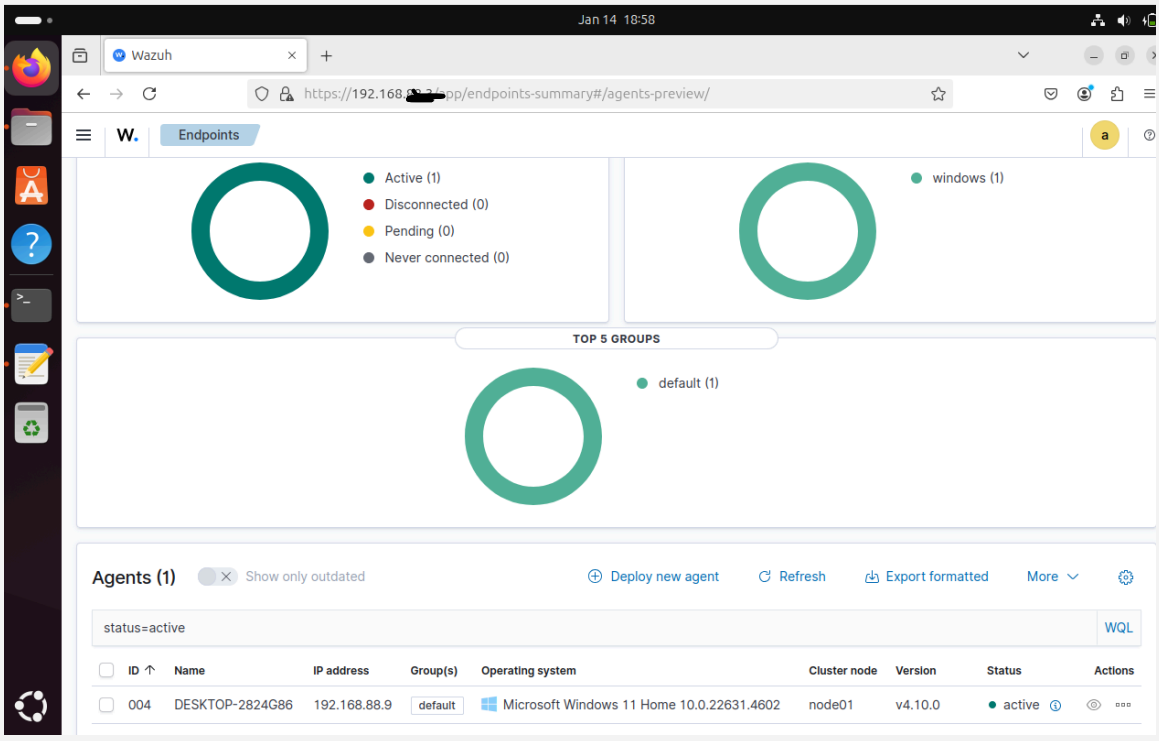
ossec.conf

File Edit View

```
<!--
  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.[redacted]</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>
  </client>
```

- Reconnected to Wazuh server on Windows Powershell as admin

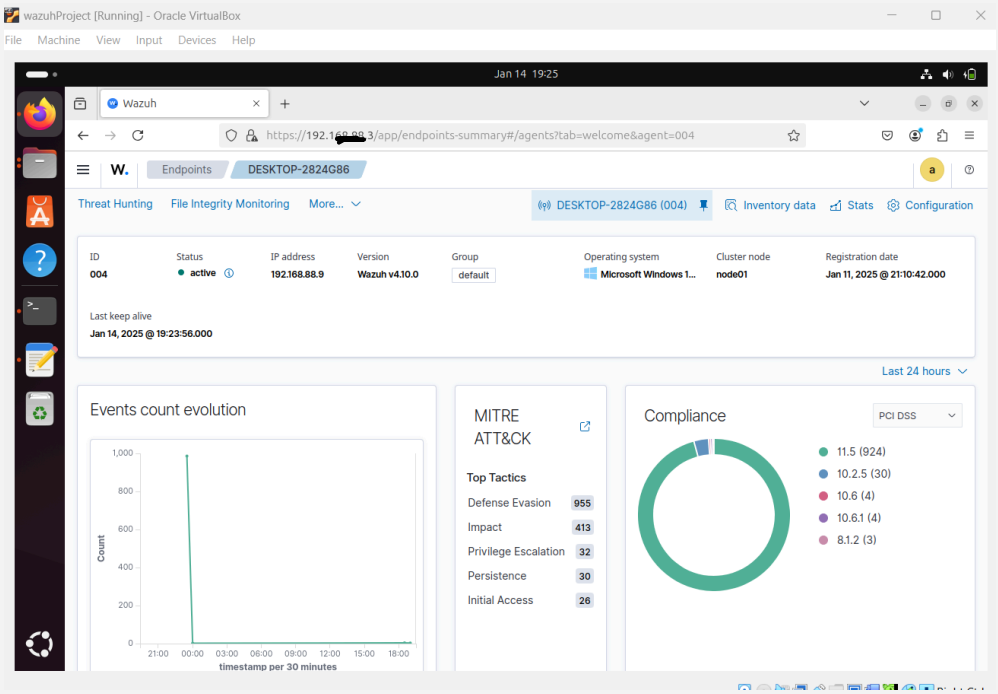
```
S C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.10.0-1.msi -OutFile
env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.[redacted]' WAZUH_AGENT_NAME='leelLaptop'
S C:\WINDOWS\system32> NET START WazuhSvc
he Wazuh service is starting.
he Wazuh service was started successfully.

S C:\WINDOWS\system32>
```



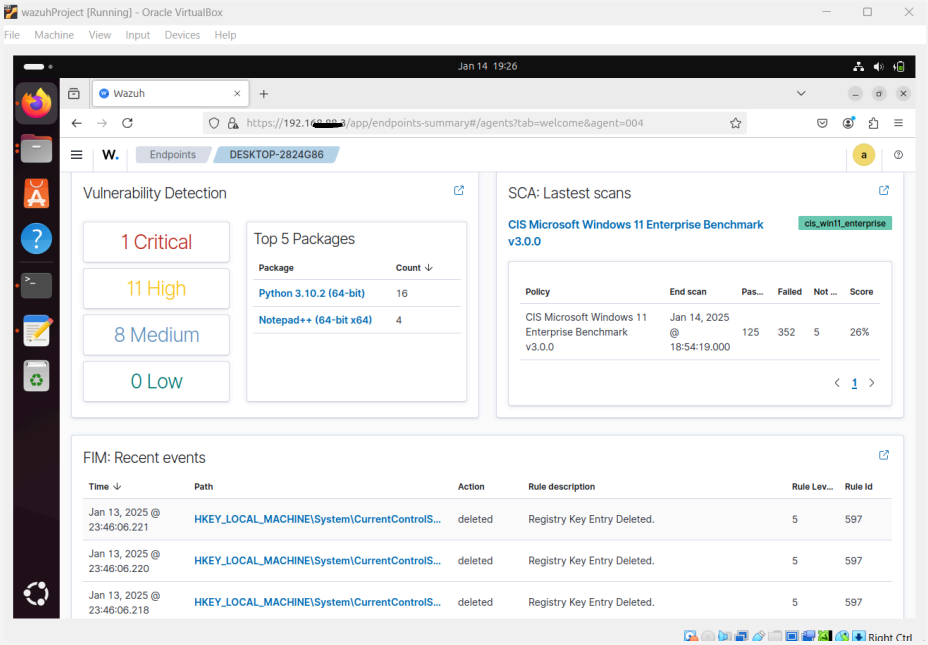
- Successfully reconnected Window machine to Wazuh

Wazuh Dashboard

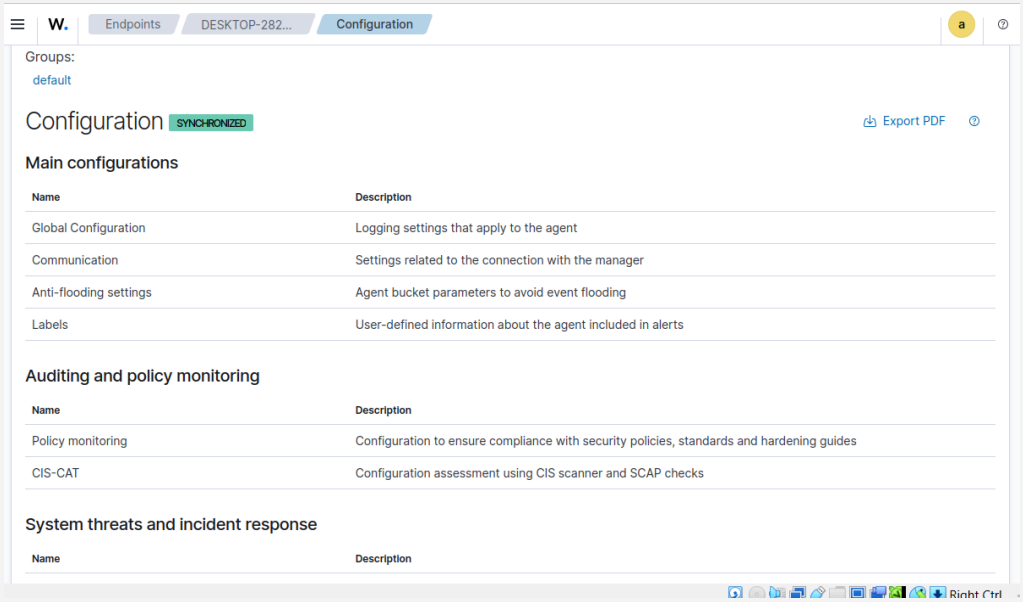
Endpoint monitoring:



- Provides essential information of each endpoint to help monitor and improve security structure. Wazuh utilizes industry known standards/regulations and databases aligned with known vulnerabilities/malware to scan endpoint devices to highlight important insights.



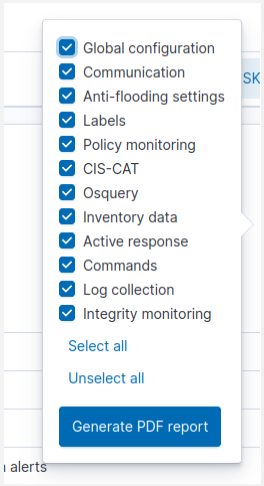
Endpoint configuration:



Main configurations such as:

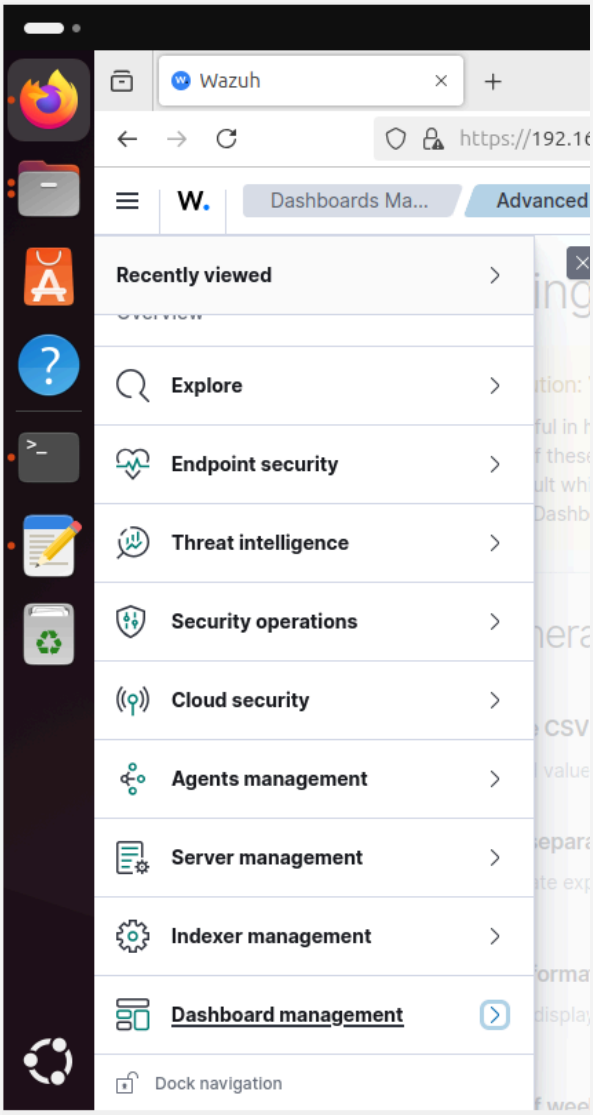
- Auditing and policy monitoring
- System threats and incident response
- Log data analysis
- Cloud security monitoring

May also export a PDF report of selected sections:



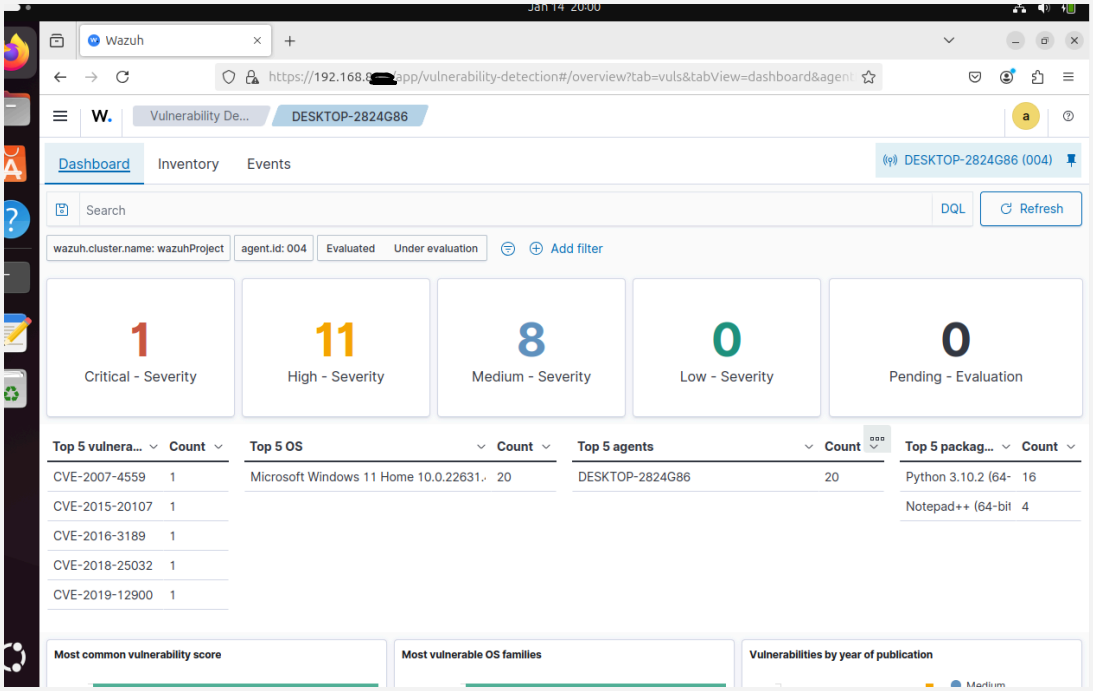
-

Tabs to navigate to:

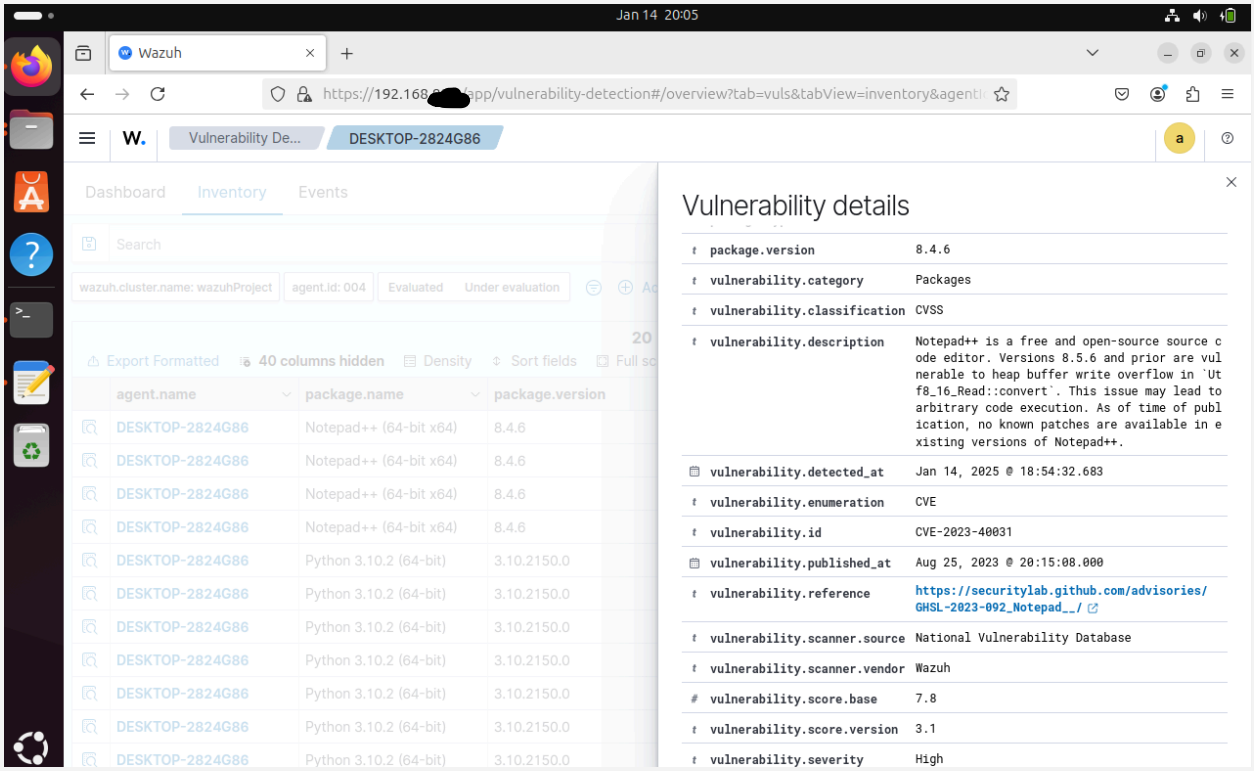


Many great capabilities with this tool. Opportunities for integrations with other tools and even cloud. Exploring each tab enables further options to enhance an individual's or group's security structure and security operations.

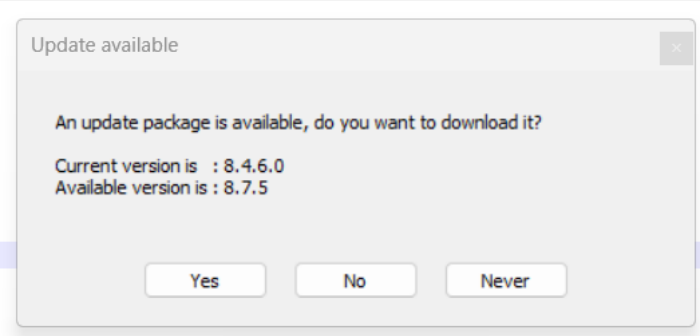
Mitigating Vulnerabilities and Improving Security Structure



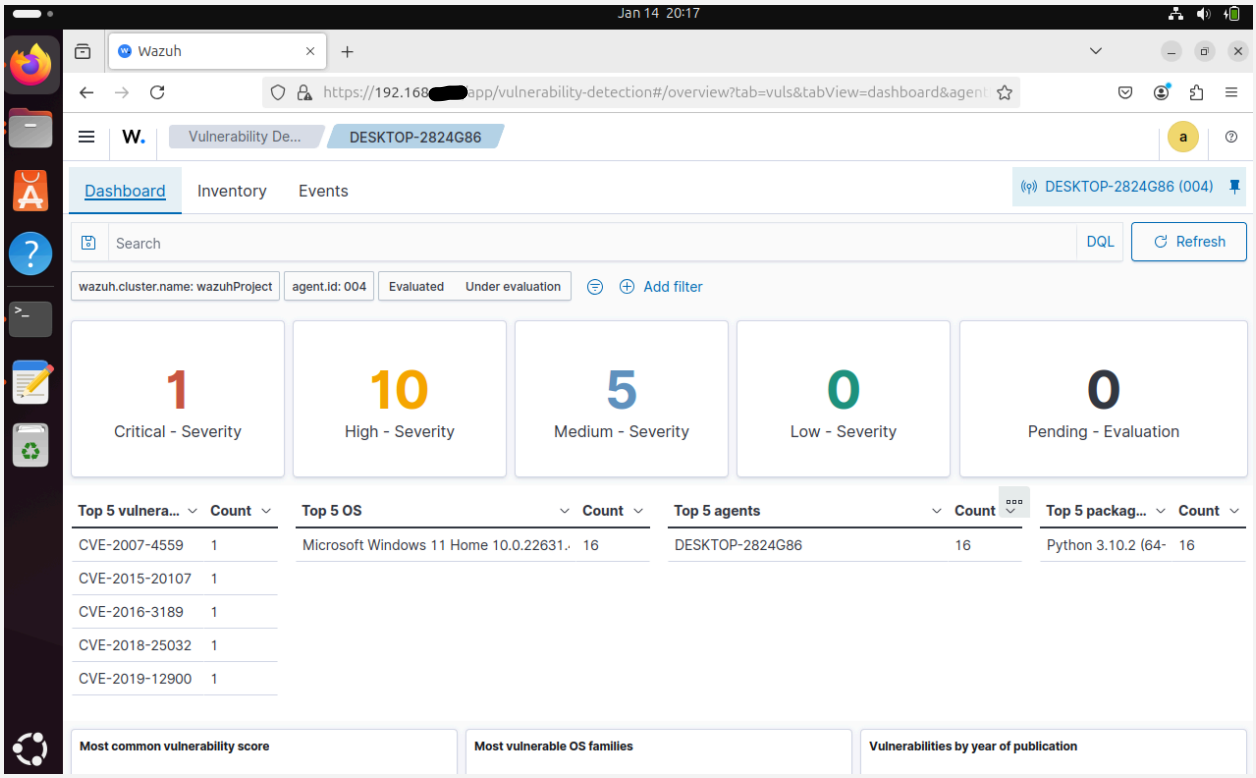
- Python v 3.10.2 and Notepadd ++ are presented as the packages that contain vulnerabilities
- Inspected a listed vulnerability and updated the app's version to view updated Wazuh dashboard



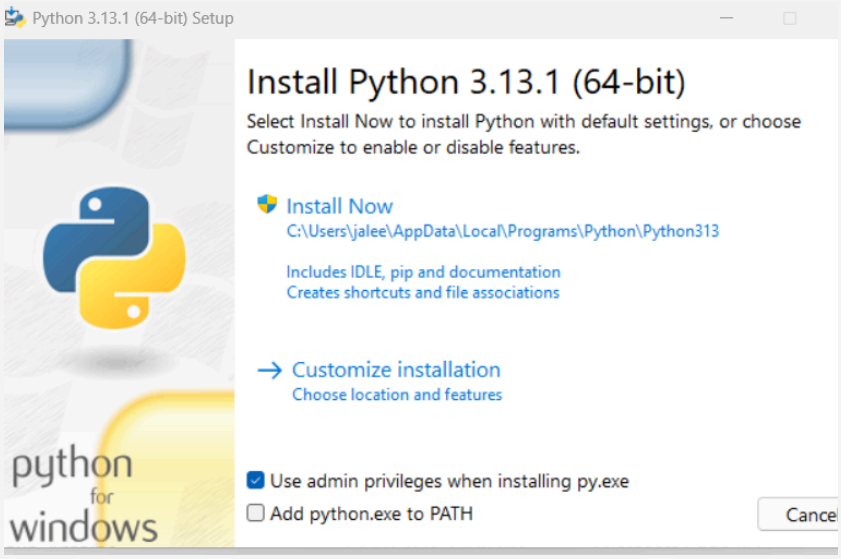
Updating notepad ++



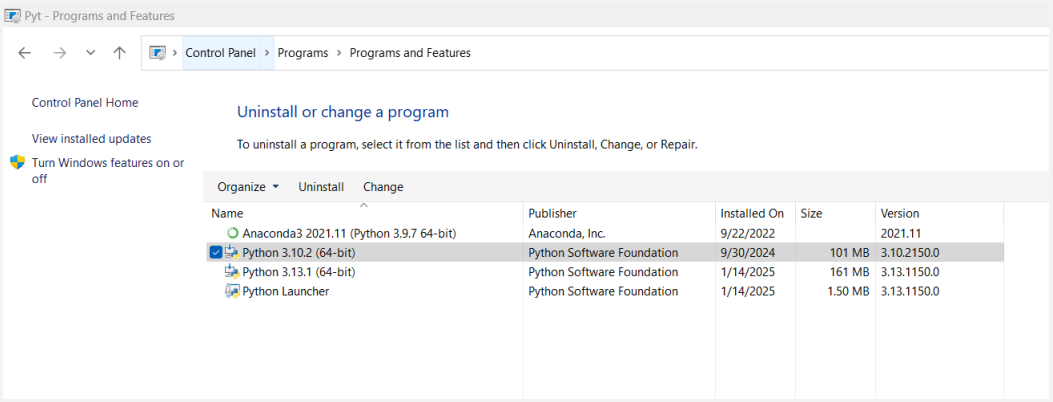
- Restarted Wazuh server on Window Machine
- Would like to possibly modify the config file on Windows machine to have Wazuh server automatically refresh when apps are updated in future scope



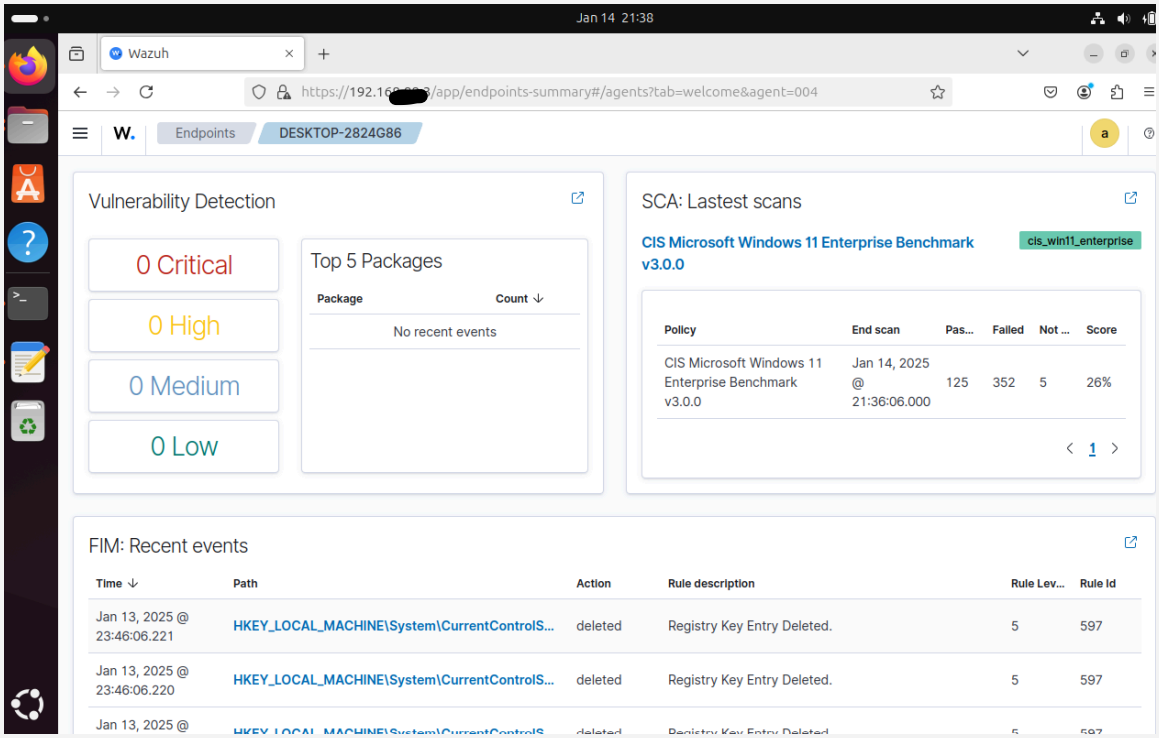
Upgraded current python to newest version



- Navigate to control panel - Program and features - Search up the package name to uninstall on windows machine

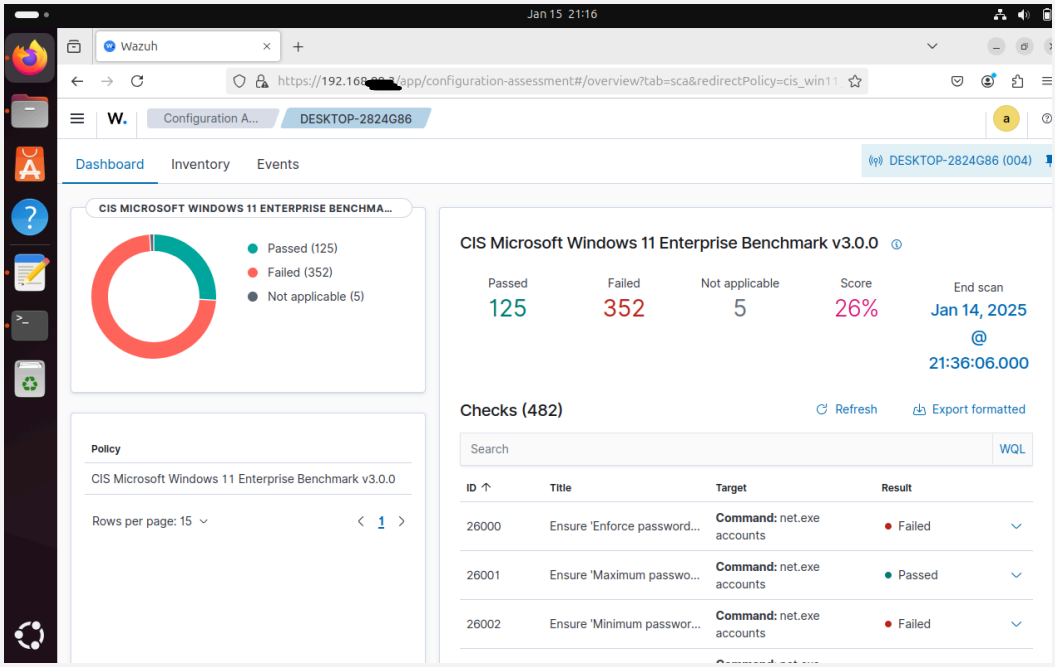


-
- Restarted Wazuh server on windows machine and viewed updated dashboard

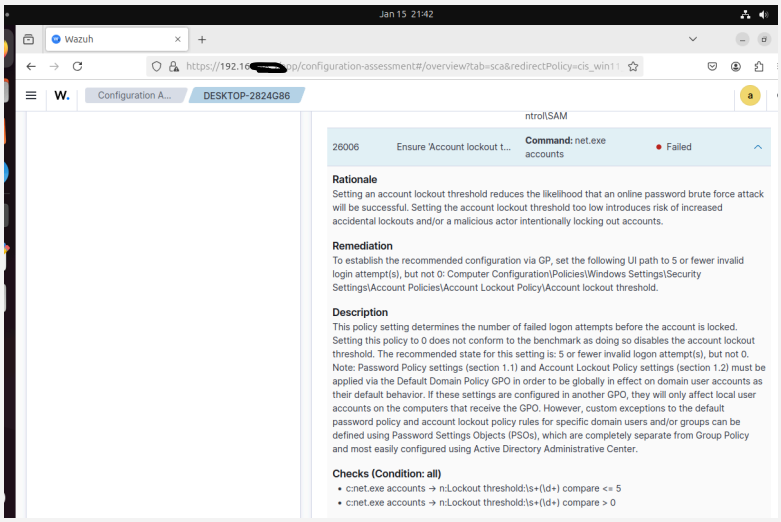

Jan 14 21:38
Wazuh
https://192.168.[redacted]/app/endpoints-summary#/agents?tab=welcome&agent=004
Endpoints
DESKTOP-2824G86
Vulnerability Detection
0 Critical
0 High
0 Medium
0 Low
Top 5 Packages
Package
Count
No recent events
SCA: Lastest scans
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0
cis_win11_enterprise
Policy
End scan
Pas...
Failed
Not ...
Score
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0
Jan 14, 2025 @ 21:36:06.000
125
352
5
26%
1
FIM: Recent events
Time
Path
Action
Rule description
Rule Lev...
Rule Id
Jan 13, 2025 @ 23:46:06.221
HKEY_LOCAL_MACHINE\System\CurrentControlS...
deleted
Registry Key Entry Deleted.
5
597
Jan 13, 2025 @ 23:46:06.220
HKEY_LOCAL_MACHINE\System\CurrentControlS...
deleted
Registry Key Entry Deleted.
5
597
Jan 13, 2025 @

SCA implements

SCA (Security Configuration Assessment) latest scan compliance/noncompliance with CIS (Center for Internet Security) Microsoft windows 11 Enterprise benchmark v3.0.0:

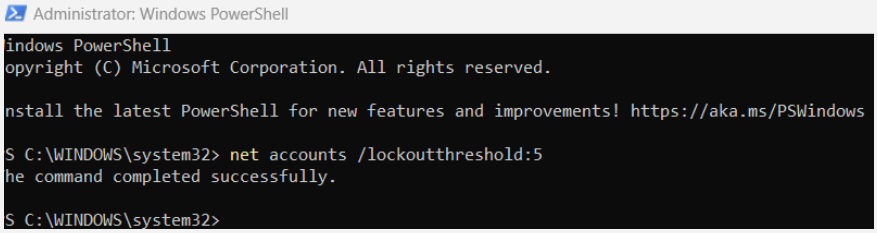


- Window device's configurations/misconfigurations that do or do not meet CIS standards.
- Used analysis to remediate risks and harden device(s) based on CIS standards to improve security settings.
- Remediated a failed control for account lockout:

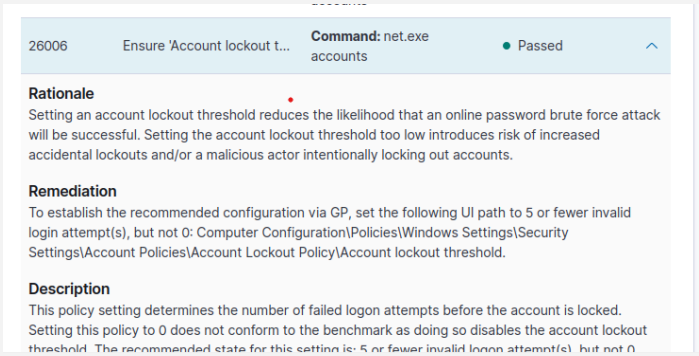


  - Provides essential information such as descriptions and remediation suggestions

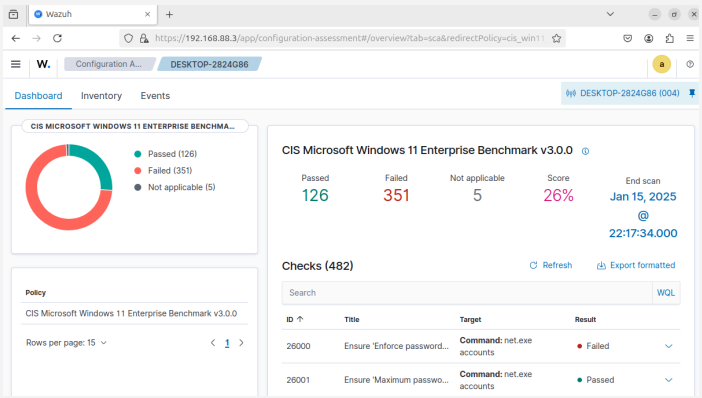
- Navigated to Windows powershell and run the following command to set threshold:



- Restarted Wazuh server on windows machine and restarted window machine
- Control updated to “pass” status, ensuring compliance with CIS policy
-



-

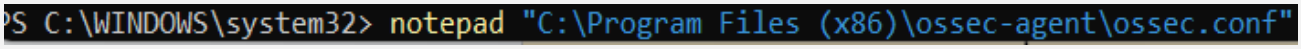


-

File integrity monitoring:

Windows Wazuh agent:

- Opened config file “ossec.conf” with admin role on Windows powershell:

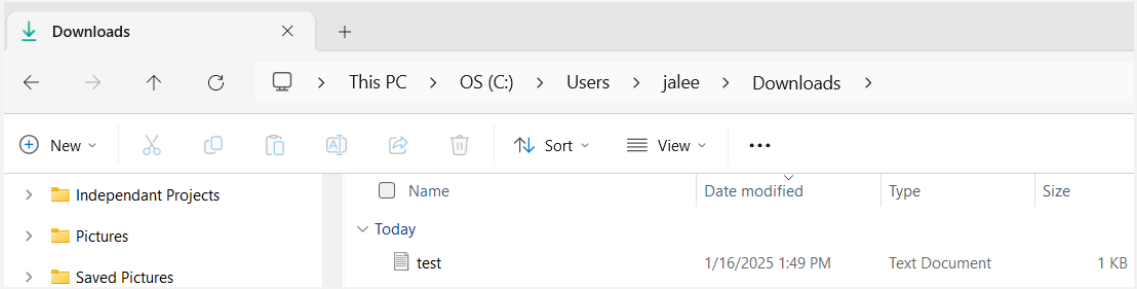


- Added Downloads directory within <syscheck> tag in config file for file monitoring in *realtime*:

```
</sca>

<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
  <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\jalee\Downloads</directories>
```

- Saved file and restarted Wazuh server on Windows agent's machine

- Added a test text file in Downloads directory.
- Modified test text file adding a sample text.

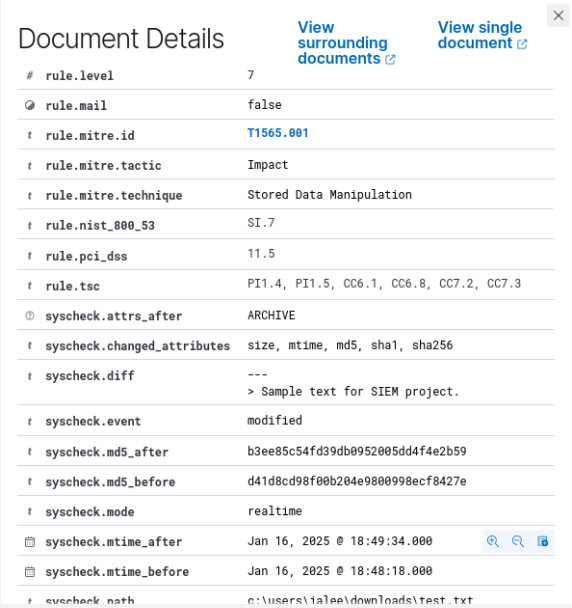


- Wazuh dashboard provided events based on the above actions

FIM: Recent events

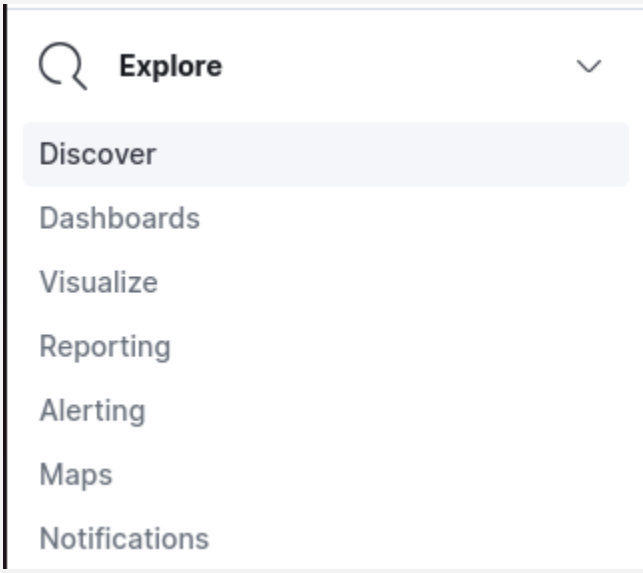
Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Jan 16, 2025 @ 18:49:34.507	c:\users\jalee\downloads\test.txt	modified	Integrity checksum changed.	7	550
Jan 16, 2025 @ 18:48:24.317	c:\users\jalee\downloads\test.txt	added	File added to the system.	5	554

- Can inspect each FIM event and analyze the info Wazuh provides:



- Data such as hash values before and after file modification
- Agent's id and ip address
- Event type
- Text value modified of before and after
- Time frames of last file modification or creation and most recent file modification
- Compliance assurance

Additional capabilities:



- Dashboard, visual, reporting capabilities for creating visualization or clustered information from Wazuh and its resources.

- Alerting enables Wazuh server logs to be reviewed and contains capabilities of using the Alert Ids in the “Ossec.conf” file to set up alert rules
- Notification options such as by email for reporting or alerts
- Detecting and removing malware using VirusTotal integration using file monitoring feature Wazuh obtains
- Blocking a known malicious actor
- Integrating a network IDS and various security tools