CySA+ Lab Series

Lab 21: Host Intrusion Detection with OSSIM

Document Version: 2022-10-10

Material in this Lab Aligns to the Following	
CompTIA CySA+ (CS0-002) Exam Objectives	1.3 - Given a scenario, perform vulnerability management activities 1.4 - Given a scenario, analyze the output from common vulnerability tools 1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities 3.1 - Given a scenario, analyze data as part of security monitoring activities 3.2 - Given a scenario, implement configuration changes to existing controls to improve security 3.4 - Compare and Contrast automation concepts and technologies 4.2 - Given a scenario, apply the appropriate incident response procedure 4.3 - Given an incident, analyze potential indicators of compromise 5.2 - Given a scenario, apply security concepts in support of organizational risk mitigation
All-In-One CompTIA CySA+ Second Edition ISBN-13: 978-1260464306 Chapters	3: Vulnerability Management Activities 4: Vulnerability Assessment Tools 7: Mitigating Controls for Attacks and Software Vulnerabilities 11: Data Analysis in Security Monitoring Activities 12: Implement Configuration Changes to Existing Controls to Improve Security 14: Automation Concepts and Technologies 16: Appropriate Incident Response Procedures 17: Analyze Potential Indicators of Compromise 20: Security Concepts in Support of Organizational Risk Mitigation

Contents

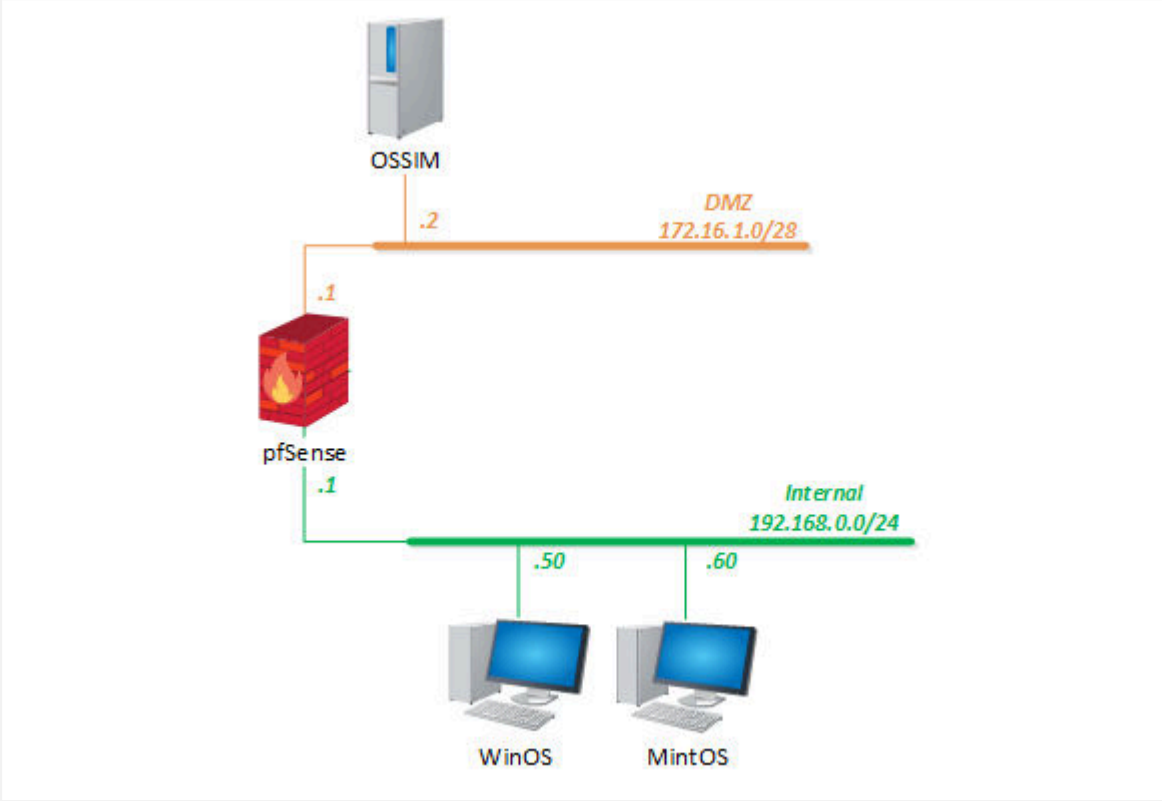
Introduction

In this lab, you will be using the Host Intrusion Detection (HIDS) agents to identify, respond, and audit the events that are occurring on the hosts in a network. In the security analyst's role, these are basic skills that are needed to be able to successfully operate a SIEM system. On top of these skills, it is also important for a SOC analyst to be able to audit the activity and identify the policies and procedures needed to mitigate the problem. Then to tie it all together, a report will need to be produced.

Objectives

- Deploying HIDS Agents
- Generate HIDS Events
- Create Custom Status Views
- Review Alarms
- Creating Reports

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
WinOS (Server 2019)	192.168.0.50	Administrator	NDGlabpass123!
MintOS (Linux Mint)	192.168.0.60	sysadmin	NDGlabpass123!
OSSIM (AlienVault)	172.16.1.2	root	NDGlabpass123!
UbuntuSRV (Ubuntu Server)	172.16.1.10	sysadmin	NDGlabpass123!
Kali	203.0.113.2	sysadmin	NDGlabpass123!
pfSense	203.0.113.1 172.16.1.1 192.168.0.1	admin	NDGlabpass123!

1 Accessing Alien Vault OSSIM and Configuring Networks

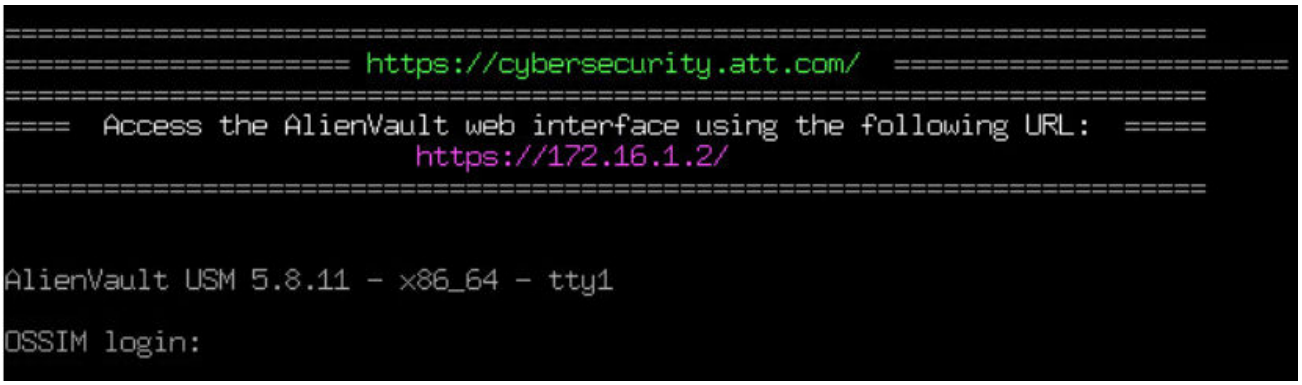
OSSIM uses network interfaces to connect to networks, monitor the networks using its IDS/IPS capabilities, run scans on assets, run vulnerability scans and generate workflows.

One of the interfaces will be designated as the Management interface. It performs network monitoring, log collection, and scanning and is the interface used to communicate to the appliance console through the Web UI. If *OSSIM* is going to be scanning only a single subnet, it is the only interface that must be configured.

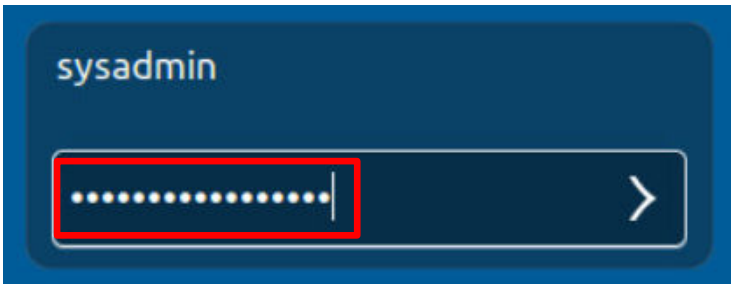
The Log Collection and Scanning interface reaches networks that are passing data back to *OSSIM* for analysis and reporting. It is also used to scan networks for assets, vulnerabilities, and availability.

Before beginning the lab, make sure that the *OSSIM* appliance has completed booting up.

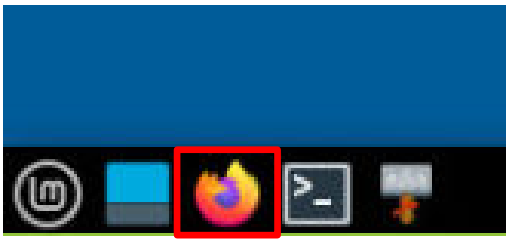
1. Set the focus to the **OSSIM** appliance.
2. Wait for the *AlianVault OSSIM* login screen to be displayed.



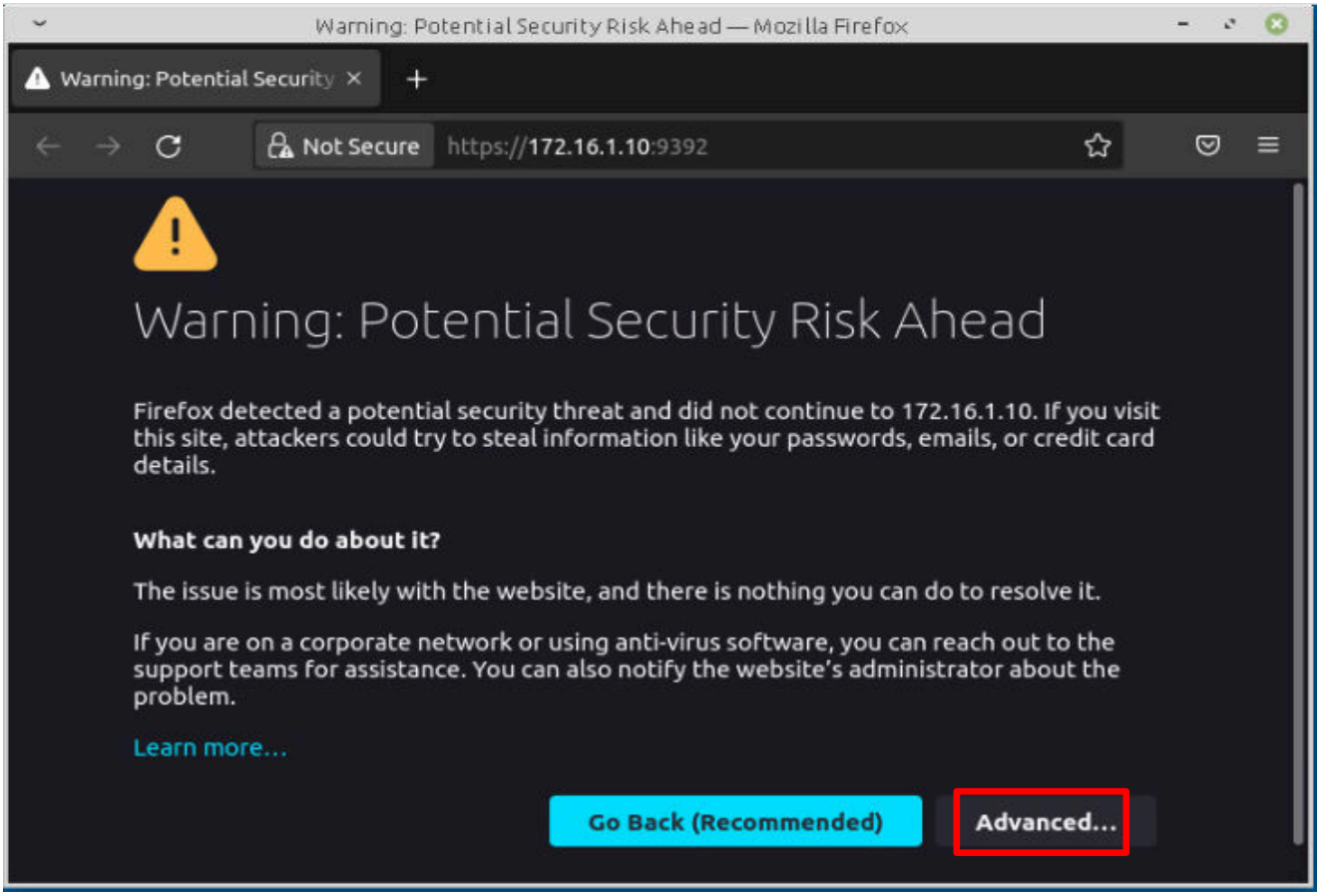
3. Set the focus on the **MintOS** computer.
4. Log in to the *sysadmin* account using the password: `NDGlabpass123!`



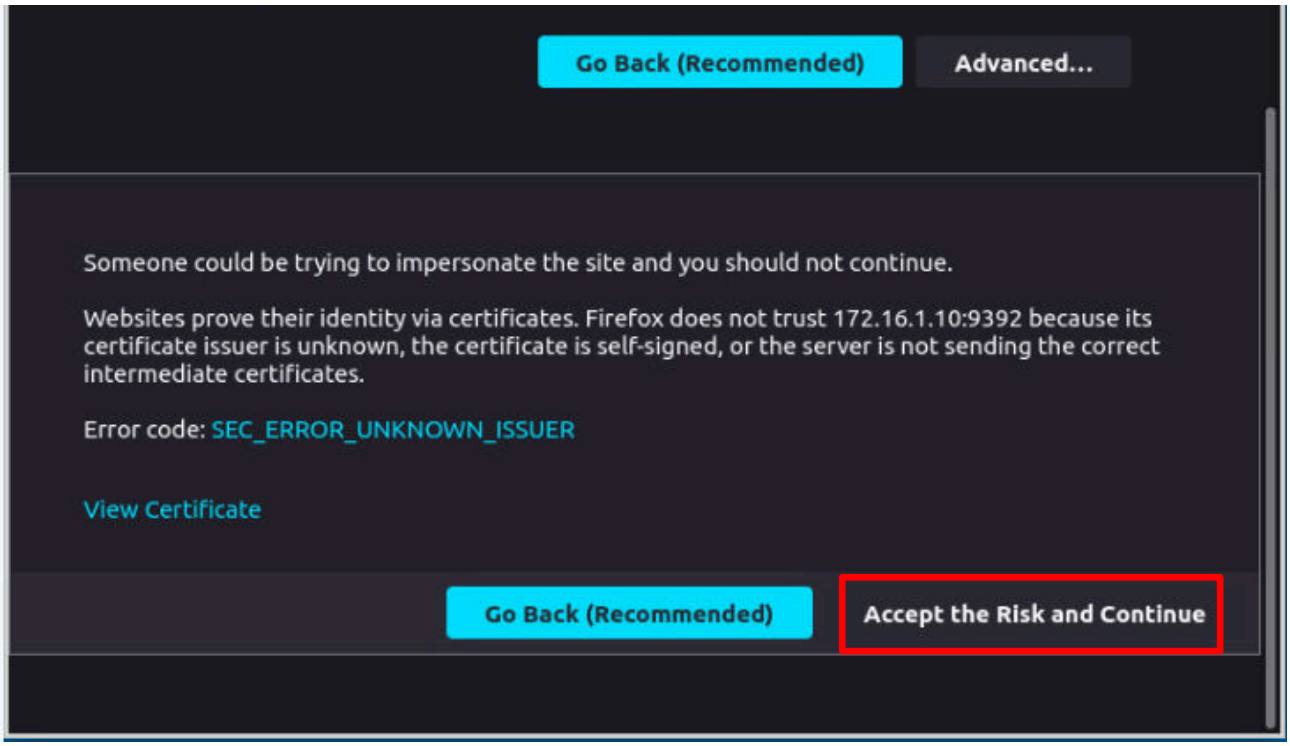
5. Open the browser by clicking on the **Firefox** icon in the toolbar at the bottom of the window.



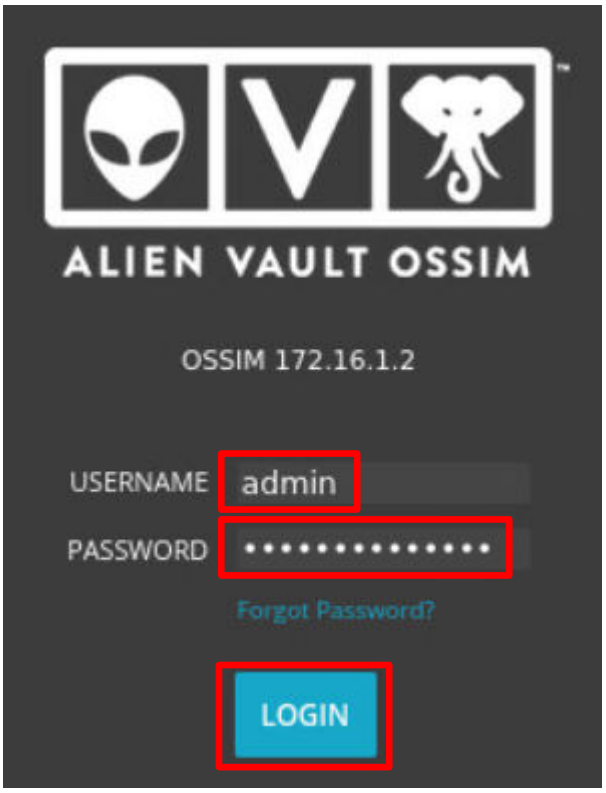
6. In the address bar of the browser, type the IP address of the *AlienVault OSSIM* appliance, `https://172.16.1.2`.
7. On the *Warning: Potential Security Risk Ahead*, click on the **Advanced** button.



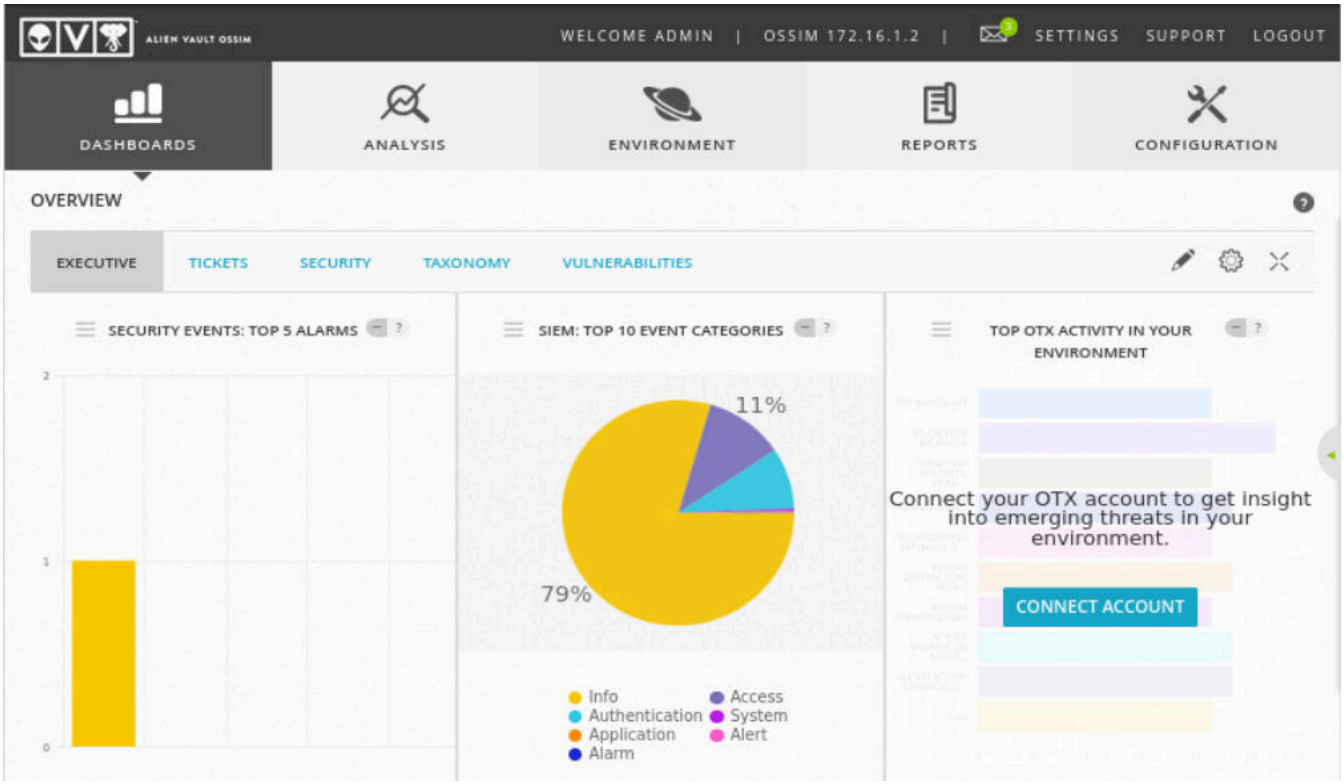
8. Scroll to the bottom of the window and click the **Accept the Risk and Continue** button.



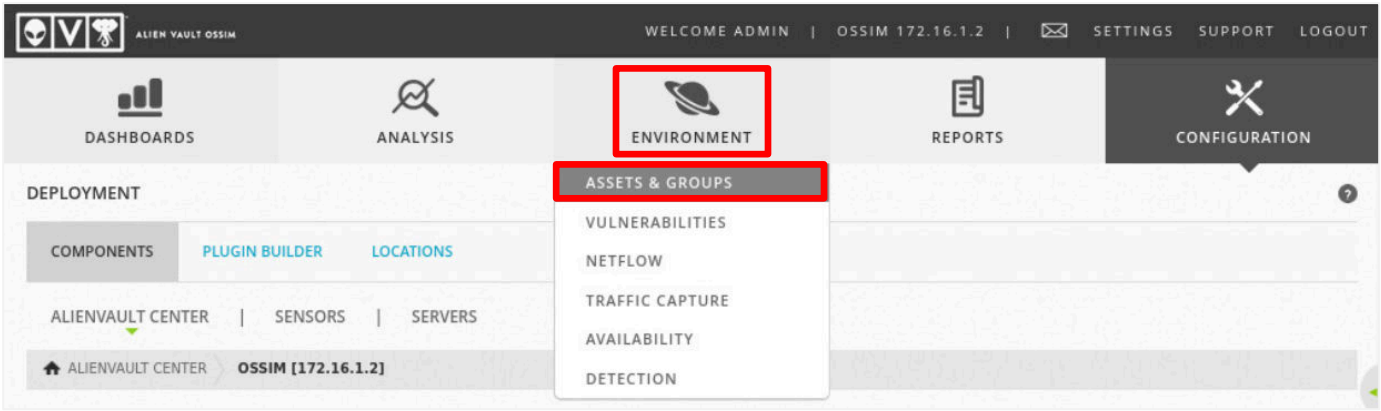
9. Log in as `admin` using the password `NDGlabpass123!` and click the **LOGIN** button.



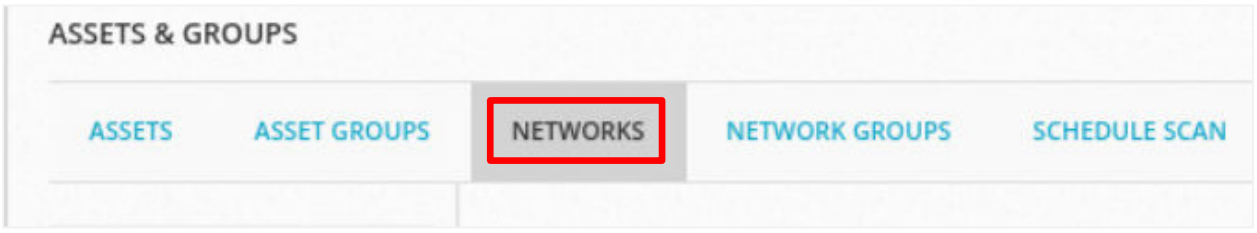
10. You will see the *OSSIM Dashboard*. The *Dashboard* displays a collection of graphs and charts that provides a high-level overview of network activity related to security events and issues.



11. You will now be adding the *Internal* network as an asset. On the top-level menu, hover over **ENVIRONMENT** and then click on **ASSETS & GROUPS**.

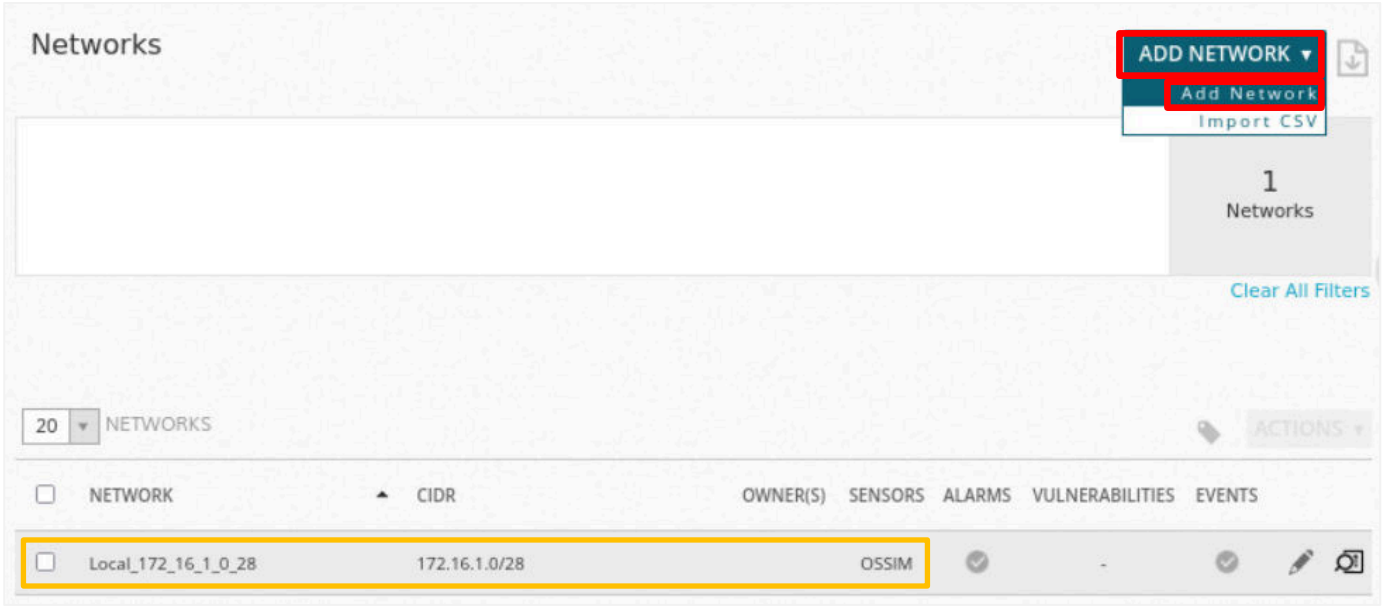


12. On the *ASSETS & GROUPS* page, click on **NETWORKS**.



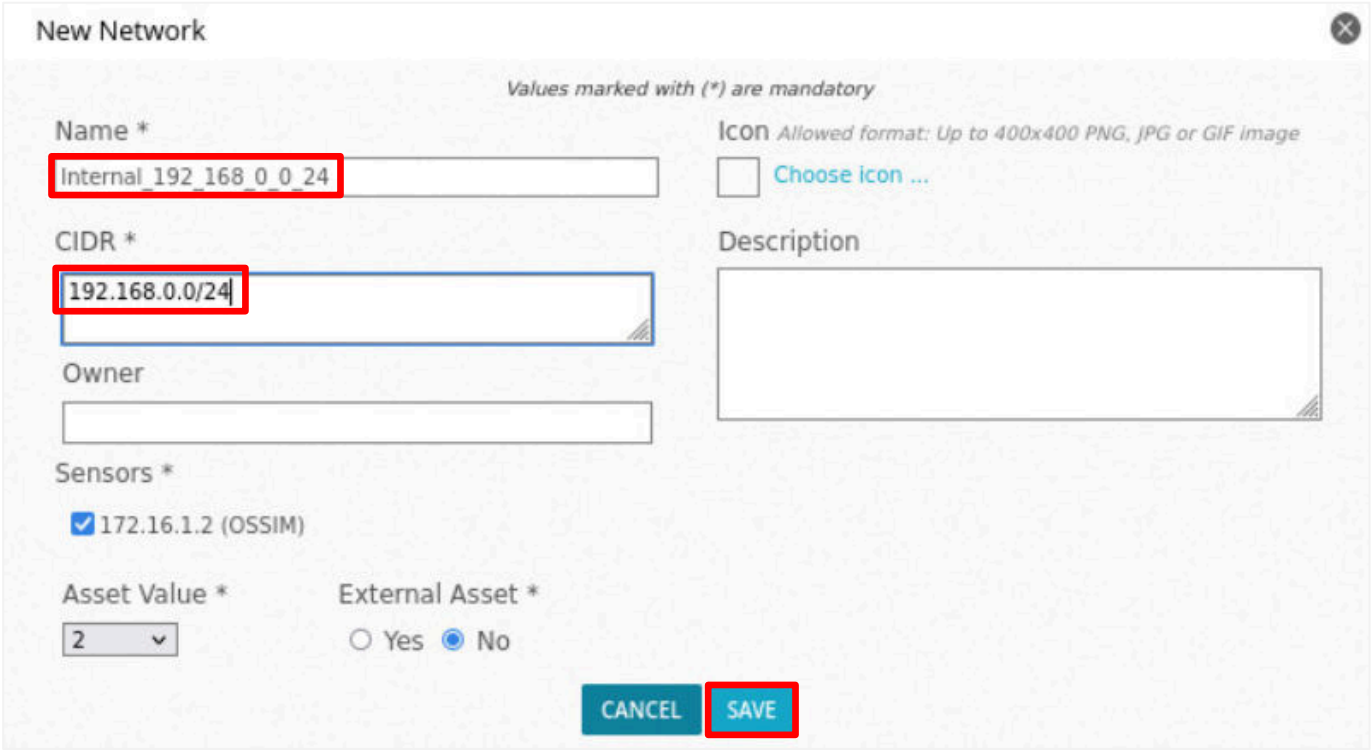
Looking at the bottom of the window, you should see the *DMZ* network, *Local_172_16_1_0_28*. This network was established when the Alien Vault OSSIM was installed.

13. On the right side of the window, click on the **ADD NETWORK** list button and click on **Add Network.**

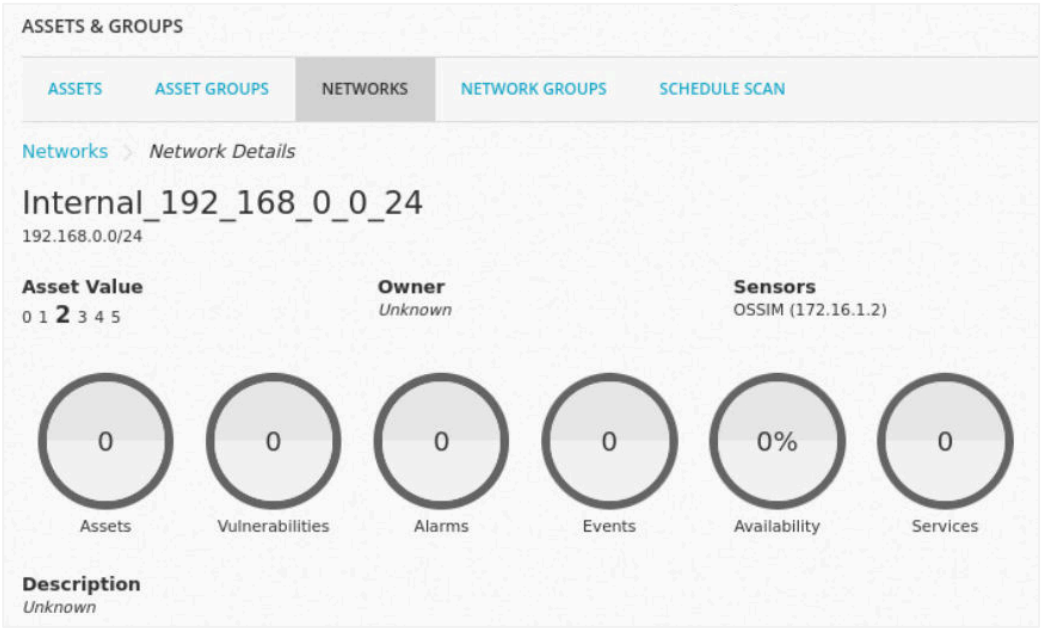


14. On the *New Network* window, type in the following and then click on the **SAVE** button at the bottom of the page.

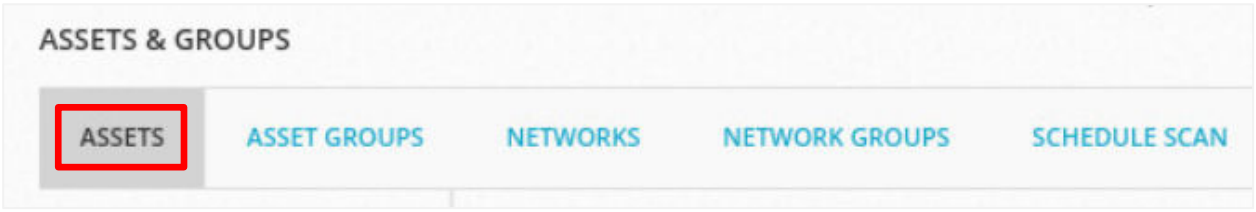
Name	`Internal_192_168_0_0_24` (the name of the network (Internal) followed by the network IP address and the subnet)
CIDR	`192.168.0.0/24` (the CIDR is the IP network address and subnet using CIDR notation)



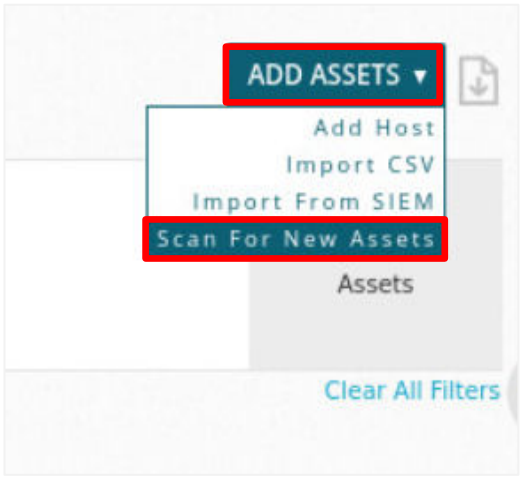
You will see the new network has been added.



15. Now search the networks for assets. Click on **ASSETS**.

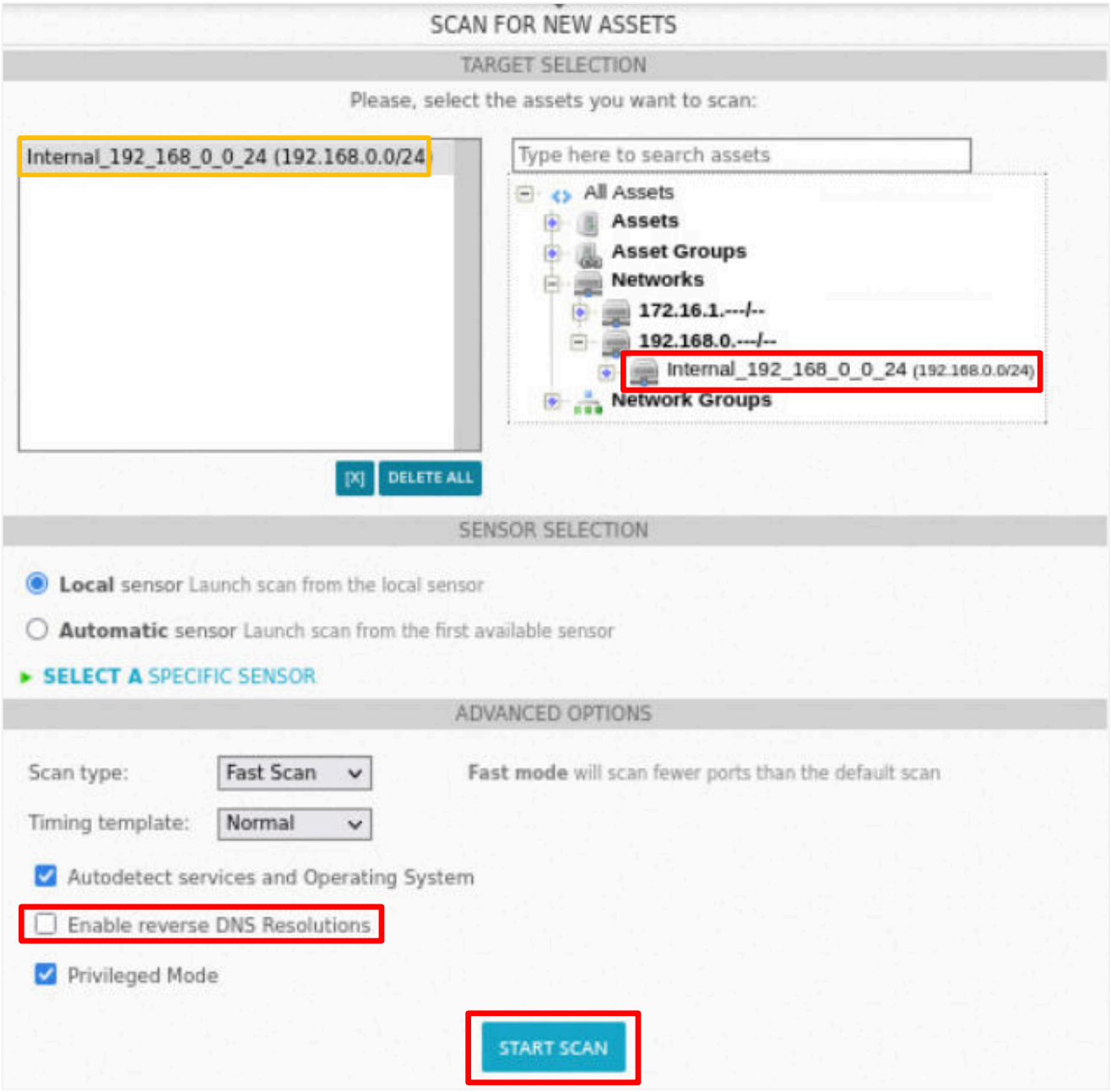


16. On the right side of the window, click on the **ADD ASSETS** list button and click on **Scan for New Assets**.

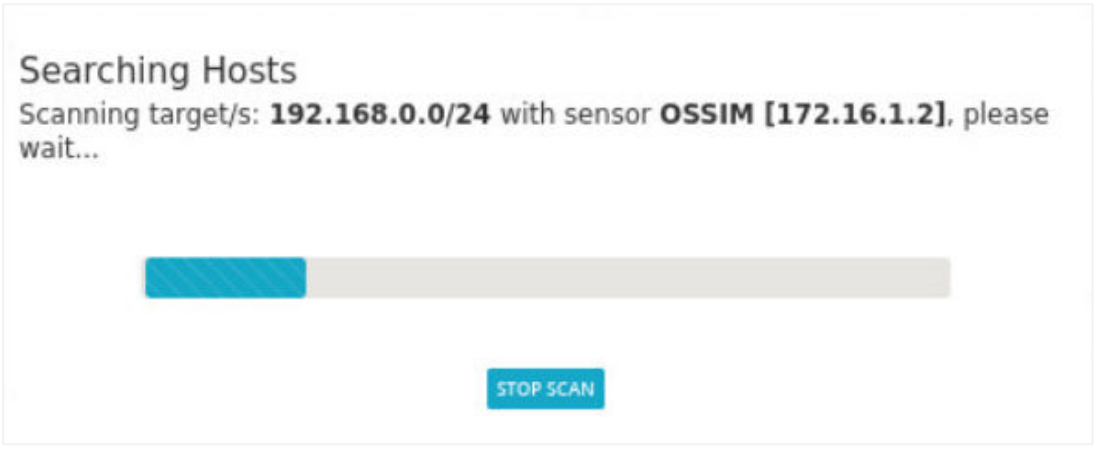


17. On the *SCAN FOR NEW ASSETS* window:

- On the right, expand **All Assets → Networks → 192.168.0.---/--**
- Click on **Internal_192_168_0_0_24 (192.168.0.0/24).**
- You will see the network added to the list on the left.
- Under the *ADVANCED OPTIONS*, uncheck **Enable reverse DNS Resolution.**
- Click on **START SCAN.**

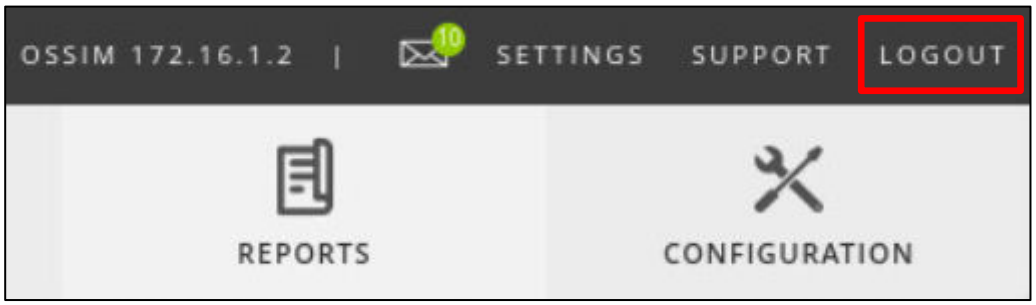


While the scan is searching for hosts, the following window will be shown:

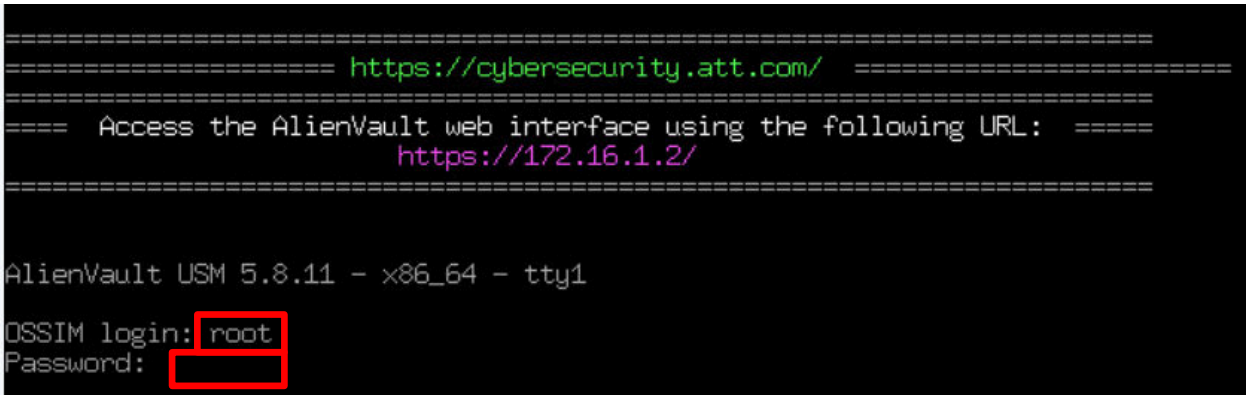


Ignore the estimated time shown at the bottom of the window. It should take less than 5 minutes to perform the scan.

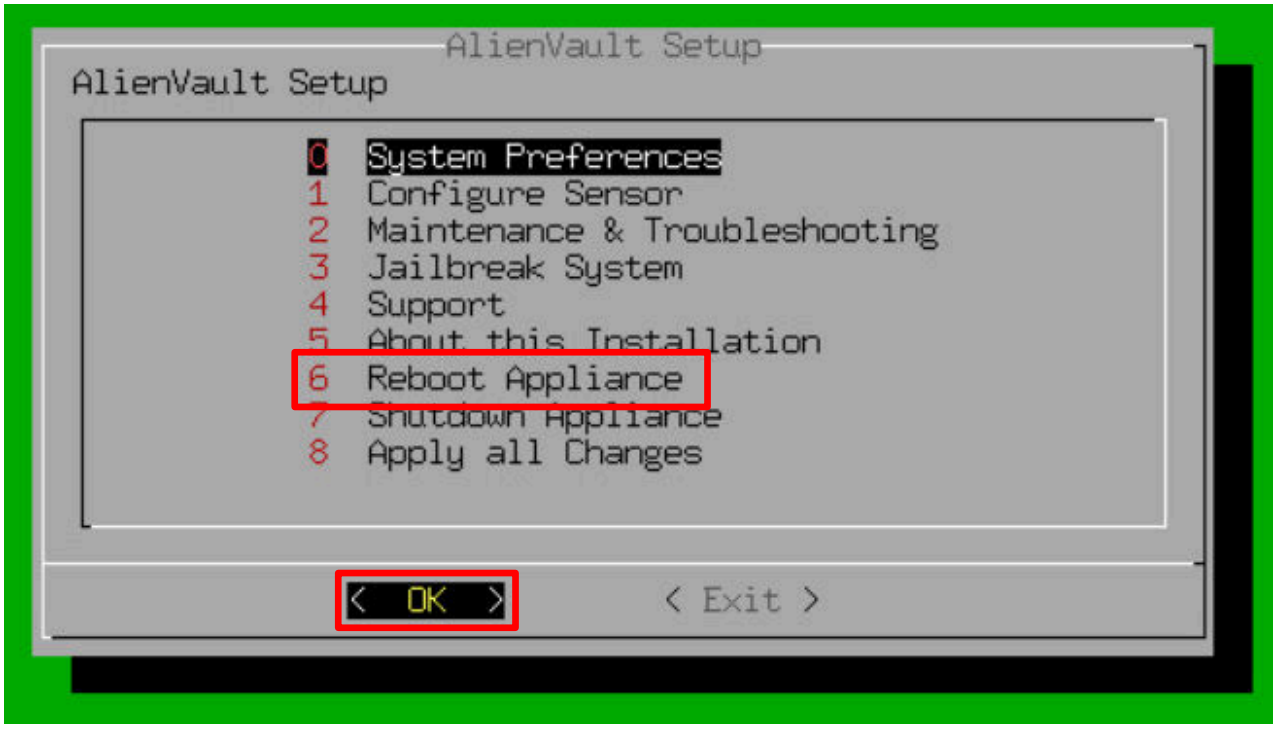
18. On the top-right side of the *AlienVault OSSIM* Web UI, click on **LOGOUT.**



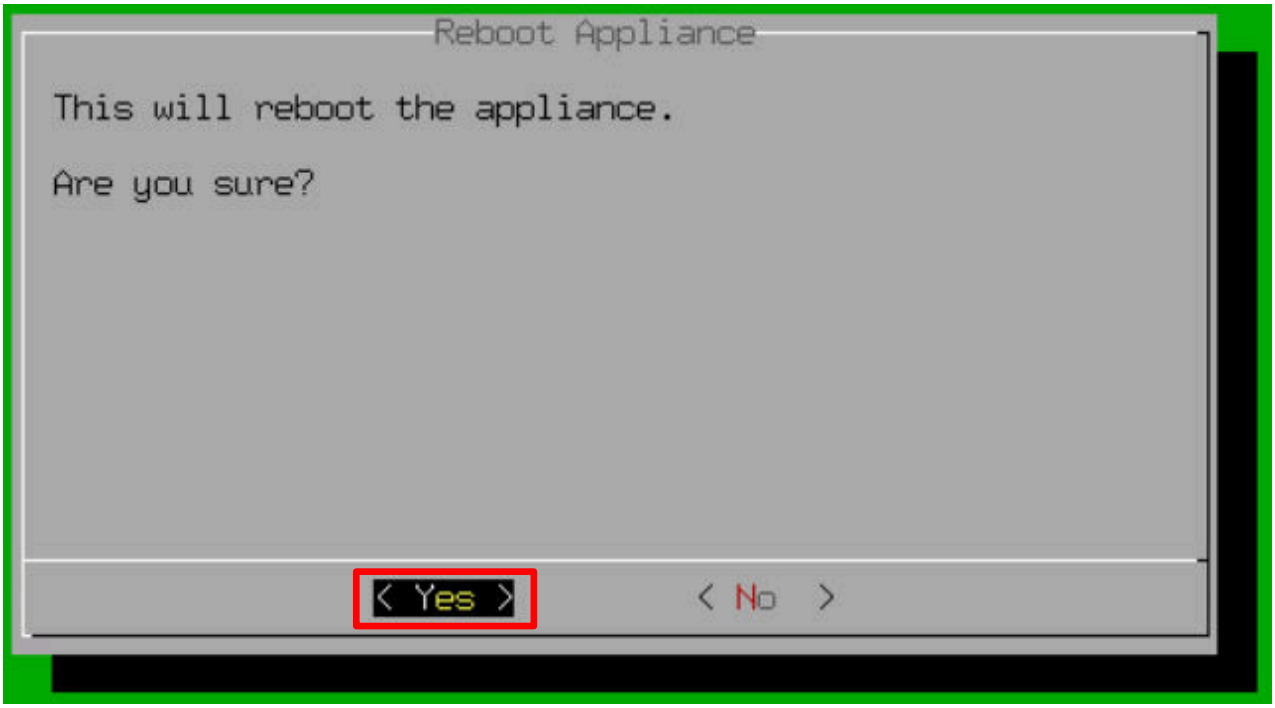
19. Close the web browser.
20. Change the focus to **OSSIM** computer.
21. Log in as `root` using `NDGlabpass!` for the password.



22. On the *AlienVault Setup* menu, select option **6 – Reboot Appliance** and press **Enter** for *OK*.

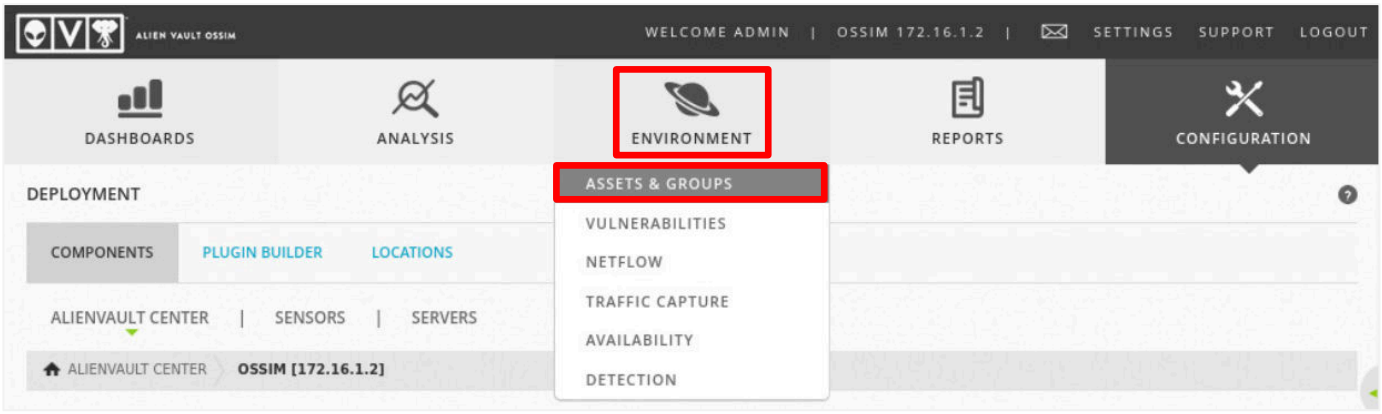


23. On the *Reboot Appliance* window, press **Enter** for *Yes*.

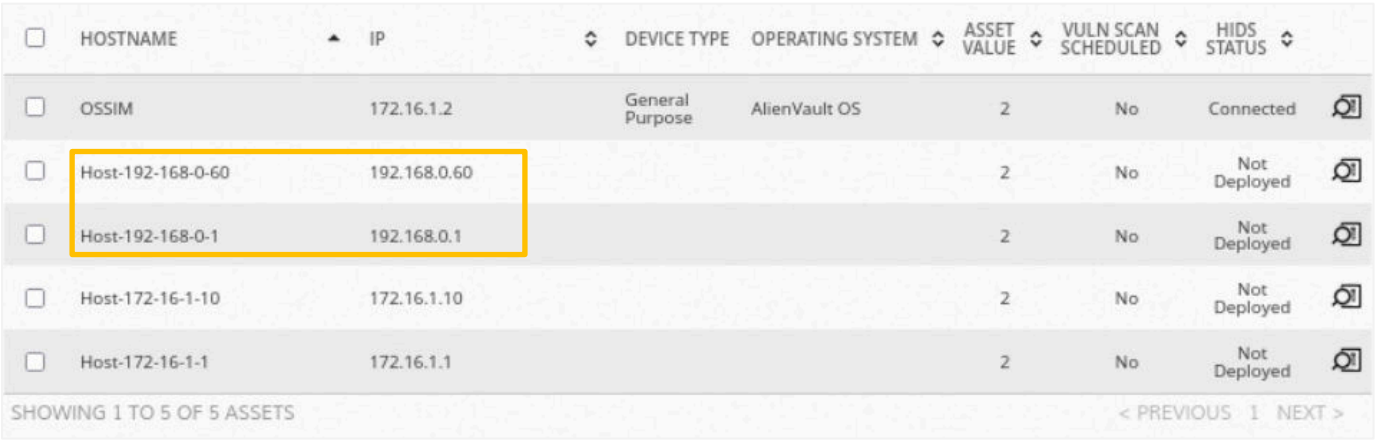


Wait for the *AlienVault OSSIM* appliance to finish rebooting before proceeding.

24. Change the focus to the **MintOS** computer.
25. Open the *Firefox* web browser, type the `address https://172.16.1.2` and log back into the *AlienVault OSSIM* appliance using `admin` for the *USERNAME* and `NDGlabpass123!` for the *PASSWORD*.
26. On the top-level menu, hover over **ENVIRONMENT** and then click on **ASSETS & GROUPS**.



Scroll down to the bottom of the page, and you will see *Host-192-168-0-60* added to the list of assets.

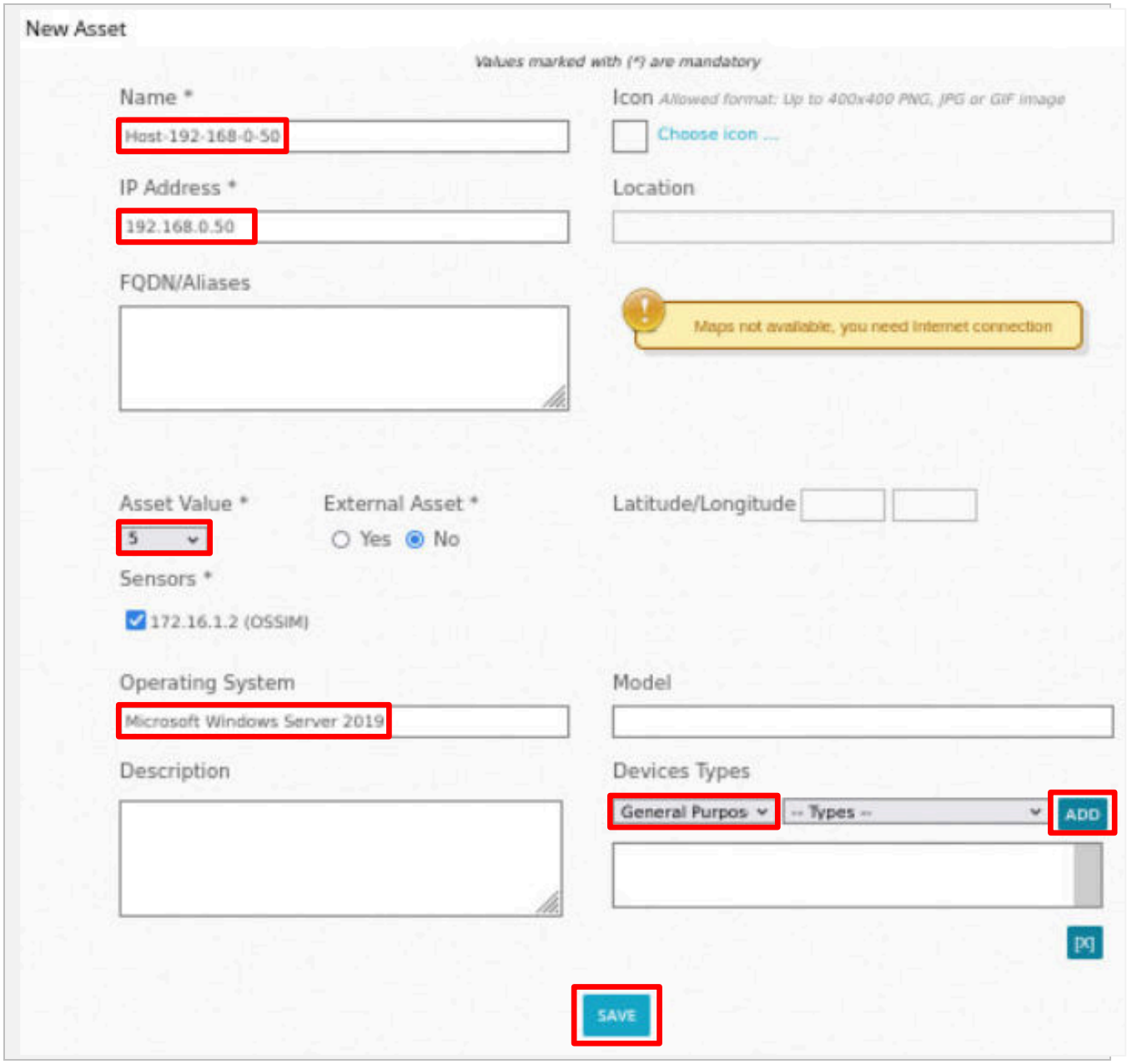


Since the *WinOS* computer has its firewall turned on, it will not be discoverable on the Asset scan. You will need to add the *WinOS* computer manually.

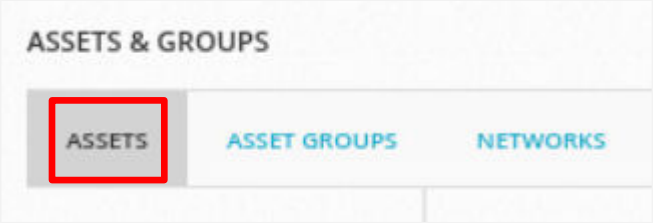
27. On the right side of the window, click on the **ADD ASSETS** list button and click on **Add Host**.

28. Type the following and then click on the **SAVE** button at the bottom of the page.

Name	`Host-192-168-0-50`
IP Address	`192.168.0.50`
Asset Value	Use the list arrow to select **5**
Operating System	**Microsoft Windows 2019 Server** (select from list)
Device Type	Use the list arrow to select **General Purpose** and click **ADD**



29. Click the **ASSETS** tab at the top of the window.



You will see the *Windows Server* host on the asset list.

HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
OSSIM	172.16.1.2	General Purpose	AlienVault OS	2	No	Connected
Host-192-168-0-60	192.168.0.60			2	No	Not Deployed
Host-192-168-0-50	192.168.0.50	General Purpose	Microsoft Windows Server 2019	5	No	Not Deployed
Host-192-168-0-1	192.168.0.1			2	No	Not Deployed
Host-172-16-1-10	172.16.1.10	General Purpose	Linux 2.6.X	5	No	Not Deployed
Host-172-16-1-1	172.16.1.1			2	No	Not Deployed

30. Remain on the *AlienVault OSSIM Web UI* and continue to the next task.

2 HIDS Event Monitoring and Reporting

"A host-based intrusion detection system (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responds by logging the activity and notifying the designated authority. A HIDS can be thought of as an agent that monitors and analyzes whether anything or anyone, whether internal or external, has circumvented the system's security policy. In this task you will generate network traffic that will alert HIDS that a potential network threat has been detected and then send an alert for identification and analysis."

https://www.techopedia.com/definition/12826/host-based-intrusion-detection-system-hids

In *Lab 20: Network Intrusion Detection with OSSIM,* you configured and used the *NIDS* built into *AlienVault OSSIM,* which uses sensors on the network to monitor the assets on the network by detecting and analyzing inbound and outbound packets in real-time.

By comparison, a *HIDS* installs agents onto specific computers which can detect and analyze traffic and monitor key system files for malicious activity.

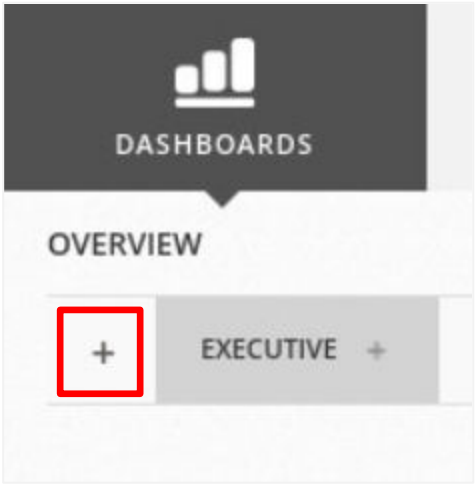
In this task, you will be deploying *HIDS Agents* on Windows and Linux computers, generating *HIDS Events*, analyzing alarms that were set by *HIDS* in reaction to the malicious events, and then compiling a report on the event for review and mitigation.

2.1 Create a Custom Dashboard View Showing HIDS Events

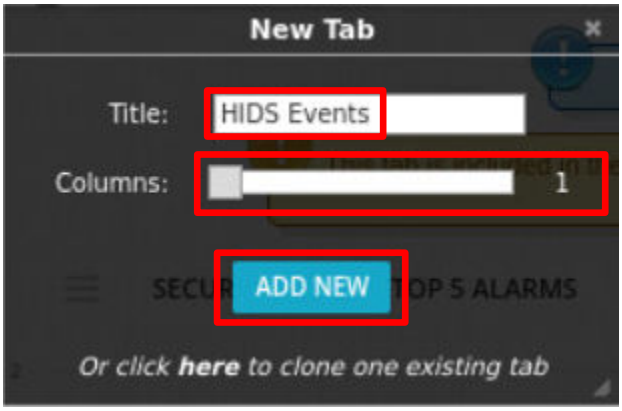
1. On the top-level menu, hover over **DASHBOARDS** and then click on **Overview**.

2. On the right side of the page, click on the **Switch to Edit Mode** icon (the pencil).

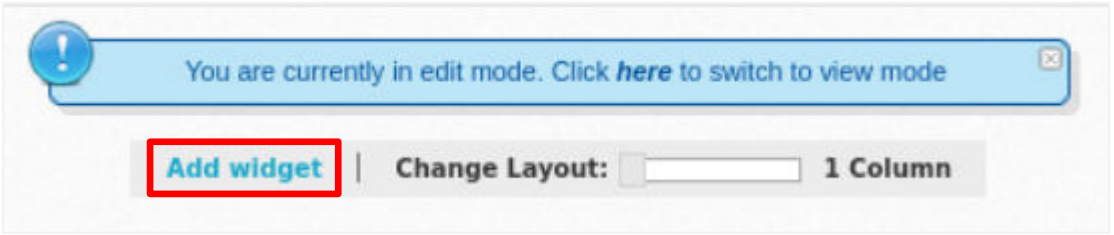
3. You will be in the **Edit Mode** for the *Dashboard*. On the left side of the tab list, click on the **+** icon on the left side of the *Tab* list.



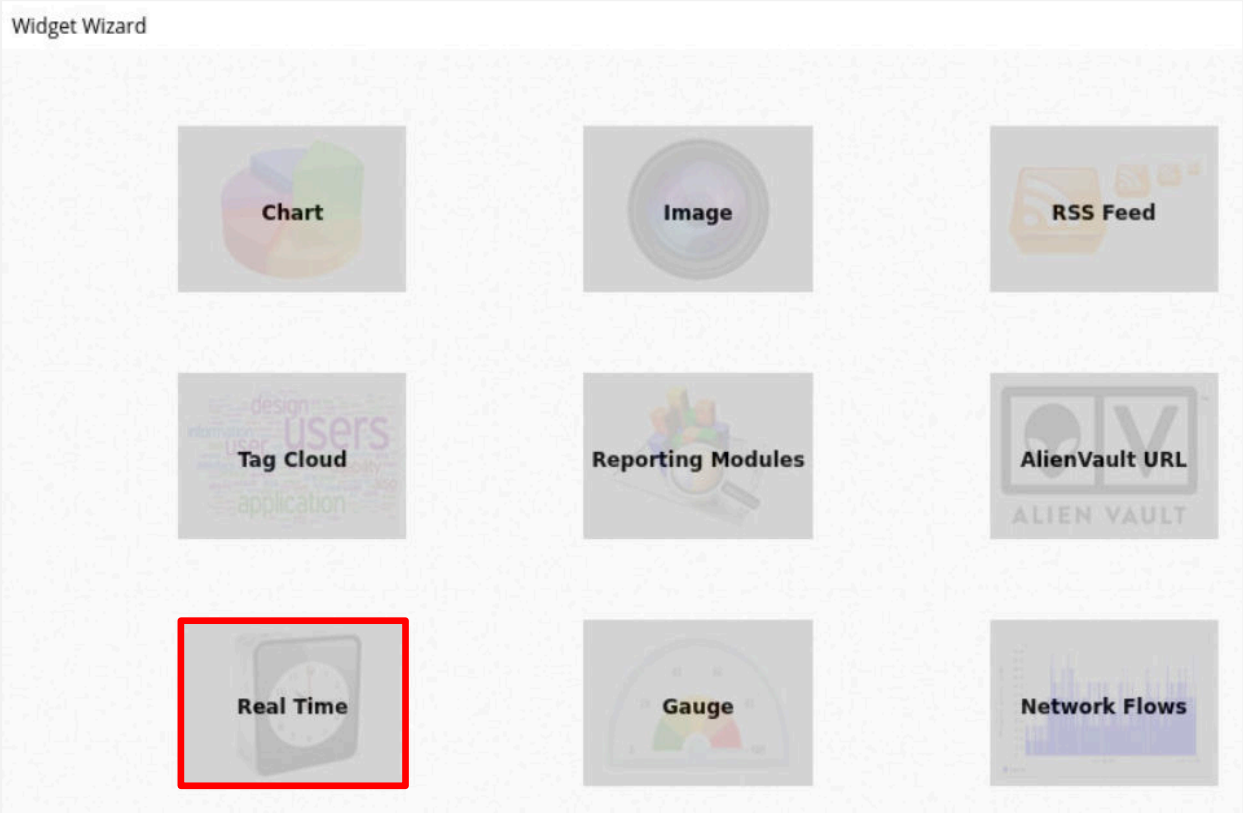
4. In the *New Tab* window, type `HIDS Events` for the *Title* and move the slider to **1** in *Columns*. Then click on the **ADD NEW** button.



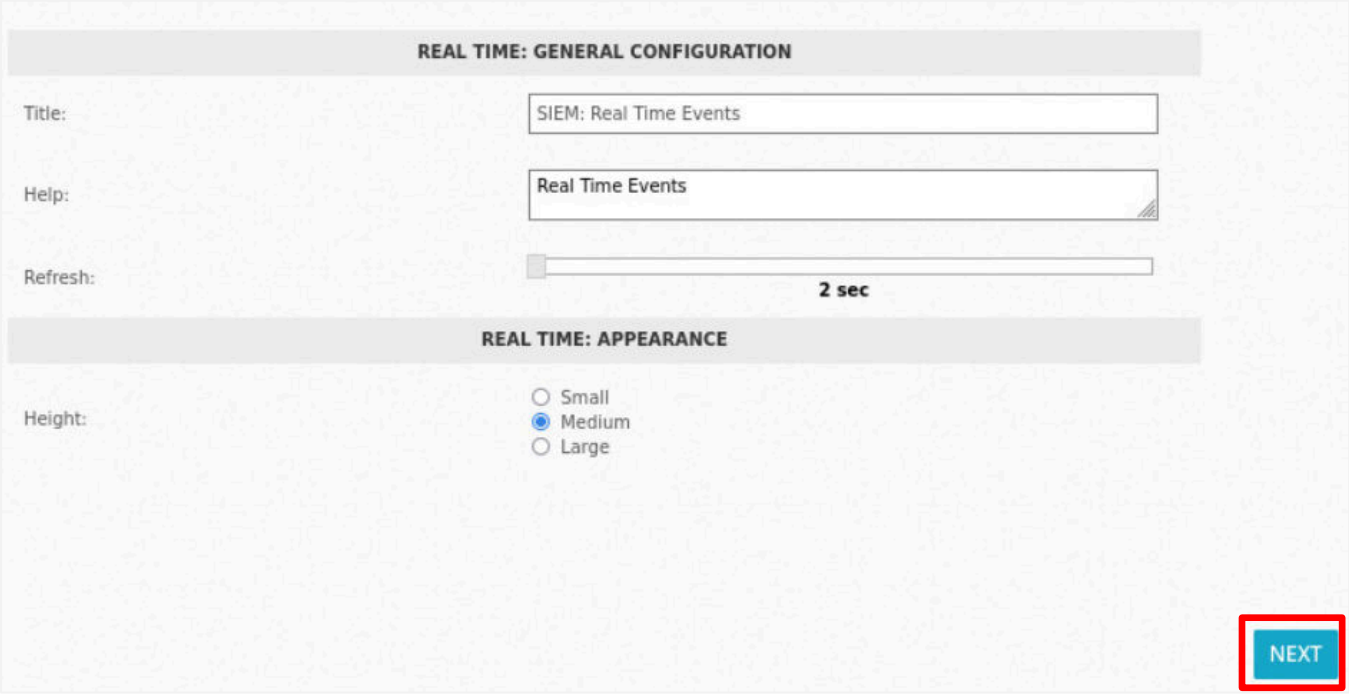
5. Click on the **Add Widget** link.



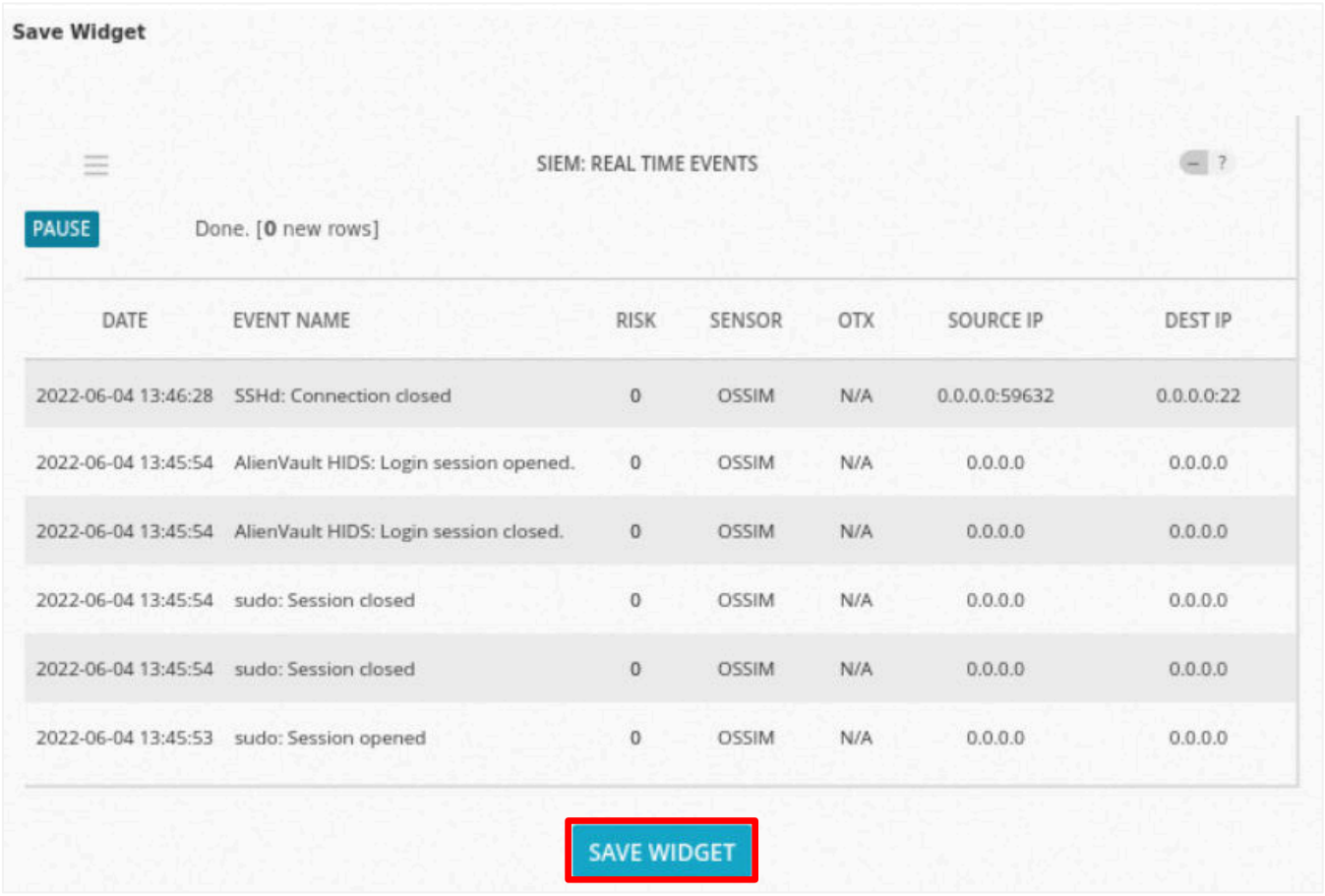
6. On the *Widget Wizard* page, click on **Real Time.**



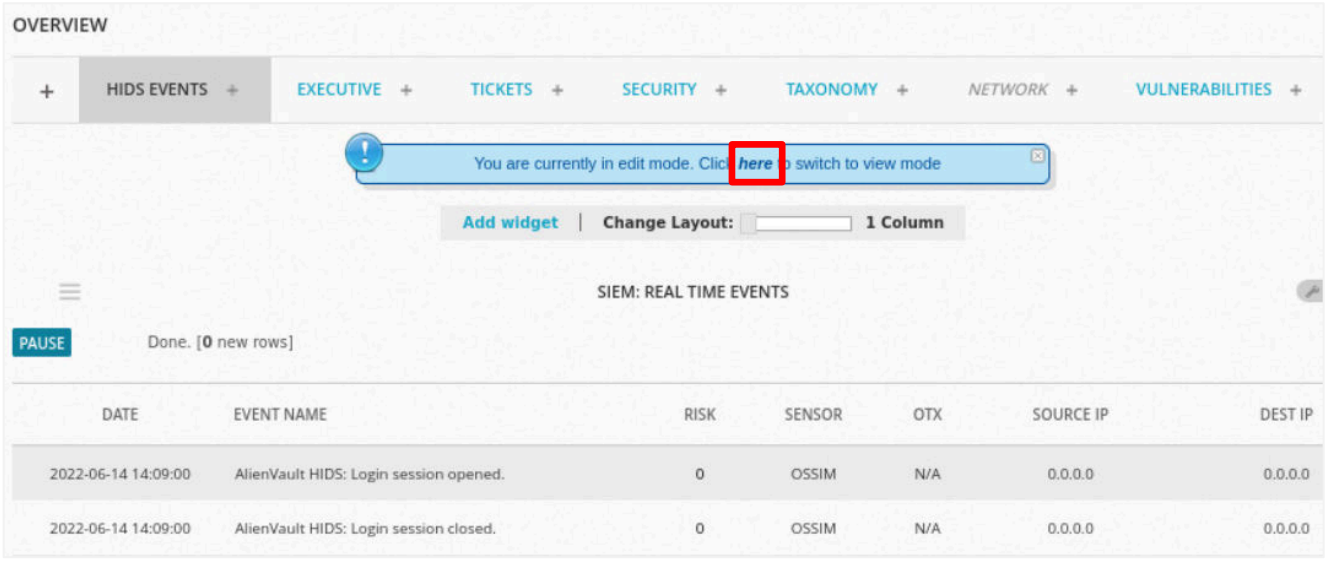
7. On the *Customize Widget* page, leave the default settings for both *REAL TIME: GENERAL CONFIGURATION* and *REAL TIME: APPEARANCE* and click **NEXT.**



8. On the *Save Widget* page, click on the **SAVE WIDGET** button.



9. Finally, on the *Overview* page, click on the **here** link in the information box to return to view mode.



2.2 Deploy HIDS *Agents* on Networked Hosts

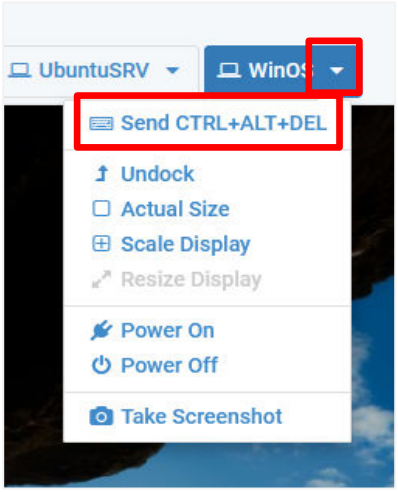
In this part of the task, you will be deploying *HIDS Agents*.

2.2.1 Deploy HIDS on a Windows Host

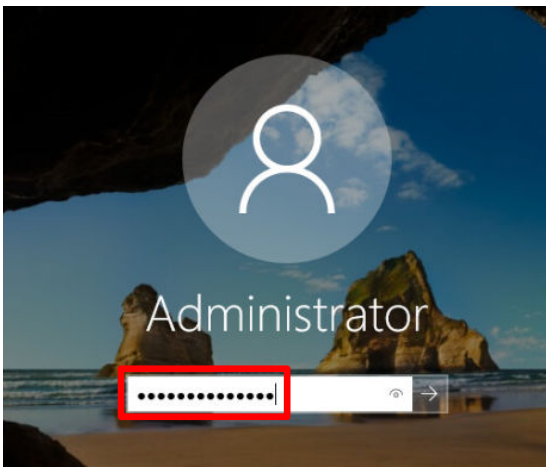
AlienVault OSSIM includes a mechanism for installing the Windows *HIDS Agent* from the *Asset List View*, but the *Windows* firewall will block the installation of the *HIDS Agent*. Before the *HIDS Agent* can be installed on the *WinOS* computer, a custom *Windows Firewall* rule will need to be created.

In *Lab 01: Network Enumeration* , a custom firewall rule was created using the wizard on the *Windows Defender Firewall*. In this lab, the custom rule will be created using *Windows PowerShell* command line

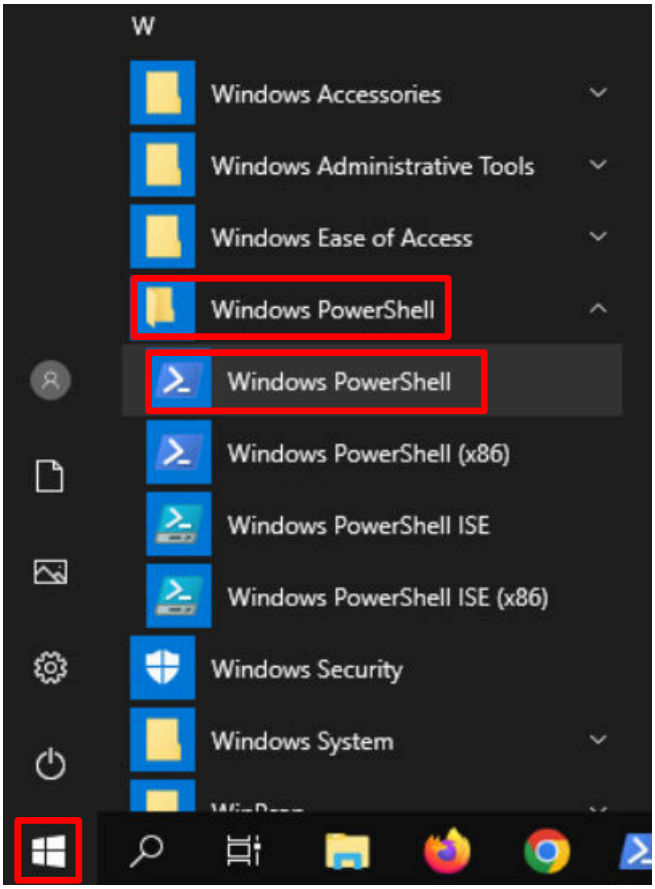
1. Set the focus to the **WinOS** computer.
2. Bring up the login window by sending a Ctrl + Alt + Delete. To do this, click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



3. Log in as *Administrator* using the password: `NDGlabpass123!`



4. Click on the **Windows Start** button, navigate to **Windows PowerShell** (folder), and then click on **Windows PowerShell**.

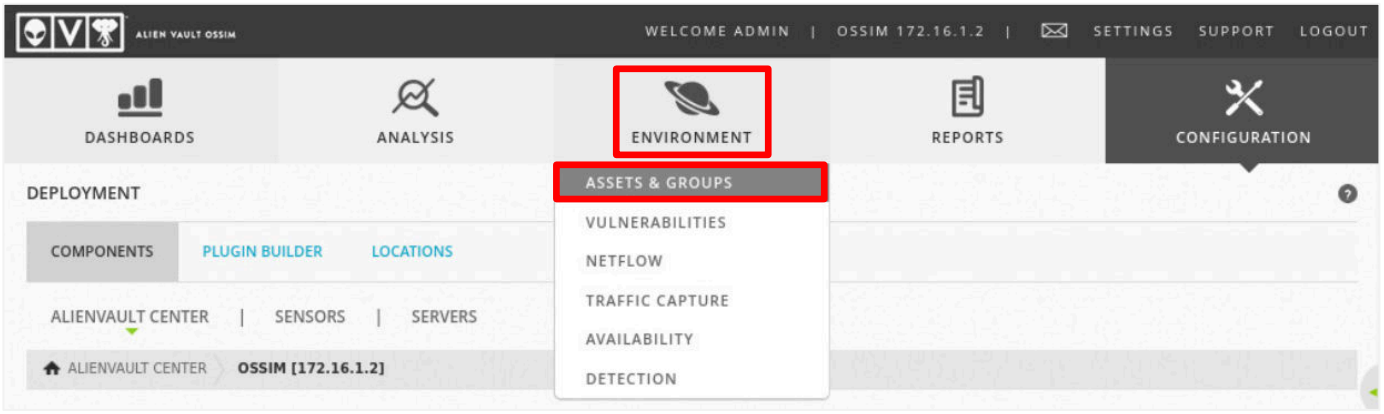


5. Type the following command to create a rule to allow access from the *OSSIM* appliance at **172.16.1.2**:

```
New-NetFirewallRule –DisplayName “Allow Access from OSSIM” –Name “OSSIM_Access” –
Direction Inbound –Action Allow –RemoteAddress “172.16.1.2” –Enabled True
```

```
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "Allow Access from OSSIM"
-Name "OSSIM_Access" -Direction Inbound -Action Allow -RemoteAddress "172.16.1.2"
-Enabled True


Name                  : OSSIM_Access
DisplayName           : Allow Access from OSSIM
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

6. Close the **Windows PowerShell** window.
7. Set the focus to the **MintOS** computer.
8. On the top-level menu, hover over **ENVIRONMENT** and then click on **ASSETS & GROUPS**.



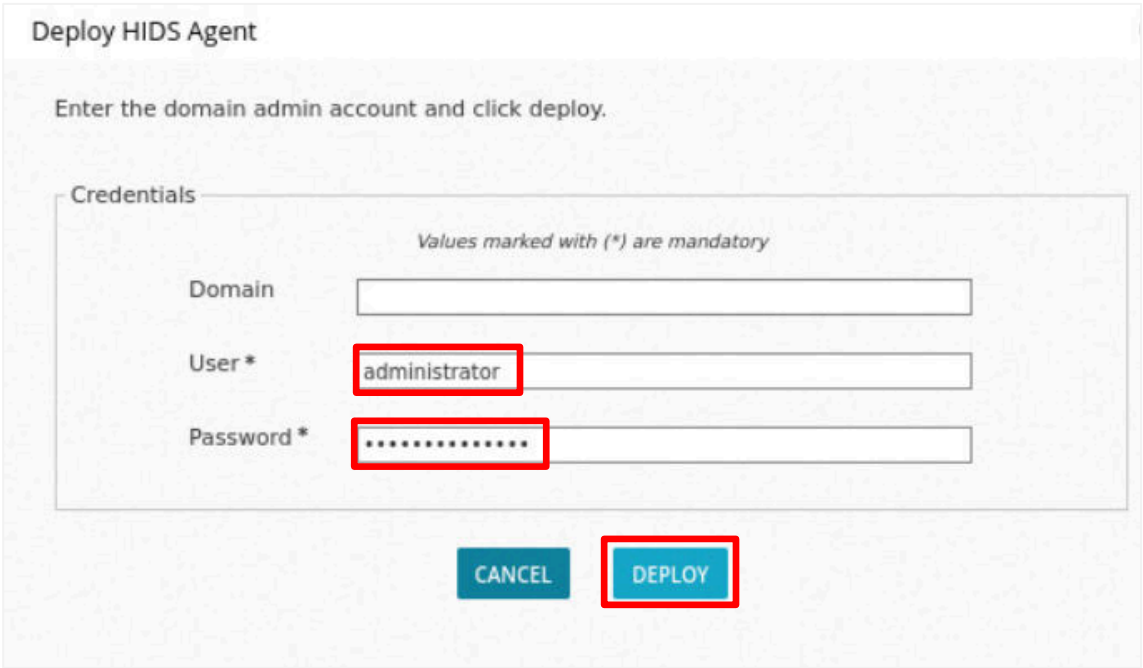
Scroll down to the bottom of the page, and you will see the list of assets.

9. Click on the **Asset Details** icon for *Host-192-168-0-50 / Microsoft Server 2019*.

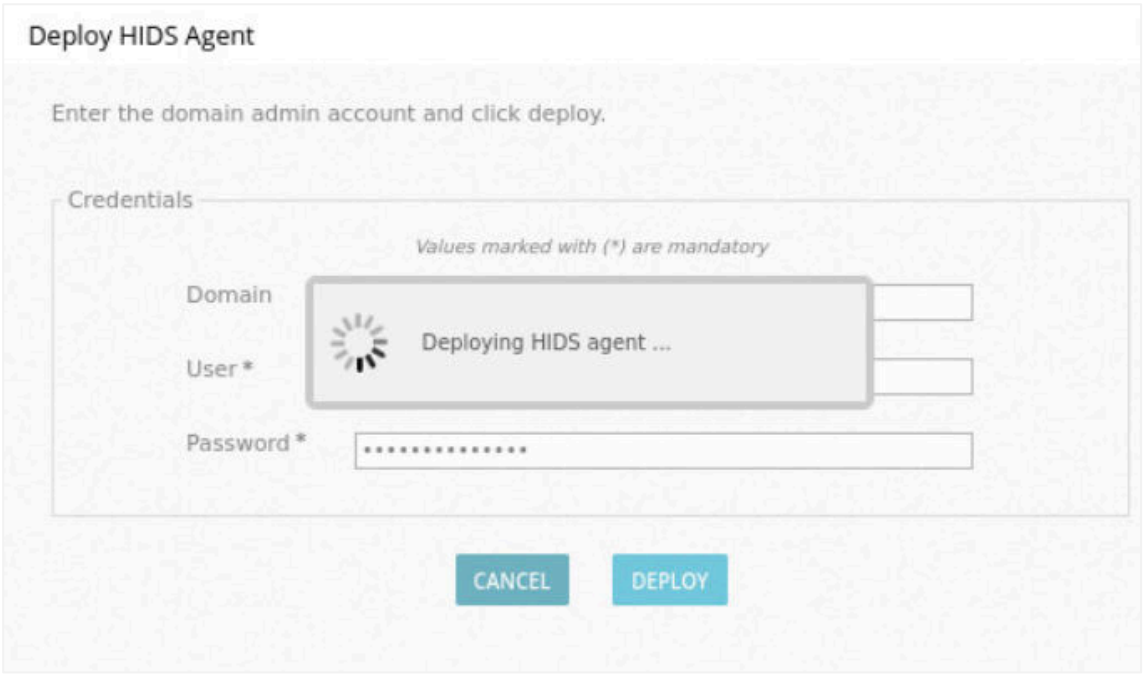
10. Click on the **ACTIONS** list box, and then click on **Deploy HIDS Agent.**

11. On the *Deploy HIDS Agent* page, type the following and then click the **DEPLOY** button.

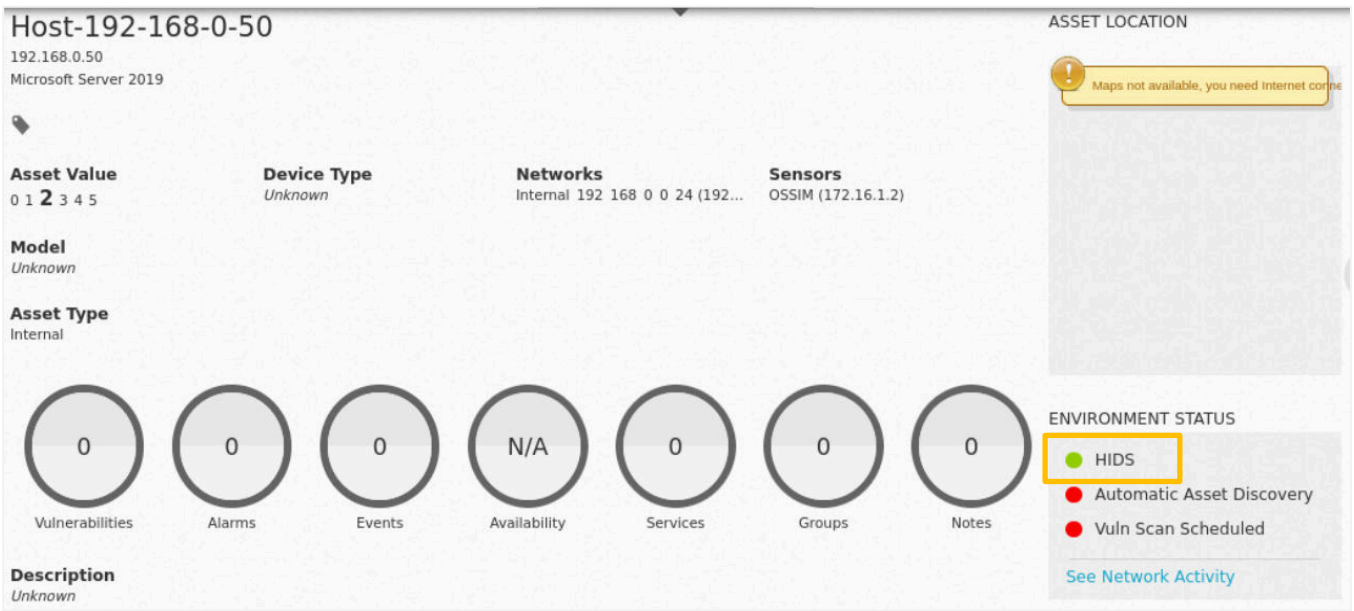
Domain	leave blank
User	`administrator`
Password	`NDGlabpass123!`



You will see the HIDS agent being deployed.

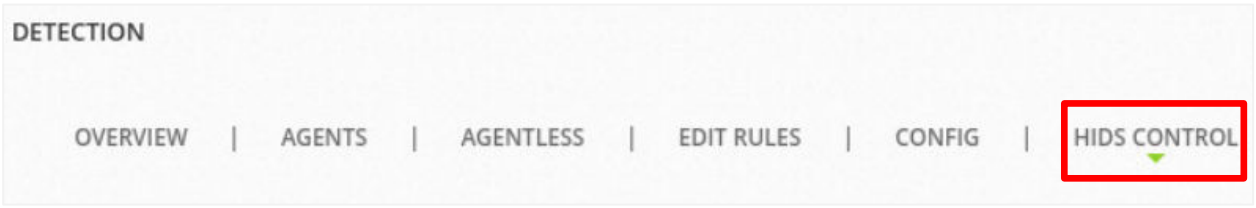


When the deployment is complete, you will see a green status indicator next to *HIDS* under *ENVIRONMENT STATUS*.

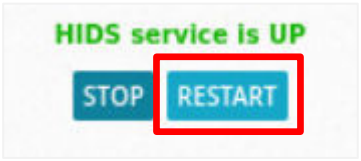


12. Hover over **ENVIRONMENT** and click on **DETECTION.**

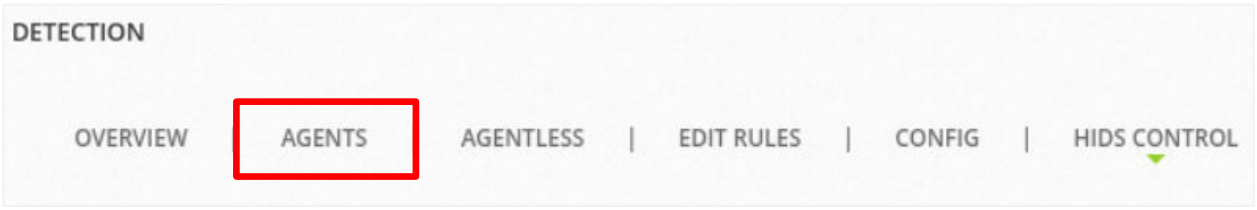
13. On the *DETECTION* page, click on **HIDS CONTROL**.



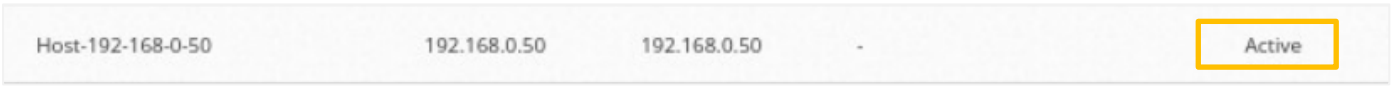
14. Under *ACTIONS,* click the **RESTART** button under *HIDS service is UP*.



15. Click the **AGENTS** tab.



16. Under *AGENT CONTROL*, in the *AGENT INFORMATION table*, you will see that the deployed status is ACTIVE.



17. Remain on the *AGENT CONTROL* tab on the *AlienVault OSSIM* Web UI and continue to the next task.

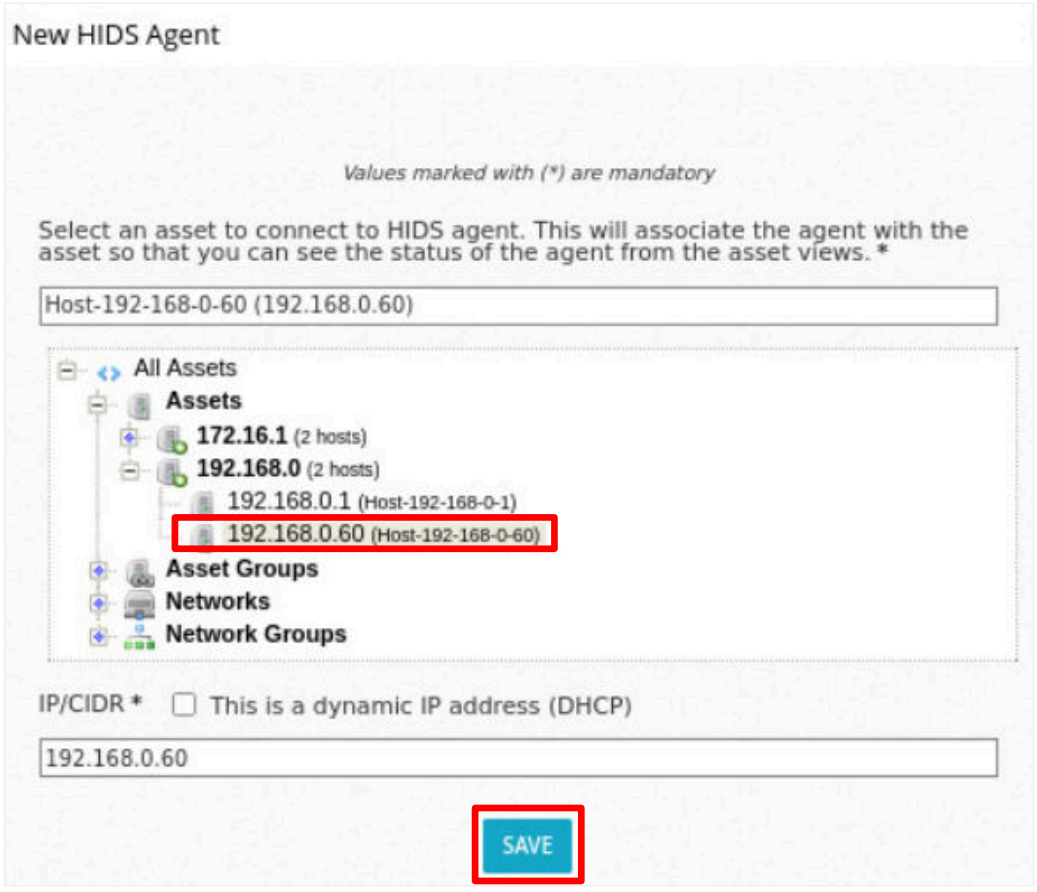
2.2.1 Deploys HIDS on a Linux Host

AlienVault OSSIM does not support deploying *HIDS Agents* to Linux hosts through the *Asset List View*. You will need to deploy the *HIDS Agent* manually.

Typically, the first step is to download and install the *OSSEC Agent*. Since the lab environment does not have internet access, the *OSSEC Agent* has already been installed for you.

1. The *AGENT CONTROL* tab should be selected. Click on the **ADD AGENT** button on the right side of the window.

2. On the *New HIDS Agent* window, expand **Assets → 192.168.0** and select **192.168.0.60**. The *Agent Name* will be populated with the hostname and *IP/CDR* with the host address. Then, click the **SAVE** button.

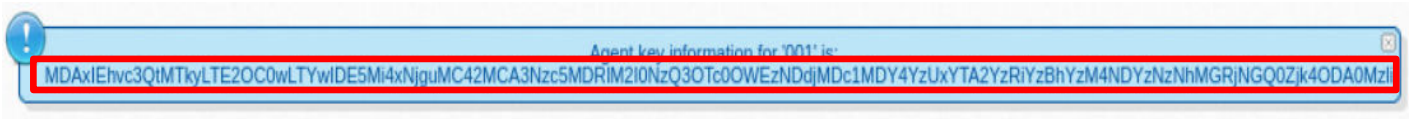


The *MintOS* computer will be added to the agent asset list under *AGENT INFORMATION*.

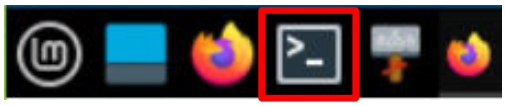
The next step is to extract the authentication key from the asset and import it to the *HIDS Agent* on the *MintOS* computer.

3. On the *AGENT INFORMATION* list, click on the **key icon** in the *ACTIONS* column on the right side of the *Host-192-168-0-60* (*MintOS*) asset.

4. The *Agent Key* will be displayed at the bottom of the window. Highlight the key and press **CTRL+C** to copy the key.



5. Open a terminal session by clicking on the **Terminal** icon in the taskbar.



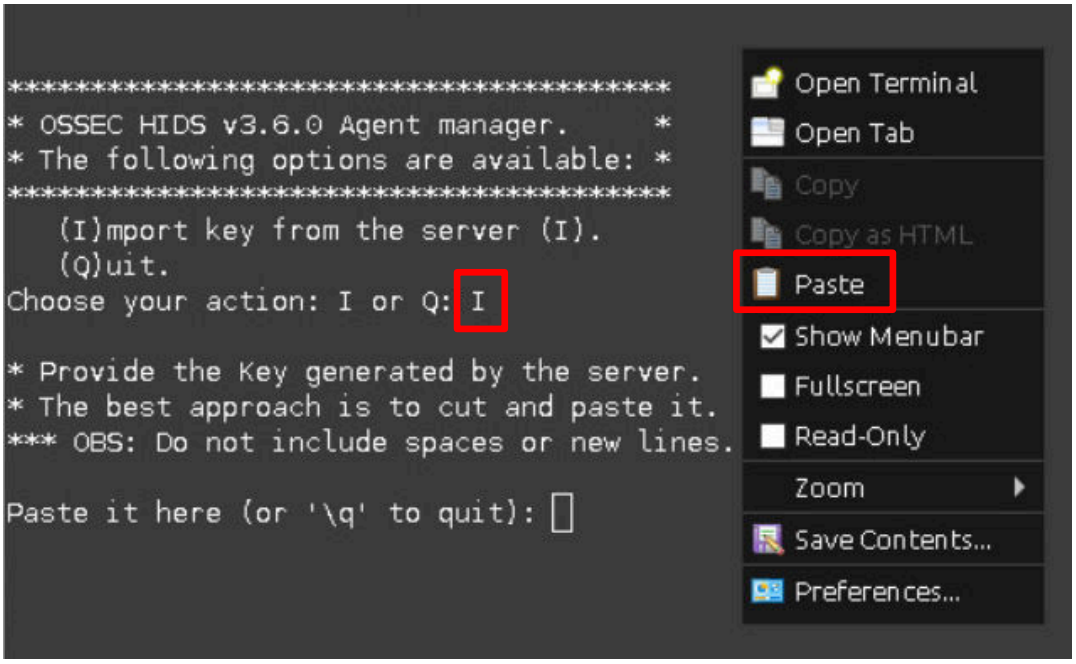
6. Type the following command to import the key:

```
sudo /var/ossec/bin/manage_agents
```

If asked for the **[sudo] password for sysadmin**, type: **NDGlabpass123!**

```
sysadmin@mintos:~$ sudo /var/ossec/bin/manage_agents
[sudo] password for sysadmin:
```

7. Type `I` followed by **Enter** to import the key, then right-click and select **Paste** from the menu (using *CTRL+V* to paste does not work in the terminal).



Press **Enter.**

```
Paste it here (or '\q' to quit): MDAxIEhvc3QtMTkyLTE2OC0wLTYwIDE5Mi4xNjguMC42MCA
3Nzc5MDRlM2I0NzQ3OTc0OWEzNDdjMDc1MDY4YzUxYTA2YzRiYzBhYzM4NDYzNzNhMGRjNGQ0Zjk4ODA
0Mzli
```

The Agent Information should show the following:

Name: Host-192-168-0-60
IP Address: 192.168.0.60

Type y followed by **Enter** to confirm the adding of the agent.

```
Agent information:
   ID:001
   Name:Host-192-168-0-60
   IP Address:192.168.0.60

Confirm adding it?(y/n): y
2022/06/12 14:50:33 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No s
uch file or directory
Added.
** Press ENTER to return to the main menu.
```

Do not worry about the Manage Agents error. The *AlienVault OSSEC HIDS Agent* is trying to delete an existing file that doesn't exist.

8. Press **Enter**, and then type `Q` followed by **Enter** to exit.

```
**************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
**************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting.
manage_agents: Exiting.
```

9. Stop the *OSSEC HIDS Agent* by typing the following command:

```
sudo /var/ossec/bin/ossec-control stop
```

```
sysadmin@mintos:~$ sudo /var/ossec/bin/ossec-control stop
Deleting PID file '/var/ossec/var/run/ossec-logcollector-3131
ossec-logcollector not running ..
ossec-syscheckd not running ..
Killing ossec-agentd ..
Killing ossec-execd ..
OSSEC HIDS v3.6.0 Stopped
```

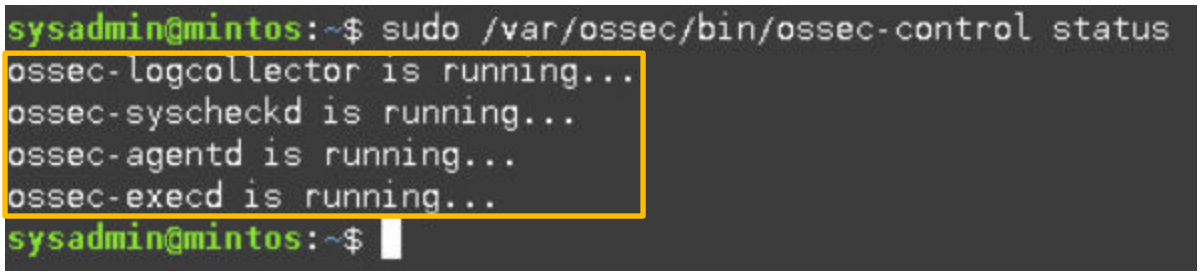
10. Start the *OSSEC HIDS Agent* and type the following command:

```
sudo /var/ossec/bin/ossec-control start
```

```
sysadmin@mintos:~$ sudo /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
Started ossec-execd...
2022/06/30 03:11:24 ossec-agentd: INFO: Using notify time: 600
econnect: 1800
2022/06/30 03:11:24 going daemon
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

11. Check the status of the agent by typing the following command:

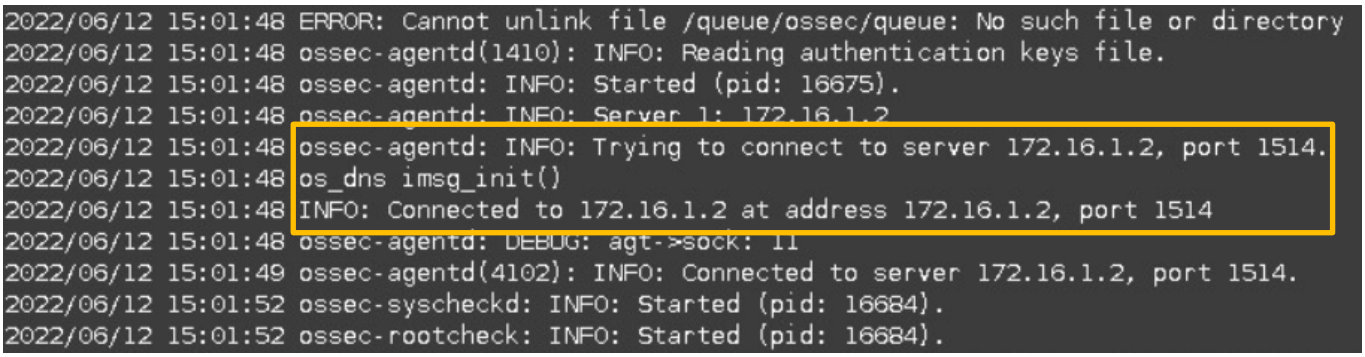
```
sudo /var/ossec/bin/ossec-control status
```



12. Check the *OSSEC HIDS* log to confirm the agent has connected to the server by typing the command:

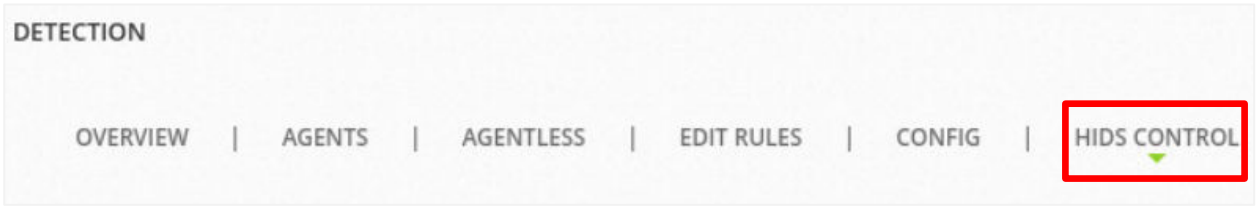
```
cat /var/ossec/logs/ossec.log | more
```

Press the **Spacebar** to advance to the next entries until you see that the *OSSEC HIDS Agent* has connected to the *AlienVault OSSIM* appliance at *172.16.1.2* (it will be near the bottom of the log file).

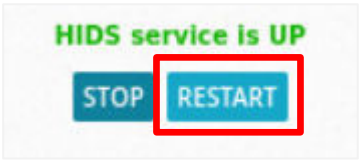


Type **Q** to exit the log listing.

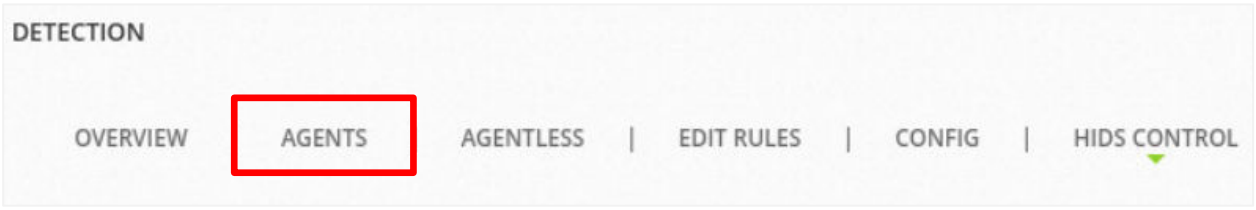
13. Minimize the terminal window and go back to the *AlienVault OSSIM* web page.
14. On the *DETECTION* page, click on **HIDS CONTROL**.



15. Under *ACTIONS* click the **RESTART** button under *HIDS service is UP*.



16. Still on the *DETECTION* page, click on **AGENTS.**



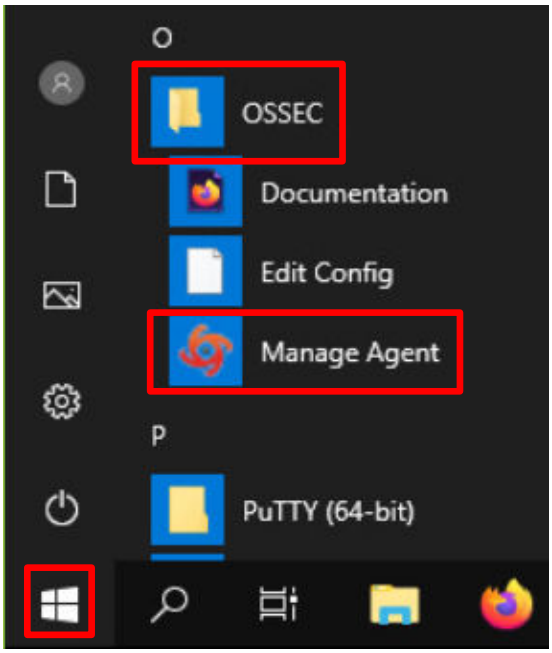
You should see that *Host-192.168-0-60* (the *MintOS* computer) is now *Active*.

2.3 Generate HIDS Events

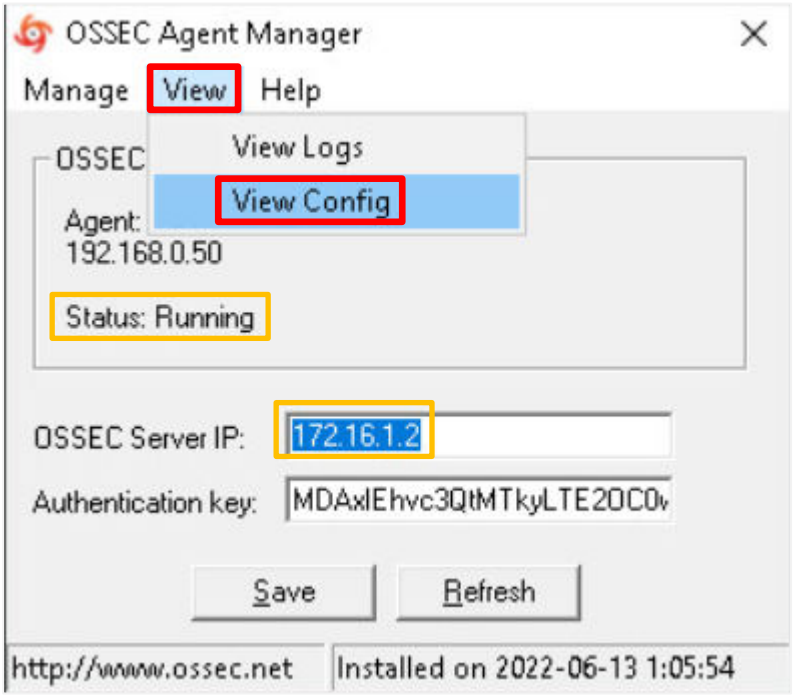
One of the OSSEC HIDS Agent's functions is to perform a System Integrity Check which monitors system files and registry entries. By default, this check is performed in Windows every 20 hours and in Linux every 22 hours. For this task, let's change the Windows timer value to *360 seconds*.

1. Set the focus on the **WinOS** Computer.

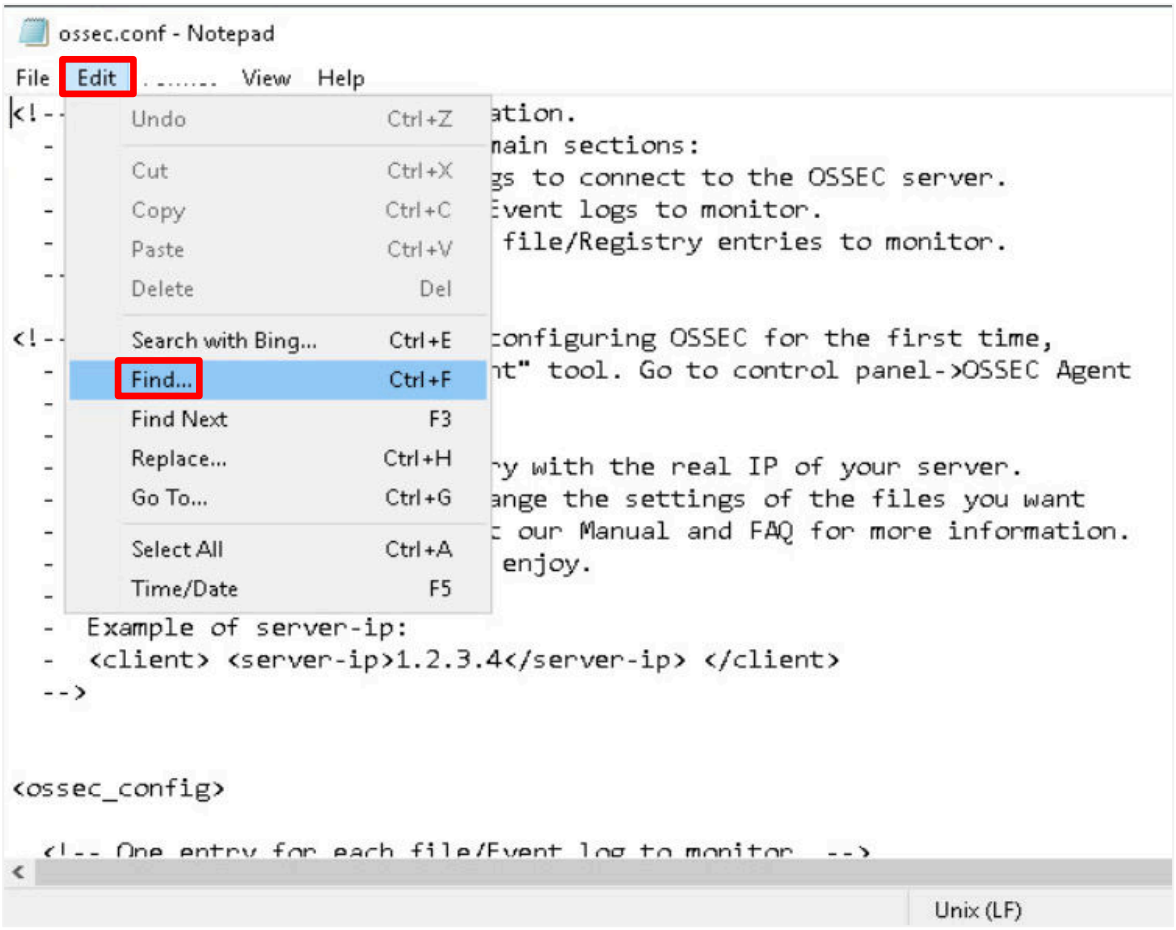
2. Click the **Start** button, open the **OSSEC** program group and click on **Manage Agent.**



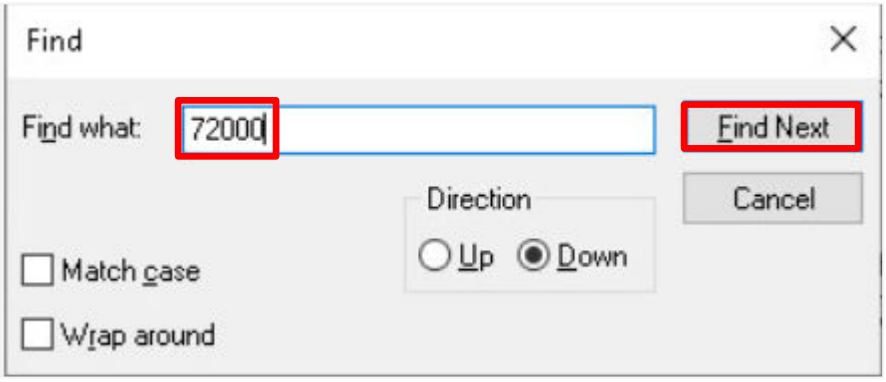
3. Confirm that the status is *Running* and the *OSSEC Server IP* is *172.16.1.2*. Click **View** on the menu bar and then click **View Config.**



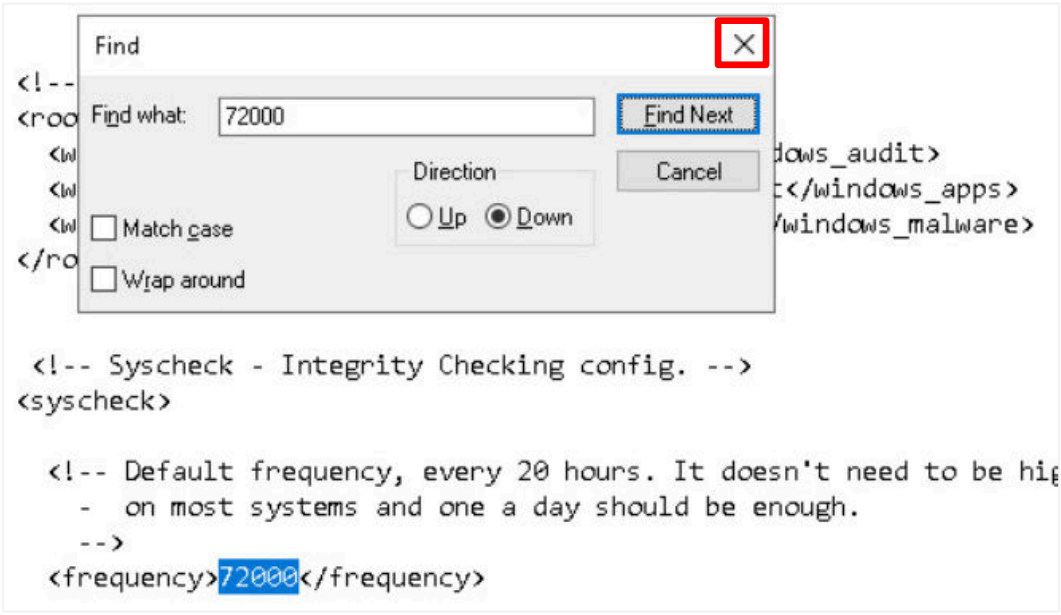
4. On the *Notepad* menu bar, click on **Edit** and then click on **Find.**



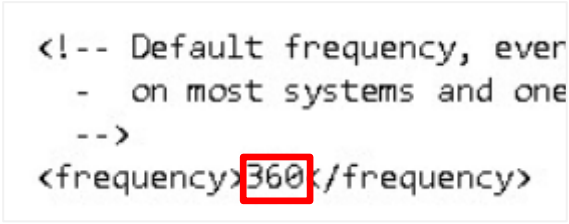
5. In the *Find* window, type `72000` in the *Find what* box and click **Find Next.**



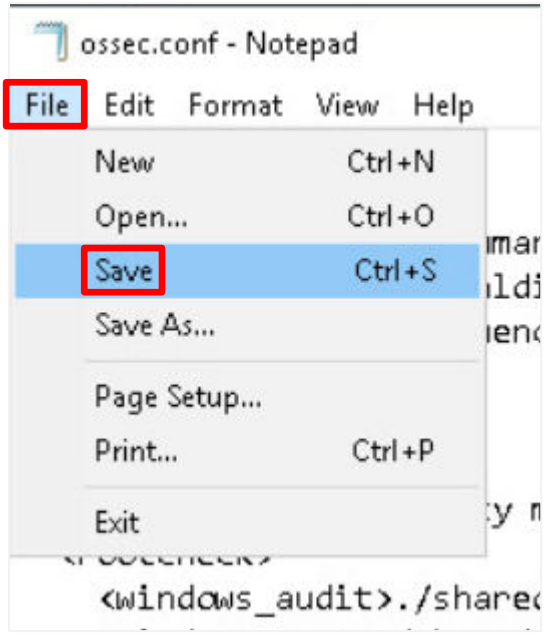
6. After finding the frequency value, close the *Find* box by clicking the **X** in the upper-right corner.



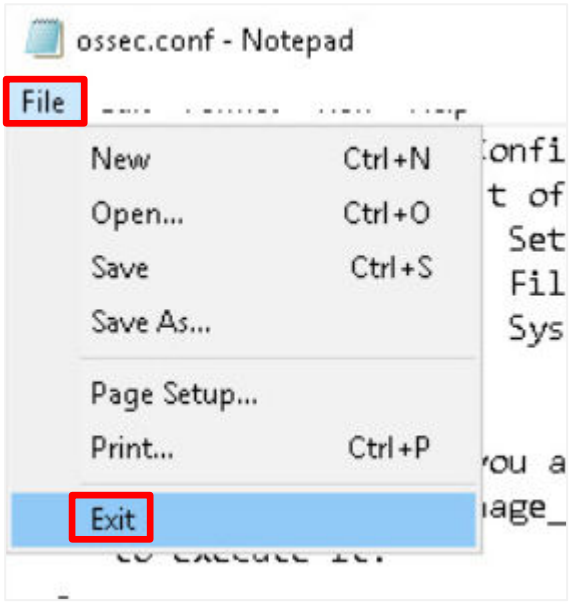
7. Change the frequency value from **72000** (seconds) to **360** (seconds).



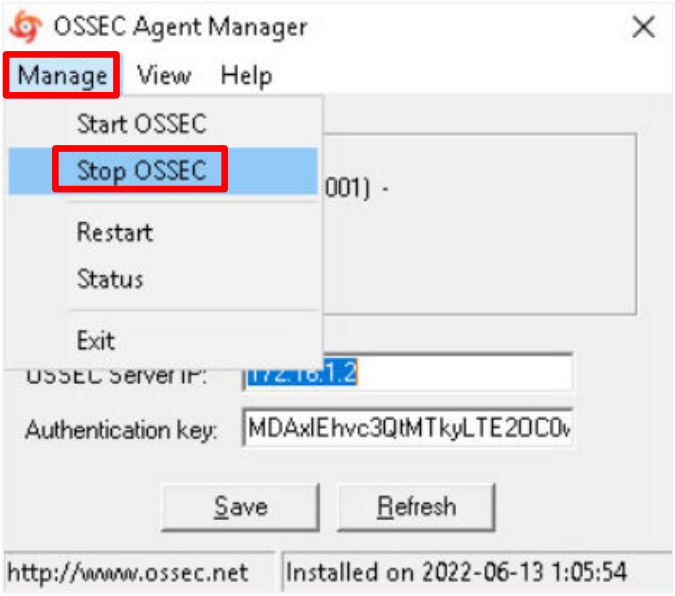
8. On the menu bar, click on **File** and then click on **Save.**



9. Close *Notepad* by clicking on **File** and then click on **Exit.**

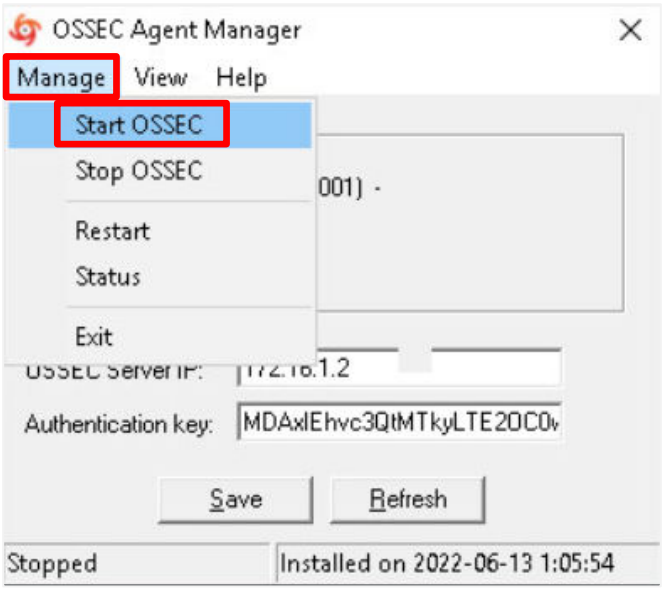


10. On the *OSSEC Agent Manager* window, click on **Manage>Stop OSSEC.**

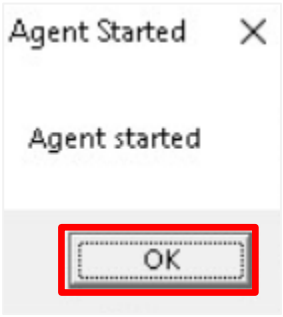


11. On the *Agent Stopped* popup, click **OK.**

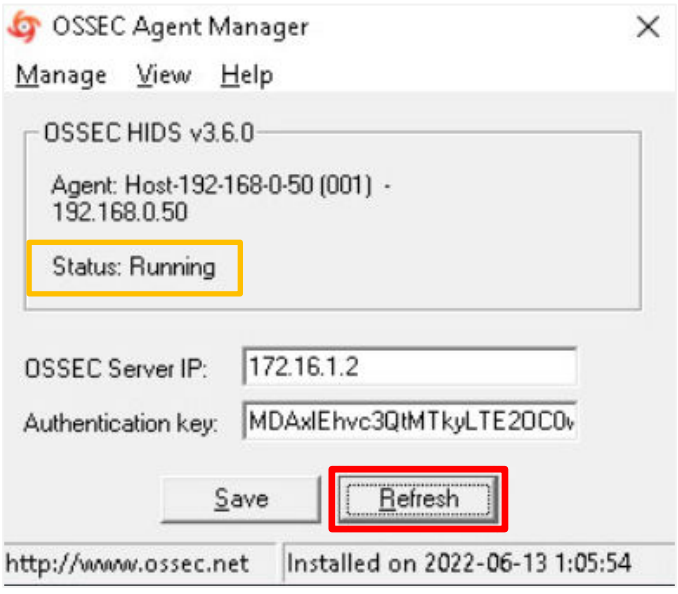
12. On the *OSSEC Agent Manager* window, click on **Manage>Start OSSEC.**



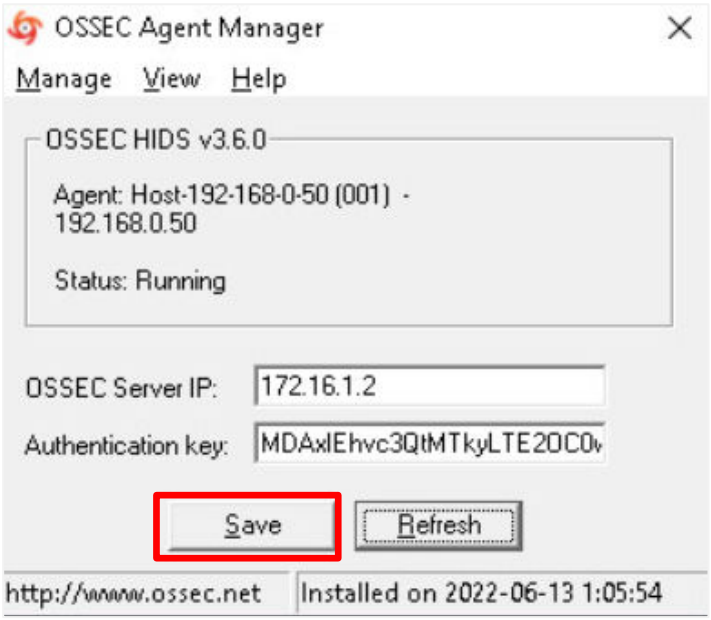
13. On the *Agent Started* popup, click **OK.**



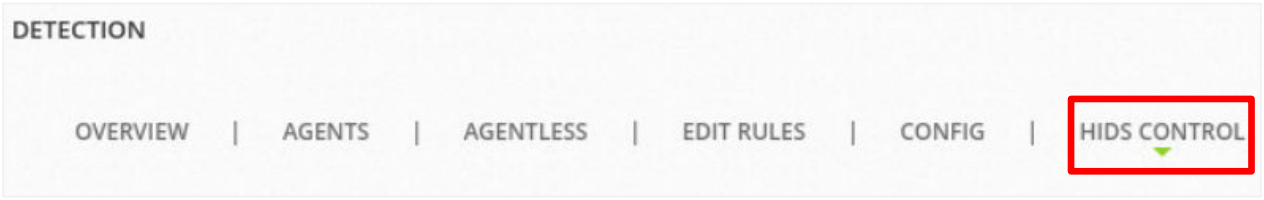
14. On the *OSSEC Agent Manager* window, click on **Refresh** to make sure the *OSSEC Agent Manager* is *Running*.



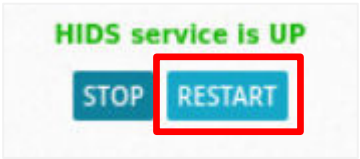
15. On the *OSSEC Agent Manager* window, click the **Save** button.



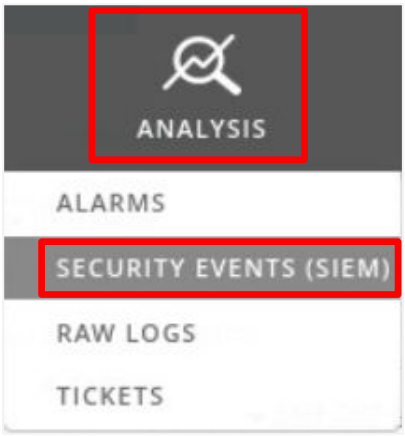
16. Set the focus to the **MintOS** computer.
17. On the *DETECTION* page, click on **HIDS CONTROL.**



18. Under *ACTIONS,* click the **RESTART** button under **HIDS service is UP**.

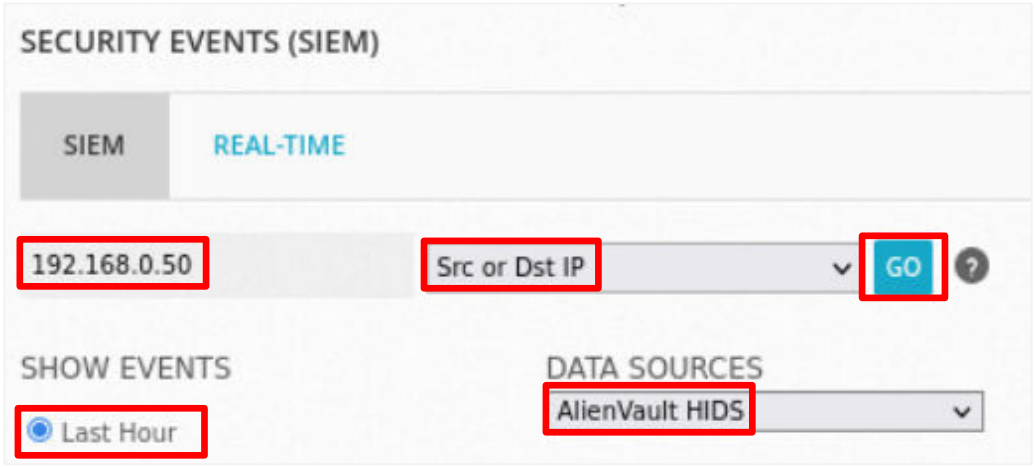


19. On the *AlienVault OSSIM* web page, hover over **ANALYSIS** and click on **SECURITY EVENTS (SIEM).**

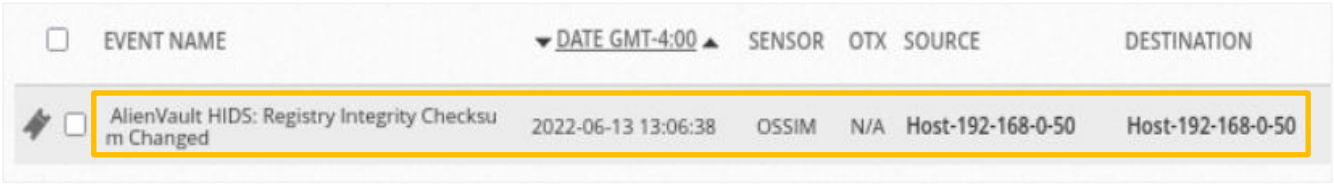


20. On the *SECURITY EVENTS (SIEM)* page, do the following:

- Under *SHOW EVENTS,* click the **Last Hour** radio box.
- Under *DATA SOURCES*, use the list arrow and select **AlienVault HIDS.**
- In the *Search* box, type `192.168.0.50`.
- In the selection box to the right of the *Search* box, use the list arrow and select **Src or Dst IP.**
- Click **GO.**



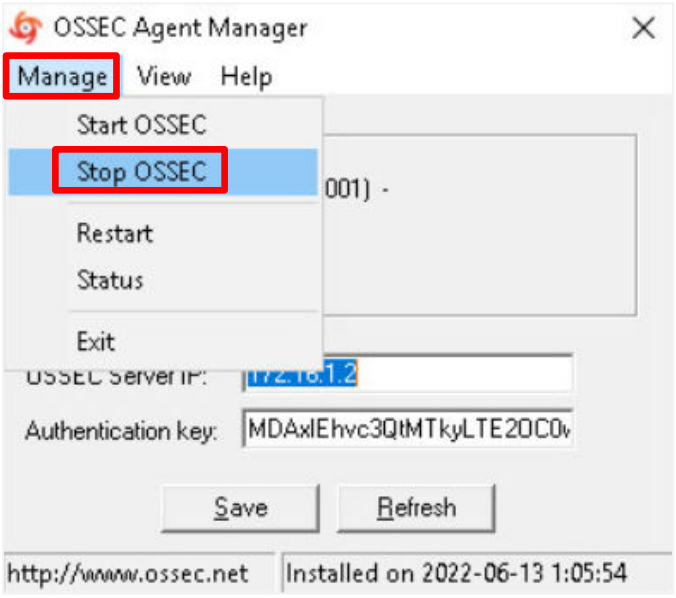
21. Scroll down to the bottom of the page, and you can see that changing the configuration file and restarting the agent created an *Integrity Checksum Changed* event.



If the event does not show up, click on **CLEAR FILTERS**, then perform step 20 again.

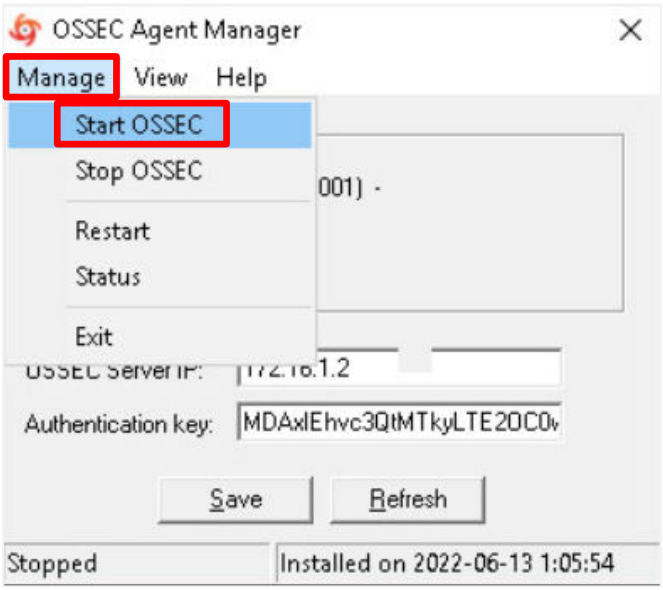
A very simple example of a potentially malicious *HIDS Event* is a brute force login attack.

22. Set the focus on the **WinOS** computer.
23. First, the *OSSEC Agent* needs to be restarted. On the *OSSEC Agent Manager* window, click on **Manage>Stop OSSEC.**

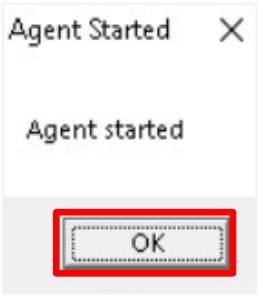


24. On the *Agent Stopped* popup, click **OK.**

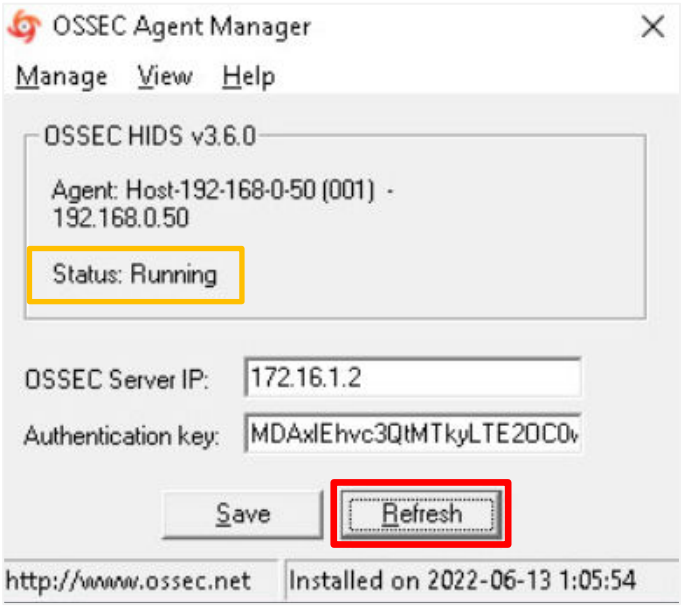
25. On the *OSSEC Agent Manager* window, click on **Manage>Start OSSEC.**



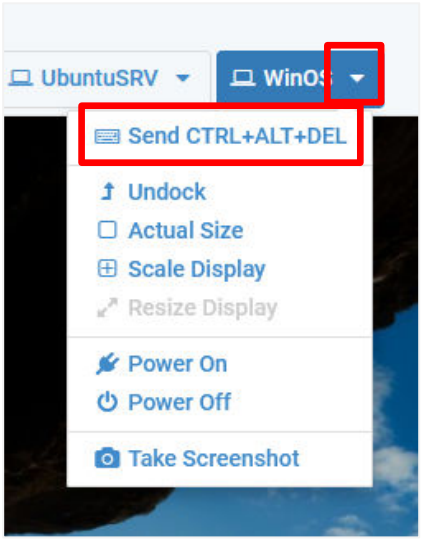
26. On the *Agent Started* popup, click **OK.**



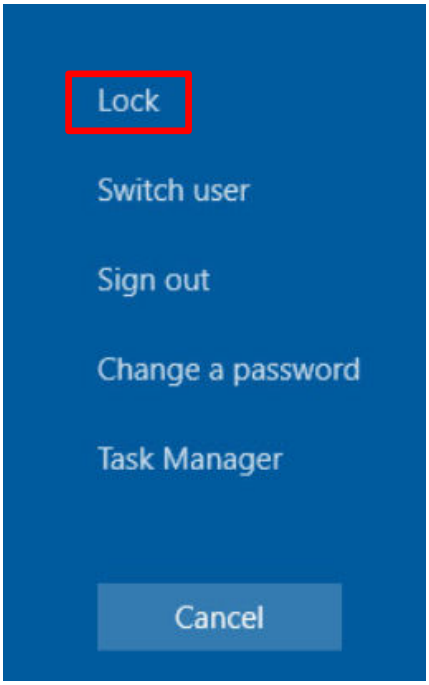
27. On the *OSSEC Agent Manager* window, click on **Refresh** to make sure the *OSSEC Agent Manager* is *Running*.



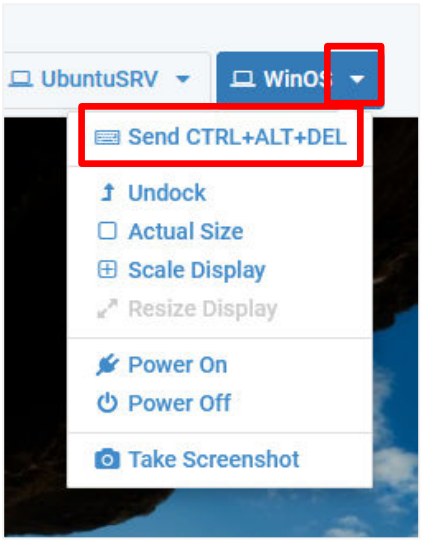
28. Lock the *WinOS* computer by clicking the **WinOS** dropdown menu, and clicking **Send CTRL+ALT+DEL**.



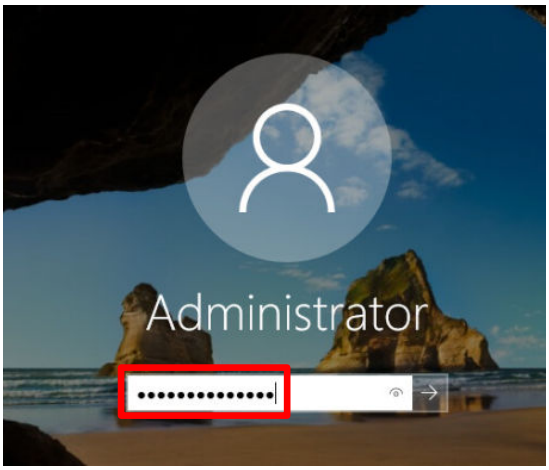
29. Click on the **Lock** link.



30. Click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.

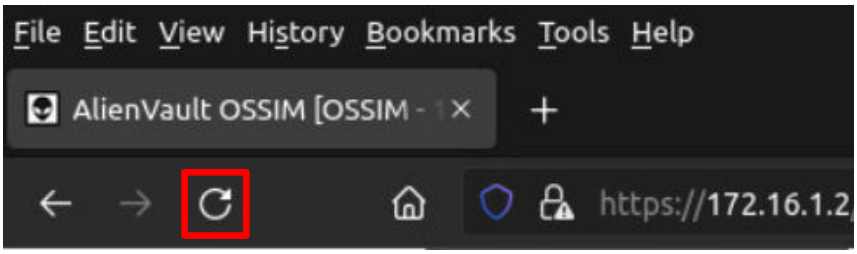


31. Attempt to log in as *Administrator* using **an incorrect password 6 times** within 30 seconds.



A very easy way to enter an incorrect password is to just press **Enter** on the *Password* entry, then click **Enter** to try again. Rinse and repeat. However, a brute force login attack is supposed to use different passwords each time

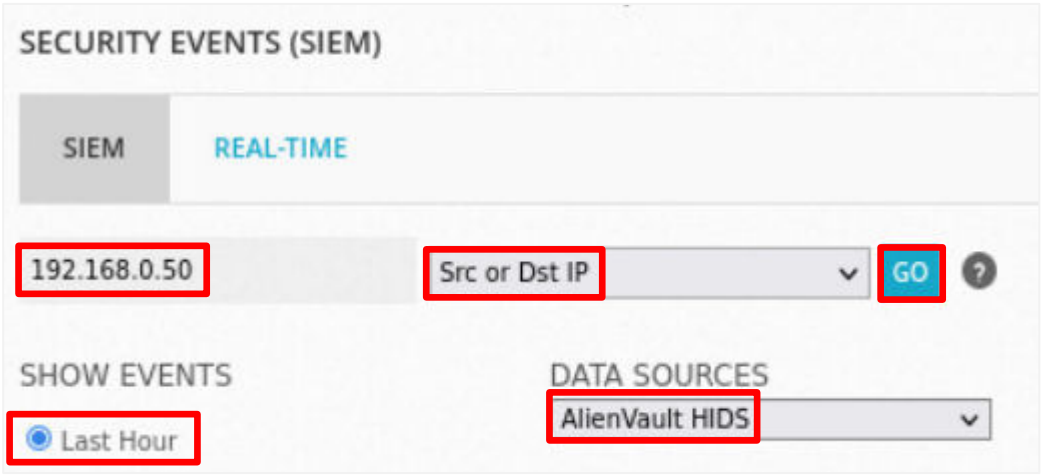
32. Return the focus to the **MintOS** computer.
33. Refresh the browser window by clicking the **Reload Current Page** icon on the browser's toolbar.



The security events that are received through *HIDS* do not change the content of the web page. Because browsers cache content, if you just change the filters, you will not see any new events. By reloading/refreshing the browser, the page will be updated and you will see new events. You can also achieve the same effect by going to a different page in the *AlienVault OSSIM* Web UI and then return to the Analysis / SIEM events page.

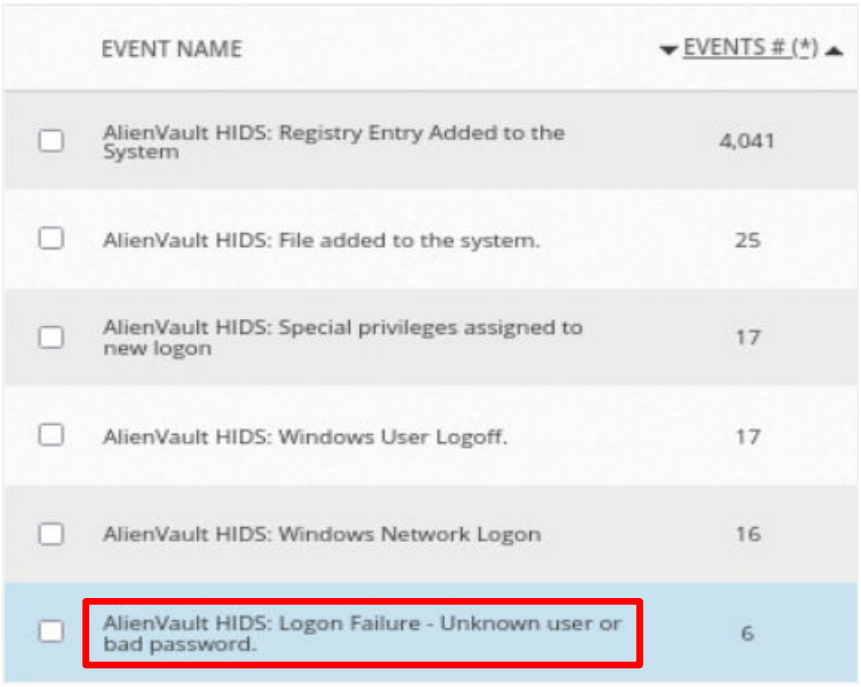
34. In the *AlienVault OSSIM* Web UI, on the *SECURITY EVENTS (SIEM)* page, do the following:

- Under *SHOW EVENTS*, click the **Last Hour** radio box.
- Under *DATA SOURCES*, use the list arrow and select **AlienVault HIDS.**
- In the *Search* box, type `192.168.0.50`**.**
- In the selection box to the right of the **Search** box, use the list arrow and select **Src or Dst IP.**
- Click **GO.**



35. Scroll down the screen and click on **GROUPED** in the menu below the filters.

36. Scroll down to the bottom of the page, and you will see *Windows Logon Failure* events. Click on **AlienVault HIDS: Logon Failure – Unknown user of bad password**.



	EVENT NAME	EVENTS # (*)
☐	AlienVault HIDS: Registry Entry Added to the System	4,041
☐	AlienVault HIDS: File added to the system.	25
☐	AlienVault HIDS: Special privileges assigned to new logon	17
☐	AlienVault HIDS: Windows User Logoff.	17
☐	AlienVault HIDS: Windows Network Logon	16
☐	AlienVault HIDS: Logon Failure - Unknown user or bad password.	6

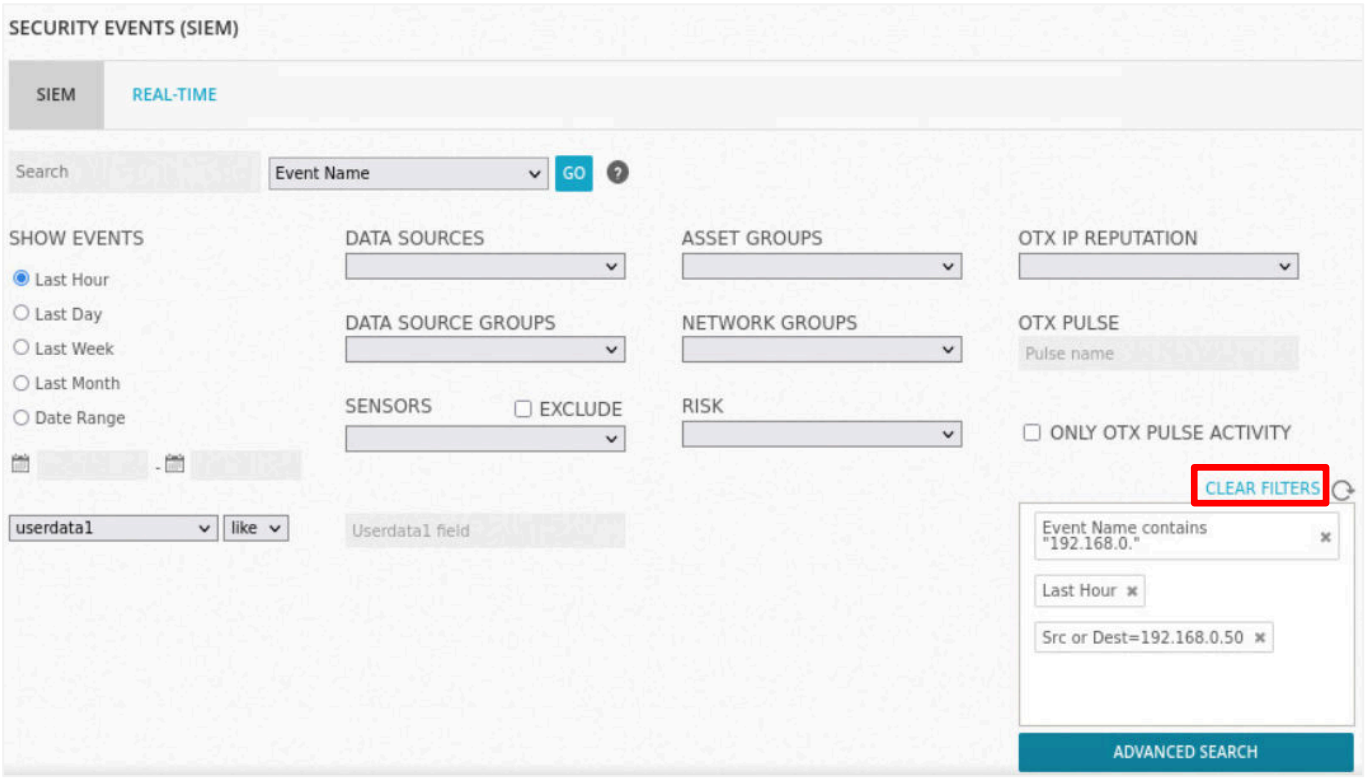
This will filter the event log showing the details for only the *Windows Logon Failures*.

EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION
AlienVault HIDS: Logon Failure - Unknown user or bad password.	2022-06-30 17:09:27	OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50
AlienVault HIDS: Logon Failure - Unknown user or bad password.	2022-06-30 17:09:23	OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50
AlienVault HIDS: Logon Failure - Unknown user or bad password.	2022-06-30 17:09:19	OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50
AlienVault HIDS: Logon Failure - Unknown user or bad password.	2022-06-30 17:09:19	OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50
AlienVault HIDS: Logon Failure - Unknown user or bad password.	2022-06-30 17:09:15	OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50
AlienVault HIDS: Logon Failure - Unknown user or bad password.	2022-06-30 17:09:11	OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50

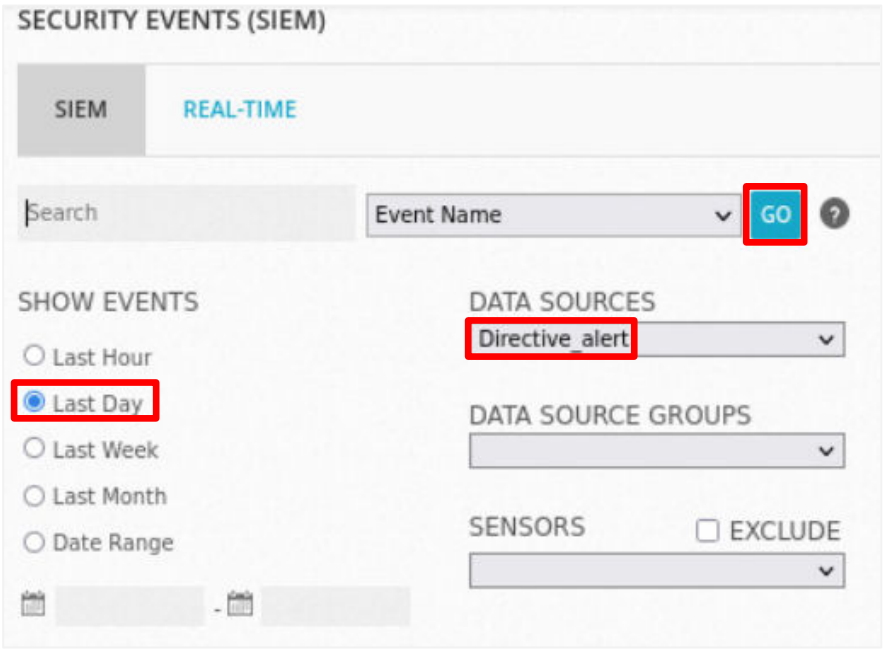
If the events do not show up,

- Set the focus to the **WinOS** computer
- Send a **CTRL+ALT+DEL**
- Log in as **Administrator** with `NDGlabpass123!` as the password
- Repeat steps **22-35**

37. Click on **CLEAR FILTERS** to clear the previous *SECURITY EVENTS (SIEM).*



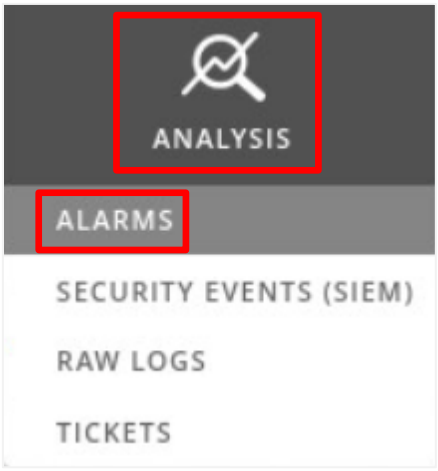
38. Click on the **Last Day** radio button and select **Directive_alert** under *DATA SOURCES,* then click **GO.**



You will see that the *Windows Logon Failure* event was correlated to a *Bruteforce* directive.

Because the Asset Value of the *WinOS* computer was set to Level 5 (very high value), the RISK is elevated to MED, which will also generate an alarm. Let's take a look at the alarm that was generated:

39. Hover over **ANALYSIS** and click on **ALARMS.**



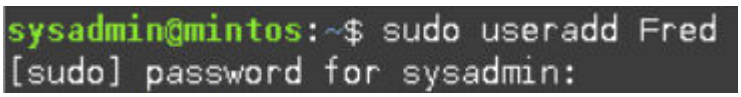
40. Scroll down to the bottom of the page, and you will see the alarm entry.

This alarm will show up in the report that you will prepare later in the lab.

Security analysts also need to monitor the creation of users and groups on host computers. In the next part of the task, you will create a new user on a Linux host and then check the *AlienVault OSSIM* security events for evidence of the action.

41. Restore the terminal window and type the following command to create a new user named Fred. If asked for the **[sudo] password for sysadmin**, type: `NDGlabpass123!`

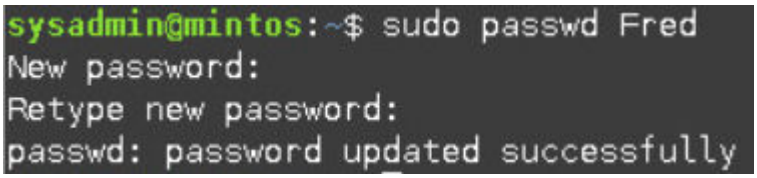
```
sudo useradd Fred
```



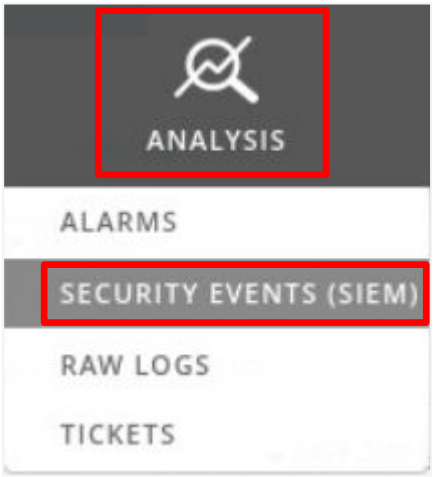
42. Type the following to set the password for **Fred.**

```
sudo passwd Fred
```

43. For the password, type `Password1` and then retype `Password1`**.**

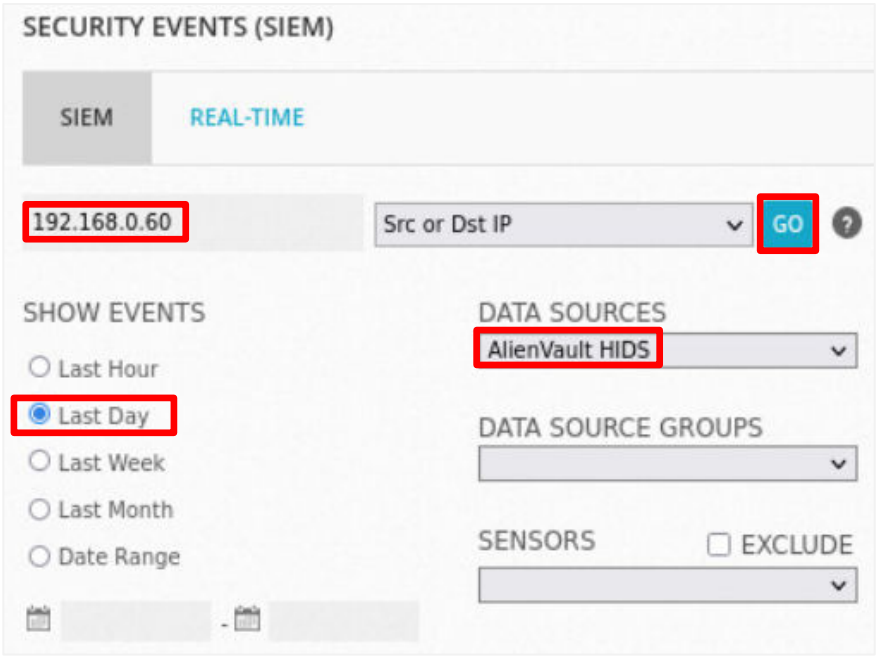


44. Minimize the terminal window.
45. Go back to the *AlienVault OSSIM* Web UI, hoer over **ANALYSIS,** and click on **SECURITY EVENTS (SIEM).**



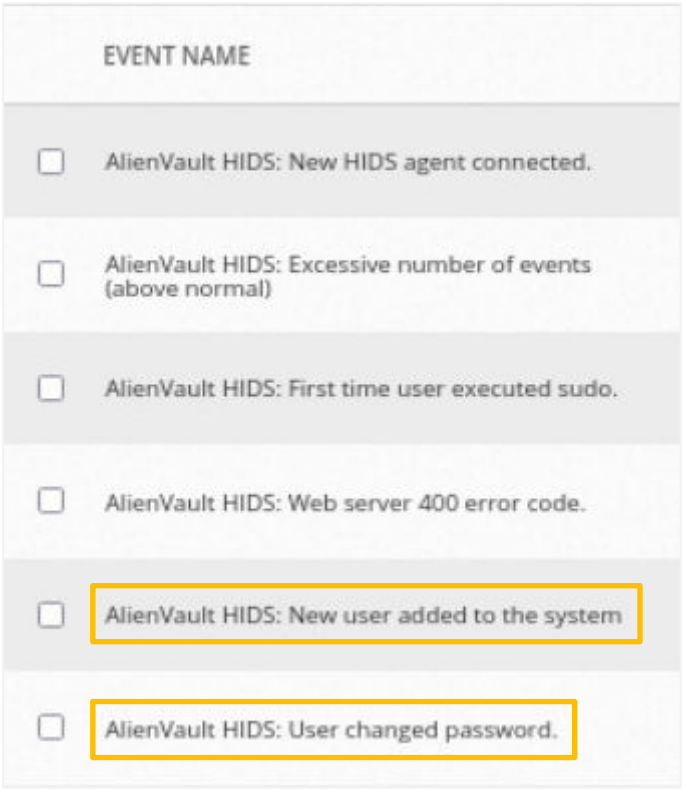
46. In the *AlienVault OSSIM* Web UI, on the *SECURITY EVENTS (SIEM)* page, do the following:

- Under *SHOW EVENTS,* click the **Last Day** radio box.
- Under *DATA SOURCES*, use the list arrow and select **AlienVault HIDS.**
- In the **Search** box, type `192.168.0.60`.
- In the selection box to the right of the *Search* box, use the list arrow and select **Src or Dst IP.**
- Click **GO.**



47. Scroll down the screen and click on **GROUPED** in the menu below the filters.

48. Scroll down to the bottom of the page, and you will see the two events, *AlienVault HIDS: New user added to the system* and *AlienVault HIDS: User changed password*.



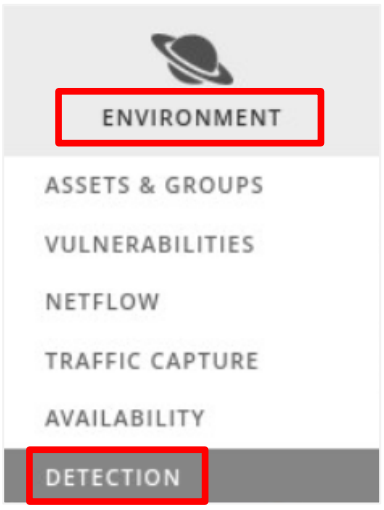
49. Remain in the *AlienVault OSSIM* Web UI and continue to the next task.

2.4 HIDS Application Events

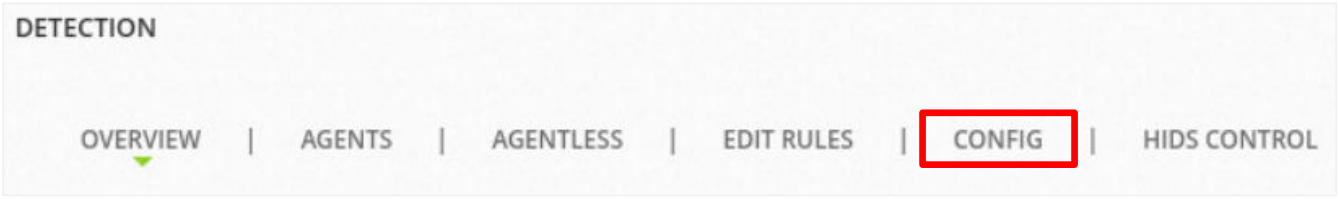
Another area of concern for security analysts is when potentially vulnerable software is installed on a host. In this task, you will set up the Windows AppLocker service, which monitors and manages applications that are run on Windows servers. You will then configure the OSSEC agent to pass the events detected by AppLocker to AlienVault OSSIM for monitoring and reporting.

2.4.1 Setup AppLocker on Windows Host

1. Hover over **ENVIRONMENT** and click on **DETECTION.**

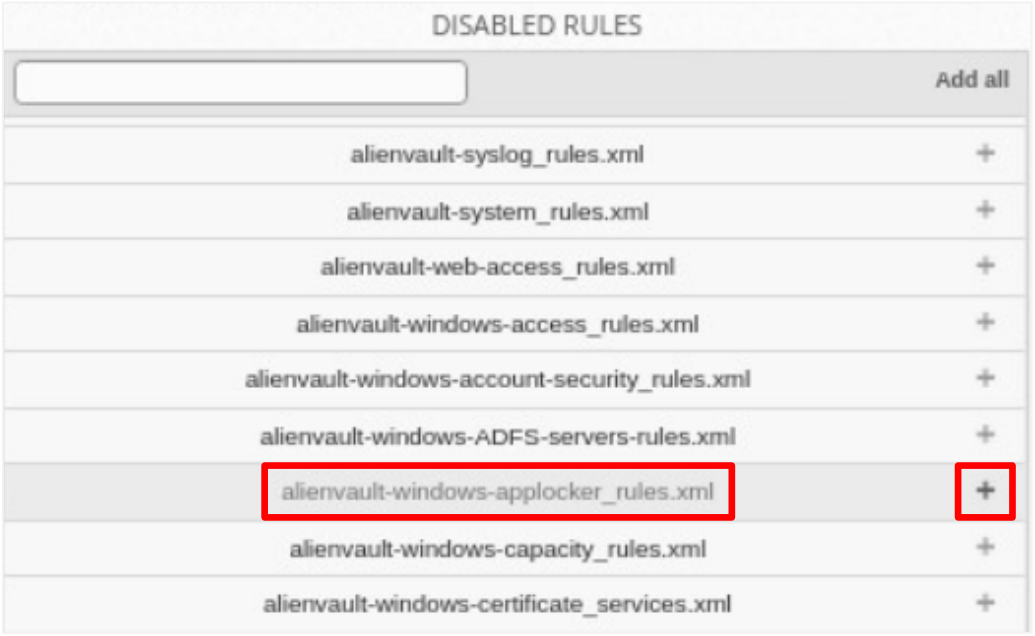


2. On the *DETECTION* page, click on **CONFIG.**

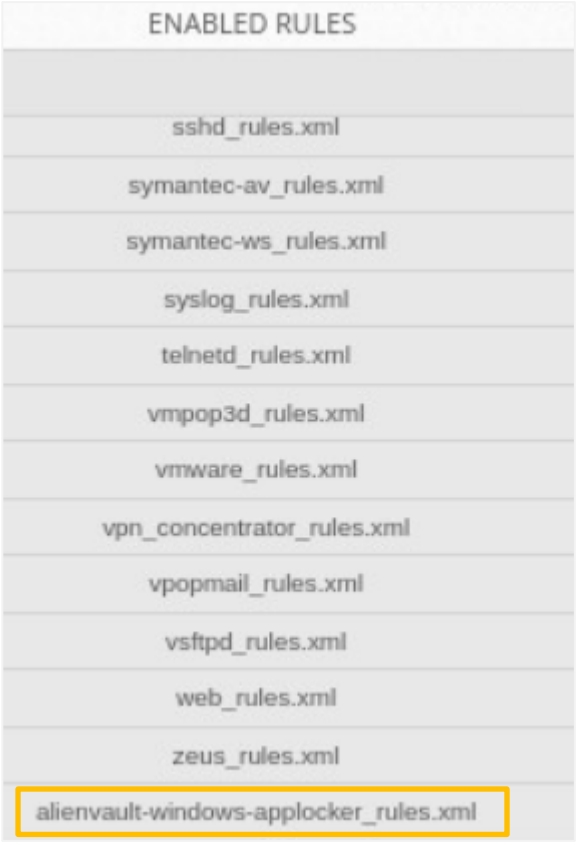


You may need to increase the width of the browser window to see the enabled and disabled rules side-by-side.

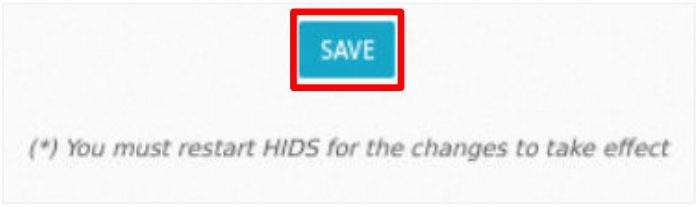
3. Scroll down the page, and you will see two lists, *ENABLED RULES* and *DISABLED RULES*. The rule for *Windows AppLocker* is disabled by default and will need to be enabled. Scroll down on the right-side list and look for **alienvault-windows-applocker_rules.xml** and click on the **+** to the right of the rule.



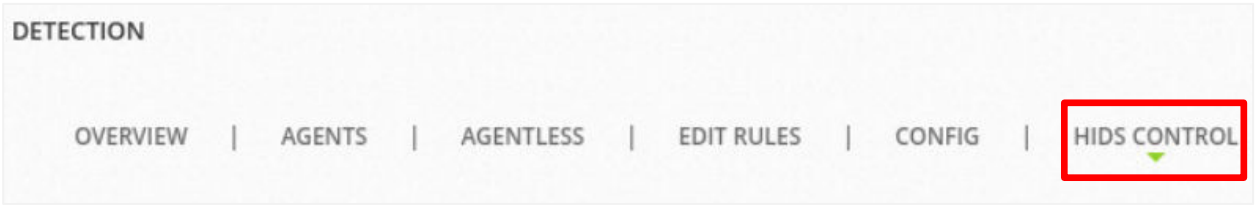
Scroll down the left side list, and you will see the *alienvault-windows-applocker_rules.xml* in the list of enabled rules.



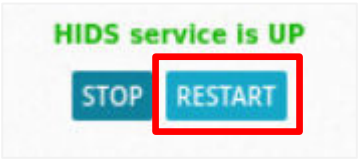
4. At the bottom of the *Rules* page, click the **SAVE** button.



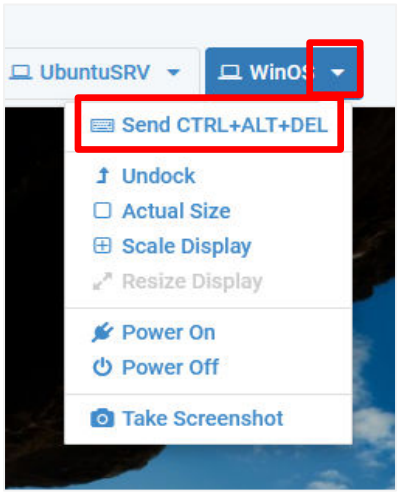
5. On the *DETECTION* page, click on **HIDS CONTROL.**



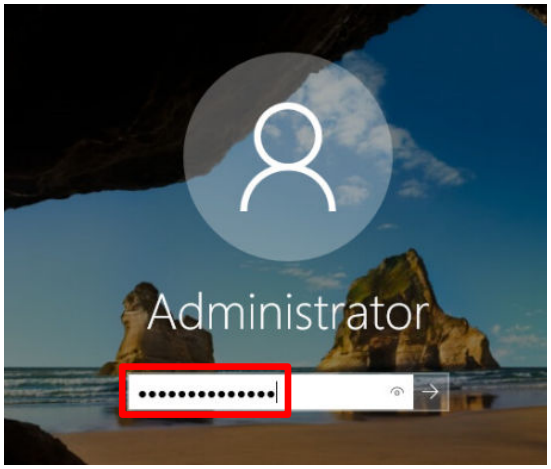
6. Under *ACTIONS,* click the **RESTART** button under **HIDS service is UP**.



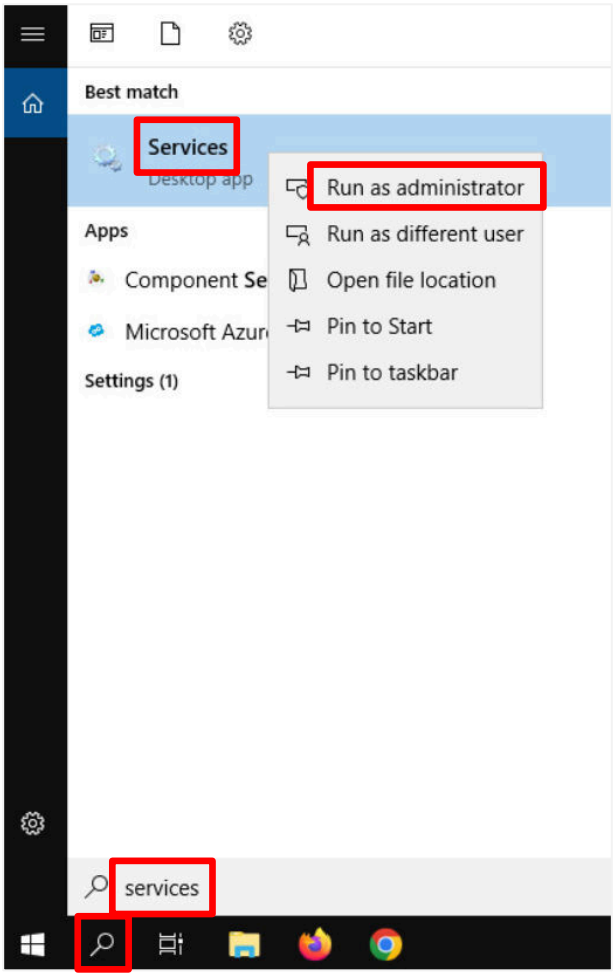
7. Set the focus to the **WinOS** computer.
8. Unlock the *WinOS* computer. Click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



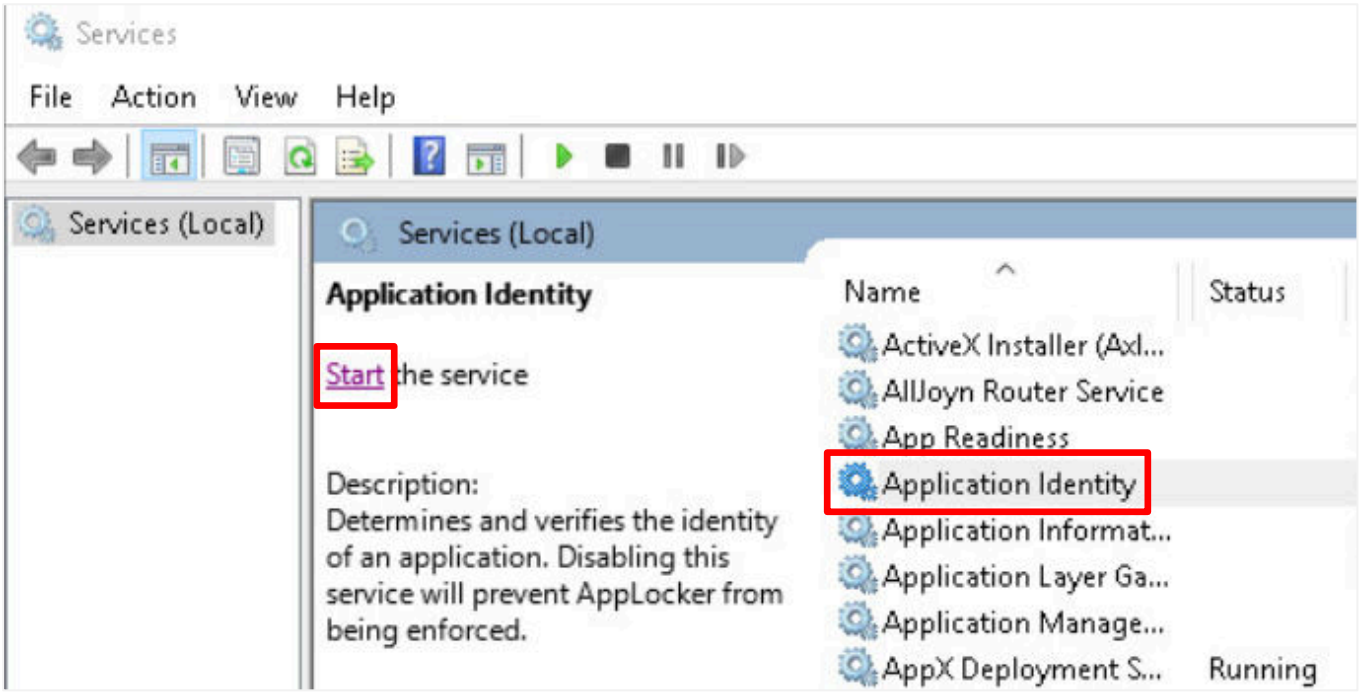
9. Log in as *Administrator* using the password: `NDGlabpass123!`



10. Click on the **Search** button and type `Services`. Under *Best match*, right-click on the menu and click **Run as administrator**.

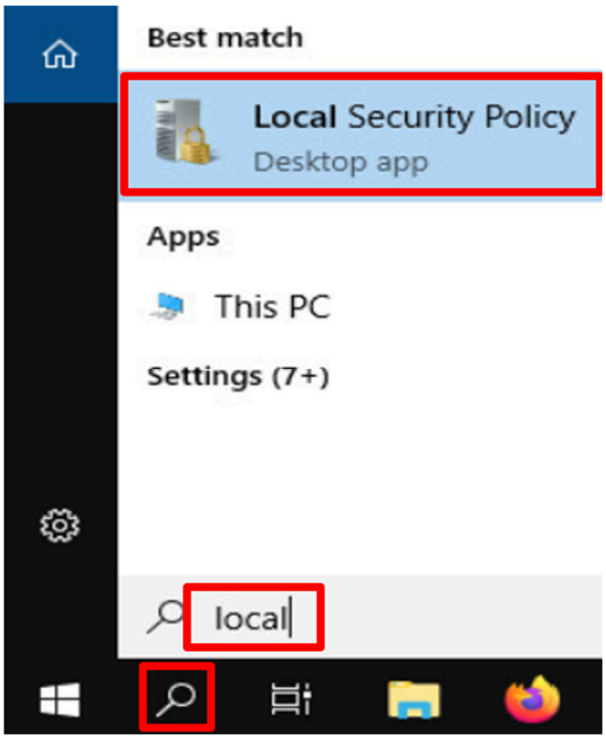


11. On the *Services* window, on the right panel, click on **Application Identity**, and then click on **Start**.

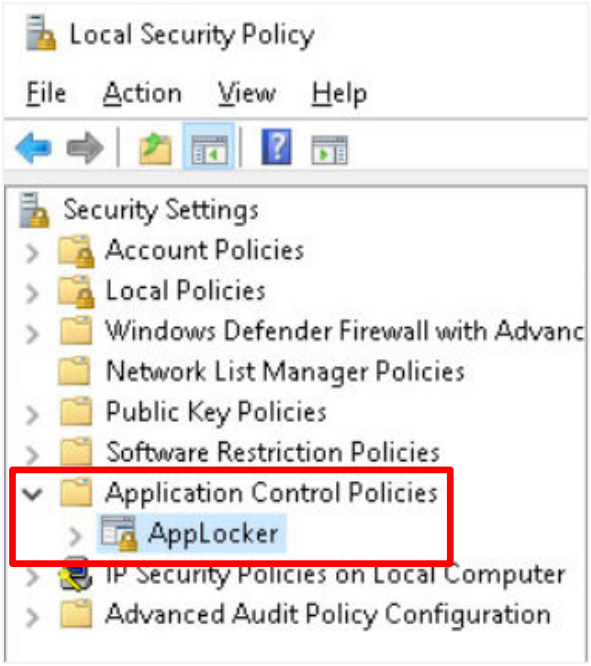


Make sure the service is *Running* before going on to the next step.

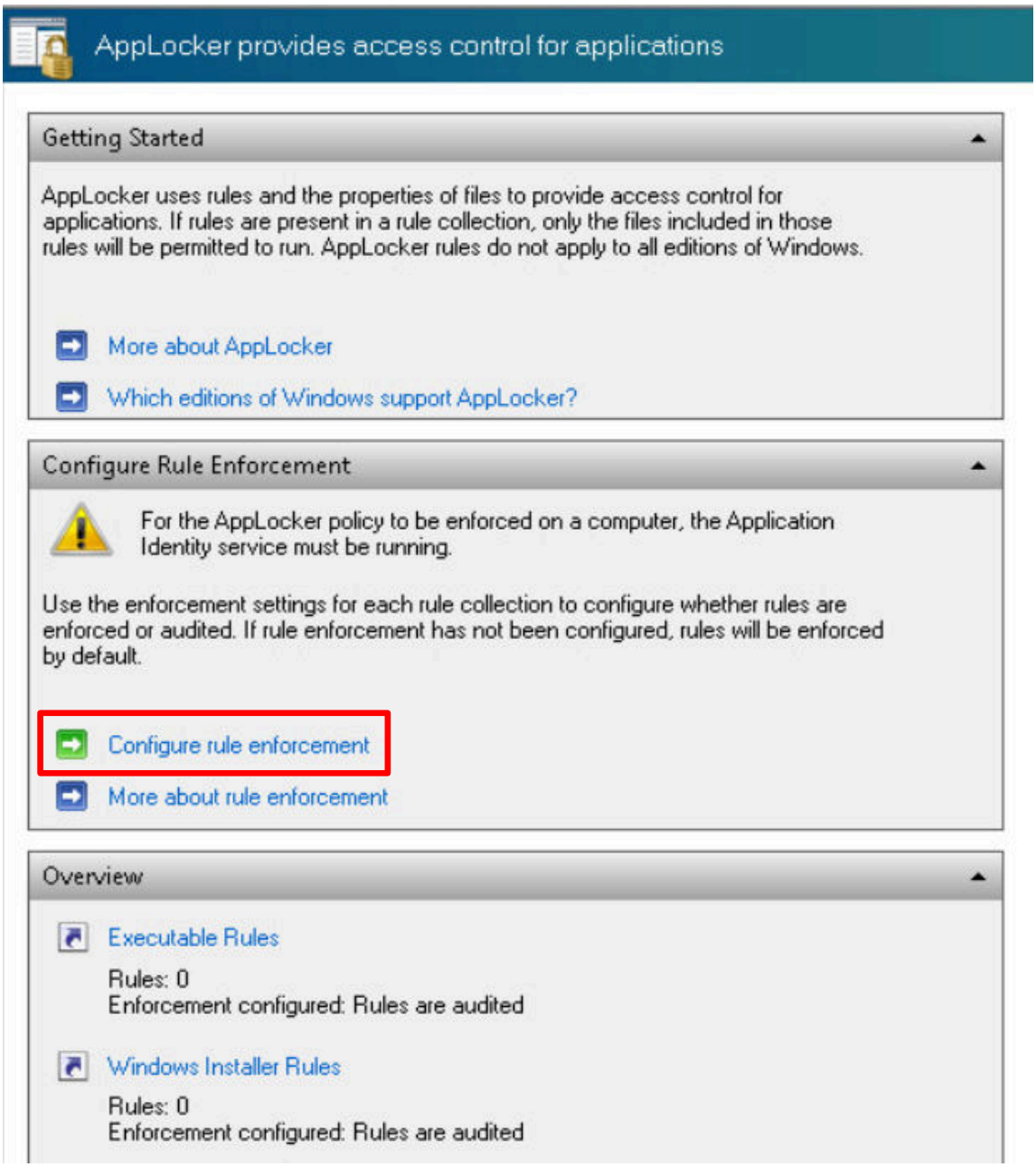
12. Close the *Services* window.
13. Click on the **Search** button and type `Local`; you should see *Local Security Policy* under *Best Match*. Click on **Local Security Policy**.



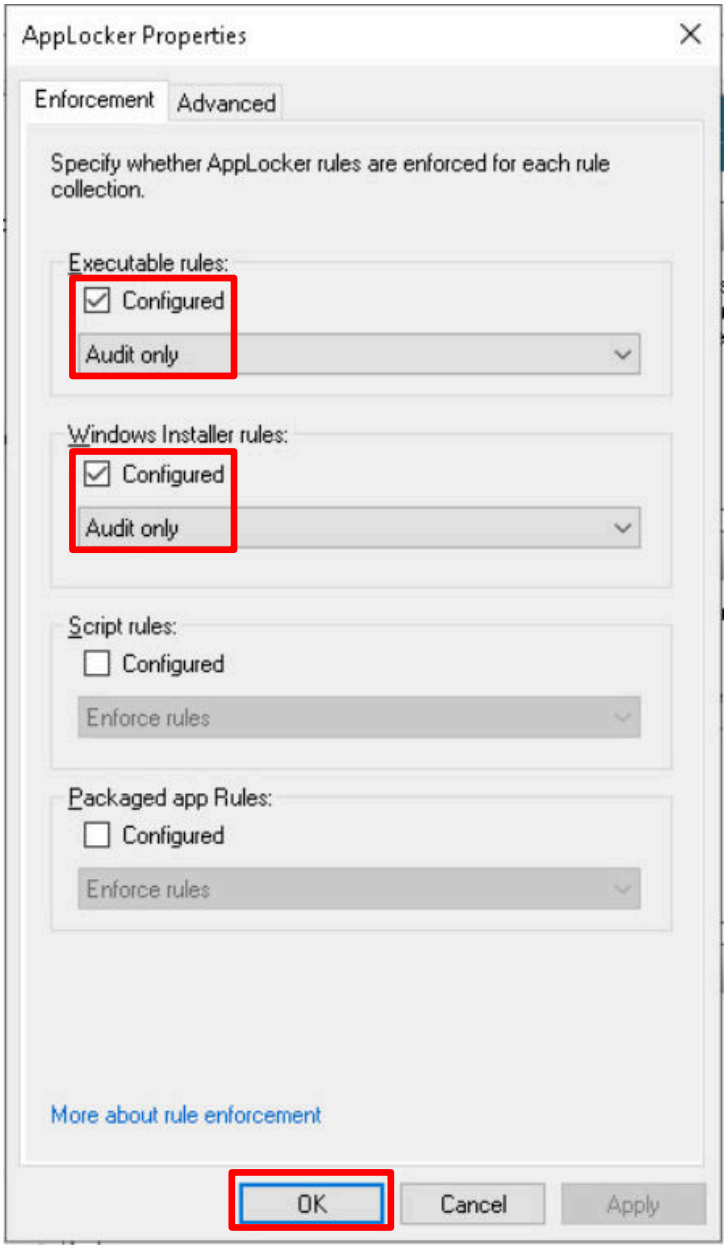
14. On the *Local Security Policy* window, on the left panel, expand **Application Control Policies,** and click on **AppLocker**.



15. On the right panel, under *Configure Rule Enforcement*, click on **Configure Rule Enforcement.**



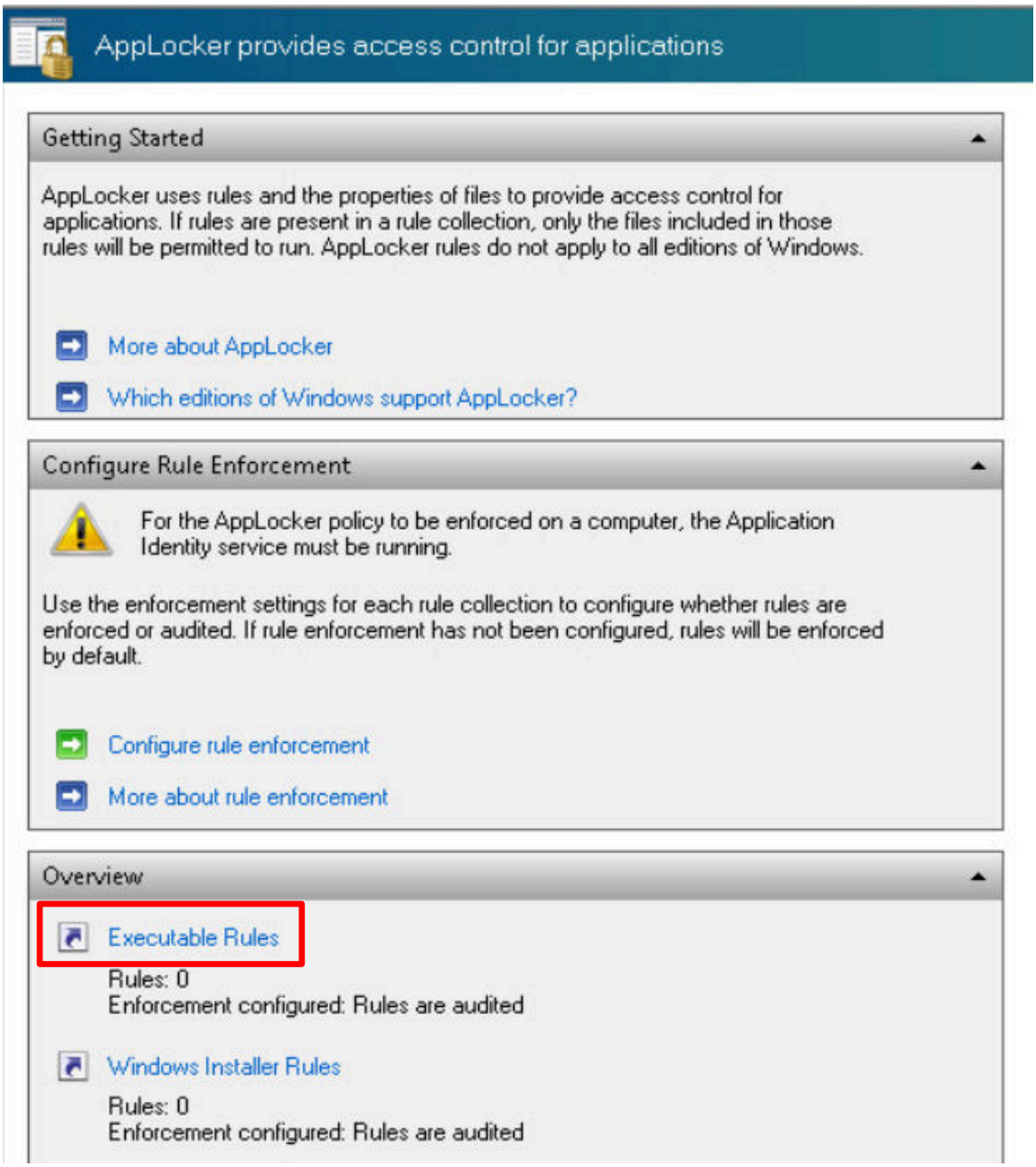
16. On the *AppLocker Properties* page, click the **Configured** checkbox under *Executable Rules* and *Windows Installer Rules,* and then click the *Enforcement* list box and select **Audit Only**.



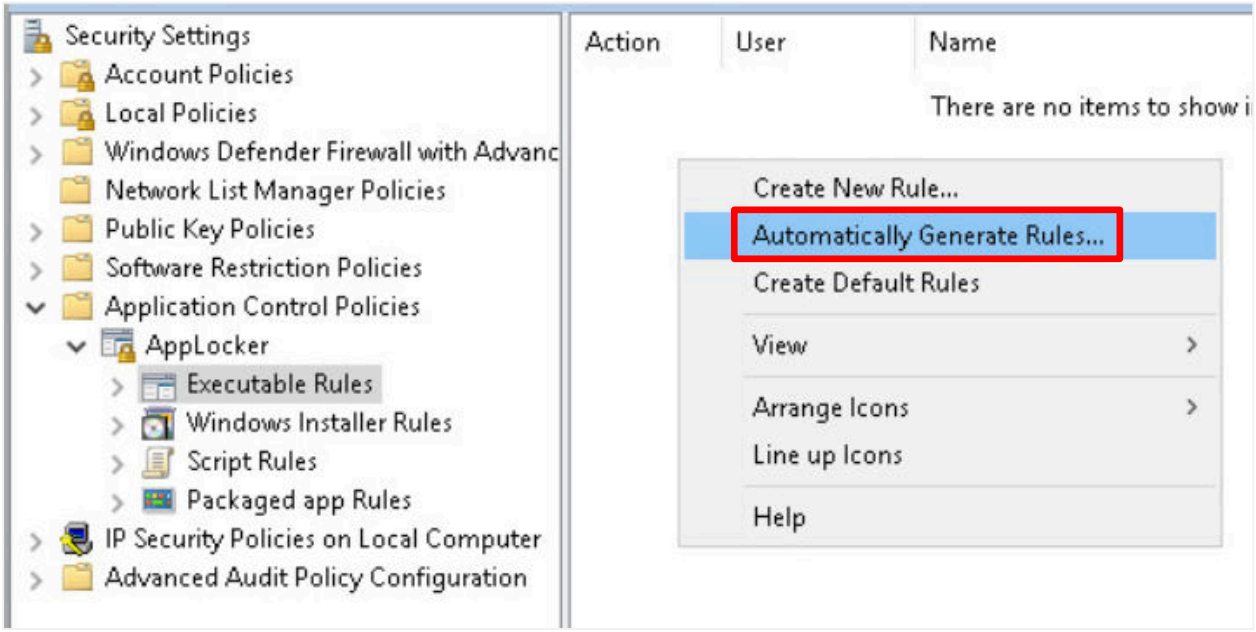
17. Click **OK.**

You will be creating rules in the next part of the task. Rules that are set to *Audit Only* will test the rule and if there is a match, will send an Information Event to the *AppLocker* event logs.

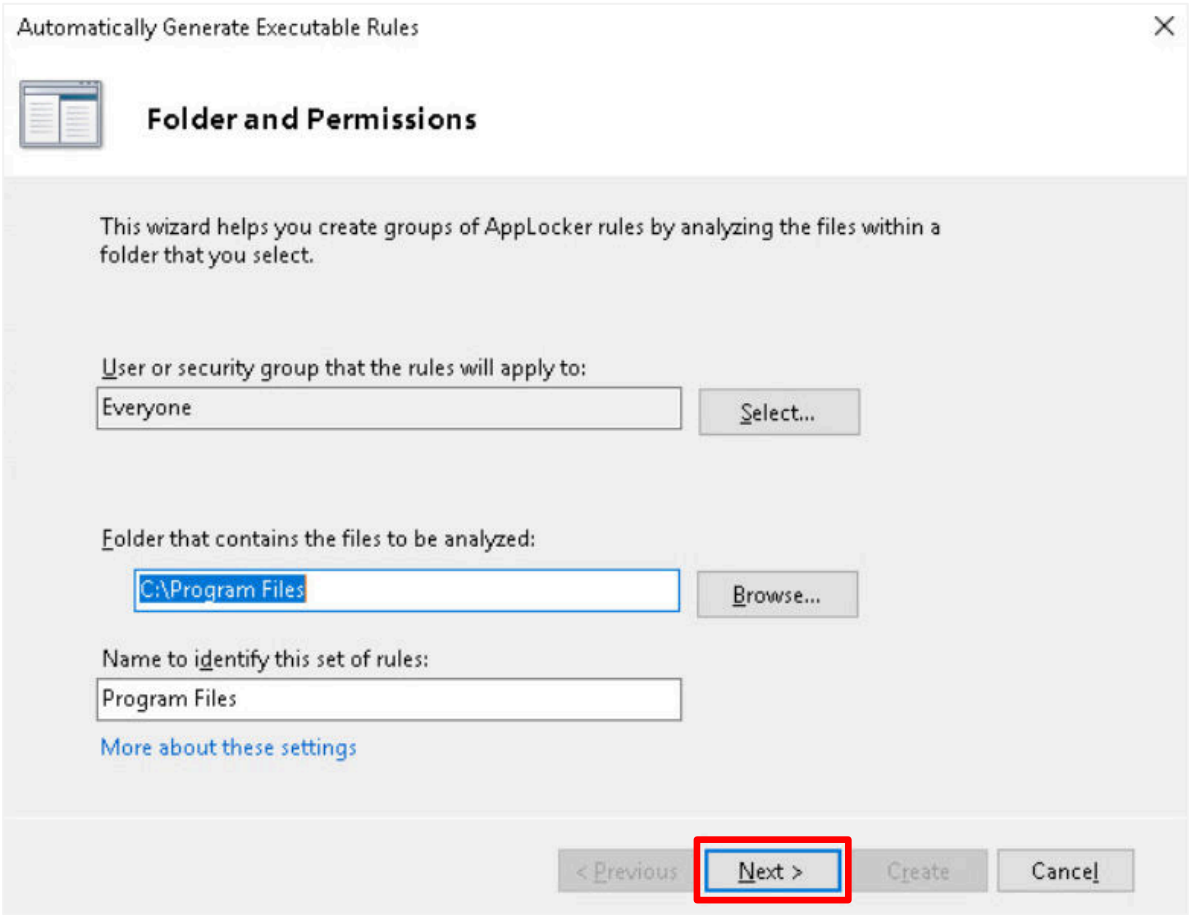
18. Under *Overview*, click on **Executable Rules.**



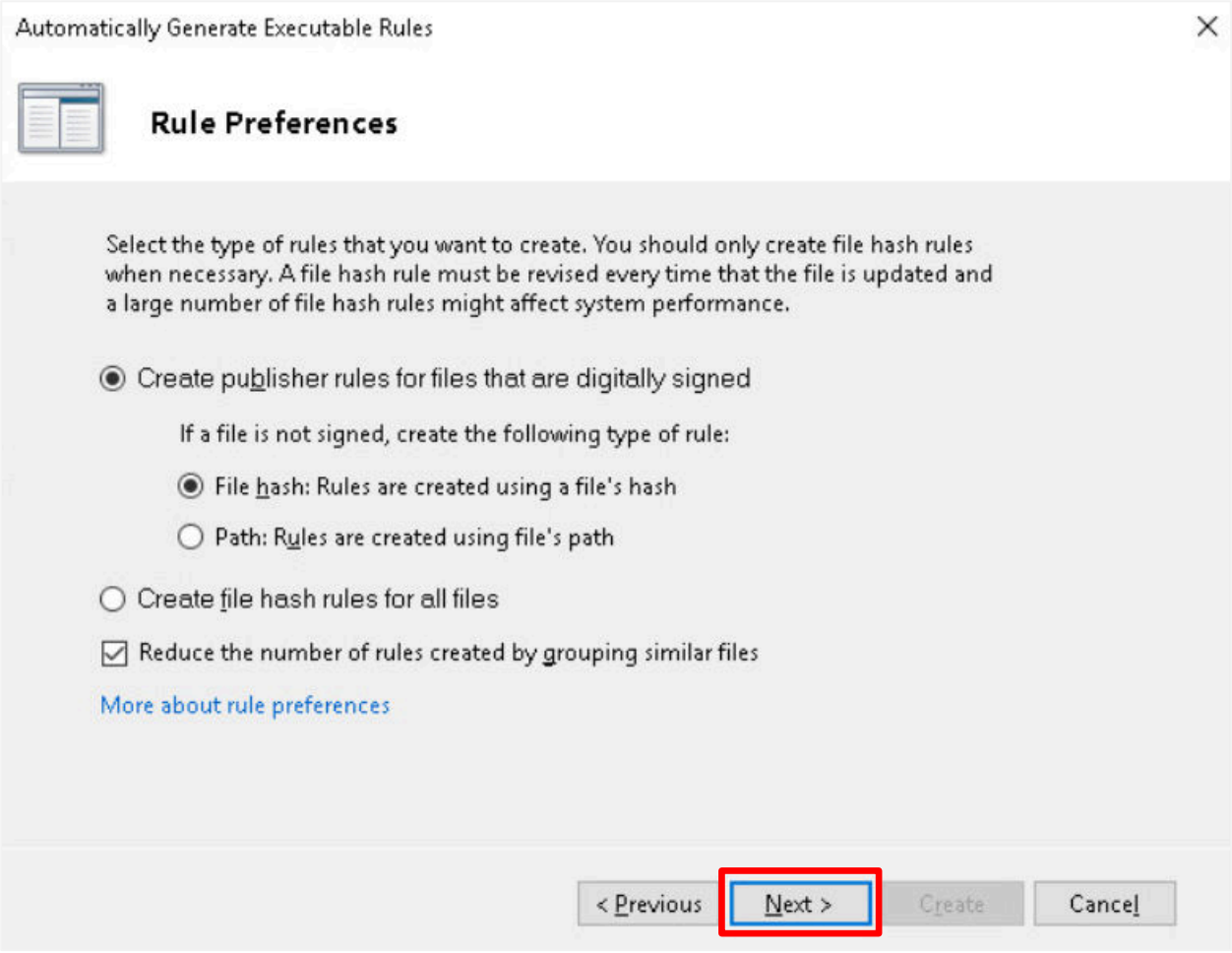
19. On the right panel, right-click on white space to bring up the context menu and click on **Automatically Generate Rules** which will create a set of rules for the software that is installed on this computer.



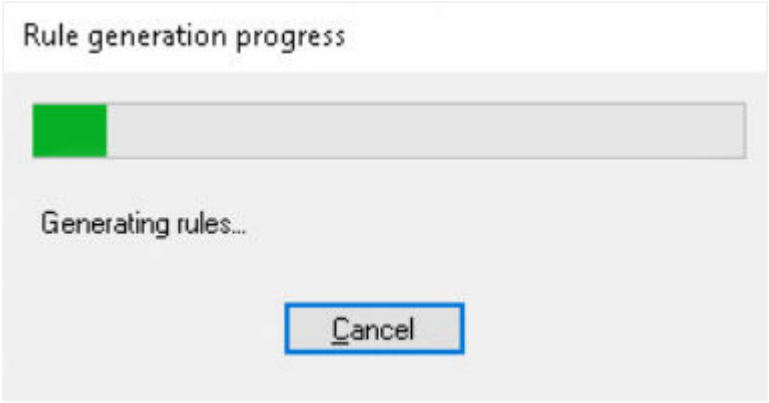
20. The first step of the wizard will analyze files within a folder. Leave the *Folder* set to `C:\Program Files` and the *Name* to `Program Files` and click **Next.**



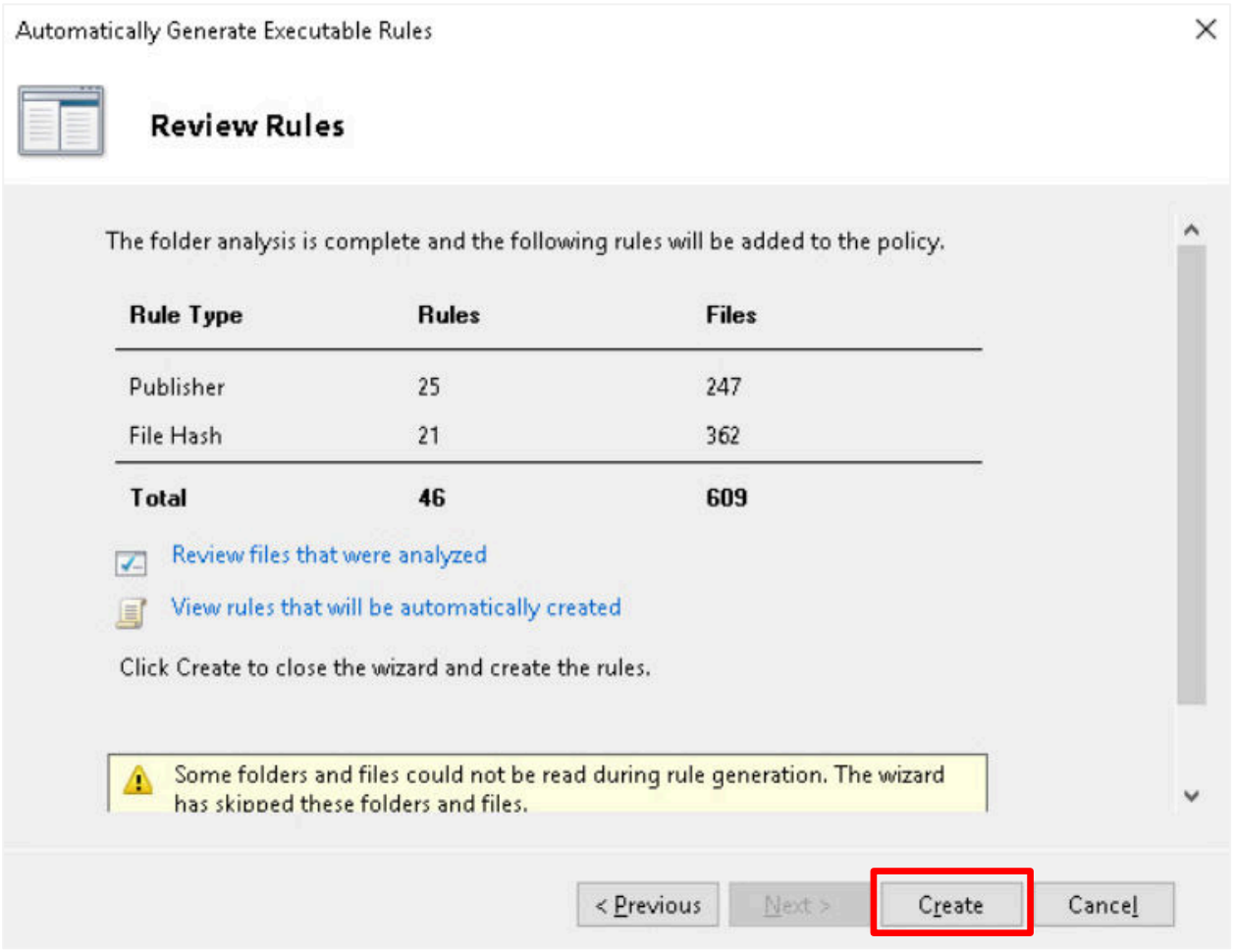
21. The next step in the wizard will allow selecting the type of rules to create. The preferred method is to **Create Publisher Rules that have been digitally signed** by the software manufacturer along with setting a hash value on software that has not been digitally signed. Leave the preferences at their defaults and click **Next**.



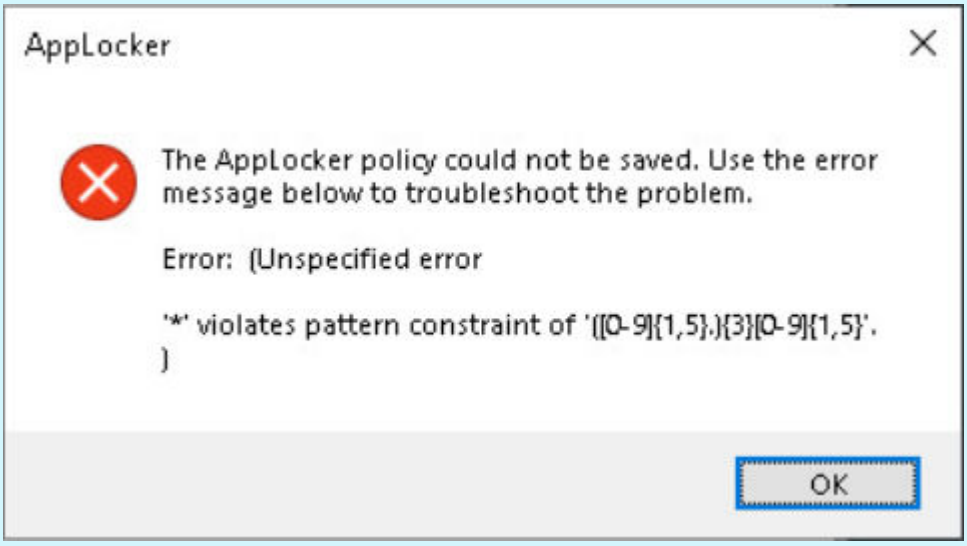
It will take less than a minute to generate the rules.



22. On the *Review Rules* page of the wizard, it will show you the number and types of rules and files that will be added to the policy. You can review the files that were analyzed and view the rules that will be created. Click the **Create** button to create the rule set policies.



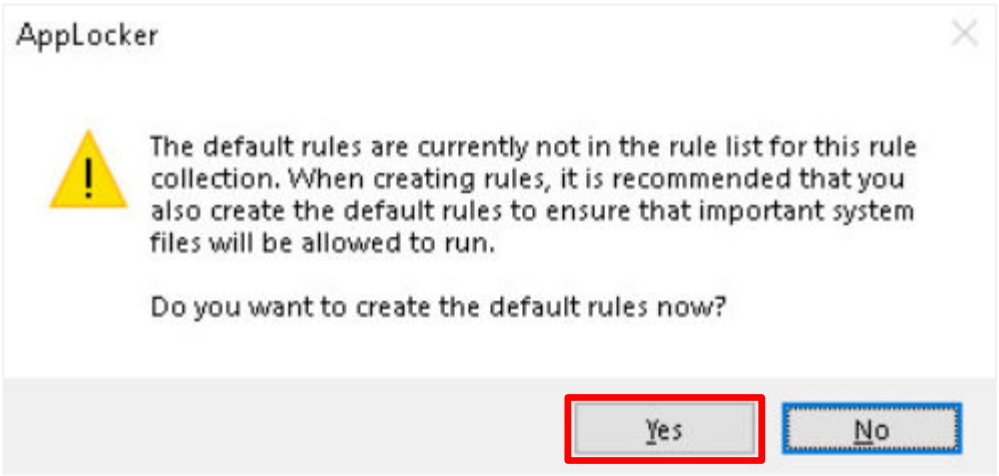
If you get the error popup window:



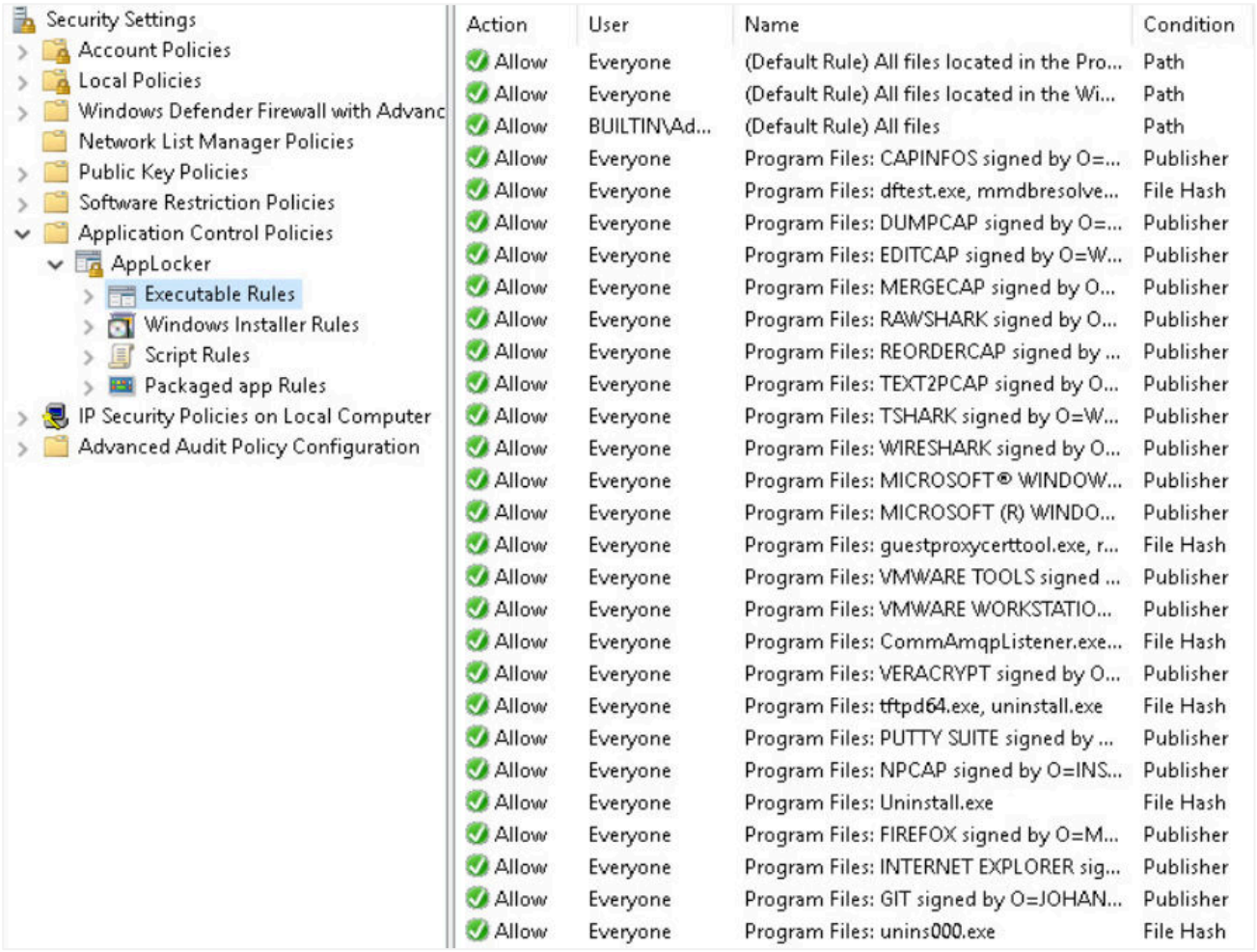
Click the **OK** button.

Even though the default rules are listed in the right panel, they have not been saved. On the right panel, right click on white space to bring up the context menu and click on **Automatically Generate Rules.**

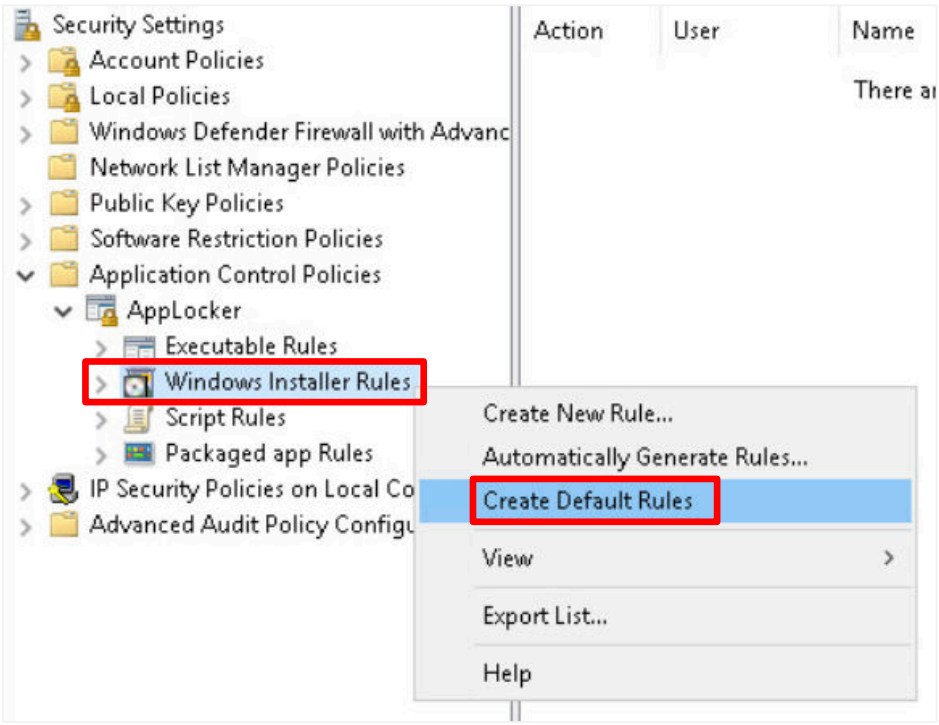
23. On the warning popup window stating, *The default rules are currently not in the rule list for this rule collection*, click on the **Yes** button to create the default rules.



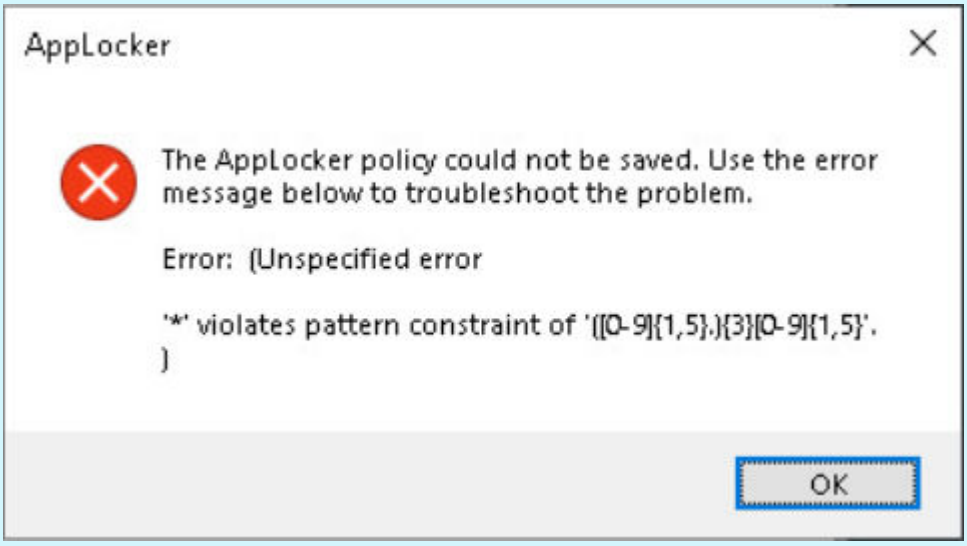
The rules will now be listed in the right panel.



24. On the left side panel, click on **Windows Installer Rules,** and on the right panel, right-click on white space to bring up the context menu and click on **Create Default Rules.**

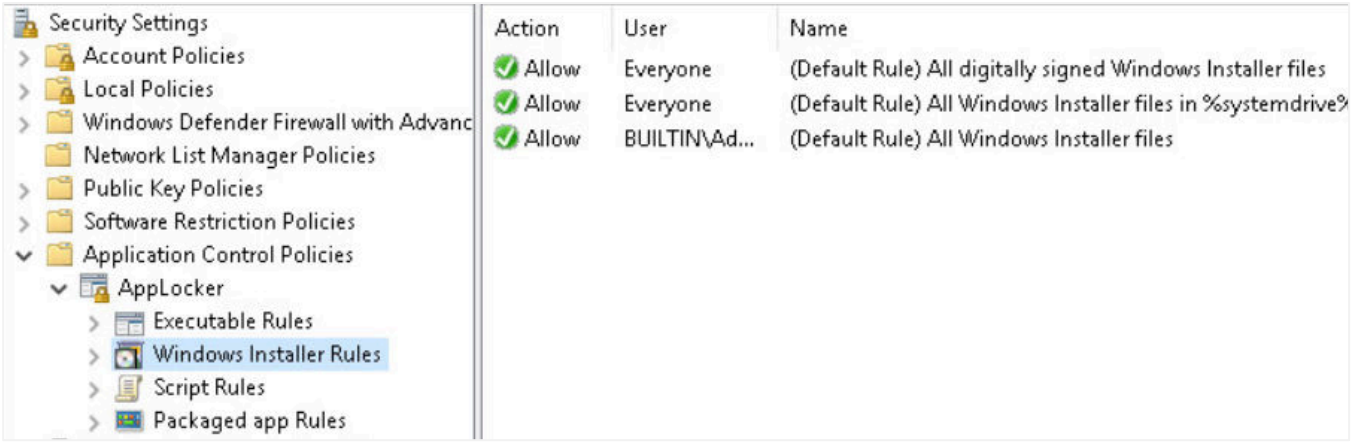


If you get the error popup window:



Click the **OK** button.

Even though the default rules are listed in the right panel, they have not been saved. On the right panel, right click on white space to bring up the context menu and click on **Create Default Rules.**

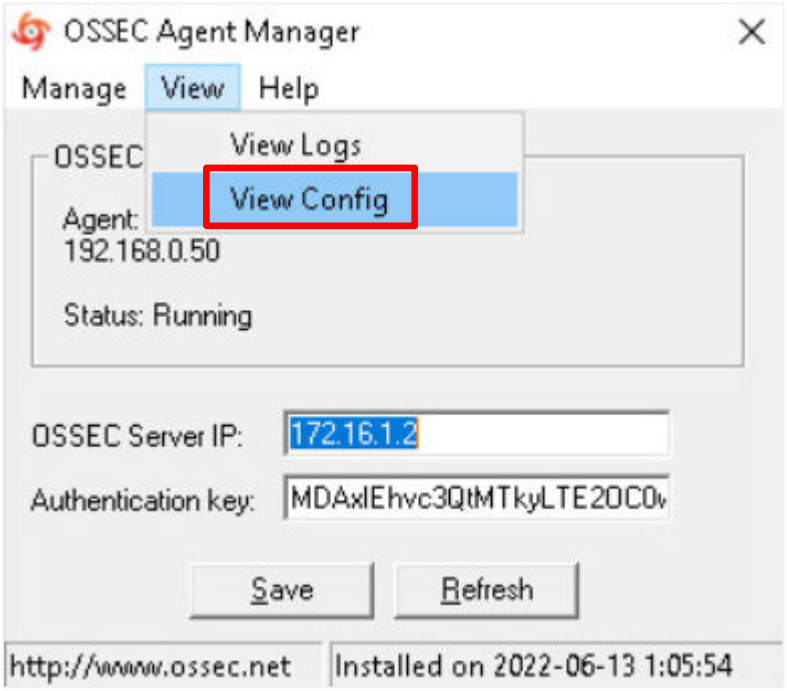


The rules will now be listed in the right panel.

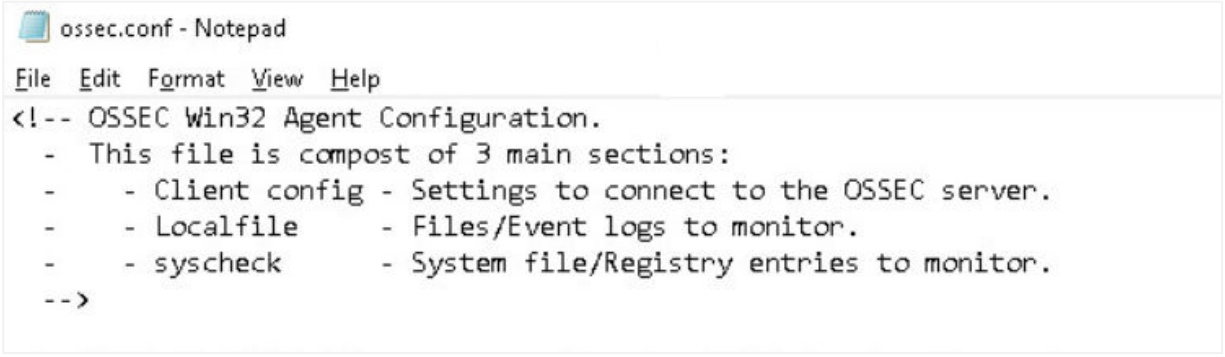
25. Close the *Local Security Policy* window.

The next part of the task will edit the *OSSEC.conf* file for the *OSSEC HIDS Agent* to push the *AppLocker Events* to the *AlienValult OSSIM*.

26. The *OSSEC Agent Manager* window should still be open on the desktop. Click on **View**, then click **View Config.**



The *OSSEC.conf* file will open in *Notepad*.

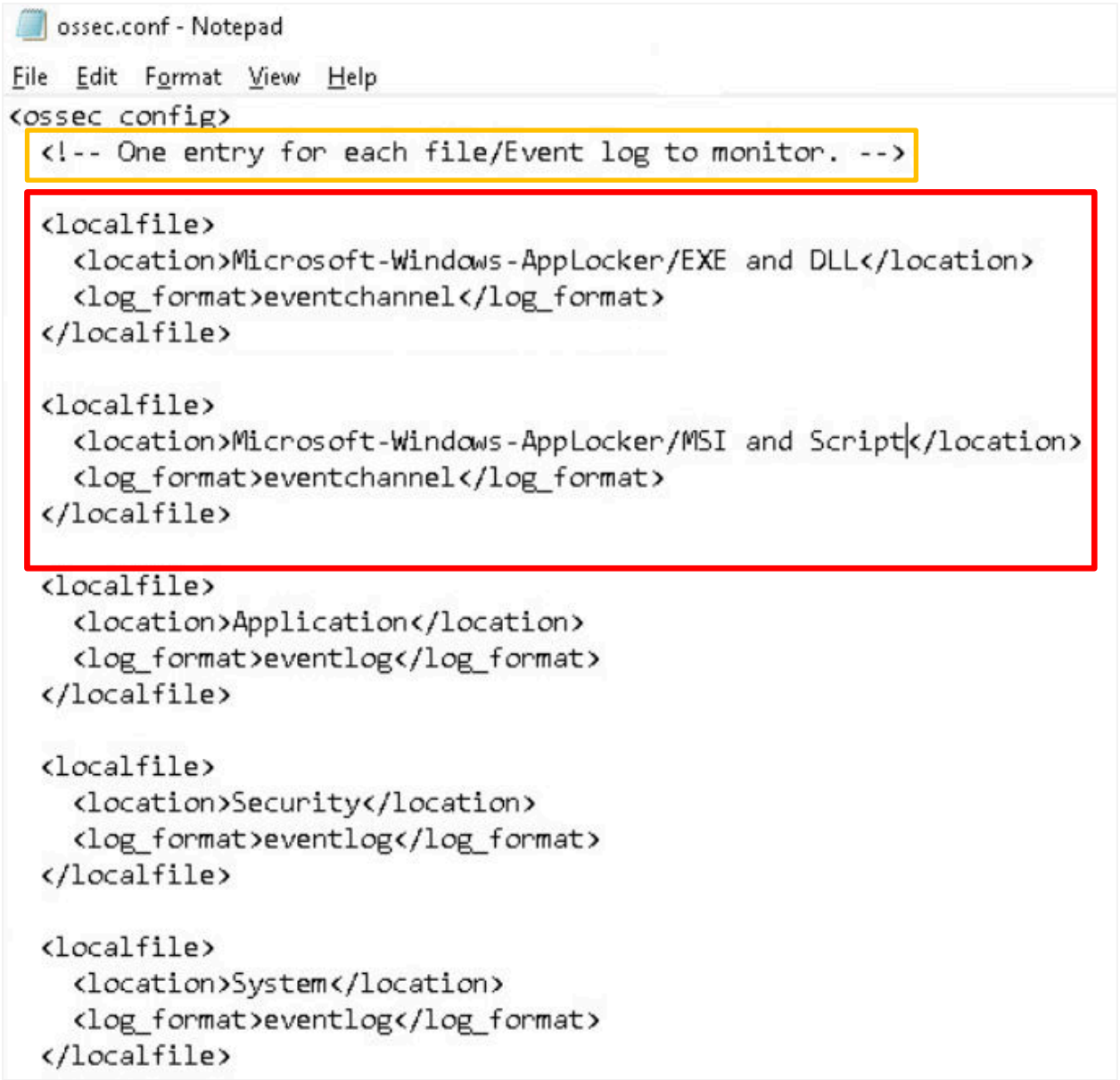


27. Scroll down to the *<ossec_config>* below the line

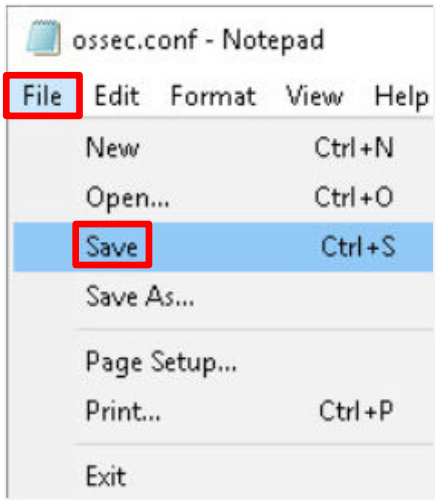
<!-- One entry for each file/Event log to monitor. -->

type the following script entries (all lines are case sensitive):

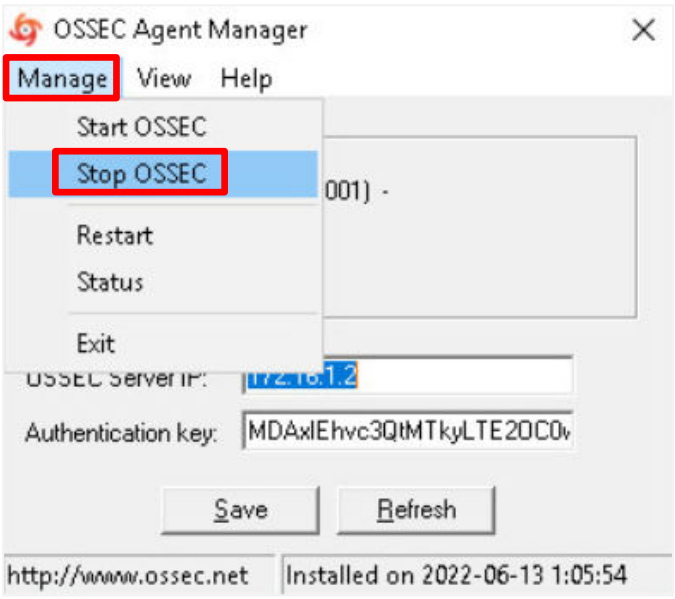
```
<localfile>
  <location>Microsoft-Windows-AppLocker/EXE and DLL</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Microsoft-Windows-AppLocker/MSI and Script</location>
  <log_format>eventchannel</log_format>
</localfile>
```



28. Save the *OSSEC.conf* file by clicking on **File>Save.**

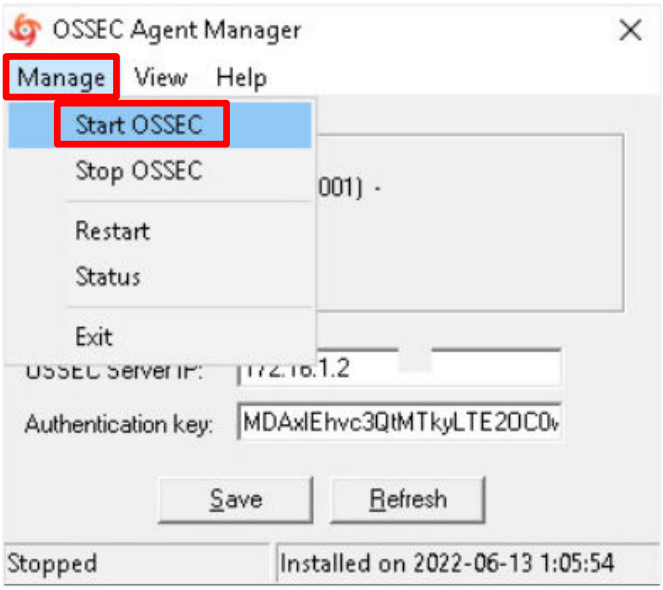


29. Close **Notepad.**
30. On the *OSSEC Agent Manager* window, click on **Manage>Stop OSSEC.**

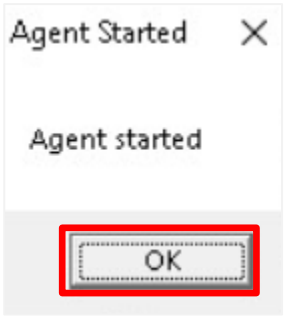


31. On the *Agent Stopped* popup, click **OK.**

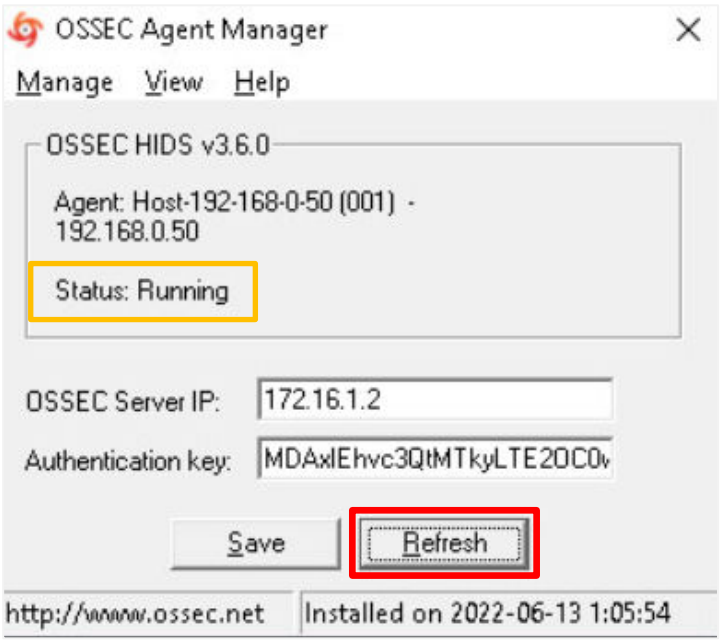
32. On the *OSSEC Agent Manager* window, click on **Manage>Start OSSEC.**



33. On the *Agent Started* popup, click **OK.**



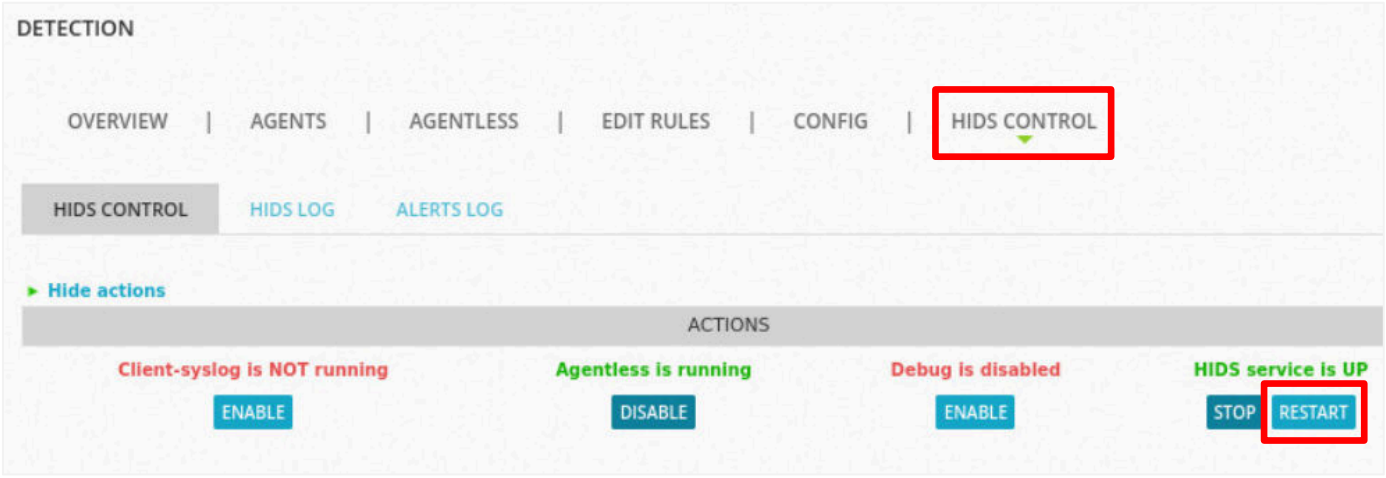
34. On the *OSSEC Agent Manager* window, click on **Refresh** to make sure the *OSSEC Agent Manager* is *Running*.



35. Close the **OSSEC Agent Manager** window.

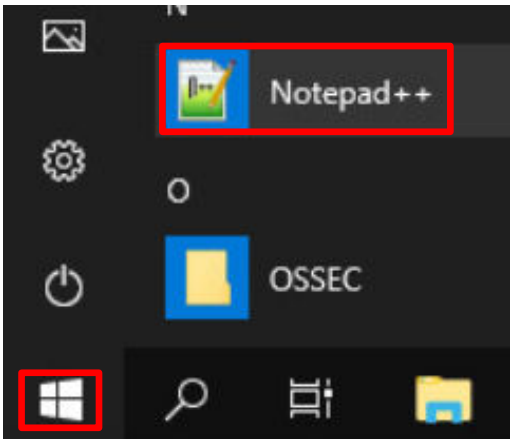
2.4.2 Collect AppLocker Events and Trigger Alarms

1. Set the focus to the **MintOS** computer.
2. You should still be on the *DETECTION* page under *HIDS CONTROL*. In the *ACTIONS* section, click **RESTART** under *HIDS service is UP*.

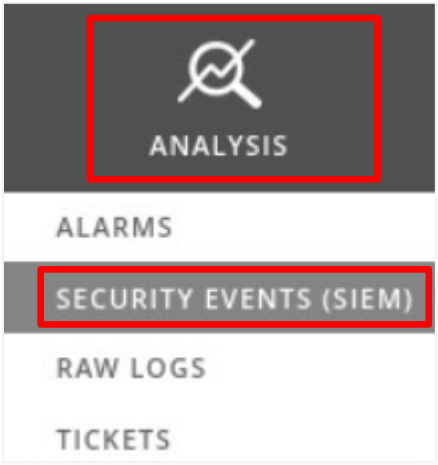


3. Set the focus back to the **WinOS** computer.

4. Run *Notepad++* by clicking the **Start** button and then clicking on **Notepad++.**

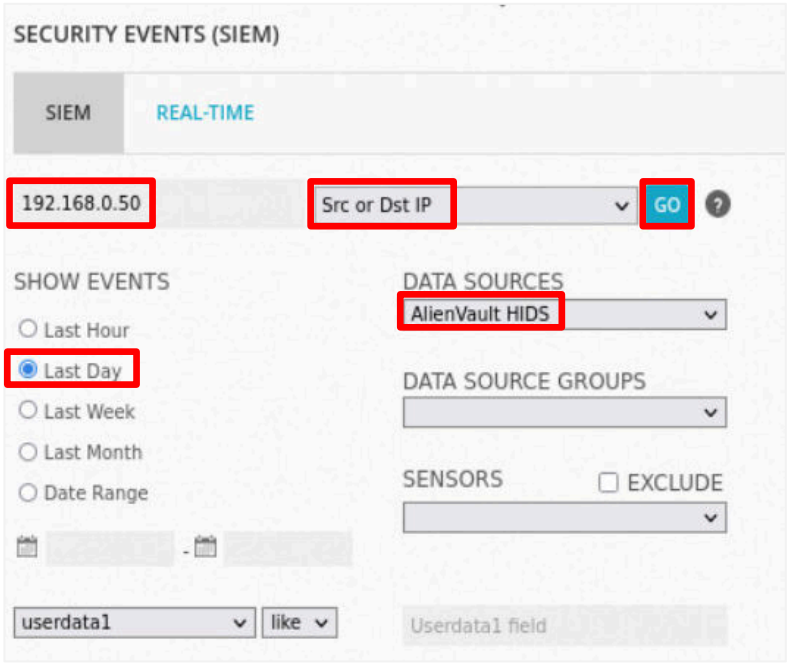


5. Close **Notepad++.**
6. Return focus to the **MintOS** computer.
7. Hover over **ANALYSIS,** then click on **SECURITY EVENTS (SIEM).**



8. In the *AlienVault OSSIM* Web UI, on the *SECURITY EVENTS (SIEM)* page, do the following:

   - Under *SHOW EVENTS,* click the **Last Day** radio box.
   - Under *DATA SOURCES*, use the list arrow and select **AlienVault HIDS.**
   - In the *Search* box, type `192.168.0.50`.
   - In the selection box to the right of the *Search* box, use the list arrow and select **Src or Dst IP.**
   - Click **GO.**



9. Scroll down the screen and click on **GROUPED** in the menu below the filters.

10. Scroll down to the bottom of the page, and you can see *AppLocker allowed a program to execute* events. Click on **AlienVault HIDS: AppLocker allowed a program to execute.**

EVENT NAME	EVENTS # (*)	UNIQUE SRC. #	UNIQUE DST. #	LATEST EVENT
AlienVault HIDS: Registry Entry Added to the System	4,091	1	1	2022-07-05 02H
AlienVault HIDS: File added to the system.	25	1	1	2022-07-05 02H
AlienVault HIDS: Special privileges assigned to new logon	14	1	1	2022-07-05 02H
AlienVault HIDS: Windows machine logon.	13	1	1	2022-07-05 02H
AlienVault HIDS: Windows User Logoff.	8	1	1	2022-07-05 02H
AlienVault HIDS: Logon Failure - Unknown user or bad password.	6	1	1	2022-07-05 02H
AlienVault HIDS: HIDS agent started.	2	1	1	2022-07-05 02H
AlienVault HIDS: Registry Integrity Checksum Changed	2	1	1	2022-07-05 03H
AlienVault HIDS: AppLocker allowed a program to execute	2	1	1	2022-07-05 02H

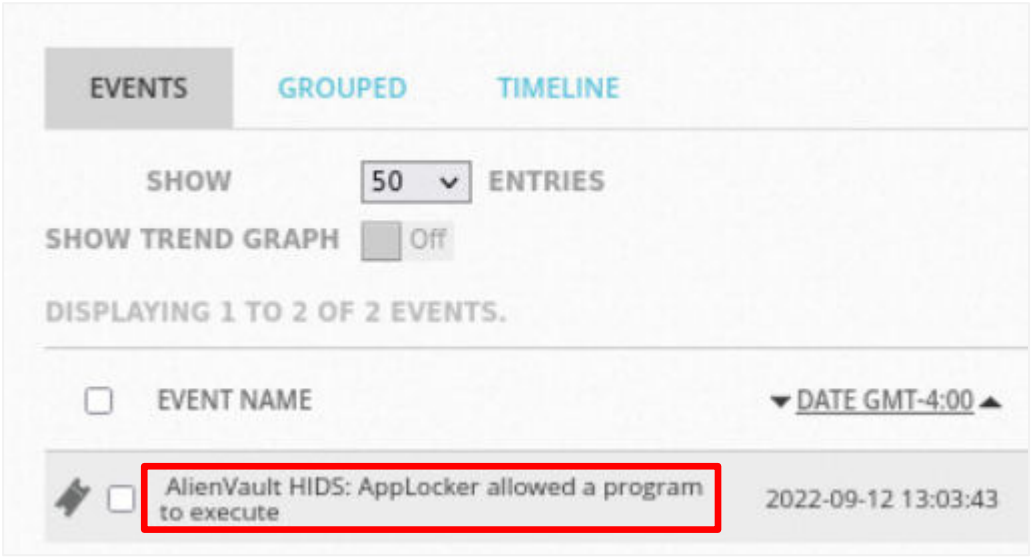
This will filter the event log showing the details for only the *AppLocker* events…

EVENT NAME	DATE GMT-4:00
AlienVault HIDS: AppLocker allowed a program to execute	2022-06-15 03:23:53

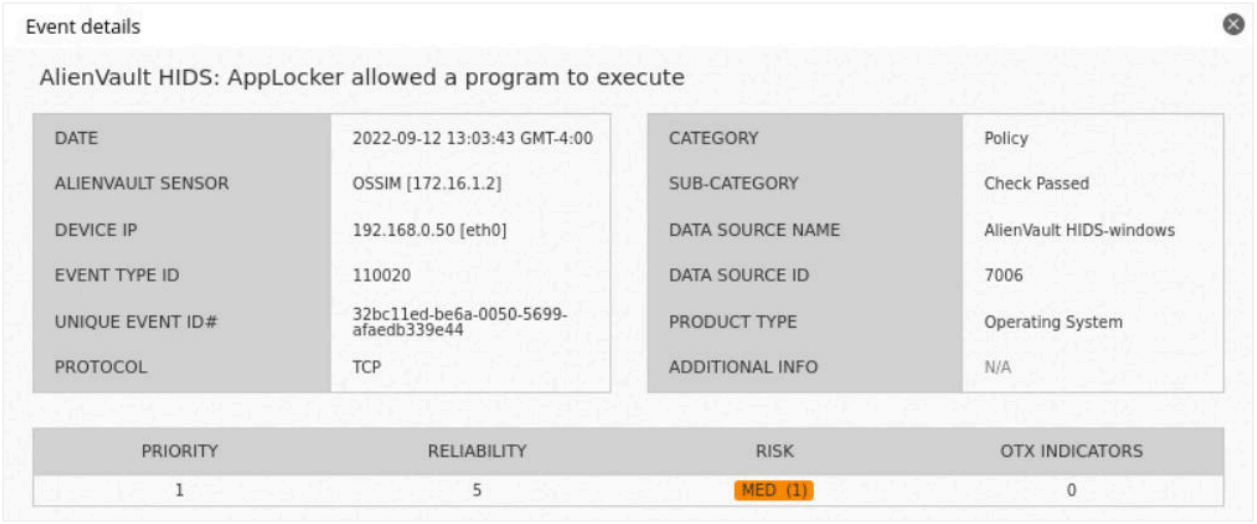
with a *RISK* of *MED*, which will also trigger an *ALARM*.

DESTINATION	ASSET S → D	RISK	
Host-192-168-0-50	5->2	MED (1)	

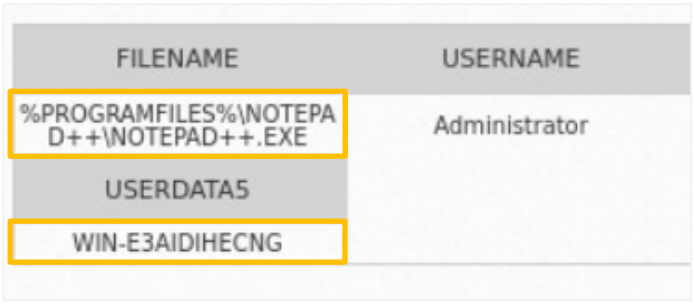
11. Click on the **Event Name.**



This will show the *Event Details*.



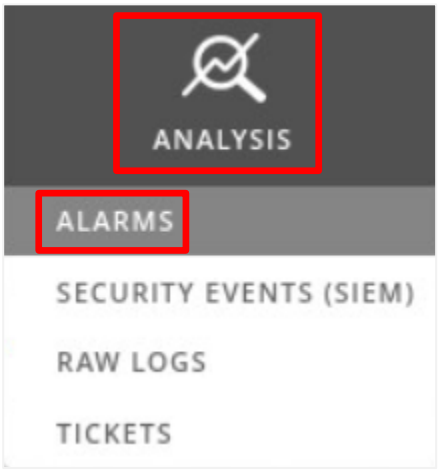
12. Scrolling down the page will show the details about which application was run, which user ran the application, and the computer on which the application was run.



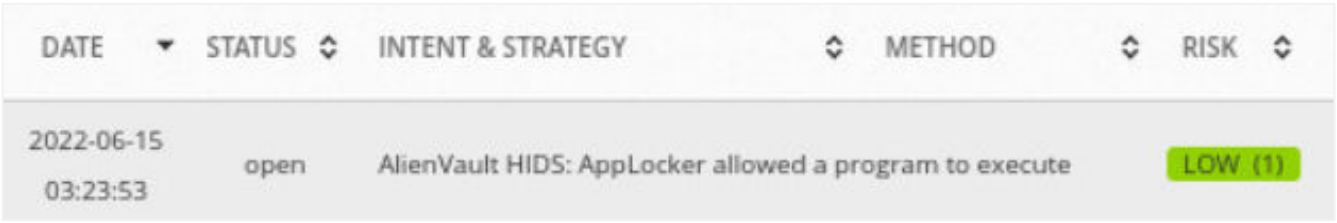
13. Close the **Event Details** window.

Let's take a look at the alarm that was generated.

14. Hover over **ANALYSIS** and click on **ALARMS.**

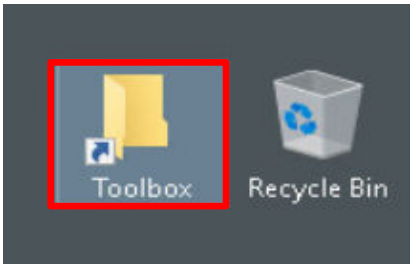


15. Scroll down to the bottom of the page, and you will see the alarm entry.

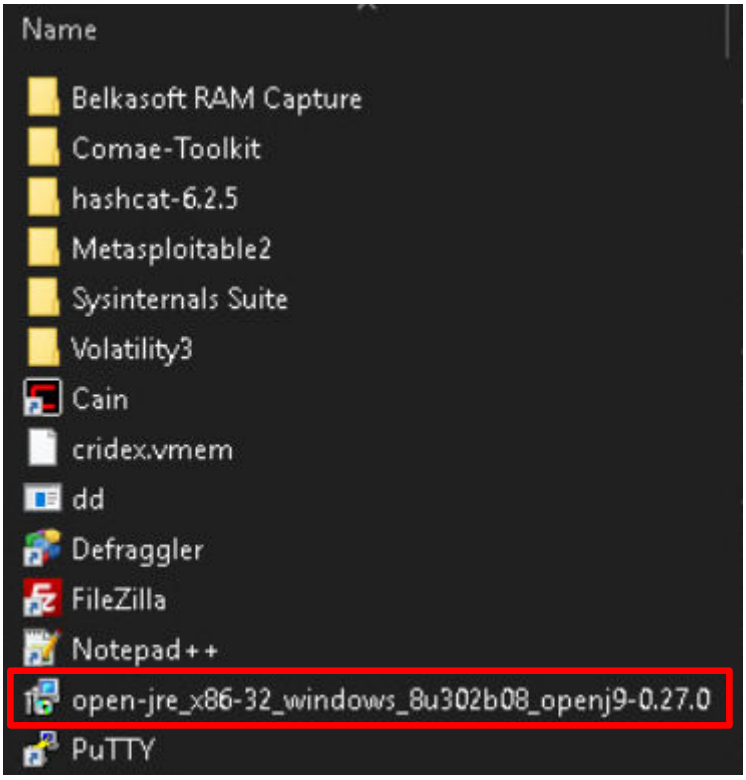


Now, install a piece of software on the Windows host.

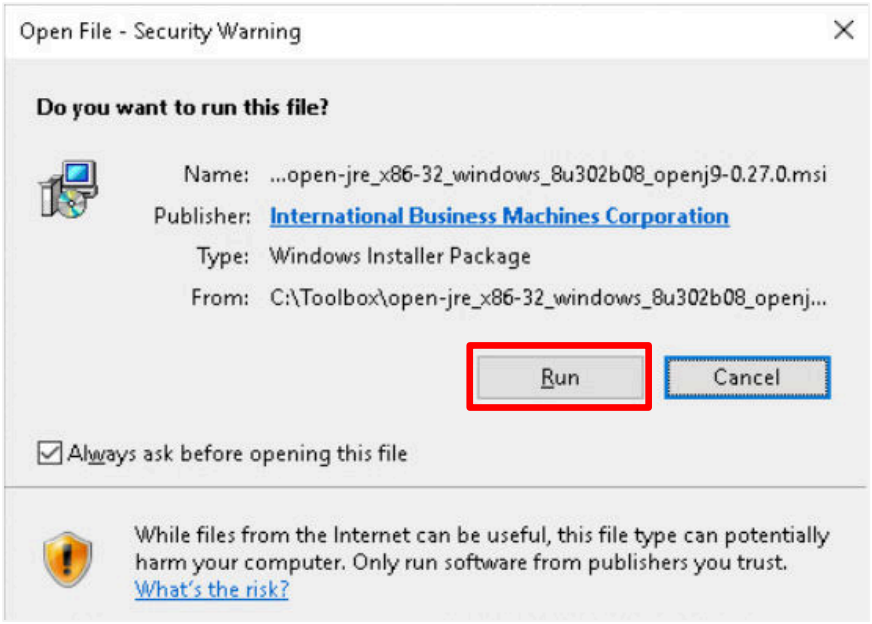
16. Set the focus on the **WinOS** computer.
17. Double-click on the **Toolbox** folder on the *desktop.*



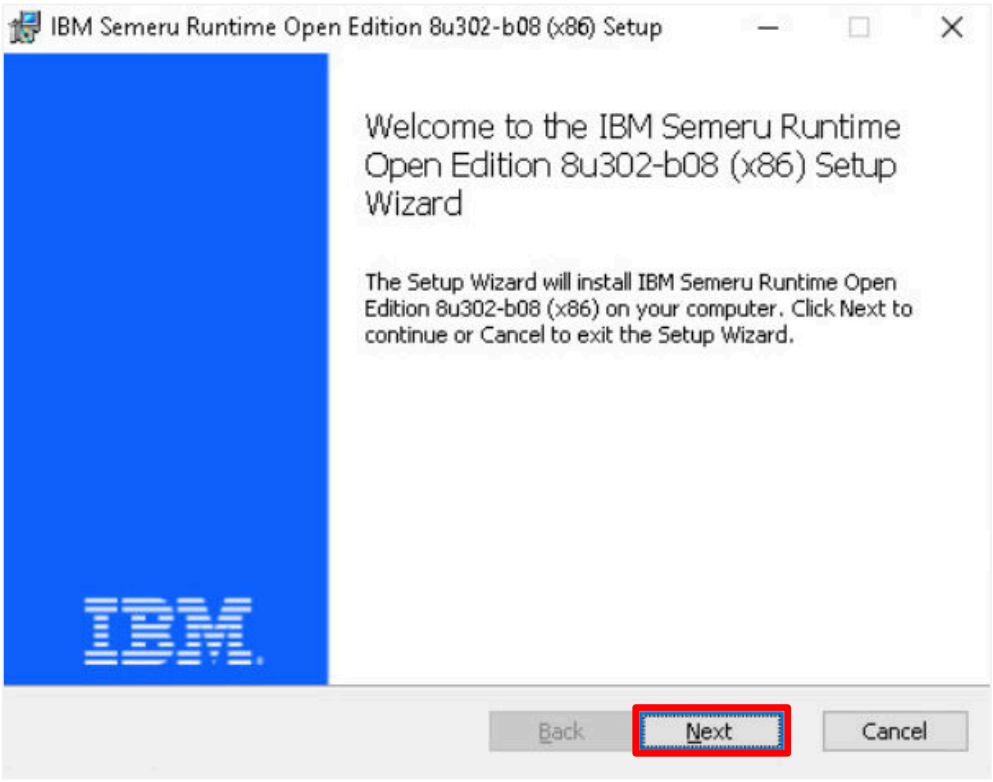
18. In the *Toolbox* folder, find the **open-jre_x86-32_windows_8u302b08** application and double-click to install.



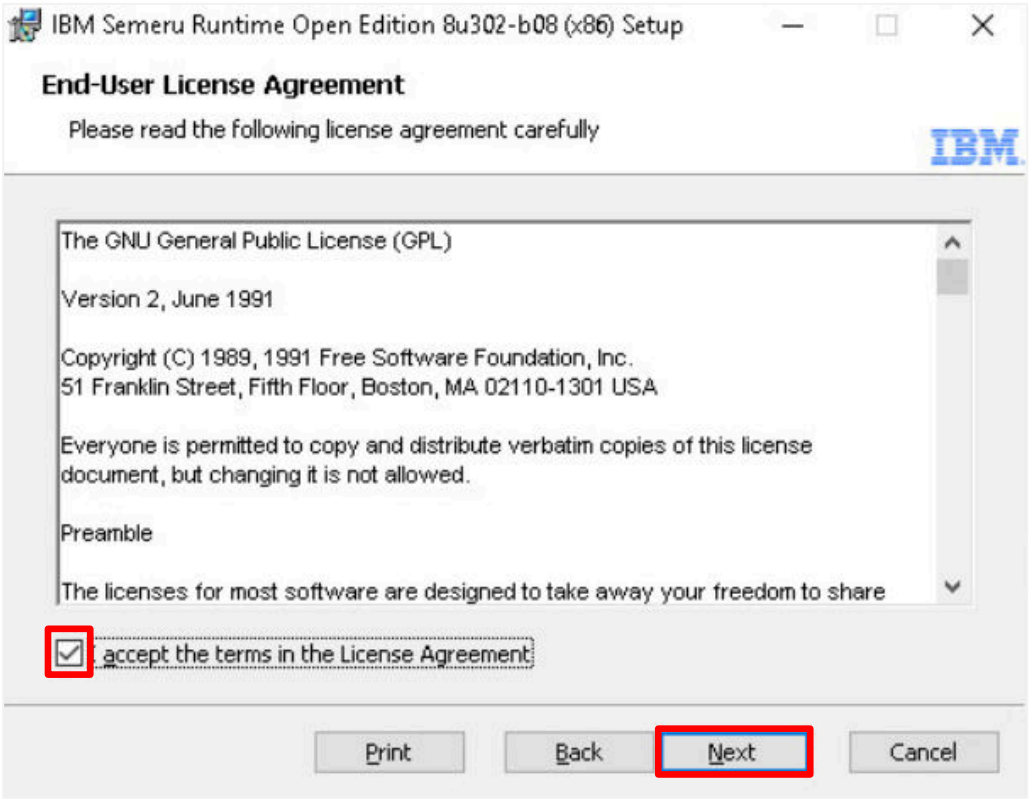
19. On the *Open File – Security Warning* window, click **Run**.



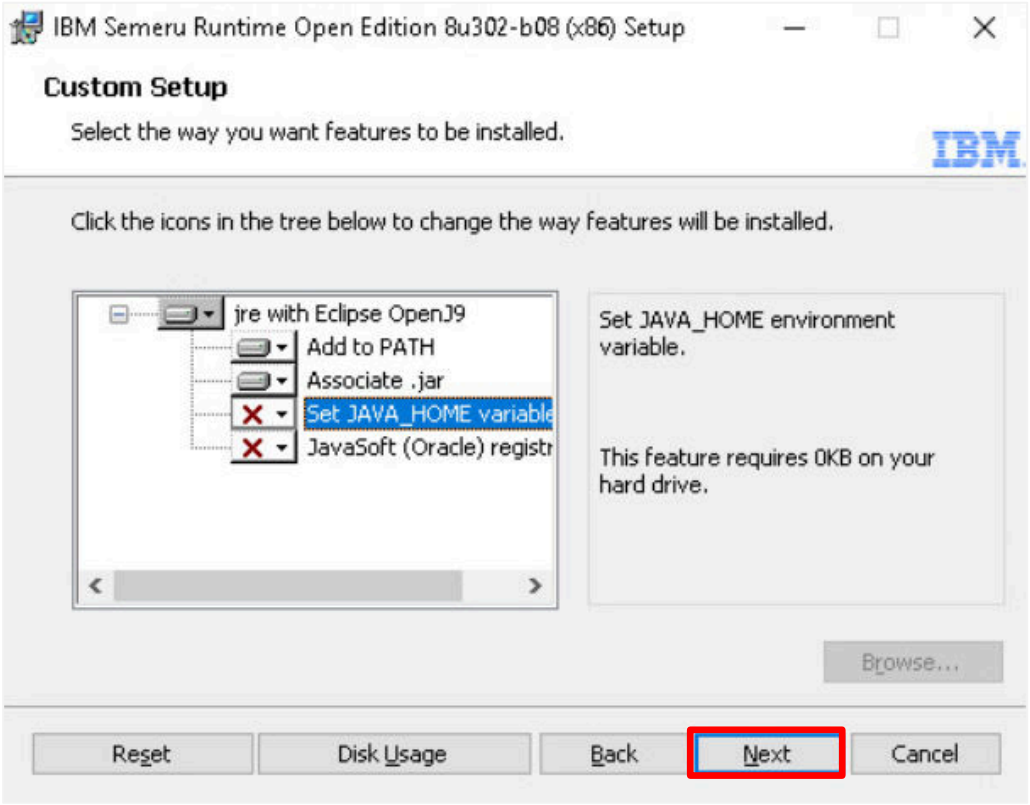
20. On the *Welcome* window, click **Next.**



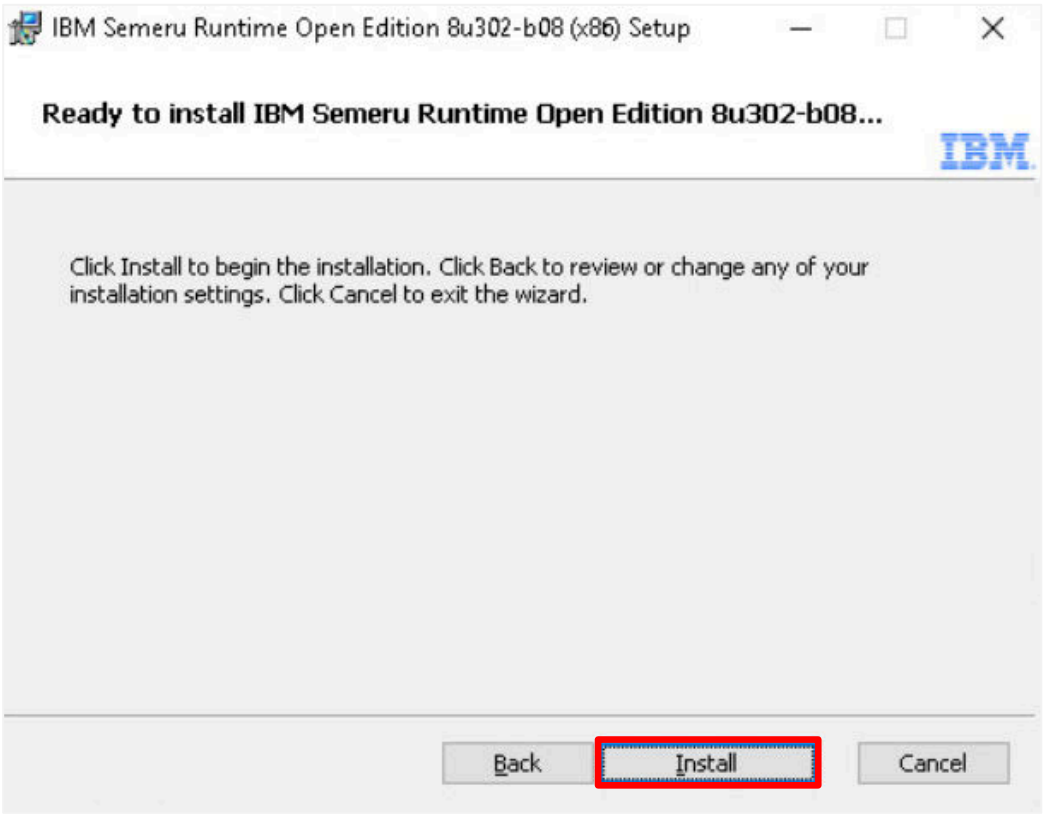
21. On the *License Agreement* window, click the **I accept the terms in the License Agreement** checkbox and click **Next.**



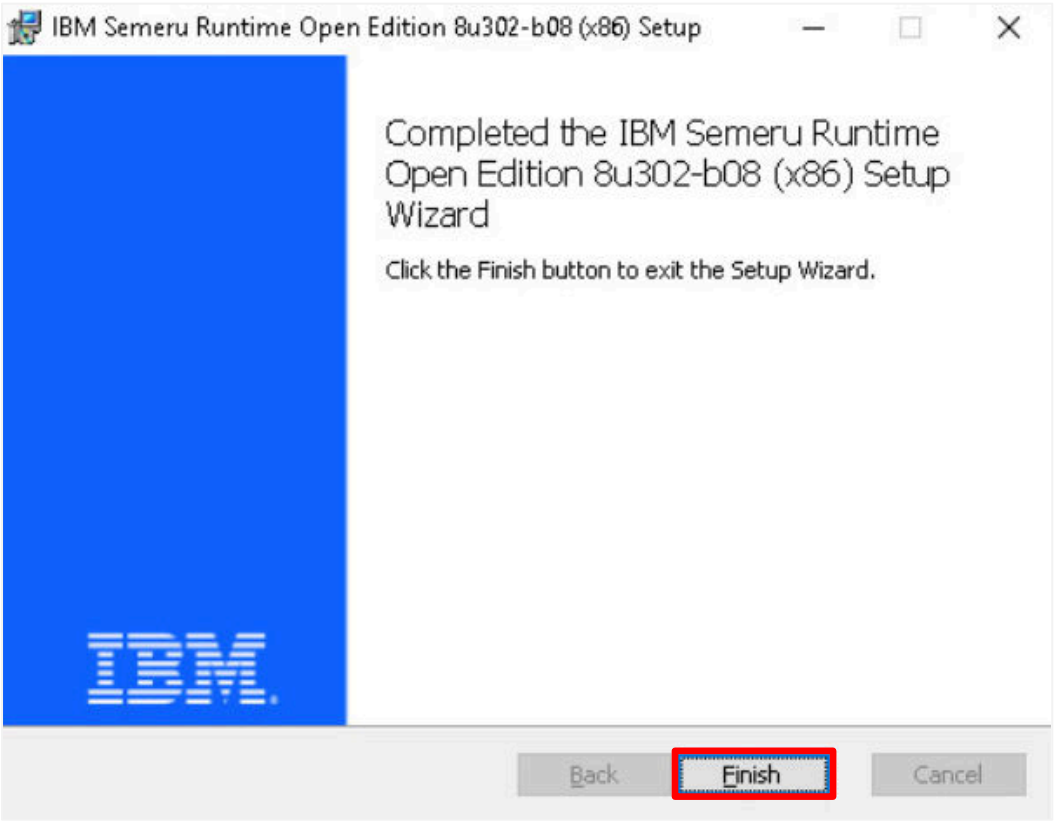
22. On the *Custom Setup* window, accept the defaults and click **Next.**



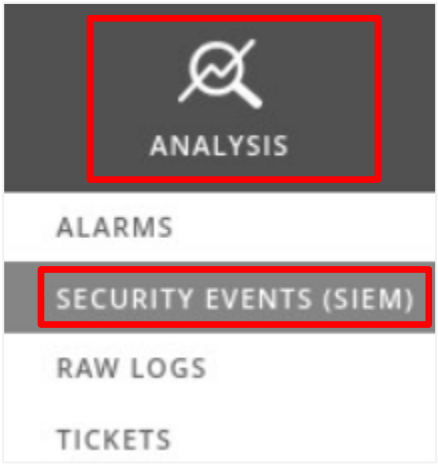
23. On the *Ready to Install* page, click **Install.**



24. On the *Completed* window, click **Finish**.

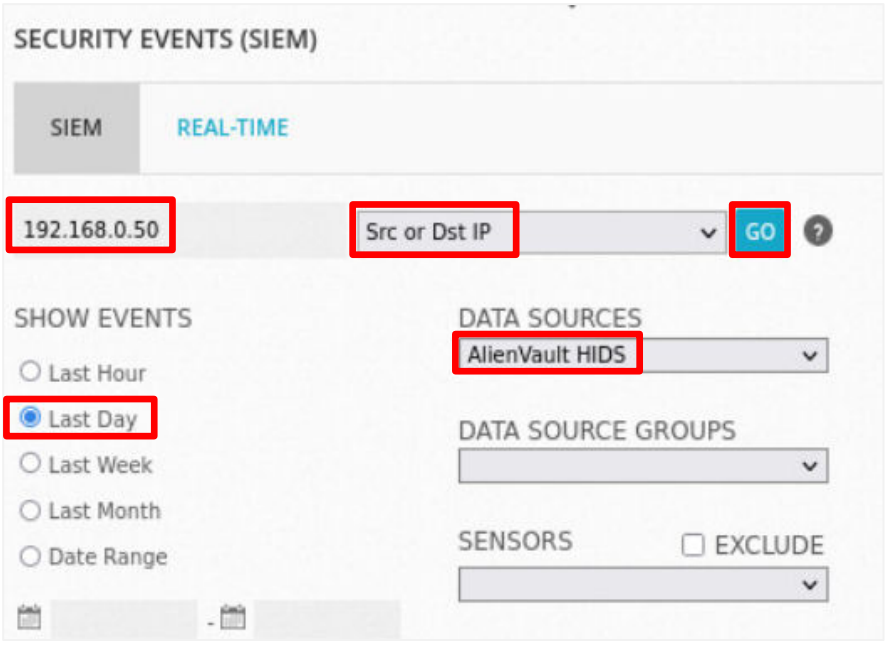


25. Set the focus back to the **MintOS** computer.
26. Hover over **ANALYSIS,** then click on **SECURITY EVENTS (SIEM).**



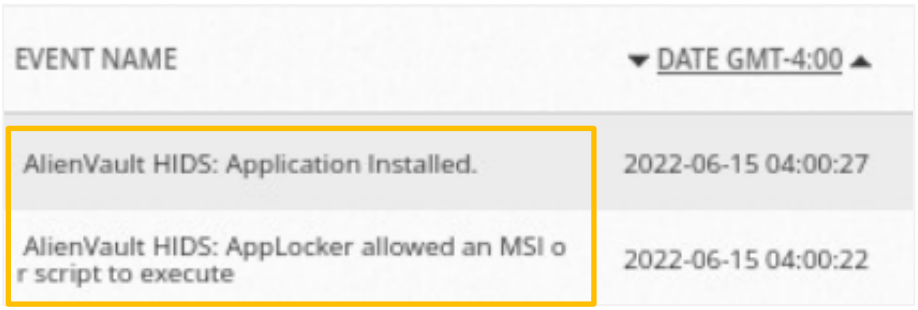
27. In the *AlienVault OSSIM* Web UI, on the *SECURITY EVENTS (SIEM)* page, do the following:

- Under *SHOW EVENTS,* click the **Last Day** radio box.
- Under DATA SOURCES, use the list arrow and select **AlienVault HIDS.**
- In the *Search* box, type `192.168.0.50`**.**
- In the selection box to the right of the **Search** box, use the list arrow and select **Src or Dst IP.**
- Click **GO.**

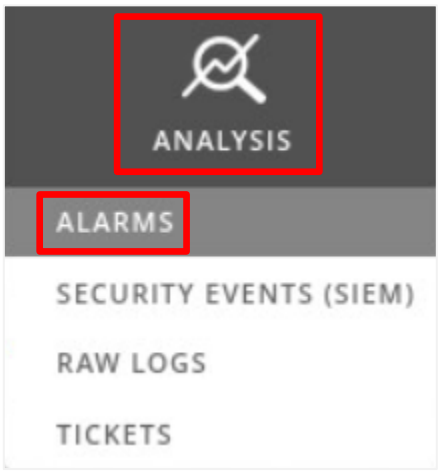


28. Scroll down to the bottom of the page, and you can see the events:

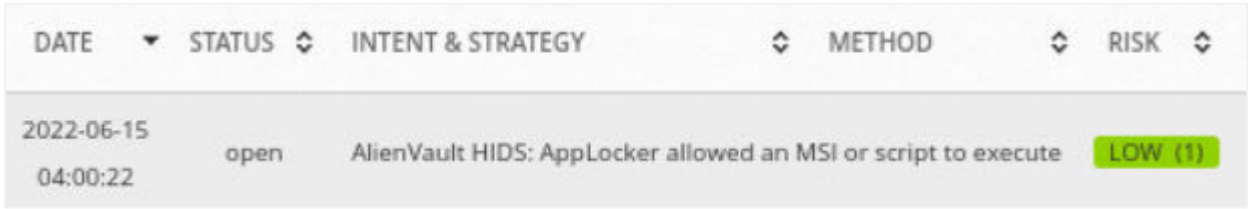
- *AlienVault HIDS: Application Installed*
- *AlienVault HIDS: AppLocker allowed an MSI or Script to execute*



29. Hover over **ANALYSIS** and click on **ALARMS.**



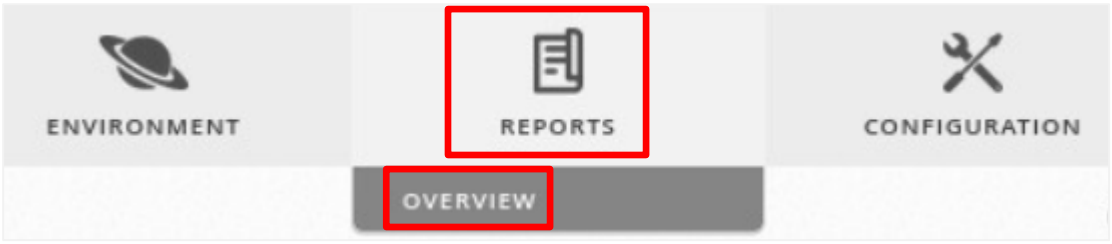
30. Scroll down to the bottom of the page, and you will see the alarm entry.



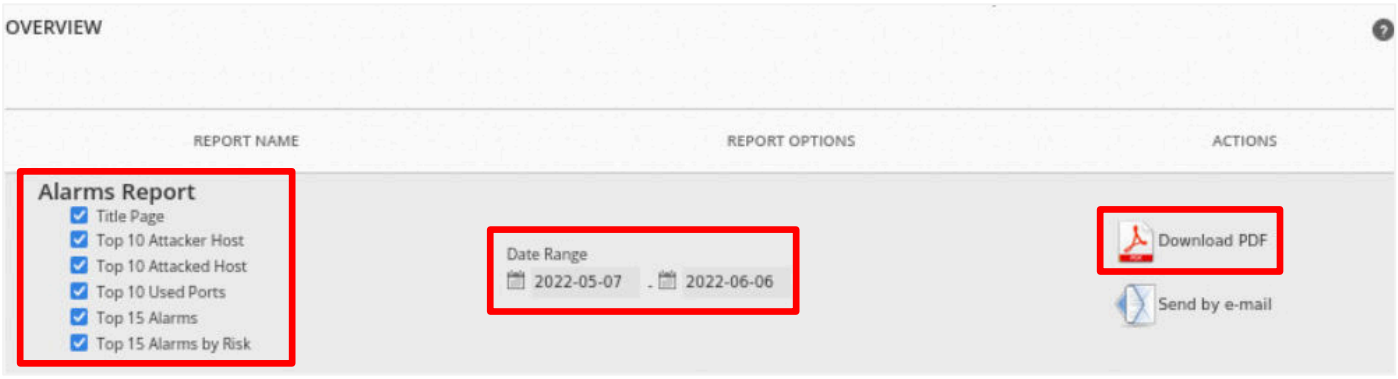
31. Remain on the *AlienVault OSSIM* Web UP and proceed to the next task.

2.5 Compile and Generate HIDS Reports

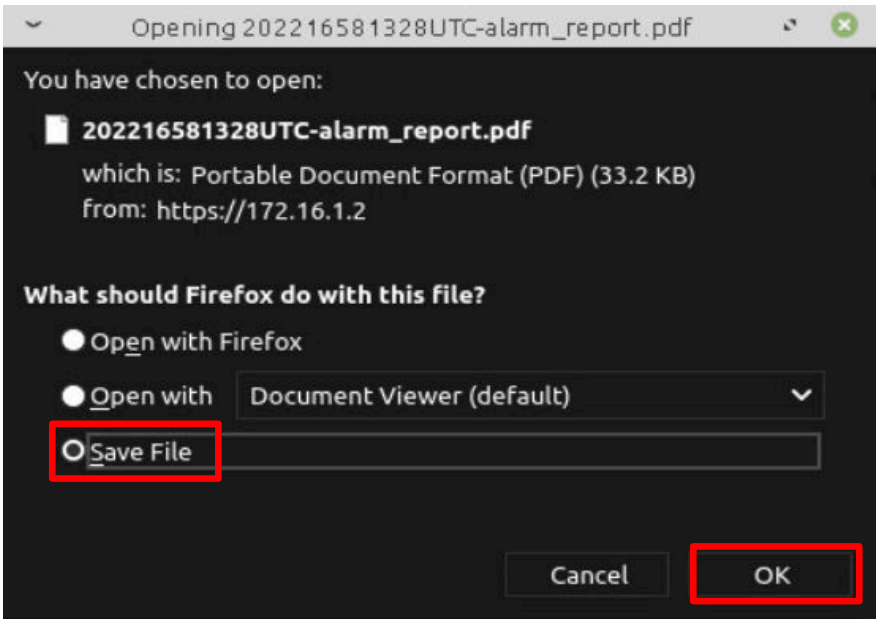
1. Set the focus to the **MintOS** computer.
2. Hover over the **REPORTS** button on the menu bar and click on **OVERVIEW**.



3. On the *OVERVIEW* page, you will generate an *Alarms Report*. Under *Alarms Report*, make sure all of the report pages are checked and that the date range shows a range that includes the current date. Click the **Download PDF** button.



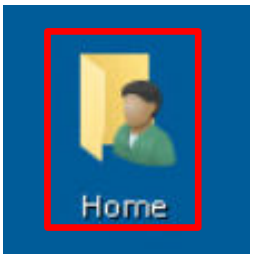
4. When the report is complete, make sure the **Save File** radio button is selected on the *What should Firefox do with this file?* popup window and click the **OK** button.



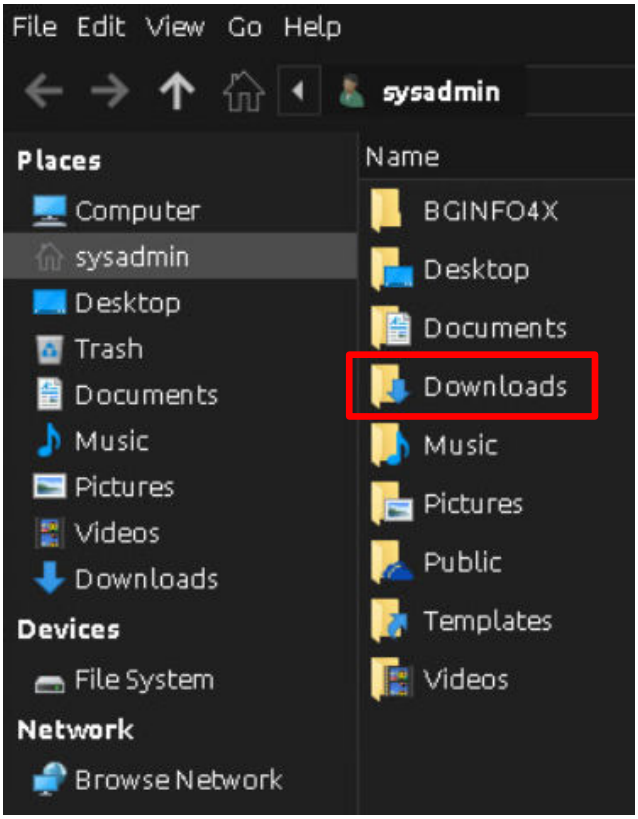
5. Minimize the web browser.

The file will be saved in the *Downloads* folder for the sysadmin user on the *MintOS* computer.

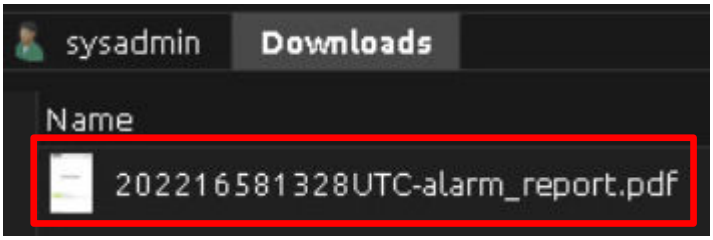
6. Double-click on the **Home** folder on the *MintOS* desktop.



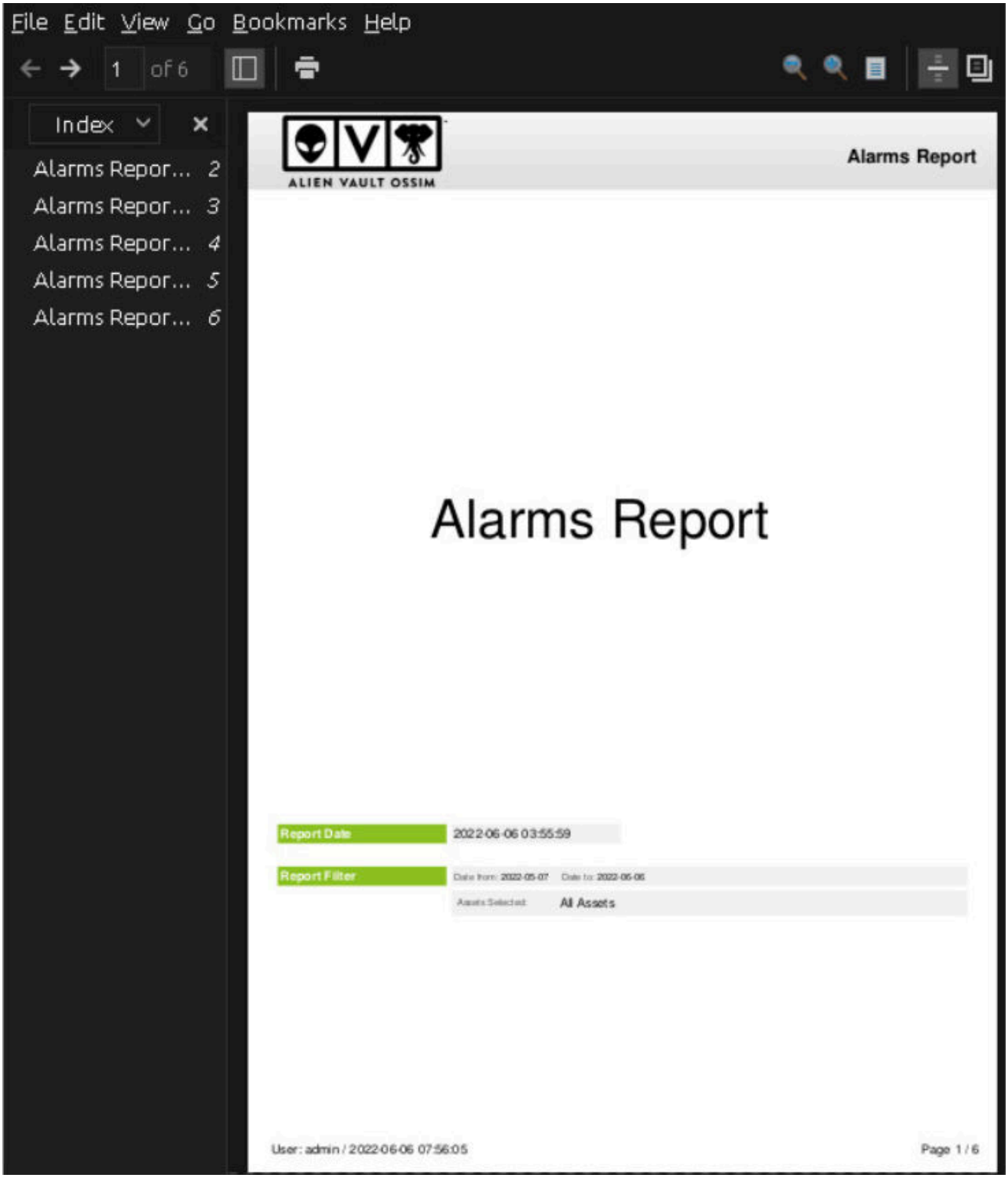
7. In the *sysadmin* window, double-click on the **Downloads** folder.



8. In the *Downloads* folder, you should see the report that was just downloaded from *AlienVault OSSIM*. Double-click on the **file** to open it.



You will now see the *Alarms Report* that was just generated. This report can be used for further analysis.



9. The lab is now complete; you may now end the reservation.