



## 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

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB+ is a registered trademark of Network Development Group, Inc.  
KALI LINUX™ is a trademark of Offensive Security.  
ALIEN VAULT OSSIM V is a trademark of AlienVault, Inc.  
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.  
Greenbone is a trademark of Greenbone Networks GmbH.  
SECURITY ONION is a trademark of Security Onion Solutions LLC.  
Android is a trademark of Google LLC.  
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").  
All trademarks, logos, and brand names are the property of their respective owners.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology.....	4
Lab Settings.....	5
1 Accessing Alien Vault OSSIM and Configuring Networks .....	6
2 HIDS Event Monitoring and Reporting .....	19
2.1 Create a Custom Dashboard View Showing HIDS Events .....	19
2.2 Deploy HIDS Agents on Networked Hosts .....	23
2.2.1 Deploy HIDS on a Windows Host .....	23
2.2.1 Deploys HIDS on a Linux Host .....	29
2.3 Generate HIDS Events .....	34
2.4 HIDS Application Events.....	52
2.4.1 Setup AppLocker on Windows Host .....	53
2.4.2 Collect AppLocker Events and Trigger Alarms .....	73
2.5 Compile and Generate HIDS Reports .....	85

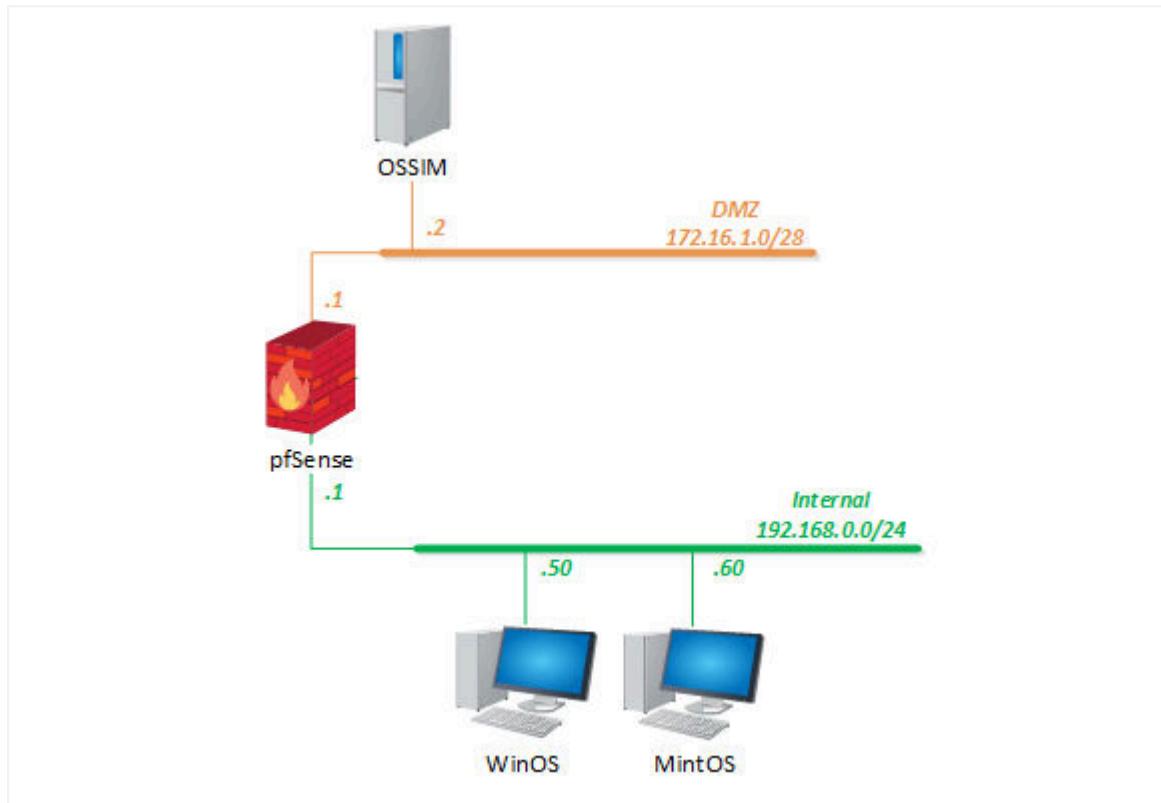
## Introduction

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.

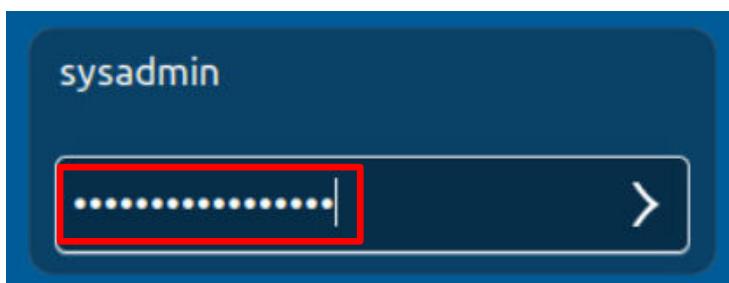
Before beginning the lab, make sure that the *OSSIM* appliance has completed booting up.

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

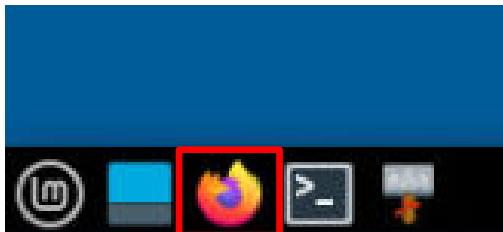
```
=====
===== https://cybersecurity.att.com/ =====
===== Access the AlienVault web interface using the following URL: =====
===== https://172.16.1.2/ =====
=====

AlienVault USM 5.8.11 - x86_64 - tty1
OSSIM login:
```

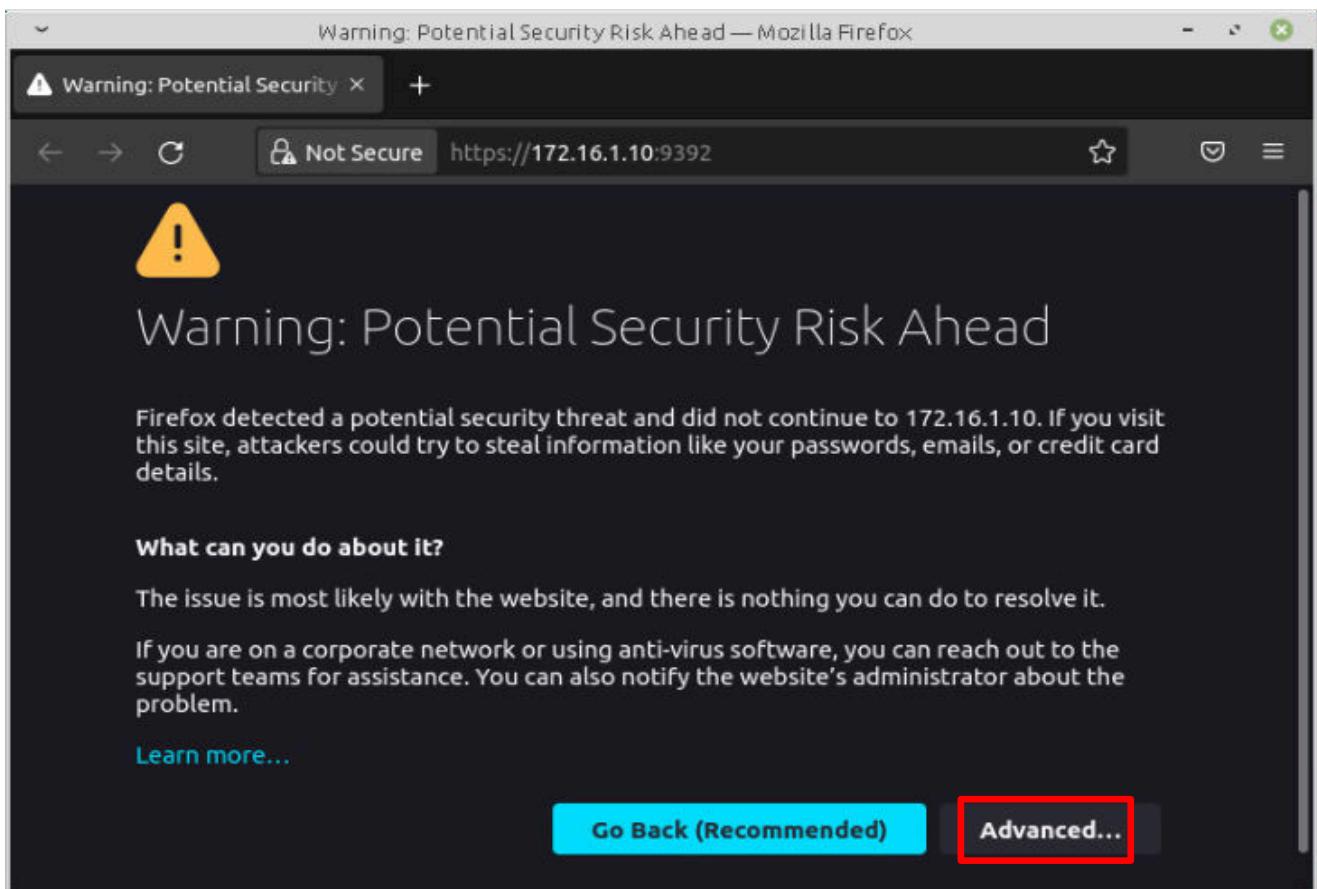
3. Set the focus on the **MintOS** computer.
4. Log in to the *sysadmin* account using the password: NDGLabpass123!



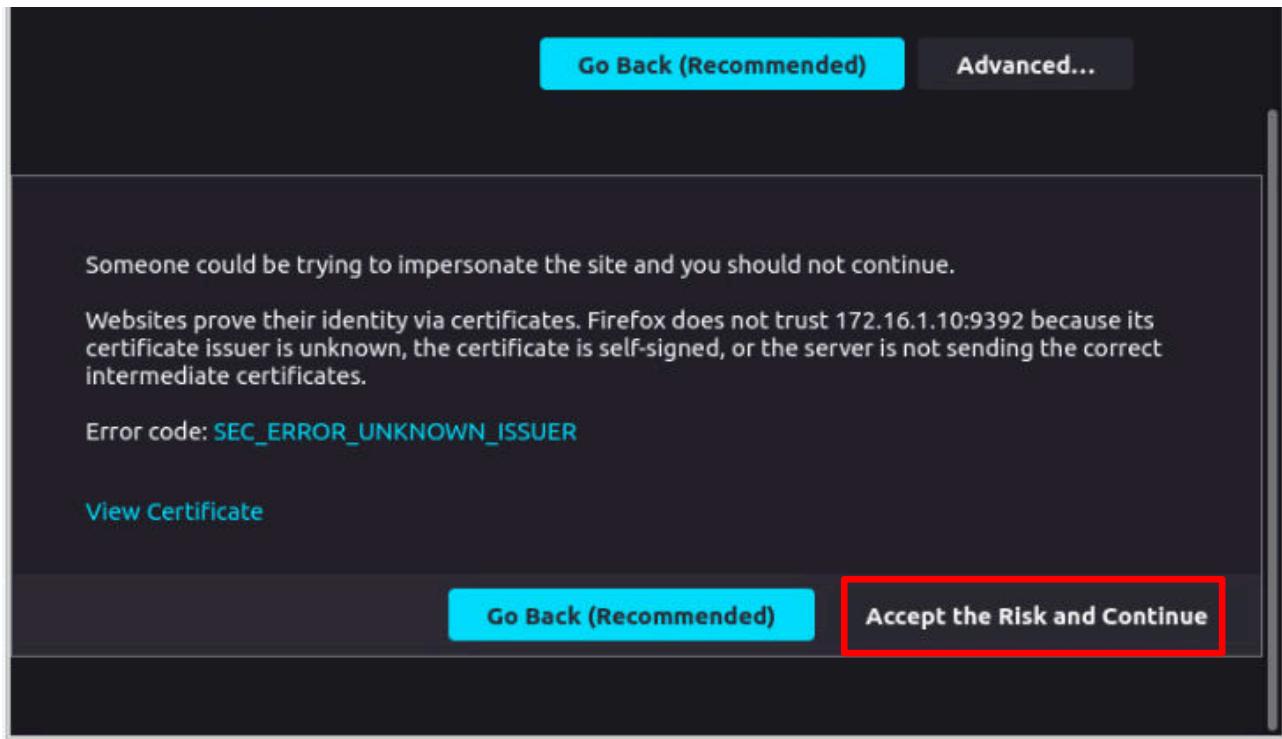
5. Open the browser by clicking on the **Firefox** icon in the toolbar at the bottom of the window.



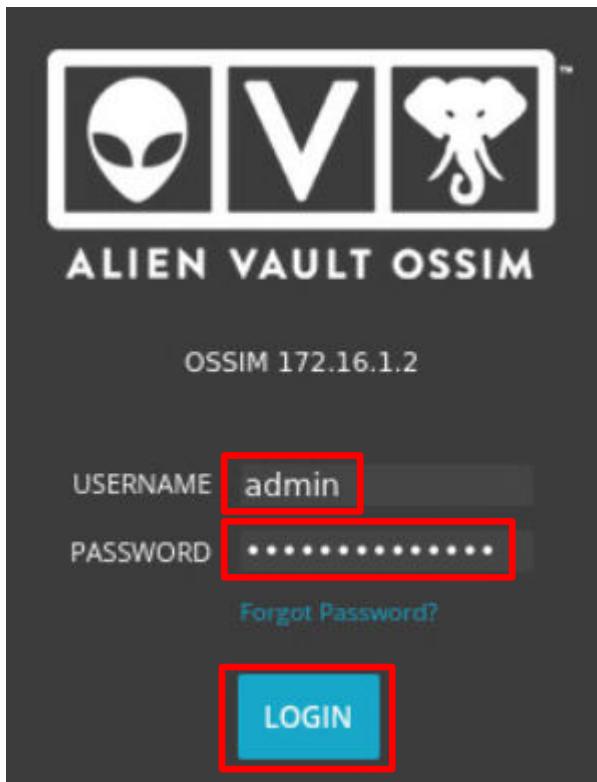
6. In the address bar of the browser, type the IP address of the *AlienVault OSSIM* appliance, <https://172.16.1.2>.
7. On the *Warning: Potential Security Risk Ahead*, click on the **Advanced** button.



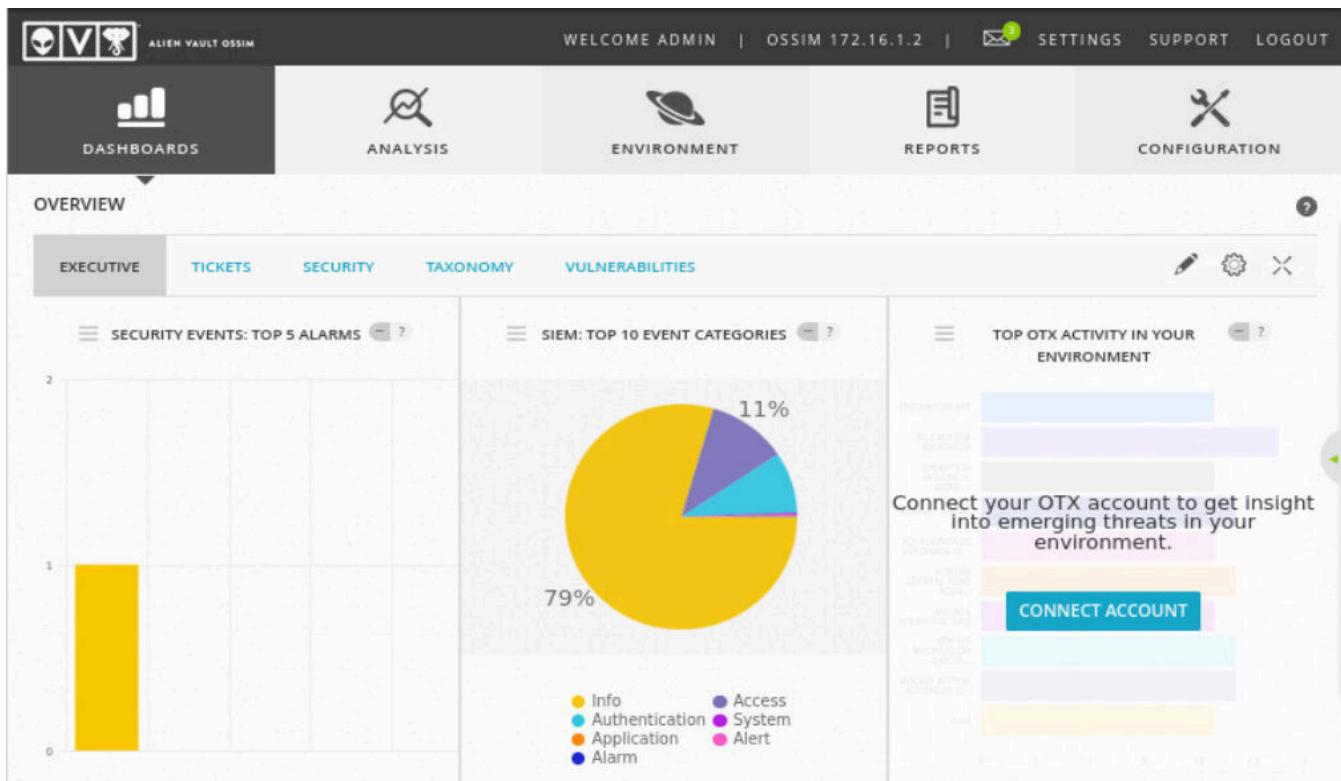
8. Scroll to the bottom of the window and click the **Accept the Risk and Continue** button.



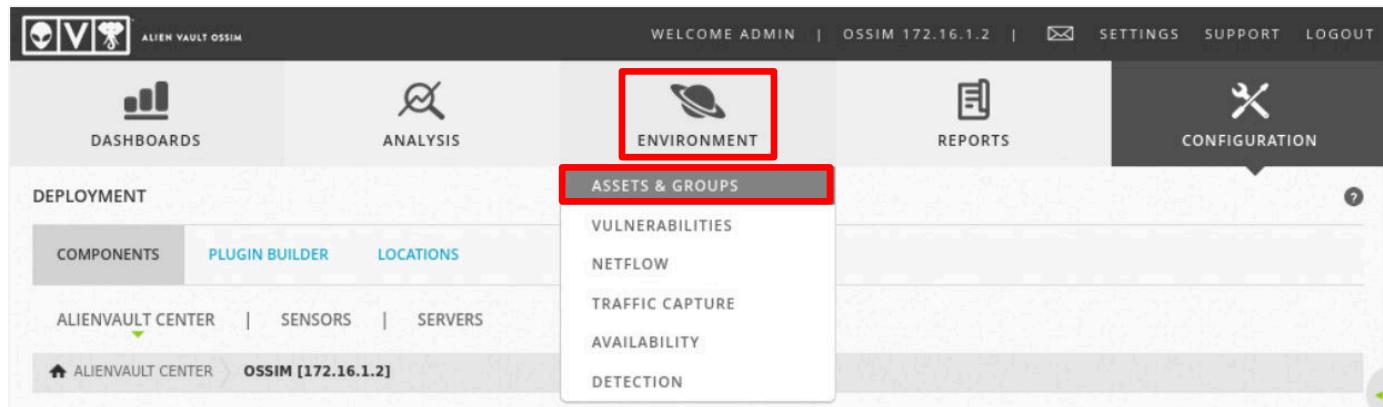
9. Log in as admin using the password NDGLabpass123! and click the **LOGIN** button.



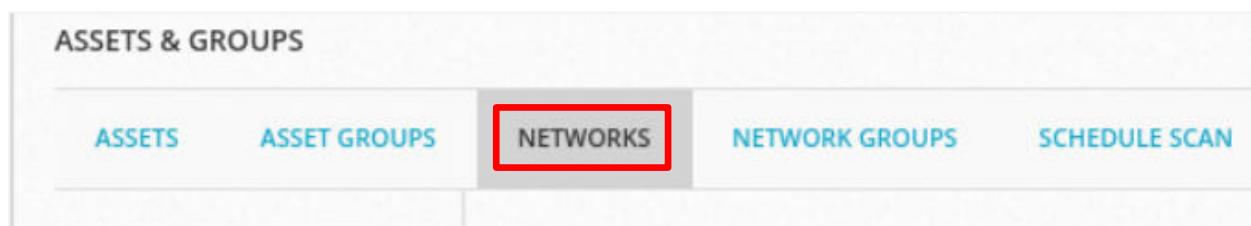
10. You will see the *OSSIM Dashboard*. The *Dashboard* displays a collection of graphs and charts that provides a high-level overview of network activity related to security events and issues.



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**.

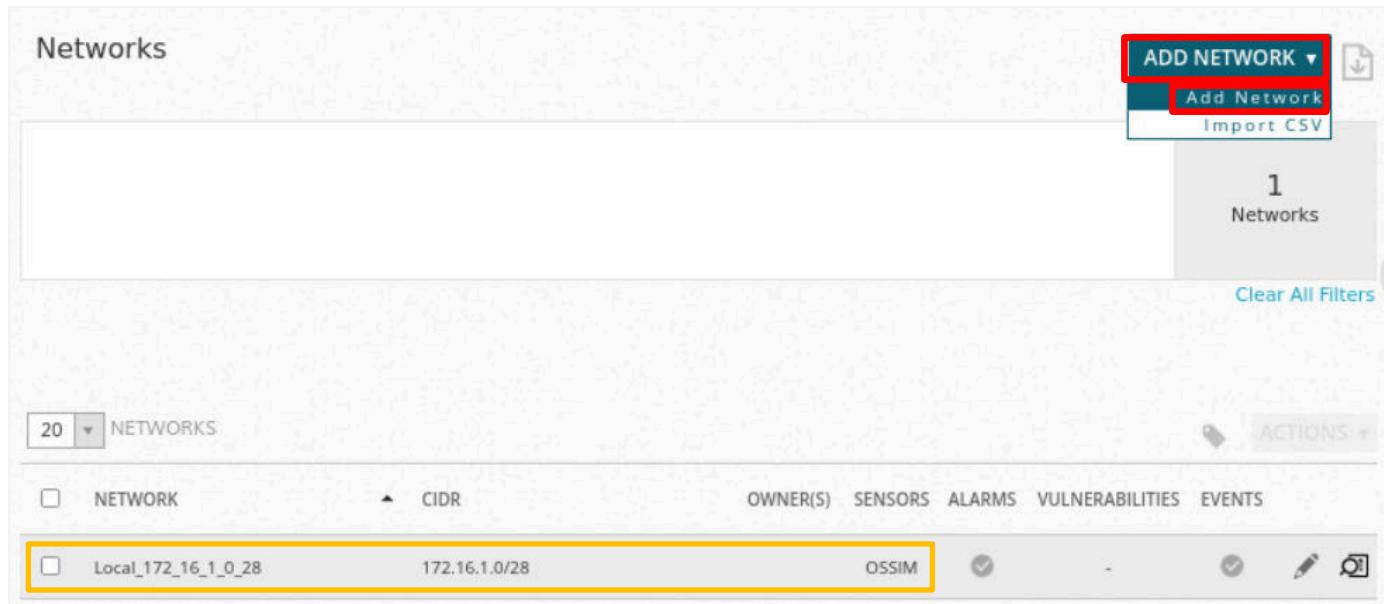


12. On the **ASSETS & GROUPS** page, click on **NETWORKS**.



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**.



The screenshot shows the 'Networks' section of the AlienVault OSSIM interface. At the top right, there is a 'ADD NETWORK' dropdown menu with 'Add Network' selected. Below the header, a message indicates '1 Networks'. A 'Clear All Filters' link is also present. The main table displays a single network entry: 'Local\_172\_16\_1\_0\_28' with CIDR '172.16.1.0/28' and owner 'OSSIM'. The entire row for this network is highlighted with a yellow border. The table has columns for 'NETWORK', 'CIDR', 'OWNER(S)', 'SENSORS', 'ALARMS', 'VULNERABILITIES', and 'EVENTS'. There are also 'ACTIONS' buttons for each row.

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

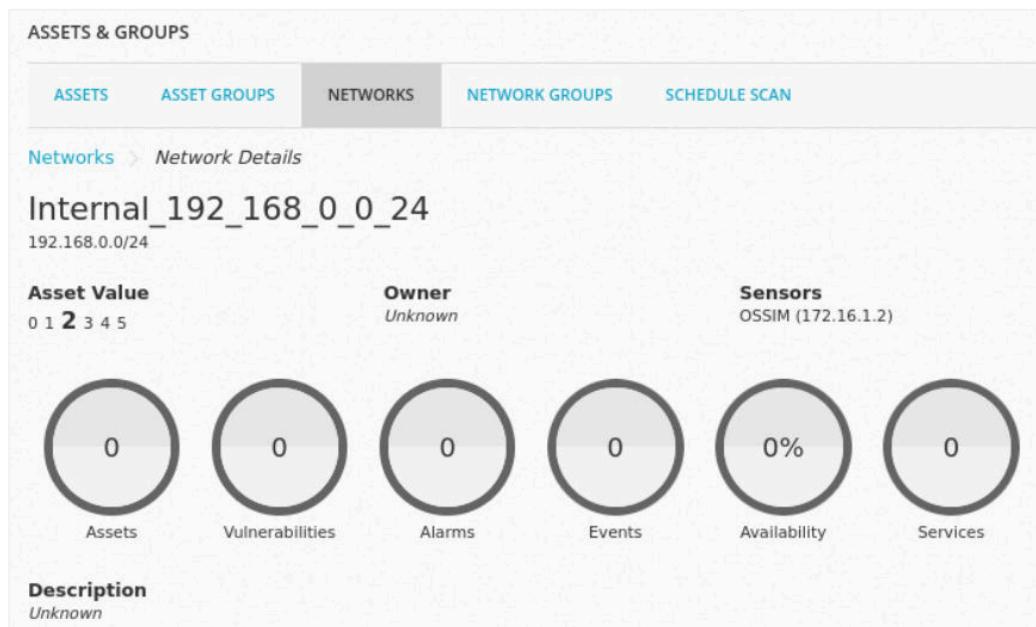
<i>Name</i>	Internal_192_168_0_0_24 (the name of the network (Internal) followed by the network IP address and the subnet)
<i>CIDR</i>	192.168.0.0/24 (the CIDR is the IP network address and subnet using CIDR notation)

**New Network**

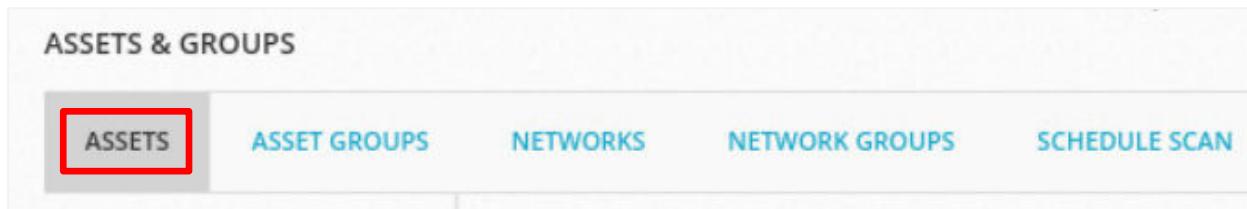
Values marked with (\*) are mandatory

<b>Name *</b>	<input type="text" value="Internal_192_168_0_0_24"/>	<b>Icon</b> Allowed format: Up to 400x400 PNG, JPG or GIF image <input type="checkbox"/> Choose icon ...
<b>CIDR *</b>	<input type="text" value="192.168.0.0/24"/>	<b>Description</b> <input type="text"/>
<b>Owner</b>	<input type="text"/>	
<b>Sensors *</b>	<input checked="" type="checkbox"/> 172.16.1.2 (OSSIM)	
<b>Asset Value *</b>	<input type="text" value="2"/>	<b>External Asset *</b> <input type="radio"/> Yes <input checked="" type="radio"/> No
<b>CANCEL</b> <b>SAVE</b>		

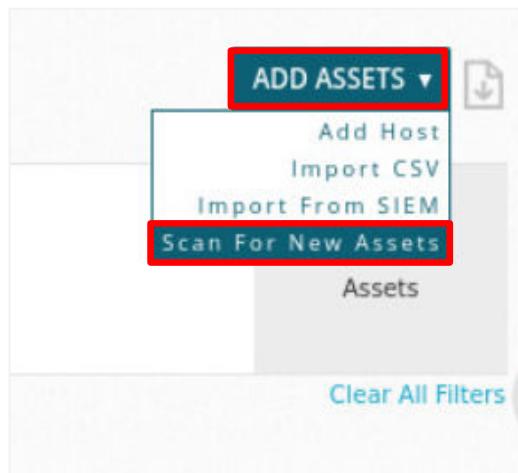
You will see the new network has been added.



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

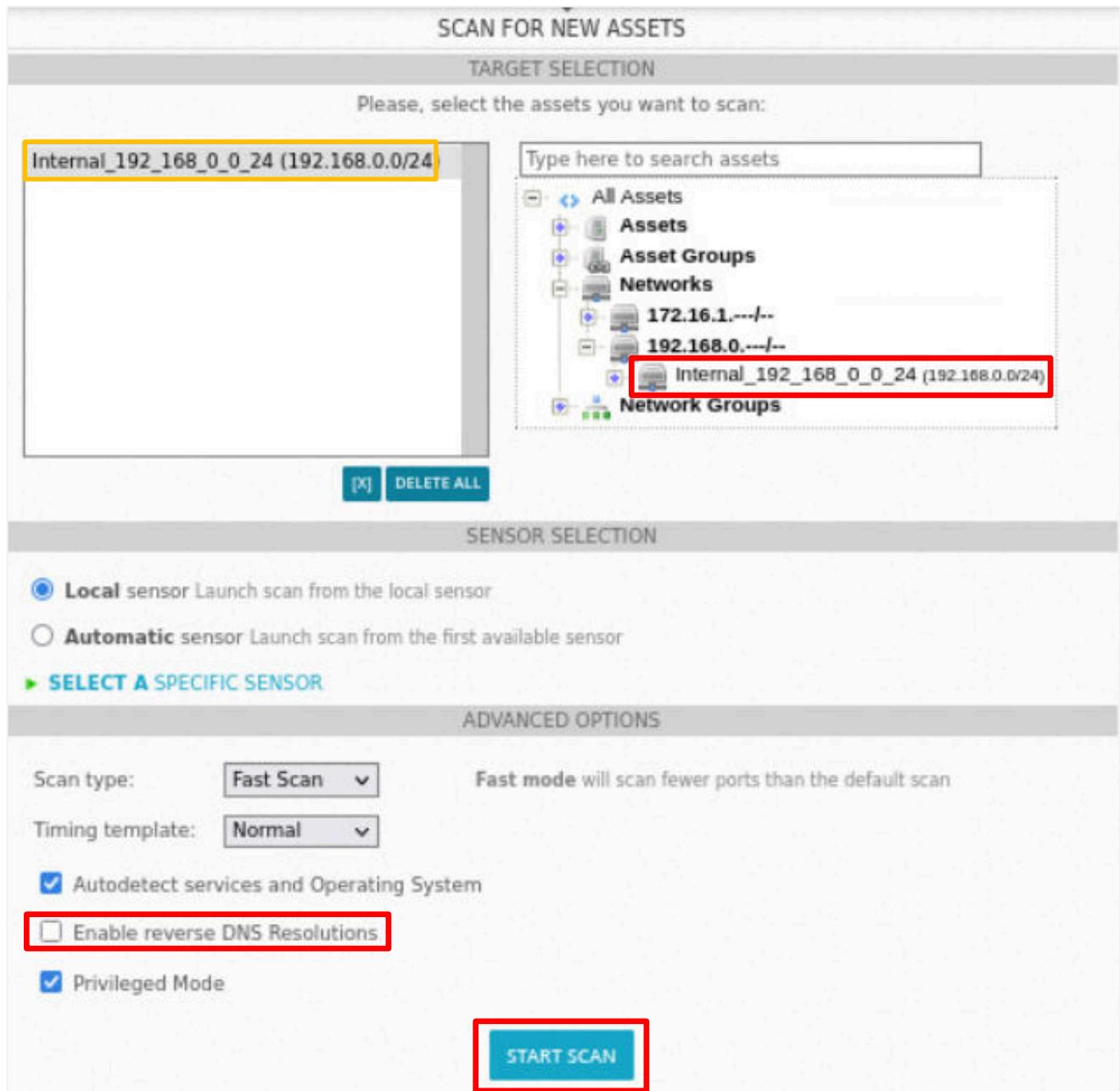


16. On the right side of the window, click on the **ADD ASSETS** list button and click on **Scan for New Assets**.



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

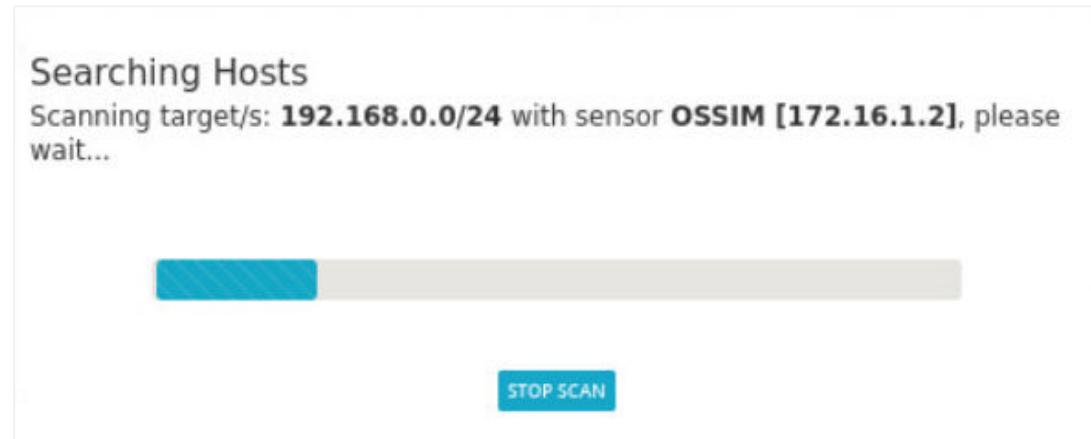
- On the right, expand **All Assets** → **Networks** → **192.168.0.---/--**
- Click on **Internal\_192\_168\_0\_0\_24 (192.168.0.0/24)**.
- You will see the network added to the list on the left.
- Under the **ADVANCED OPTIONS**, uncheck **Enable reverse DNS Resolution**.
- Click on **START SCAN**.



The screenshot shows the 'SCAN FOR NEW ASSETS' configuration interface. It is divided into several sections:

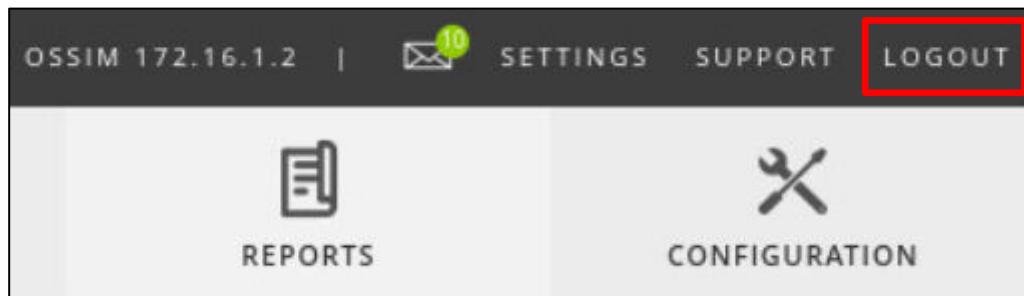
- TARGET SELECTION:** A list of assets to be scanned. The item "Internal\_192\_168\_0\_0\_24 (192.168.0.0/24)" is highlighted with a yellow border. To its right is a search bar and a tree view of asset categories. The category "Networks" is expanded, showing "192.168.0.---/--" and "Internal\_192\_168\_0\_0\_24 (192.168.0.0/24)", which is also highlighted with a red border.
- SENSOR SELECTION:** Options for launching the scan. The "Local sensor" radio button is selected. Below it are two other options: "Automatic sensor" and "SELECT A SPECIFIC SENSOR".
- ADVANCED OPTIONS:** Settings for the scan type and timing. "Scan type" is set to "Fast Scan" (selected from a dropdown) and "Timing template" is set to "Normal" (selected from a dropdown). Other options include "Autodetect services and Operating System" (checked), "Enable reverse DNS Resolutions" (unchecked and highlighted with a red border), and "Privileged Mode" (checked).
- Buttons:** At the bottom are two main buttons: "DELETE ALL" and "START SCAN". The "START SCAN" button is highlighted with a red border.

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

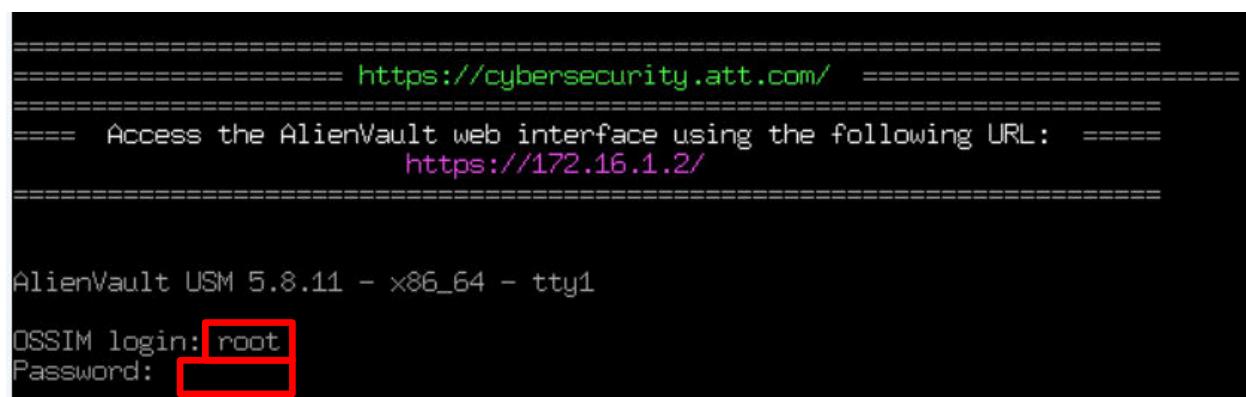


Ignore the estimated time shown at the bottom of the window. It should take less than 5 minutes to perform the scan.

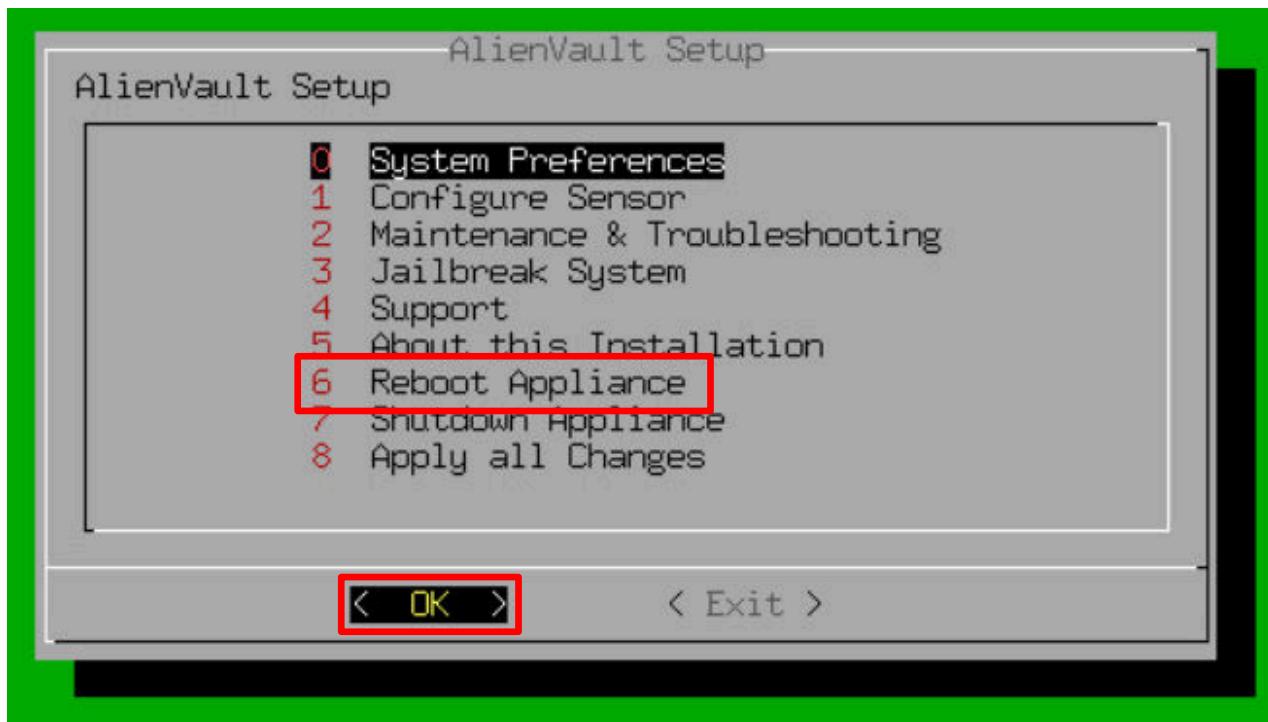
18. On the top-right side of the *AlienVault OSSIM* Web UI, click on **LOGOUT**.



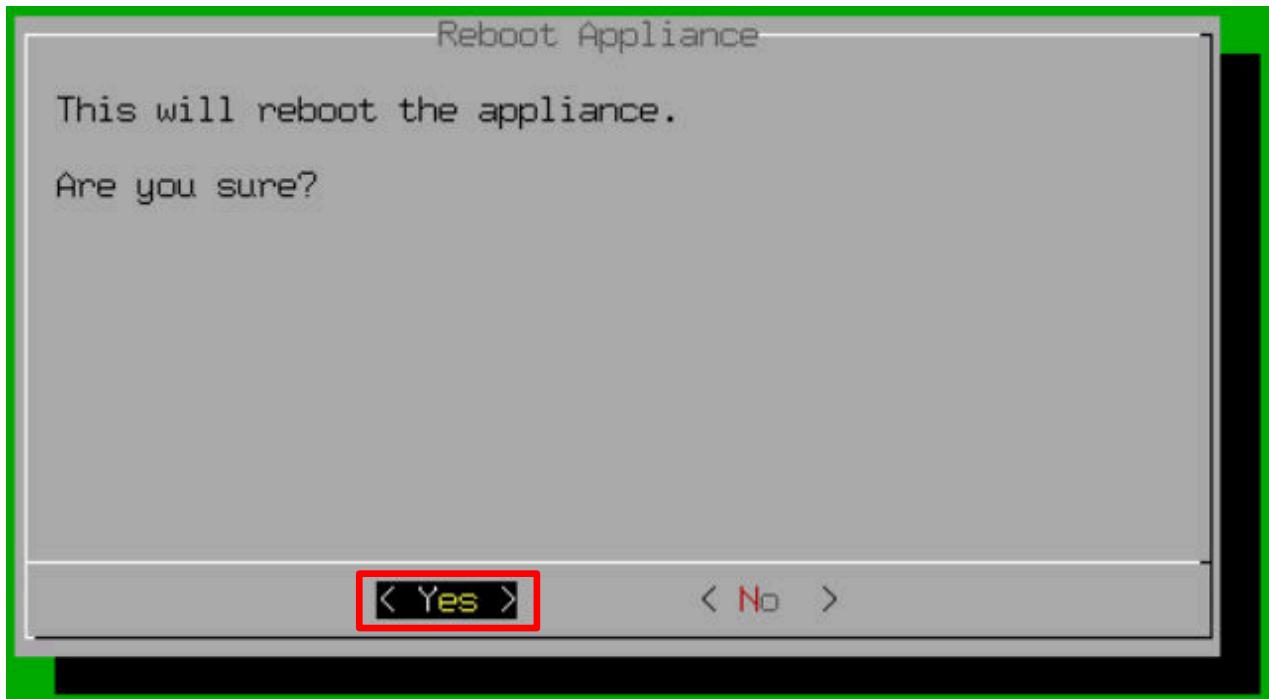
19. Close the web browser.
20. Change the focus to **OSSIM** computer.
21. Log in as **root** using **NDGlabpass!** for the password.



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**.

The screenshot shows the AlienVault OSSIM dashboard. At the top, there are links for 'WELCOME ADMIN' and 'OSSIM 172.16.1.2'. Below the navigation bar are four main tabs: 'DASHBOARDS', 'ANALYSIS', 'ENVIRONMENT' (which is highlighted with a red box), and 'REPORTS'. A dropdown menu for 'ENVIRONMENT' is open, showing options like 'ASSETS & GROUPS' (also highlighted with a red box), 'VULNERABILITIES', 'NETFLOW', 'TRAFFIC CAPTURE', 'AVAILABILITY', and 'DETECTION'. Below the tabs, there's a section for 'DEPLOYMENT' with 'COMPONENTS' selected, followed by 'PLUGIN BUILDER' and 'LOCATIONS'. At the bottom, there are links for 'ALIENVAULT CENTER', 'SENSORS', and 'SERVERS', along with a breadcrumb trail: 'ALIENVAULT CENTER / OSSIM [172.16.1.2]'. A question mark icon is in the top right corner.

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

<input type="checkbox"/>	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS	
<input type="checkbox"/>	OSSIM	172.16.1.2	General Purpose	AlienVault OS	2	No	Connected	
<input type="checkbox"/>	Host-192-168-0-60	192.168.0.60			2	No	Not Deployed	
<input type="checkbox"/>	Host-192-168-0-1	192.168.0.1			2	No	Not Deployed	
<input type="checkbox"/>	Host-172-16-1-10	172.16.1.10			2	No	Not Deployed	
<input type="checkbox"/>	Host-172-16-1-1	172.16.1.1			2	No	Not Deployed	

SHOWING 1 TO 5 OF 5 ASSETS < PREVIOUS | NEXT >

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.

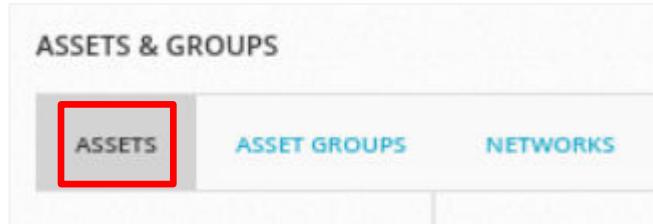
Name	Host-192-168-0-50
IP Address	192.168.0.50
Asset Value	Use the list arrow to select 5
Operating System	<b>Microsoft Windows 2019 Server</b> (select from list)
Device Type	Use the list arrow to select <b>General Purpose</b> and click <b>ADD</b>

New Asset

Values marked with (\*) are mandatory

Name *	Host-192-168-0-50	Icon Allowed format: Up to 400x400 PNG, JPG or GIF image <input type="checkbox"/> Choose icon ...
IP Address *	192.168.0.50	Location
FQDN/Aliases	Maps not available, you need internet connection	
Asset Value *	5	External Asset * <input type="radio"/> Yes <input checked="" type="radio"/> No
Sensors *	<input checked="" type="checkbox"/> 172.16.1.2 (OSSIM)	
Operating System	Latitude/Longitude <input type="text"/> <input type="text"/>	
Microsoft Windows Server 2019	Model <input type="text"/>	
Description	Devices Types <div style="display: flex; align-items: center;"> <div style="flex: 1;"> <input style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;" type="button" value="General Purpos"/> <span style="font-size: small;">... Types ...</span> </div> <div style="flex: 1; text-align: right;"> <input style="border: 1px solid #0070C0; background-color: #0070C0; color: white; padding: 2px 5px;" type="button" value="ADD"/> </div> </div>	
<input style="border: 1px solid #0070C0; background-color: #0070C0; color: white; padding: 5px;" type="button" value="SAVE"/>		

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



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

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

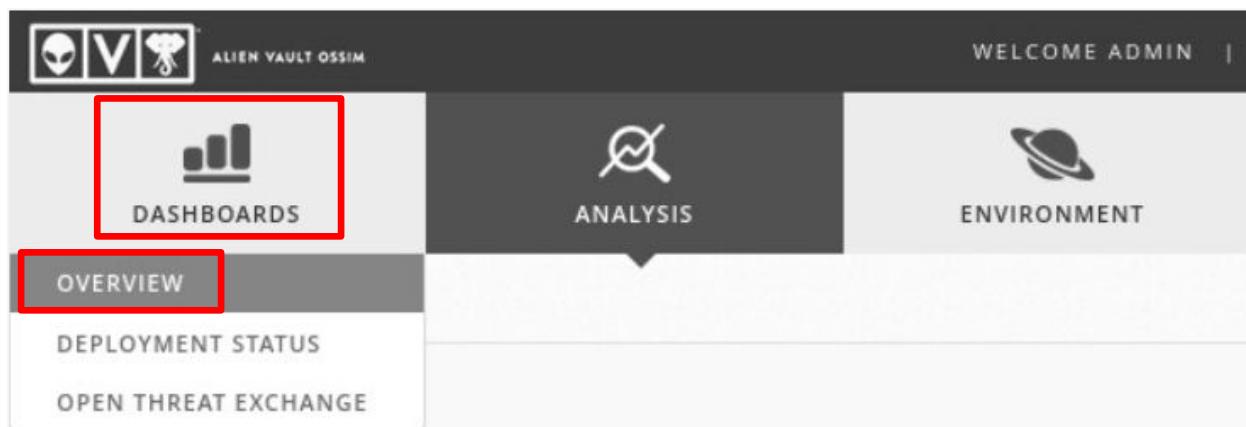
In *Lab 20: Network Intrusion Detection with OSSIM*, you configured and used the *NIDS* built into *AlienVault OSSIM*, which uses sensors on the network to monitor the assets on the network by detecting and analyzing inbound and outbound packets in real-time.

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

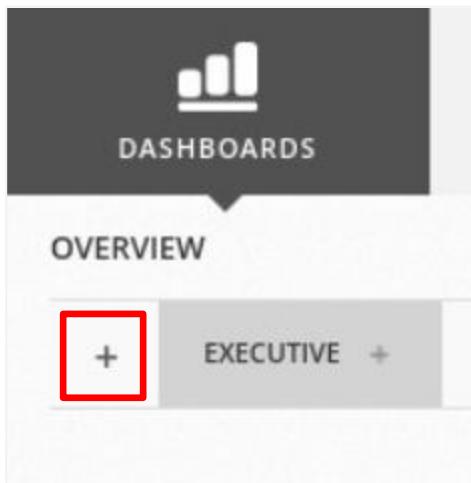
1. On the top-level menu, hover over **DASHBOARDS** and then click on **Overview**.



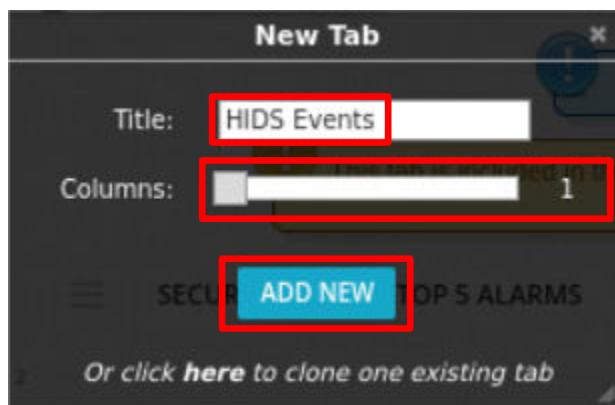
2. On the right side of the page, click on the **Switch to Edit Mode** icon (the pencil).



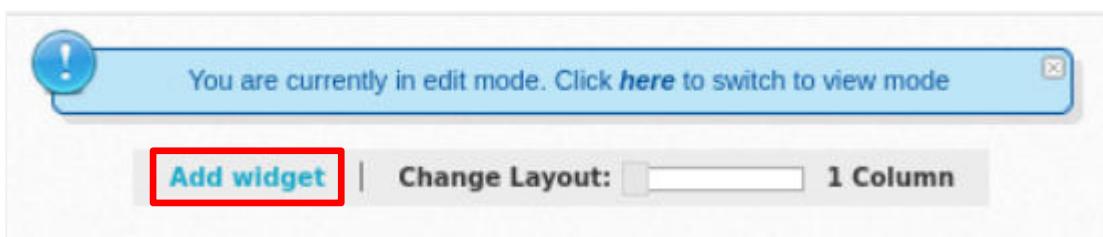
3. You will be in the **Edit Mode** for the *Dashboard*. On the left side of the tab list, click on the **+** icon on the left side of the *Tab* list.



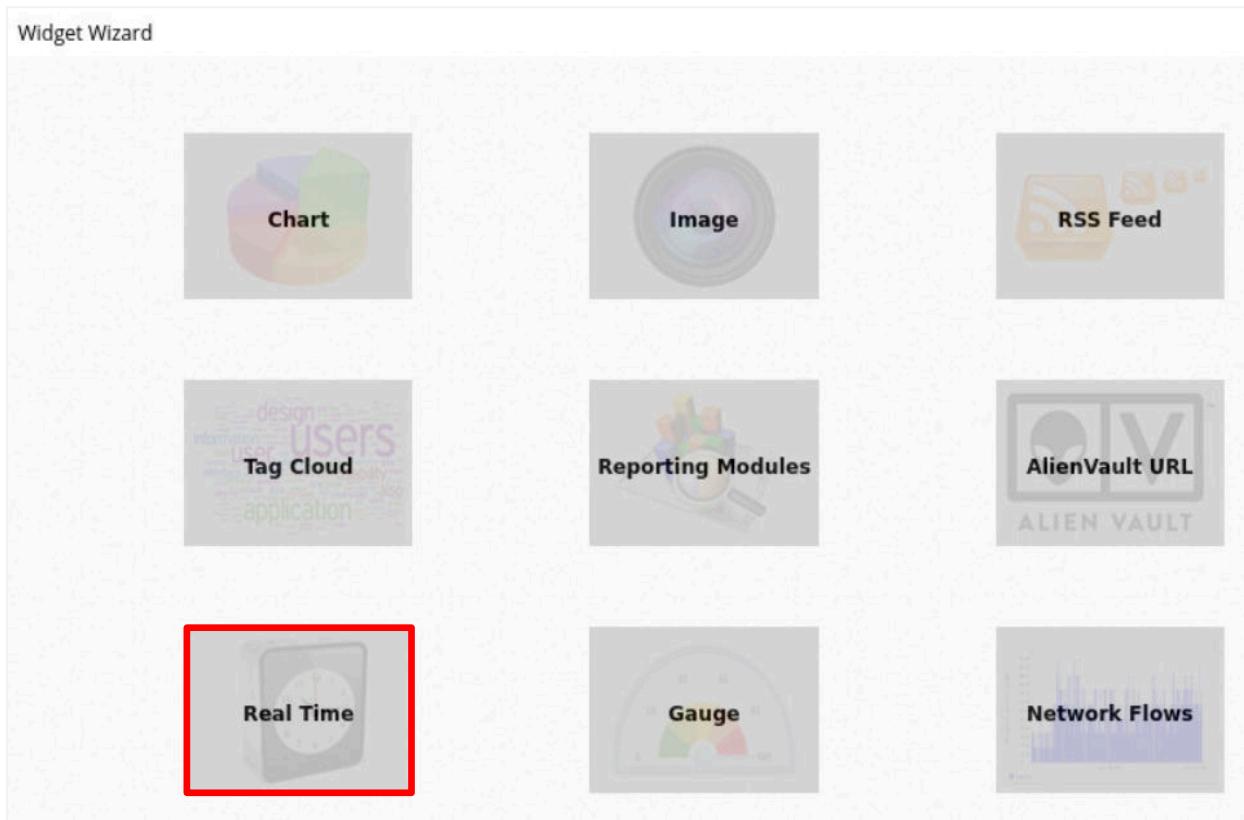
4. In the *New Tab* window, type **HIDS Events** for the *Title* and move the slider to **1** in *Columns*. Then click on the **ADD NEW** button.



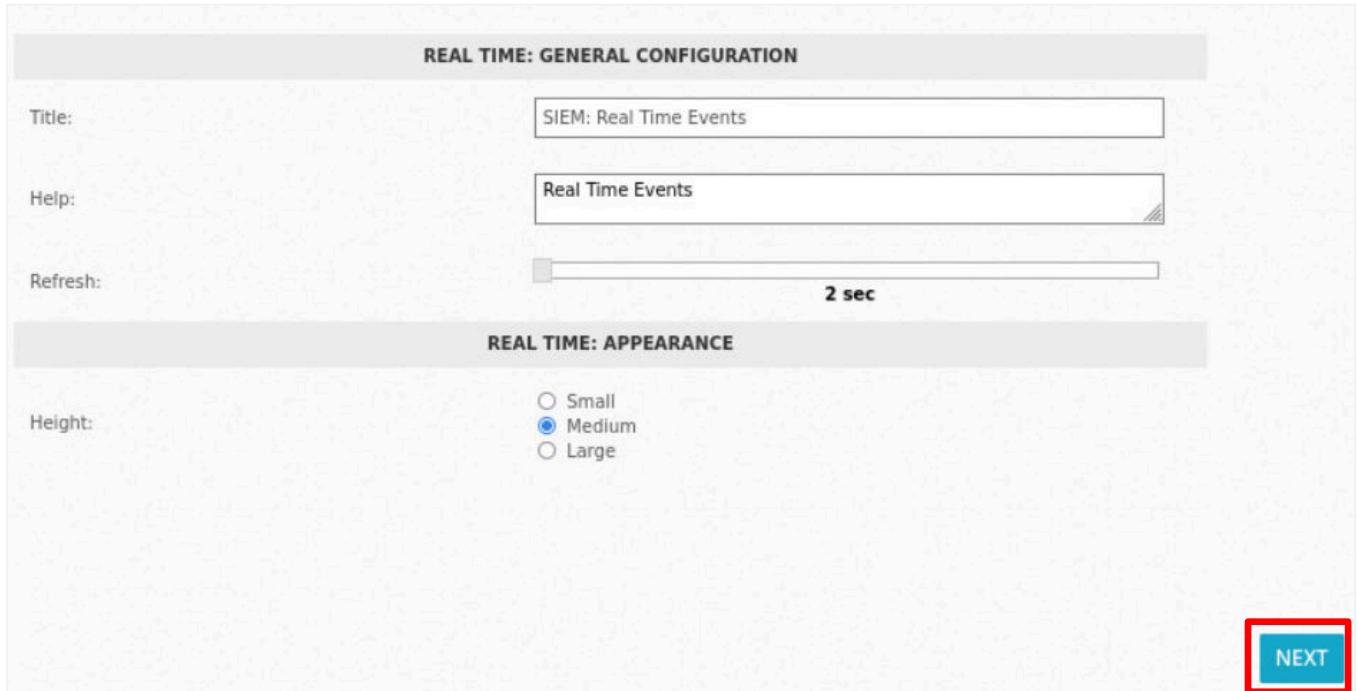
5. Click on the **Add Widget** link.



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**.



**REAL TIME: GENERAL CONFIGURATION**

Title: SIEM: Real Time Events

Help: Real Time Events

Refresh: 2 sec

**REAL TIME: APPEARANCE**

Height:  Medium

**NEXT**

The screenshot shows the 'Customize Widget' configuration page. It has two main sections: 'REAL TIME: GENERAL CONFIGURATION' and 'REAL TIME: APPEARANCE'. In the first section, the title is set to 'SIEM: Real Time Events' and the refresh interval is set to '2 sec'. In the second section, the height is set to 'Medium'. A large red box highlights the 'NEXT' button at the bottom right of the page.

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

**Save Widget**

SIEM: REAL TIME EVENTS

PAUSE Done. [0 new rows]

DATE	EVENT NAME	RISK	SENSOR	OTX	SOURCE IP	DEST IP
2022-06-04 13:46:28	SSHd: Connection closed	0	OSSIM	N/A	0.0.0.0:59632	0.0.0.0:22
2022-06-04 13:45:54	AlienVault HIDS: Login session opened.	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:54	AlienVault HIDS: Login session closed.	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:54	sudo: Session closed	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:54	sudo: Session closed	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:53	sudo: Session opened	0	OSSIM	N/A	0.0.0.0	0.0.0.0

**SAVE WIDGET**

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

OVERVIEW

HIDS EVENTS + EXECUTIVE + TICKETS + SECURITY + TAXONOMY + NETWORK + VULNERABILITIES +

You are currently in edit mode. Click **here** to switch to view mode

Add widget | Change Layout: 1 Column

SIEM: REAL TIME EVENTS

PAUSE Done. [0 new rows]

DATE	EVENT NAME	RISK	SENSOR	OTX	SOURCE IP	DEST IP
2022-06-14 14:09:00	AlienVault HIDS: Login session opened.	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-14 14:09:00	AlienVault HIDS: Login session closed.	0	OSSIM	N/A	0.0.0.0	0.0.0.0

## 2.2 Deploy HIDS Agents on Networked Hosts

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

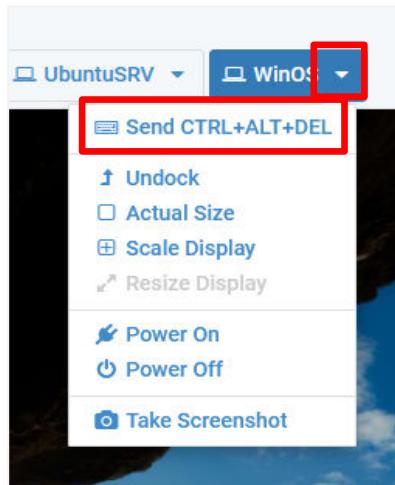
### 2.2.1 Deploy HIDS on a Windows Host

*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.

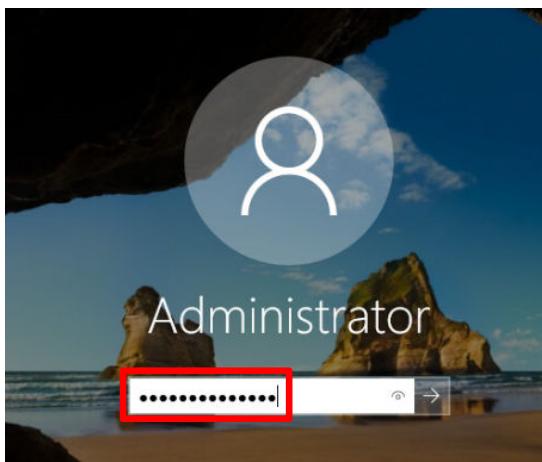


In *Lab 01: Network Enumeration*, a custom firewall rule was created using the wizard on the *Windows Defender Firewall*. In this lab, the custom rule will be created using *Windows PowerShell* command line

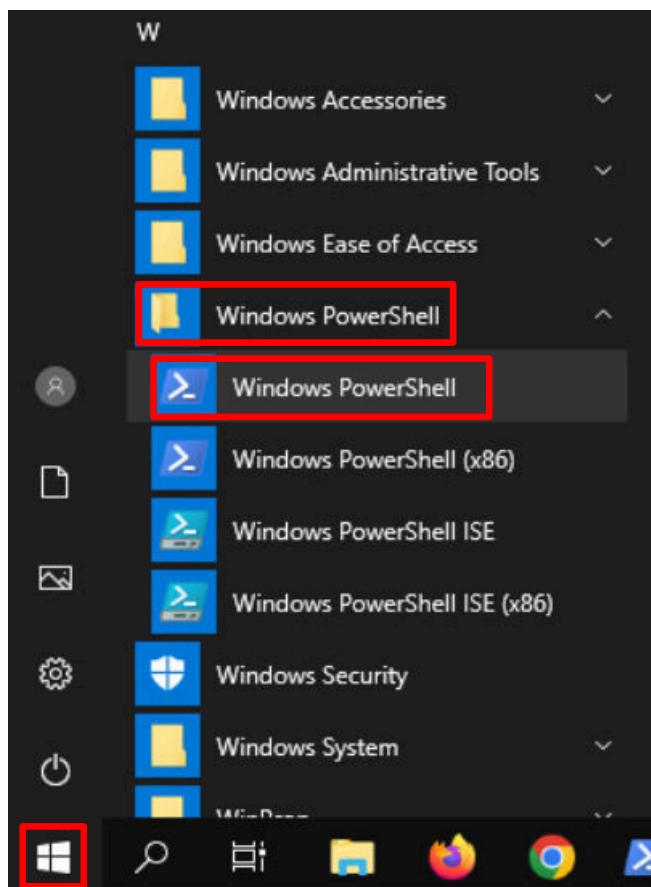
1. Set the focus to the **WinOS** computer.
2. Bring up the login window by sending a Ctrl + Alt + Delete. To do this, click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



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**.



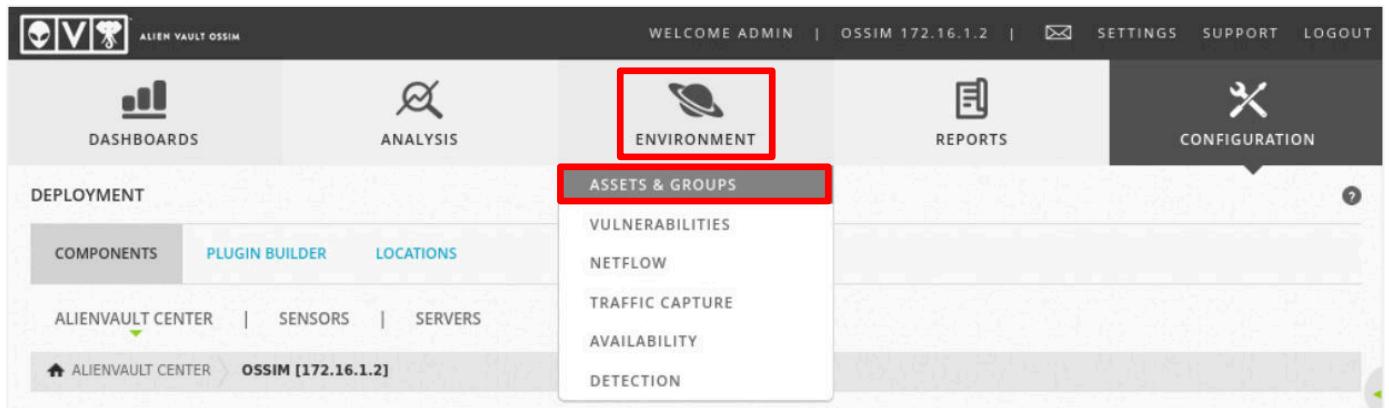
5. Type the following command to create a rule to allow access from the *OSSIM* appliance at **172.16.1.2**:

```
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*.

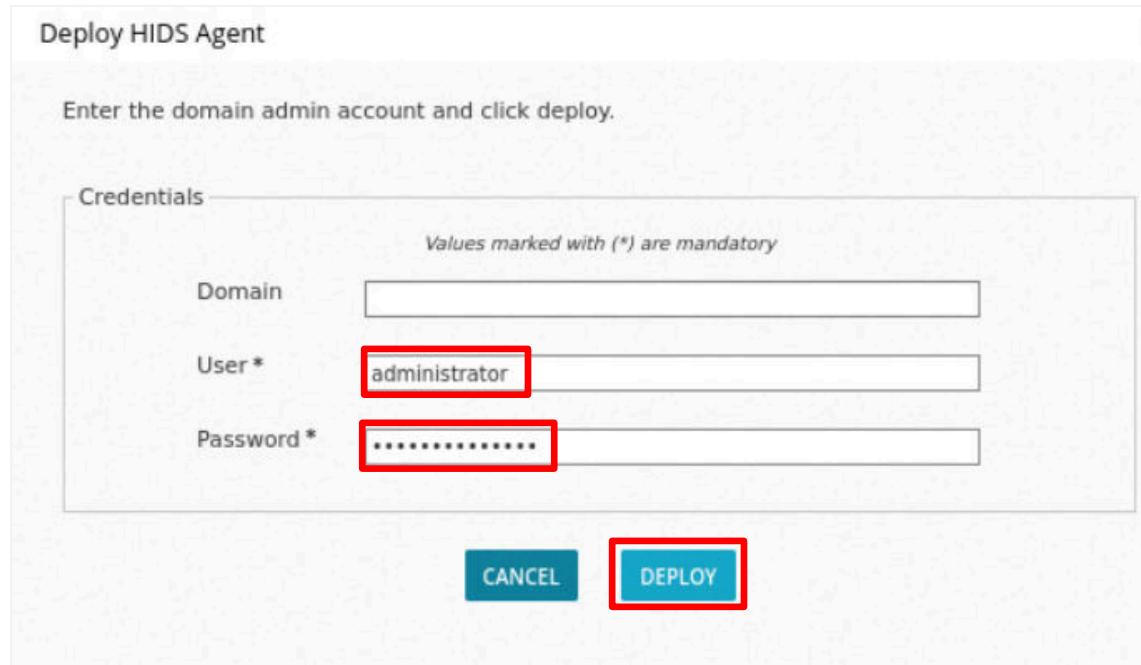
Host-192-168-0-50	192.168.0.50	Microsoft Server 2019	2	No	Not Deployed	
-------------------	--------------	-----------------------	---	----	--------------	---

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!



Deploy HIDS Agent

Enter the domain admin account and click deploy.

Credentials

Values marked with (\*) are mandatory

Domain:

User \*:

Password \*:

**CANCEL** **DEPLOY**

You will see the HIDS agent being deployed.

### Deploy HIDS Agent

Enter the domain admin account and click deploy.

Credentials

Values marked with (\*) are mandatory

Domain	 Deploying HIDS agent ...
User *	
Password *	*****

**CANCEL** **DEPLOY**

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

### Host-192-168-0-50

192.168.0.50  
Microsoft Server 2019

ASSET LOCATION

! Maps not available, you need Internet connection

<b>Asset Value</b> 0 1 <b>2</b> 3 4 5	<b>Device Type</b> Unknown	<b>Networks</b> Internal 192.168.0.0/24 (192...)	<b>Sensors</b> OSSIM (172.16.1.2)
<b>Model</b> Unknown			
<b>Asset Type</b> Internal			

**ENVIRONMENT STATUS**

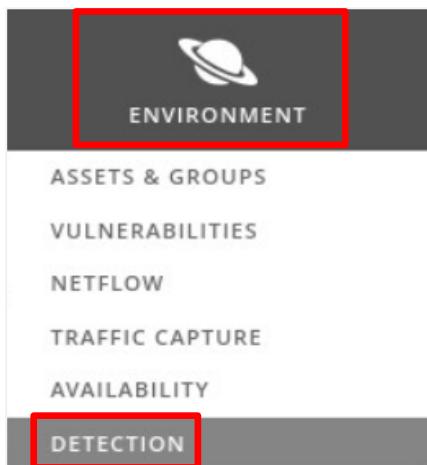
- HIDS** (Green circle)
- Automatic Asset Discovery (Red circle)
- Vuln Scan Scheduled (Red circle)

Vulnerabilities: 0 Alarms: 0 Events: 0 Availability: N/A Services: 0 Groups: 0 Notes: 0

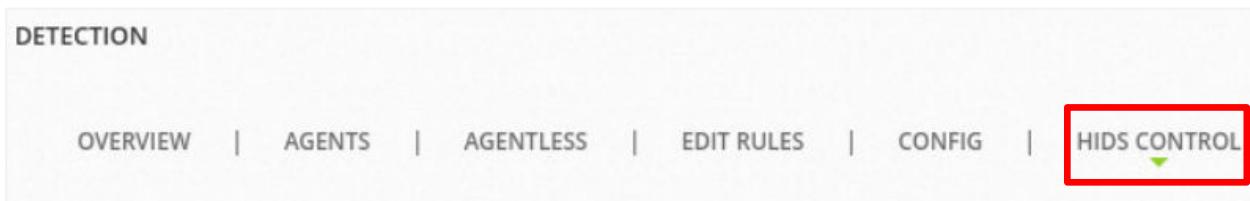
Description: Unknown

See Network Activity

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



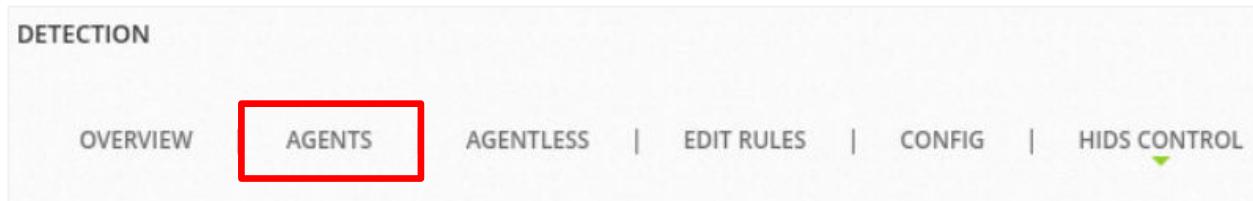
13. On the **DETECTION** page, click on **HIDS CONTROL**.



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**.

Host-192-168-0-50	192.168.0.50	192.168.0.50	-	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.

The screenshot shows the OSSIM interface with the 'AGENTS' tab selected. Under 'AGENT CONTROL', the 'ADD AGENT' button is highlighted with a red box. Other tabs like 'SYSCHECKS' and 'AGENT.CONF' are also visible.

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 screenshot shows the 'New HIDS Agent' configuration window. The 'Assets' tree on the left shows '192.168.0.60' selected. The 'IP/CDR' field at the bottom contains '192.168.0.60'. The 'SAVE' button at the bottom is highlighted with a red box.

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

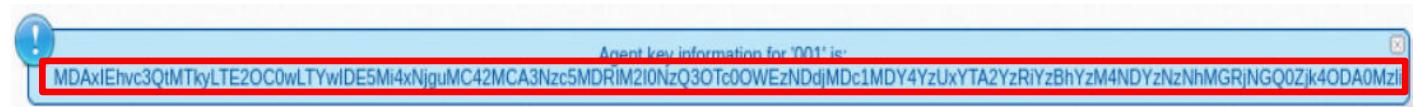
Search		AGENT INFORMATION					ADD AGENT								
ID	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS									
000	OSSIM	127.0.0.1	127.0.0.1	-	Active/local										
001	Host-192-168-0-50	192.168.0.50	192.168.0.50	-	Active										
002	Host-192-168-0-60	192.168.0.60	-	-	Disconnected										

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

- 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.



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



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



- 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).

```
*****
* 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: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): 
```

Press **Enter**.

```
Paste it here (or '\q' to quit): MDAxIEhvc3QtMTkyLTE2OCowLTYwIDESMi4xNjguMC42MCA
3Nzc5MDRlM2I0NzQ3OTc00wEzNDdjMDclMDY4YzUxYTA2YzRiYzBhYzM4NDYzNzNhMGRjNGQ0Zjk40DA
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 such 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
```

```
sysadmin@mintos:~$ sudo /var/ossec/bin/ossec-control status
ossec-logcollector is running...
ossec-syscheckd is running...
ossec-agentd is running...
ossec-execd is running...
sysadmin@mintos:~$
```

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
```

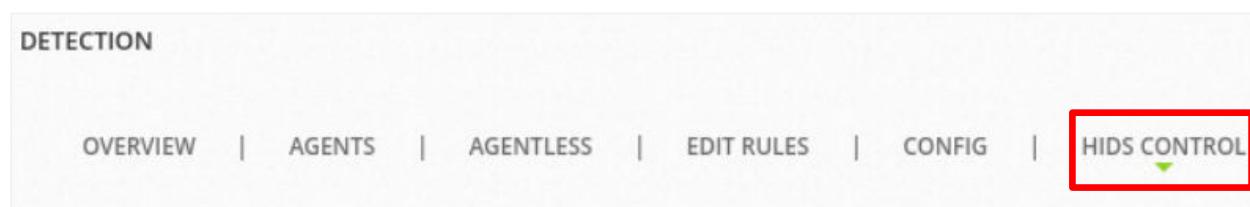
Press the **Spacebar** to advance to the next entries until you see that the *OSSEC HIDS Agent* has connected to the *AlienVault OSSIM* appliance at *172.16.1.2* (it will be near the bottom of the log file).

```
2022/06/12 15:01:48 ERROR: Cannot unlink file /queue/ossec/queue: No such file or directory
2022/06/12 15:01:48 ossec-agentd(1410): INFO: Reading authentication keys file.
2022/06/12 15:01:48 ossec-agentd: INFO: Started (pid: 16675).
2022/06/12 15:01:48 ossec-agentd: INFO: Server 1: 172.16.1.2
2022/06/12 15:01:48 ossec-agentd: INFO: Trying to connect to server 172.16.1.2, port 1514.
2022/06/12 15:01:48 os_dns imsg_init()
2022/06/12 15:01:48 INFO: Connected to 172.16.1.2 at address 172.16.1.2, port 1514
2022/06/12 15:01:48 ossec-agentd: DEBUG: agt->sock: 11
2022/06/12 15:01:49 ossec-agentd(4102): INFO: Connected to server 172.16.1.2, port 1514.
2022/06/12 15:01:52 ossec-syscheckd: INFO: Started (pid: 16684).
2022/06/12 15:01:52 ossec-rootcheck: INFO: Started (pid: 16684).
```

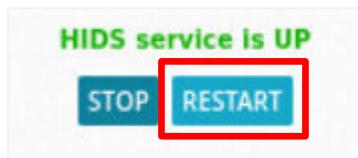
Type **Q** to exit the log listing.

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*.

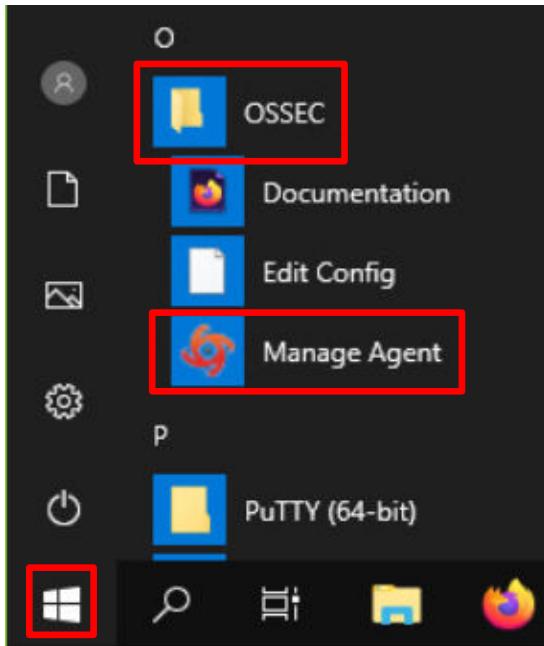
Search		AGENT INFORMATION				
ID	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	
000	OSSIM	127.0.0.1	127.0.0.1	-	Active/local	
001	Host-192-168-0-50	192.168.0.50	192.168.0.50	-	Active	
002	Host-192-168-0-60	192.168.0.60	192.168.0.60	-	Active	

## 2.3 Generate HIDS Events

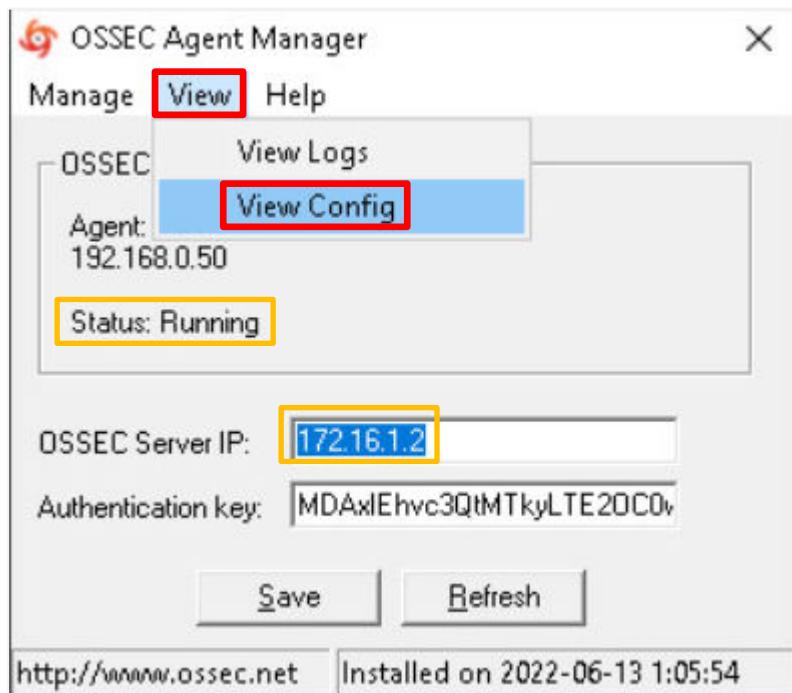
One of the OSSEC HIDS Agent's functions is to perform a System Integrity Check which monitors system files and registry entries. By default, this check is performed in Windows every 20 hours and in Linux every 22 hours. For this task, let's change the Windows timer value to 360 seconds.

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

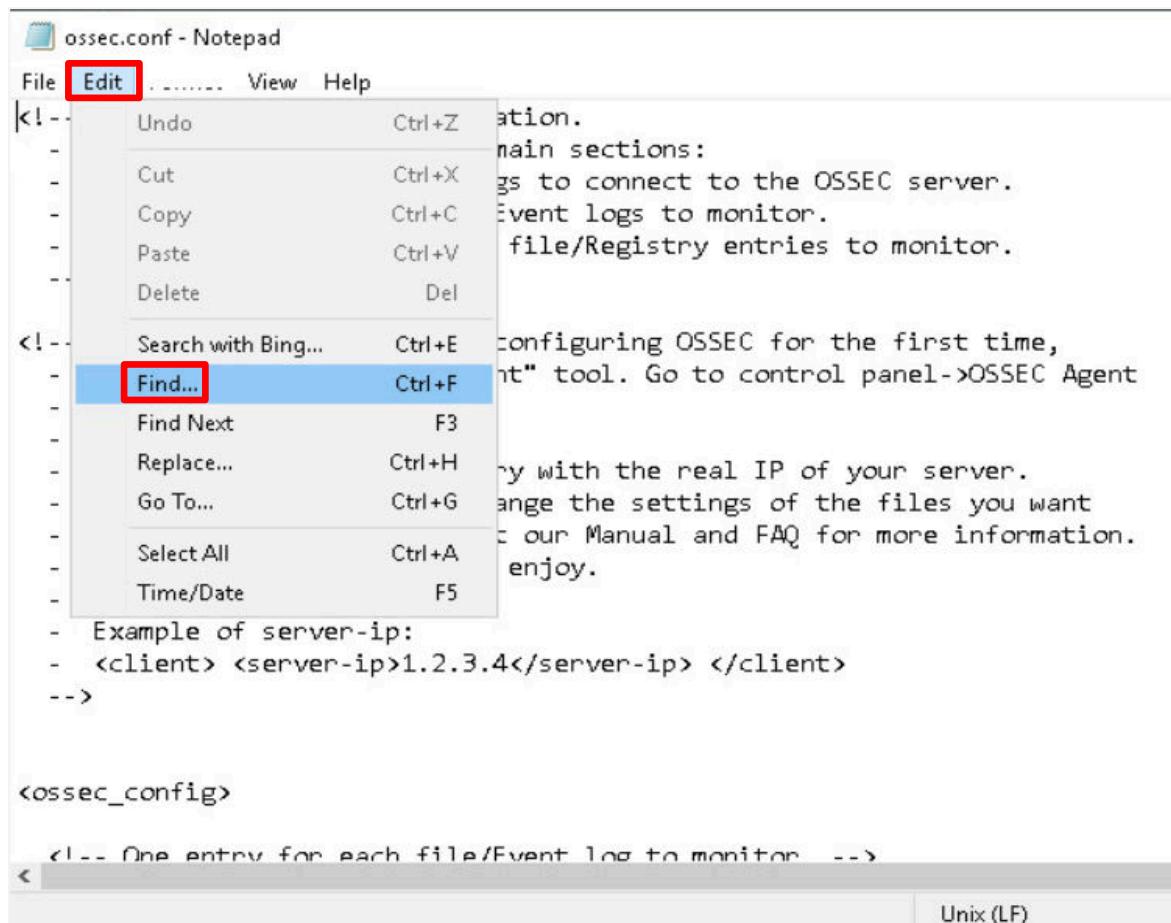
2. Click the **Start** button, open the **OSSEC** program group and click on **Manage Agent**.



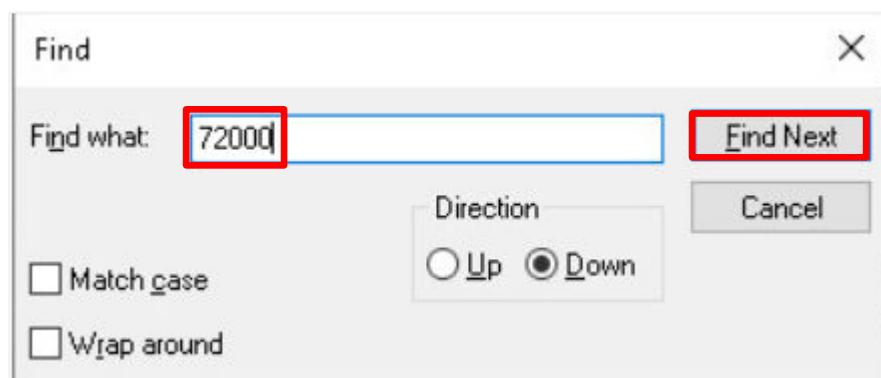
3. Confirm that the status is *Running* and the *OSSEC Server IP* is 172.16.1.2. Click **View** on the menu bar and then click **View Config**.



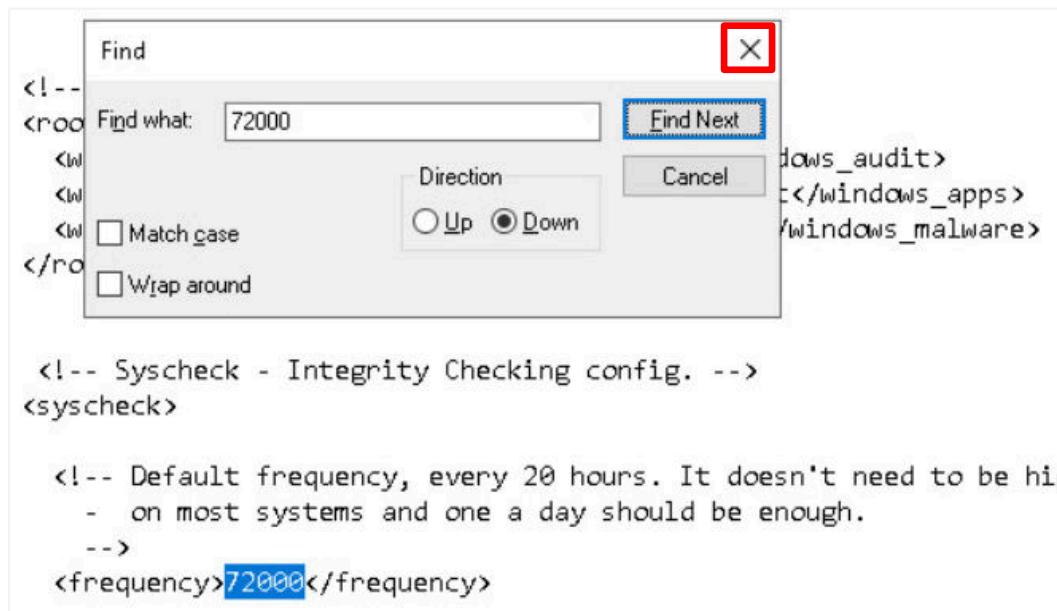
4. On the *Notepad* menu bar, click on **Edit** and then click on **Find**.



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



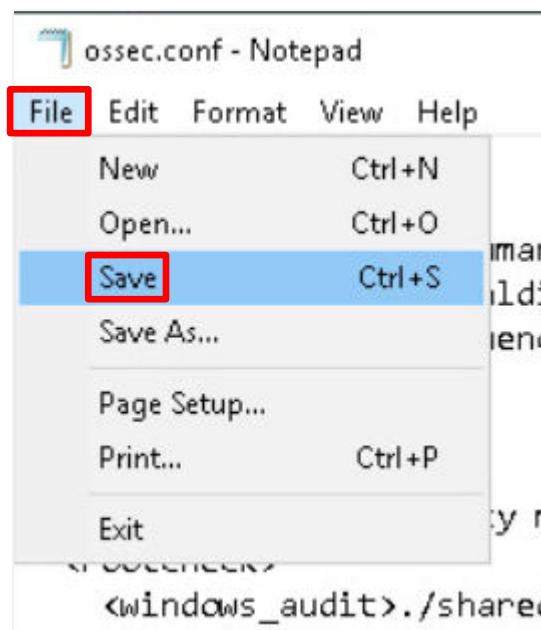
6. After finding the frequency value, close the *Find* box by clicking the X in the upper-right corner.



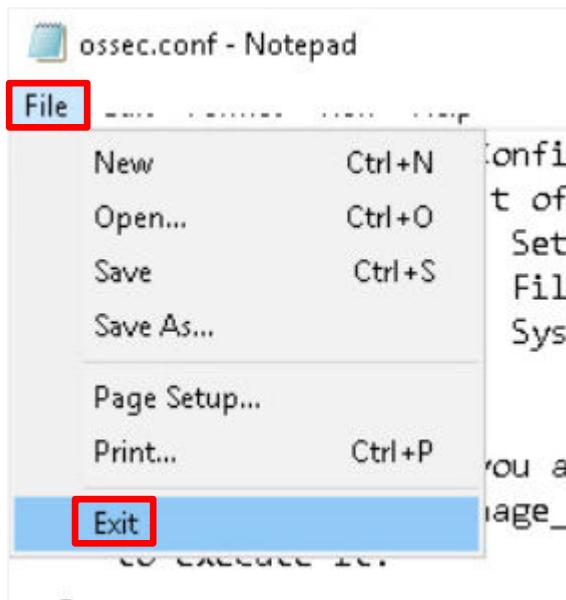
7. Change the frequency value from **72000** (seconds) to **360** (seconds).



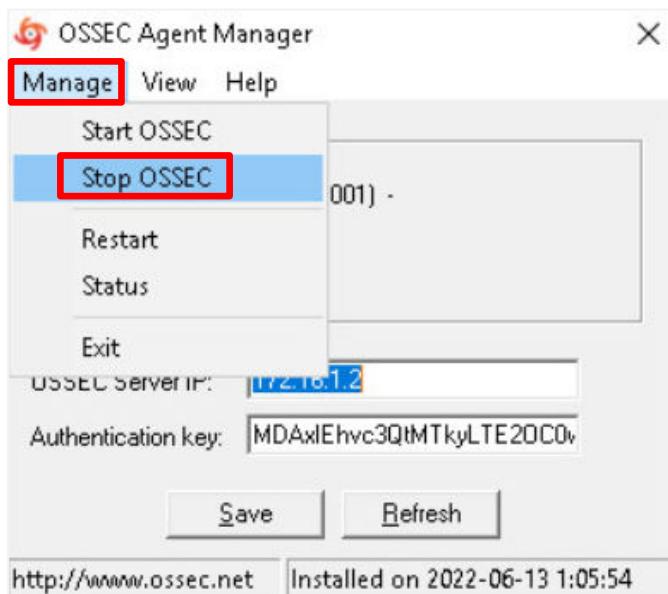
8. On the menu bar, click on **File** and then click on **Save**.



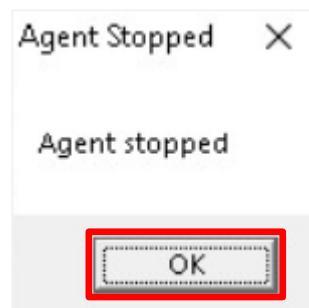
9. Close Notepad by clicking on **File** and then click on **Exit**.



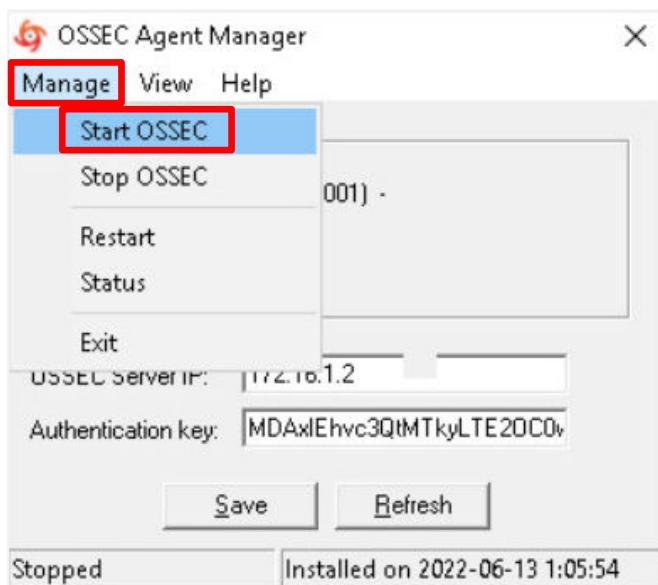
10. On the *OSSEC Agent Manager* window, click on **Manage>Stop OSSEC**.



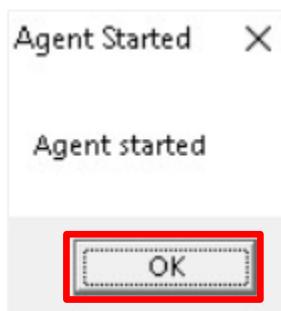
11. On the *Agent Stopped* popup, click **OK**.



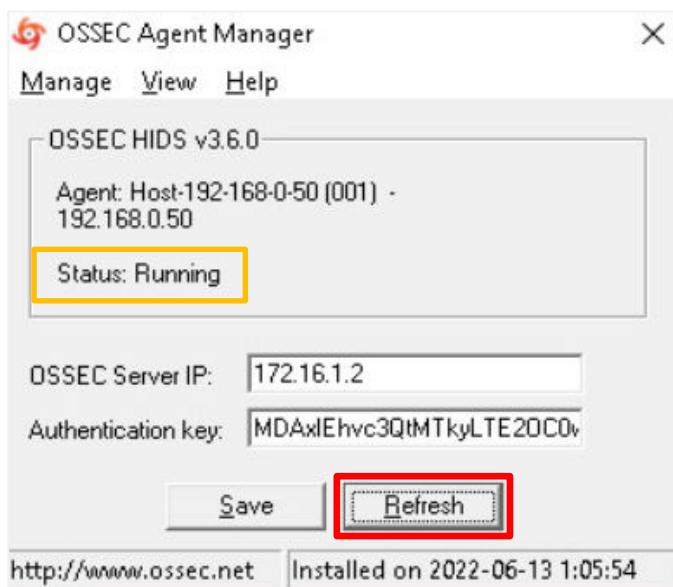
12. On the *OSSEC Agent Manager* window, click on **Manage>Start OSSEC**.



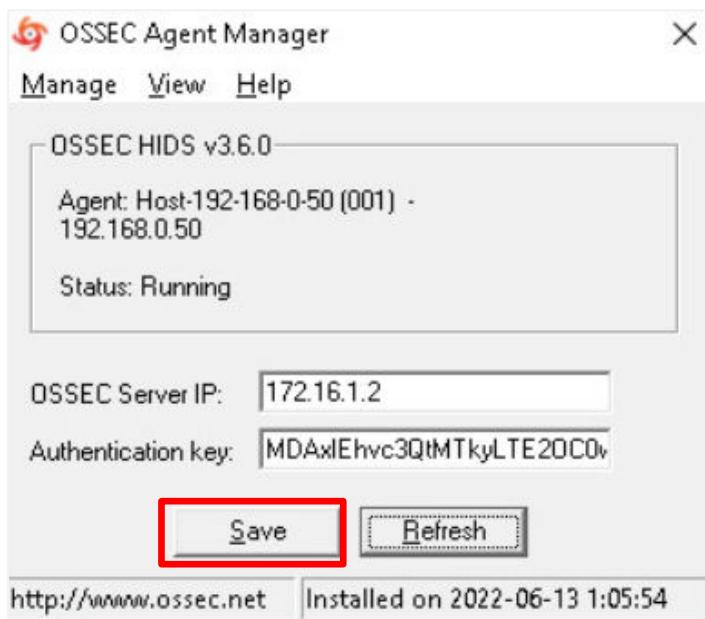
13. On the *Agent Started* popup, click **OK**.



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

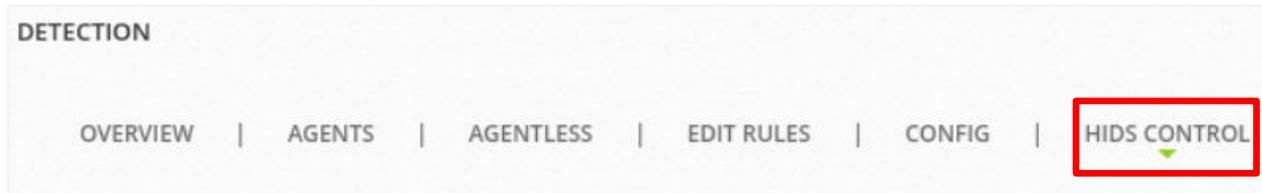


15. On the *OSSEC Agent Manager* window, click the **Save** button.

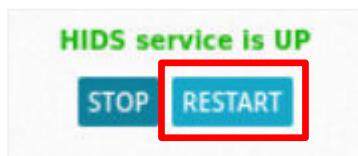


16. Set the focus to the **MintOS** computer.

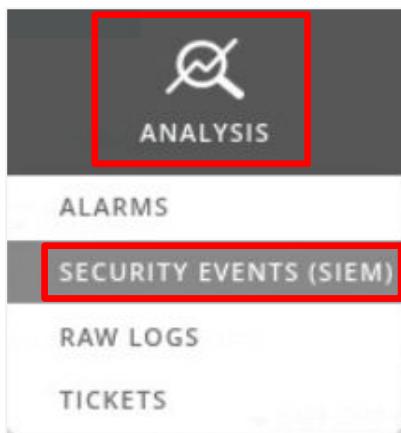
17. On the *DETECTION* page, click on **HIDS CONTROL**.



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.

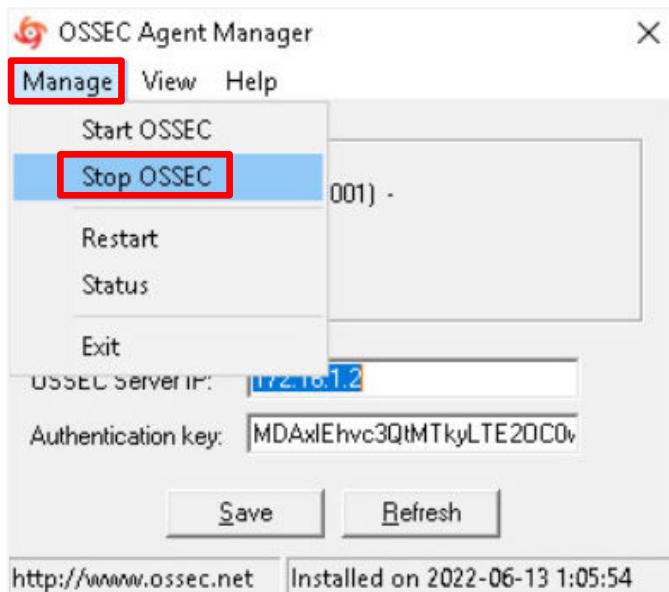
<input type="checkbox"/> EVENT NAME	▼ DATE GMT-4:00	▲	SENSOR	OTX	SOURCE	DESTINATION
<input type="checkbox"/> AlienVault HIDS: Registry Integrity Checksum Changed	2022-06-13 13:06:38		OSSIM	N/A	Host-192-168-0-50	Host-192-168-0-50



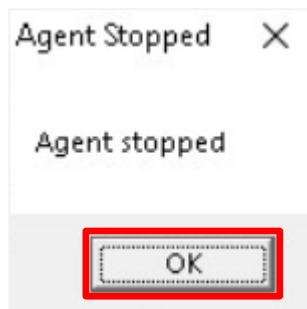
If the event does not show up, click on **CLEAR FILTERS**, then perform step 20 again.

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

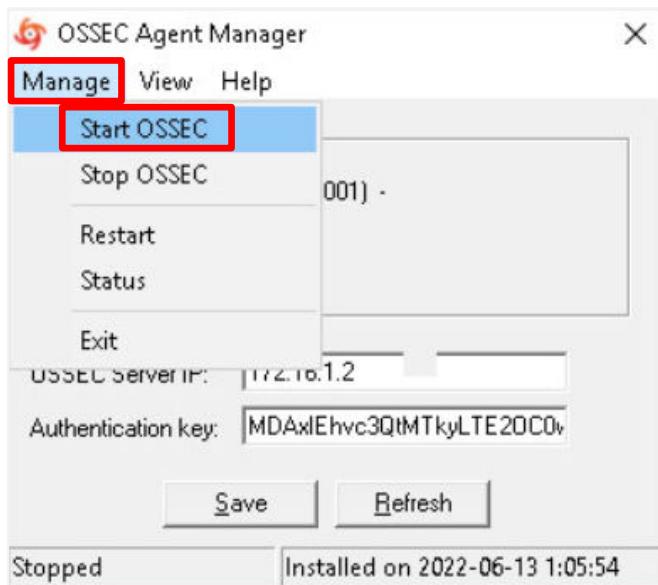
22. Set the focus on the **WinOS** computer.
23. First, the *OSSEC Agent* needs to be restarted. On the *OSSEC Agent Manager* window, click on **Manage>Stop OSSEC**.



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



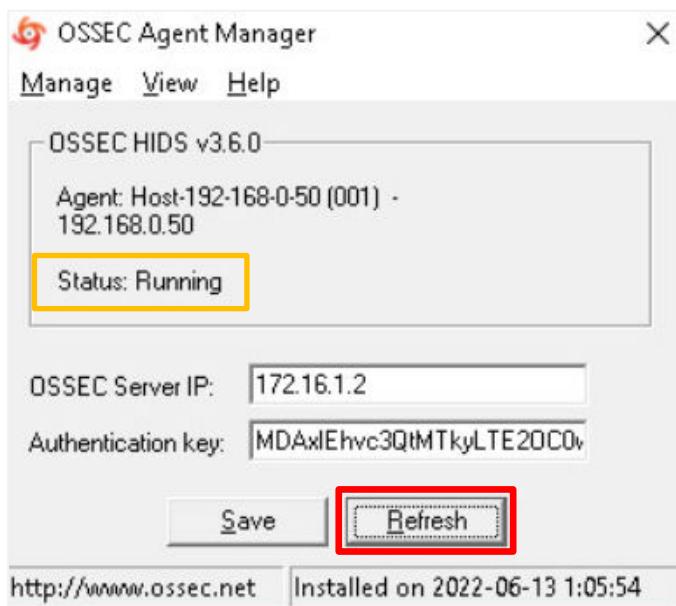
25. On the *OSSEC Agent Manager* window, click on **Manage>Start OSSEC**.



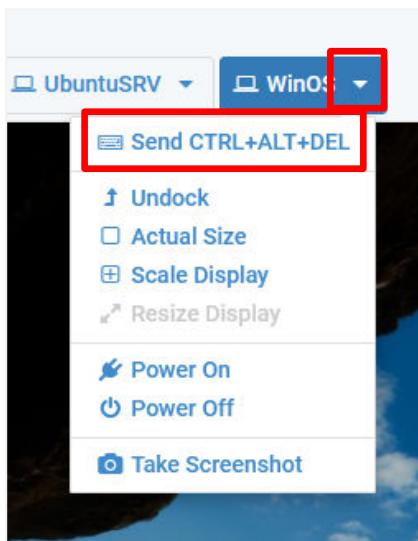
26. On the *Agent Started* popup, click **OK**.



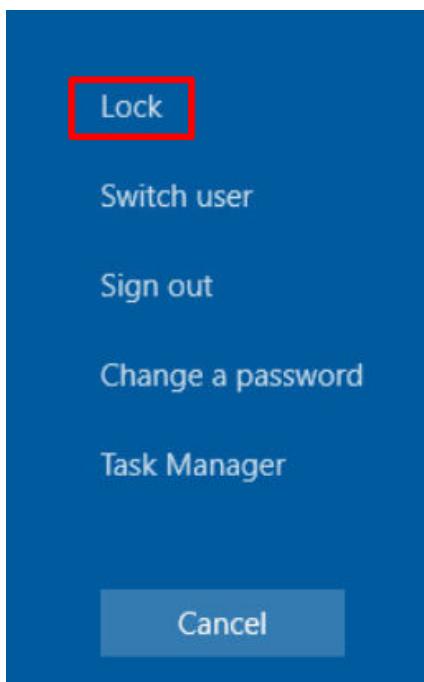
27. On the *OSSEC Agent Manager* window, click on **Refresh** to make sure the *OSSEC Agent Manager* is *Running*.



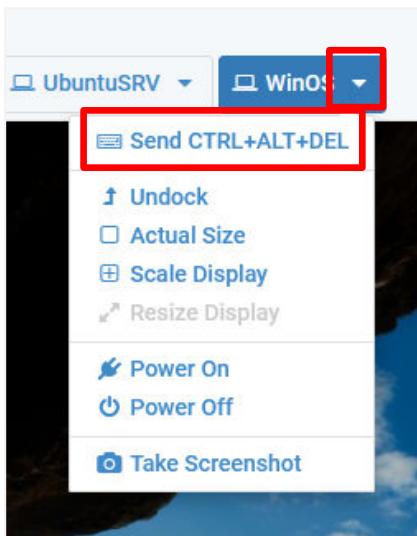
28. Lock the *WinOS* computer by clicking the **WinOS** dropdown menu, and clicking **Send CTRL+ALT+DEL**.



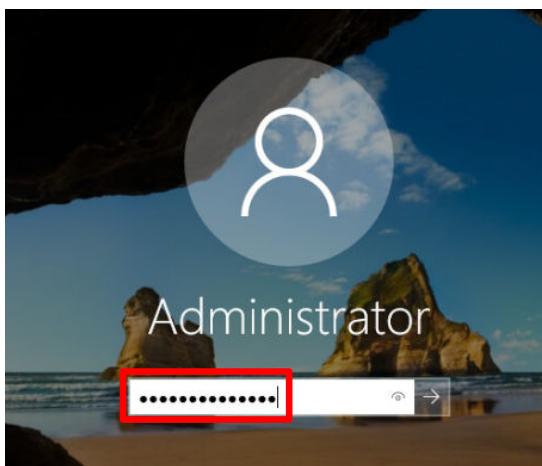
29. Click on the **Lock** link.



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

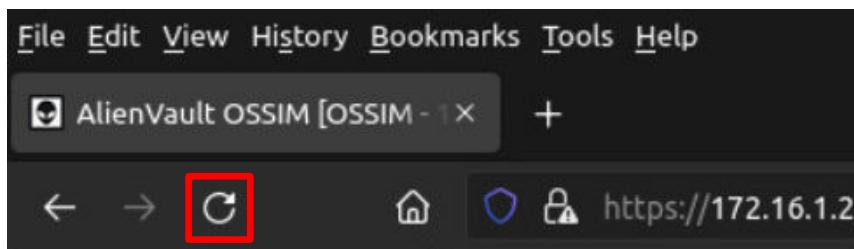


31. Attempt to log in as **Administrator** using **an incorrect password 6 times** within 30 seconds.



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 or bad password.**

EVENT NAME	▼ EVENTS # (*) ▲
<input type="checkbox"/> AlienVault HIDS: Registry Entry Added to the System	4,041
<input type="checkbox"/> AlienVault HIDS: File added to the system.	25
<input type="checkbox"/> AlienVault HIDS: Special privileges assigned to new logon	17
<input type="checkbox"/> AlienVault HIDS: Windows User Logoff.	17
<input type="checkbox"/> AlienVault HIDS: Windows Network Logon	16
<input type="checkbox"/> 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)*.

**SECURITY EVENTS (SIEM)**

**SIEM**    **REAL-TIME**

Search    Event Name  ?

**SHOW EVENTS**

- Last Hour
- Last Day
- Last Week
- Last Month
- Date Range

**DATA SOURCES**

**ASSET GROUPS**

**OTX IP REPUTATION**

**DATA SOURCE GROUPS**

**NETWORK GROUPS**

**OTX PULSE**

Pulse name

**SENSORS**     EXCLUDE

**RISK**

ONLY OTX PULSE ACTIVITY

**CLEAR FILTERS**

Userdata1    like    Userdata field

Event Name contains "192.168.0."  
Last Hour  
Src or Dest=192.168.0.50

**ADVANCED SEARCH**

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

**SECURITY EVENTS (SIEM)**

**SIEM**    **REAL-TIME**

Search    Event Name  ?

**SHOW EVENTS**

- Last Hour
- Last Day
- Last Week
- Last Month
- Date Range

**DATA SOURCES**

**Directive\_alert**

**DATA SOURCE GROUPS**

**SENSORS**     EXCLUDE

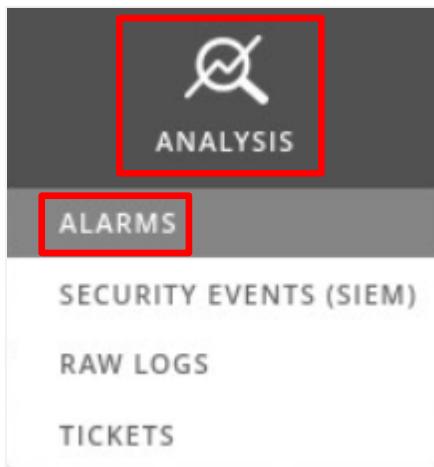
**GO**

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

<input type="checkbox"/> EVENT NAME	▼ DATE GMT-4:00	▲	SENSOR	OTX	SOURCE	DESTINATION	ASSET S + D	RISK
<input type="checkbox"/> directive_event: AV-FREE-FEED Bruteforce attack, Windows authentication attack against 192.168.0.50	2022-07-01 12:01:30		N/A	N/A	Host-192-168-0-50	Host-192-168-0-50	5->2	<span style="background-color: orange;">MED (1)</span>

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.

<input type="checkbox"/>	2022-07-01 12:01:30	open	Bruteforce Authentication	Windows Login	<span style="background-color: green;">LOW (1)</span>	N/A	Host-192-168-0-50
--------------------------	------------------------	------	---------------------------	---------------	---	-----	-------------------

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
```

```
sysadmin@mintos:~$ sudo useradd Fred  
[sudo] password for sysadmin:
```

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

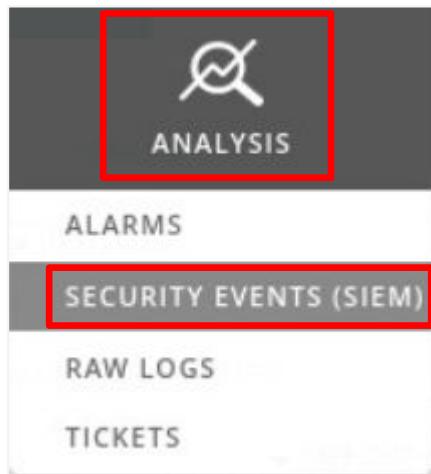
```
sudo passwd Fred
```

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

```
sysadmin@mintos:~$ sudo passwd Fred  
New password:  
Retype new password:  
passwd: password updated successfully
```

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**.

The screenshot shows the 'SECURITY EVENTS (SIEM)' page. At the top, there are two tabs: 'SIEM' (selected) and 'REAL-TIME'. Below the tabs are search fields: '192.168.0.60' (highlighted with a red box), 'Src or Dst IP' (with a dropdown arrow), and a 'GO' button (highlighted with a blue box). To the right of these are a help icon and a question mark icon. The main area has two sections: 'SHOW EVENTS' and 'DATA SOURCES'. In 'SHOW EVENTS', the 'Last Day' radio button is selected (highlighted with a red box). Other options include 'Last Hour', 'Last Week', 'Last Month', and 'Date Range'. Below these are two calendar icons. In 'DATA SOURCES', the 'AlienVault HIDS' option is selected (highlighted with a red box). There are also 'DATA SOURCE GROUPS' and 'SENSORS' dropdown menus, and an 'EXCLUDE' checkbox.

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*.

EVENT NAME
<input type="checkbox"/> AlienVault HIDS: New HIDS agent connected.
<input type="checkbox"/> AlienVault HIDS: Excessive number of events (above normal)
<input type="checkbox"/> AlienVault HIDS: First time user executed sudo.
<input type="checkbox"/> AlienVault HIDS: Web server 400 error code.
<input type="checkbox"/> AlienVault HIDS: New user added to the system
<input type="checkbox"/> AlienVault HIDS: User changed password.

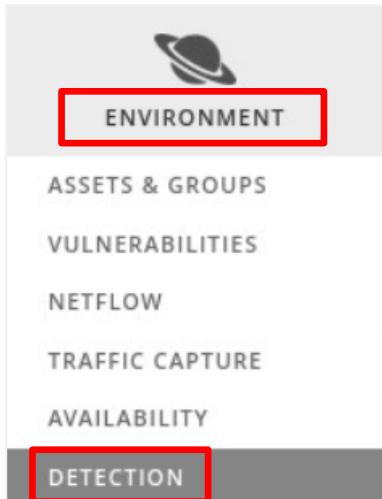
49. Remain in the *AlienVault OSSIM* Web UI and continue to the next task.

## 2.4 HIDS Application Events

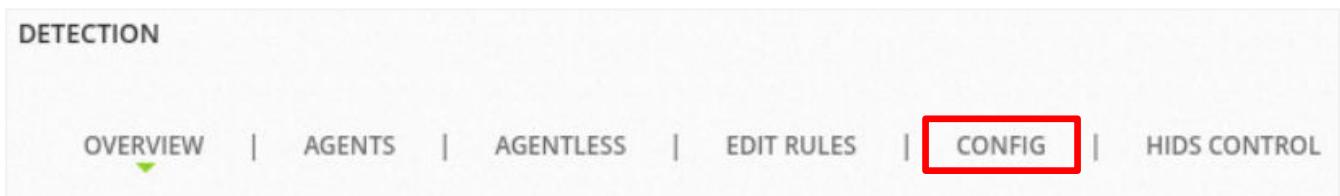
Another area of concern for security analysts is when potentially vulnerable software is installed on a host. In this task, you will set up the Windows AppLocker service, which monitors and manages applications that are run on Windows servers. You will then configure the OSSEC agent to pass the events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

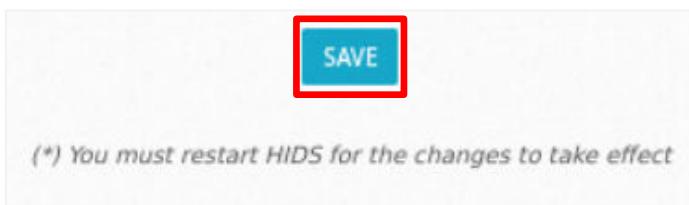
3. Scroll down the page, and you will see two lists, *ENABLED RULES* and *DISABLED RULES*. The rule for *Windows AppLocker* is disabled by default and will need to be enabled. Scroll down on the right-side list and look for **alienVault-windows-applocker\_rules.xml** and click on the + to the right of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

DISABLED RULES	
	Add all
alienVault-syslog_rules.xml	+
alienVault-system_rules.xml	+
alienVault-web-access_rules.xml	+
alienVault-windows-access_rules.xml	+
alienVault-windows-account-security_rules.xml	+
alienVault-windows-ADFS-servers-rules.xml	+
alienVault-windows-applocker_rules.xml	+
alienVault-windows-capacity_rules.xml	+
alienVault-windows-certificate_services.xml	+

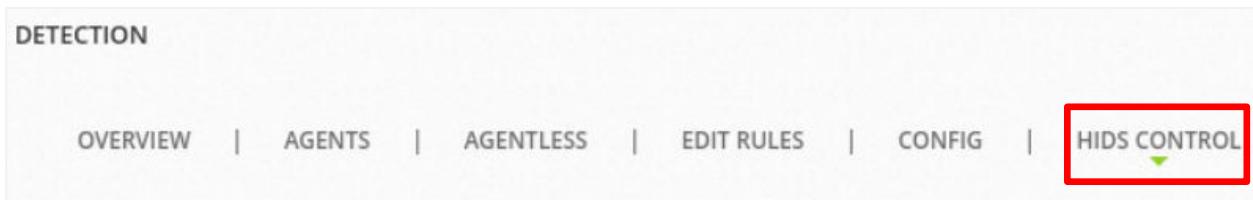
Scroll down the left side list, and you will see the *alienVault-windows-applocker\_rules.xml* in the list of enabled rules.

ENABLED RULES
sshd_rules.xml
symantec-av_rules.xml
symantec-ws_rules.xml
syslog_rules.xml
telnetd_rules.xml
vmpop3d_rules.xml
vmware_rules.xml
vpn_concentrator_rules.xml
vpopmail_rules.xml
vsftpd_rules.xml
web_rules.xml
zeus_rules.xml
alienVault-windows-applocker_rules.xml

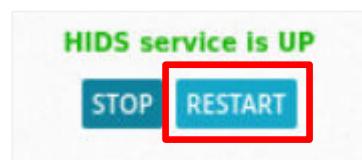
4. At the bottom of the *Rules* page, click the **SAVE** button.



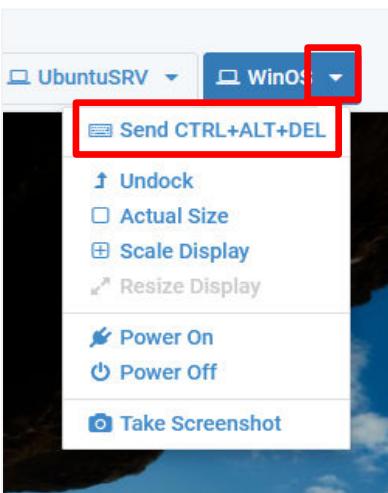
5. On the *DETECTION* page, click on **HIDS CONTROL**.



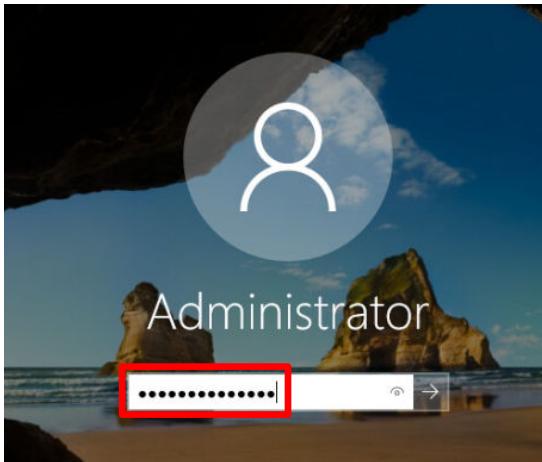
6. Under *ACT/IONS*, click the **RESTART** button under **HIDS service is UP**.



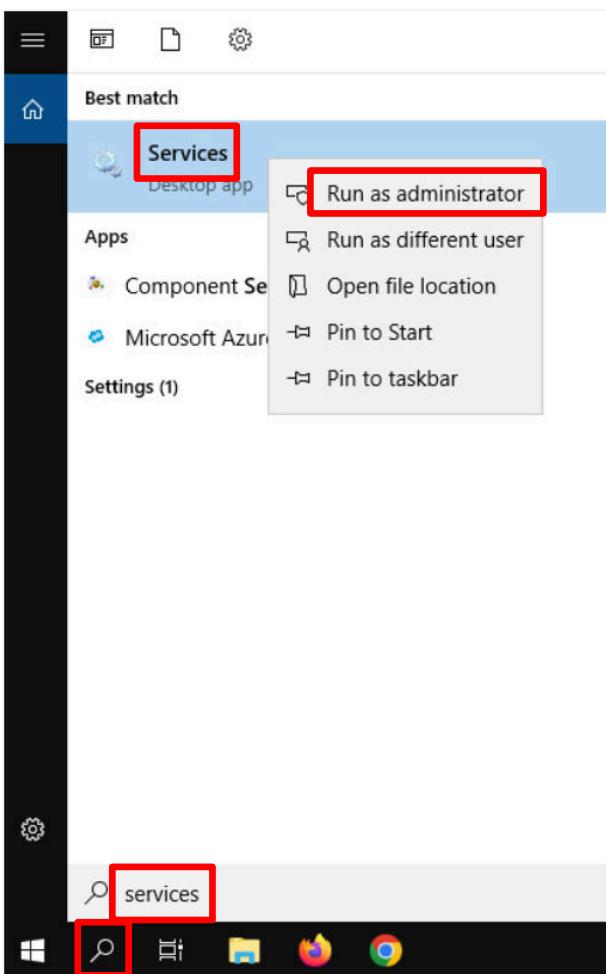
7. Set the focus to the **WinOS** computer.
8. Unlock the *WinOS* computer. Click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



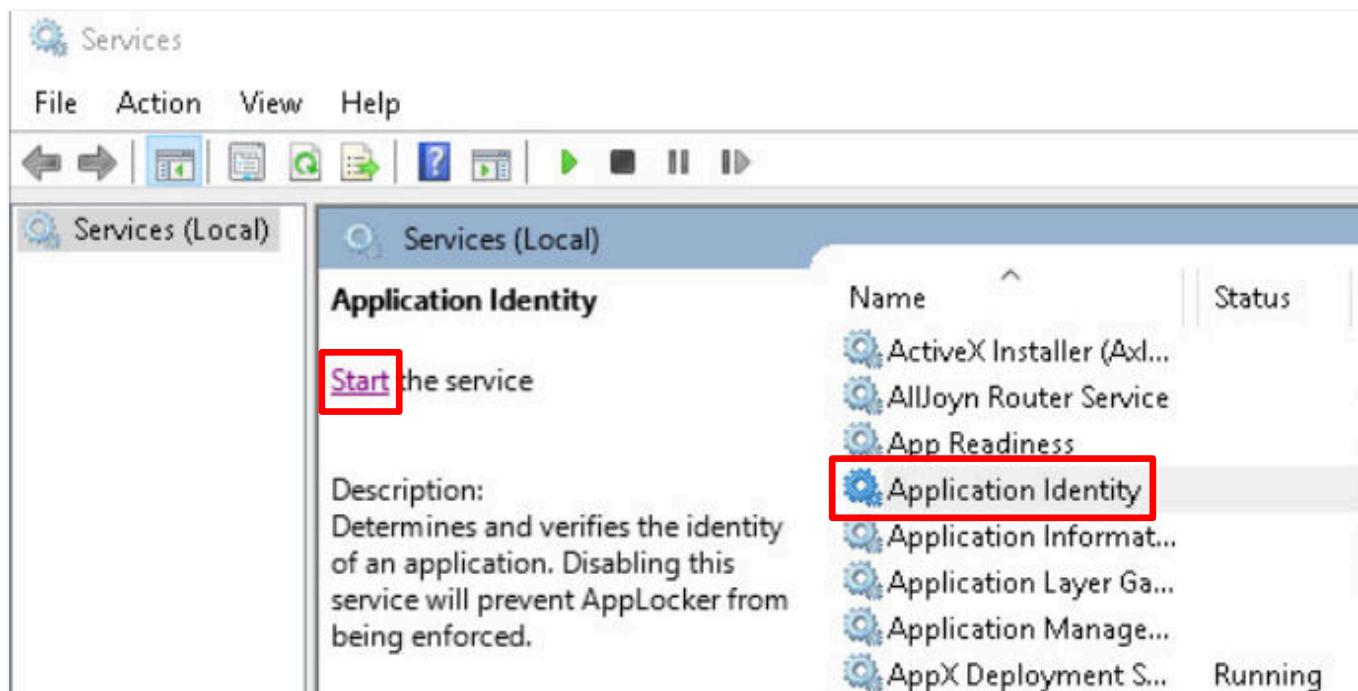
9. Log in as **Administrator** using the password: NDGLabpass123!



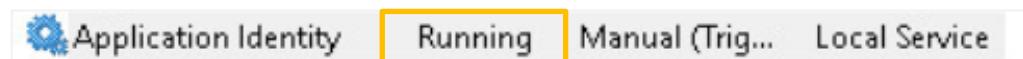
10. Click on the **Search** button and type **Services**. Under **Best match**, right-click on the menu and click **Run as administrator**.



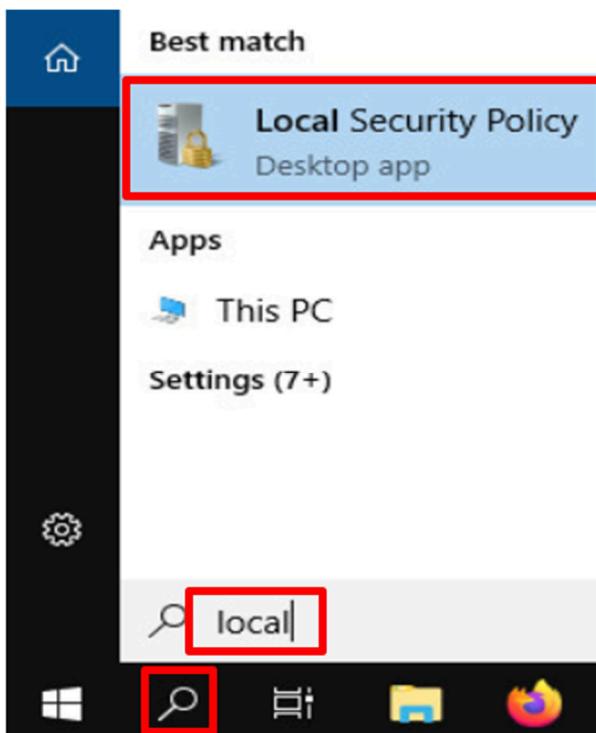
11. On the **Services** window, on the right panel, click on **Application Identity**, and then click on **Start**.



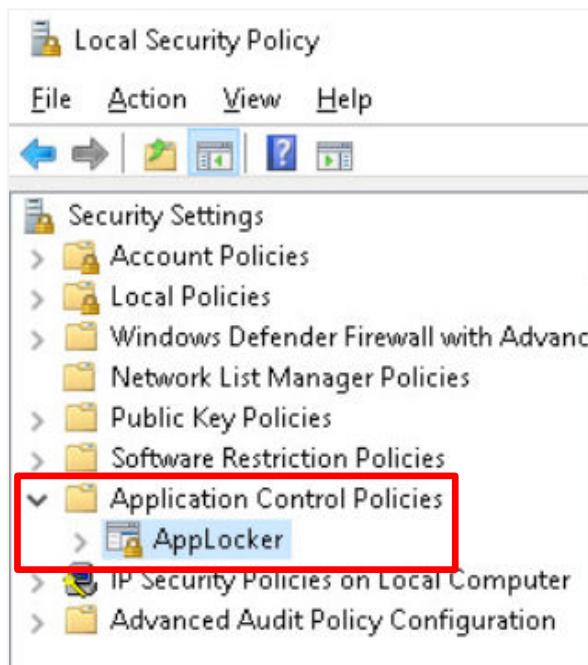
Make sure the service is *Running* before going on to the next step.



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**.

The screenshot shows the Windows AppLocker configuration interface. At the top, there's a header bar with the title "AppLocker provides access control for applications". Below it, the "Getting Started" section contains a general description of AppLocker's purpose and a note about its compatibility with different Windows editions. It includes links to "More about AppLocker" and "Which editions of Windows support AppLocker?". The main content area is titled "Configure Rule Enforcement". It features a warning icon and text stating that the AppLocker policy must be enforced by the Application Identity service. It also provides instructions for configuring enforcement settings for rule collections. A red box highlights the link "Configure rule enforcement". The "Overview" section at the bottom lists "Executable Rules" (0 rules, audited) and "Windows Installer Rules" (0 rules, audited).

AppLocker provides access control for applications

Getting Started

AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.

More about AppLocker

Which editions of Windows support AppLocker?

Configure Rule Enforcement

⚠ For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.

Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.

Configure rule enforcement

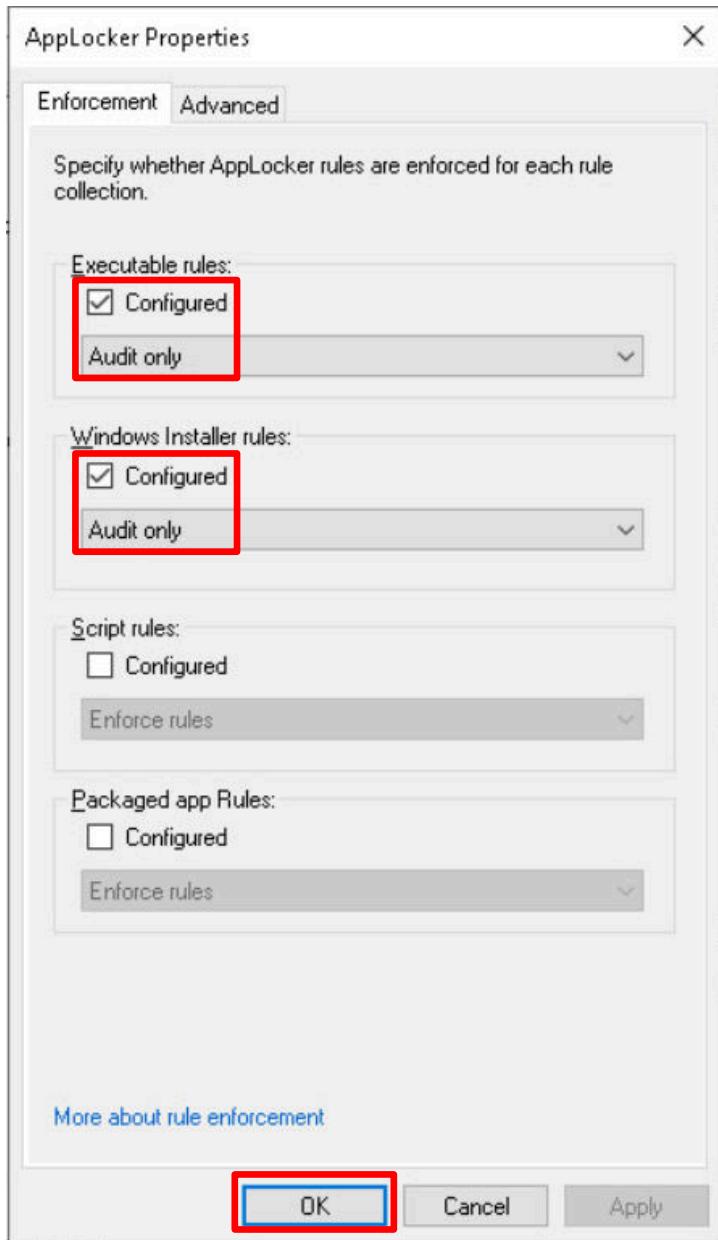
More about rule enforcement

Overview

Executable Rules  
Rules: 0  
Enforcement configured: Rules are audited

Windows Installer Rules  
Rules: 0  
Enforcement configured: Rules are audited

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**.



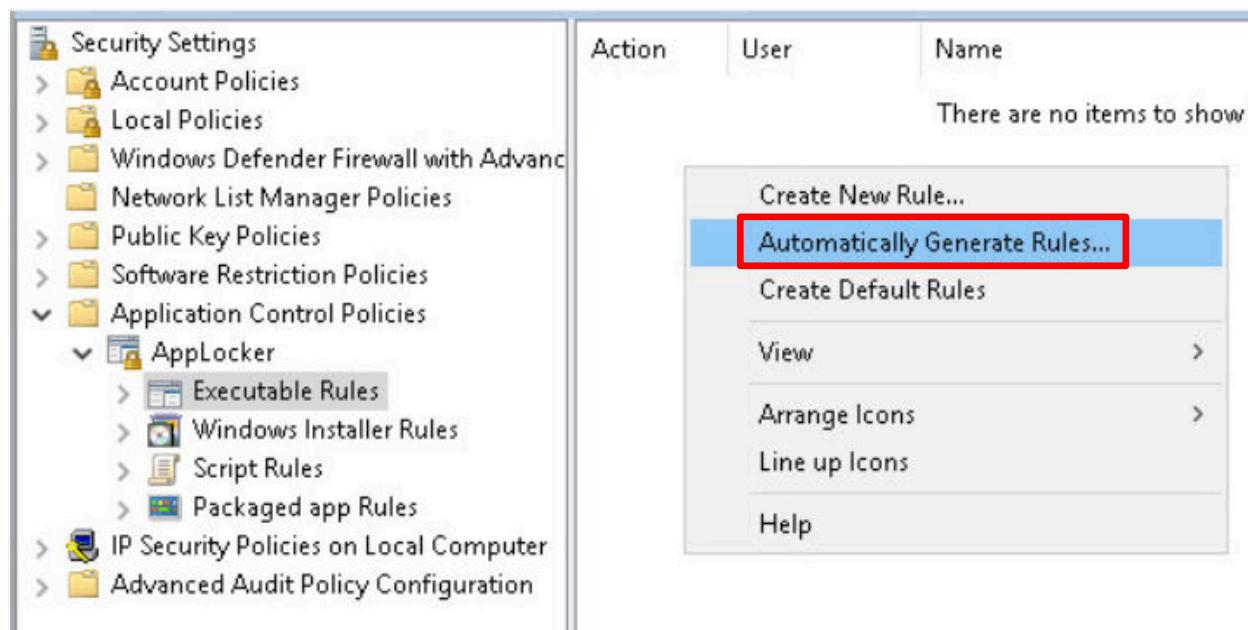
You will be creating rules in the next part of the task. Rules that are set to *Audit Only* will test the rule and if there is a match, will send an Information Event to the *AppLocker* event logs.

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

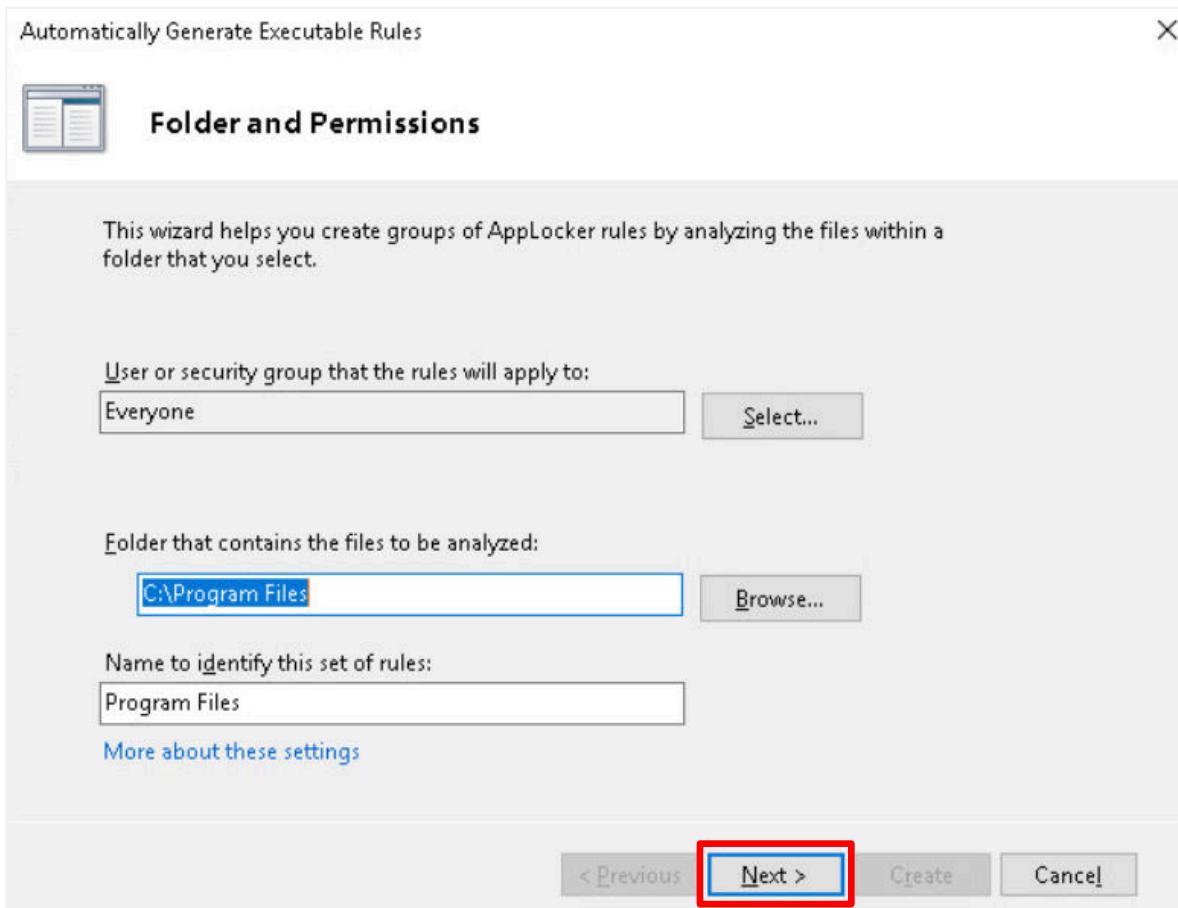
The screenshot shows the Windows AppLocker configuration interface. At the top, there's a header bar with the title "AppLocker provides access control for applications". Below it, there are three main sections: "Getting Started", "Configure Rule Enforcement", and "Overview".

- Getting Started:** Describes what AppLocker does and which Windows editions support it. It includes links to "More about AppLocker" and "Which editions of Windows support AppLocker?".
- Configure Rule Enforcement:** Contains a warning about the Application Identity service and enforcement settings. It includes links to "Configure rule enforcement" and "More about rule enforcement".
- Overview:** Shows two rule collections:
  - Executable Rules:** Selected and highlighted with a red box. It shows 0 rules and that enforcement is configured to audit.
  - Windows Installer Rules:** Unselected. It shows 0 rules and that enforcement is configured to audit.

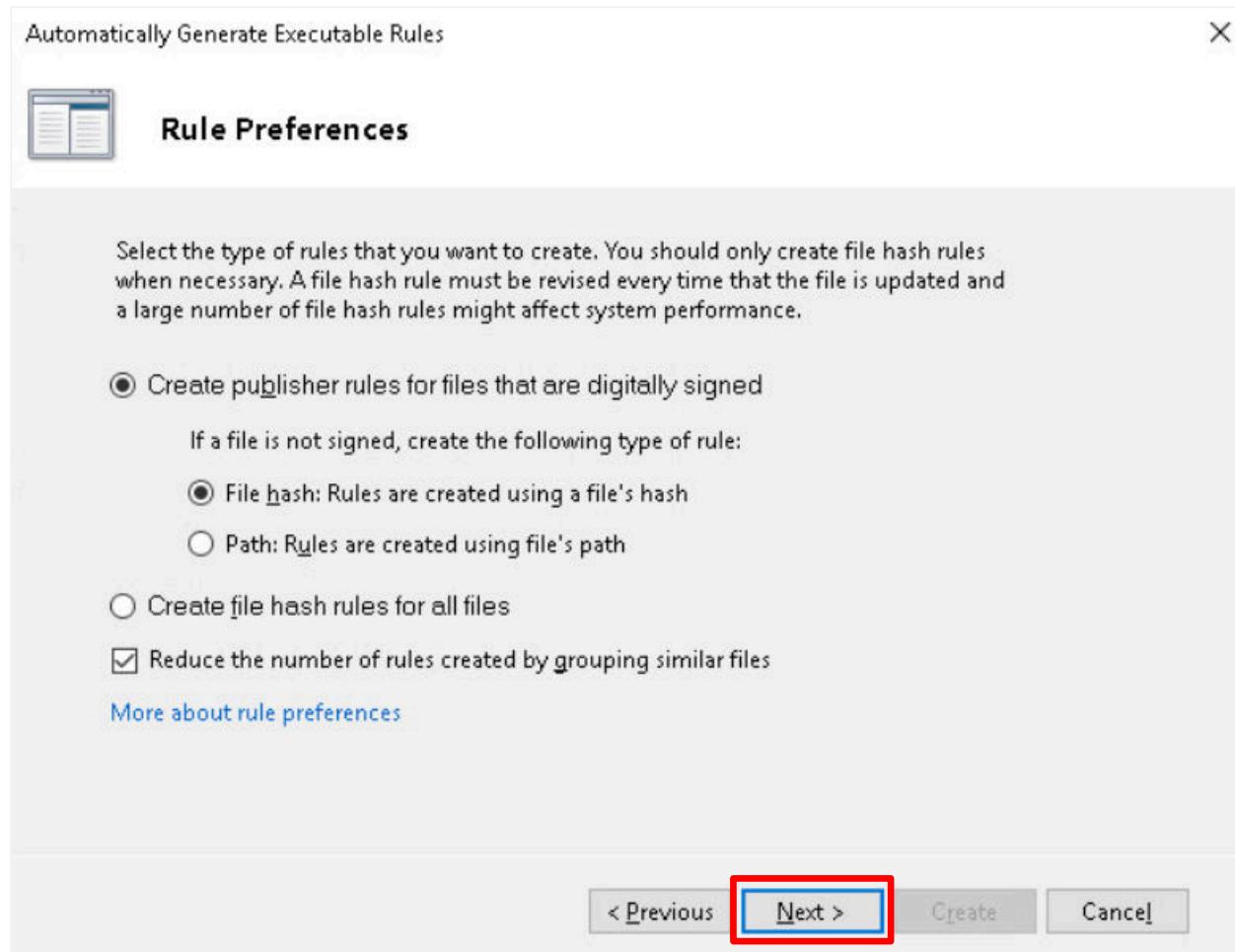
19. On the right panel, right-click on white space to bring up the context menu and click on **Automatically Generate Rules** which will create a set of rules for the software that is installed on this computer.



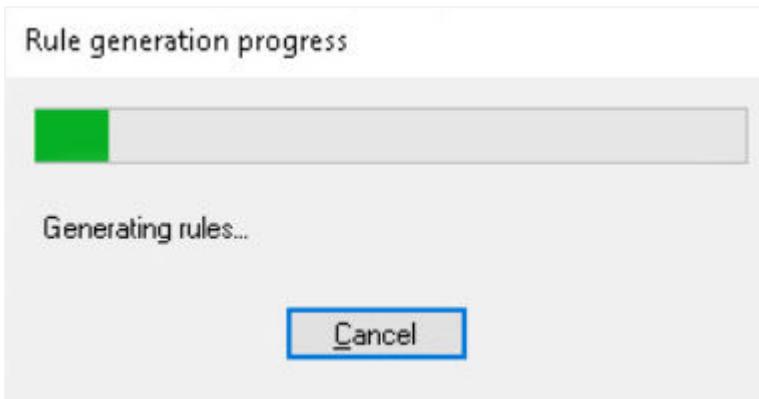
20. The first step of the wizard will analyze files within a folder. Leave the *Folder* set to C:\Program Files and the *Name* to Program Files and click **Next**.



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.

Automatically Generate Executable Rules X

### Review Rules

The folder analysis is complete and the following rules will be added to the policy.

Rule Type	Rules	Files
Publisher	25	247
File Hash	21	362
<b>Total</b>	<b>46</b>	<b>609</b>

[Review files that were analyzed](#)  
 [View rules that will be automatically created](#)

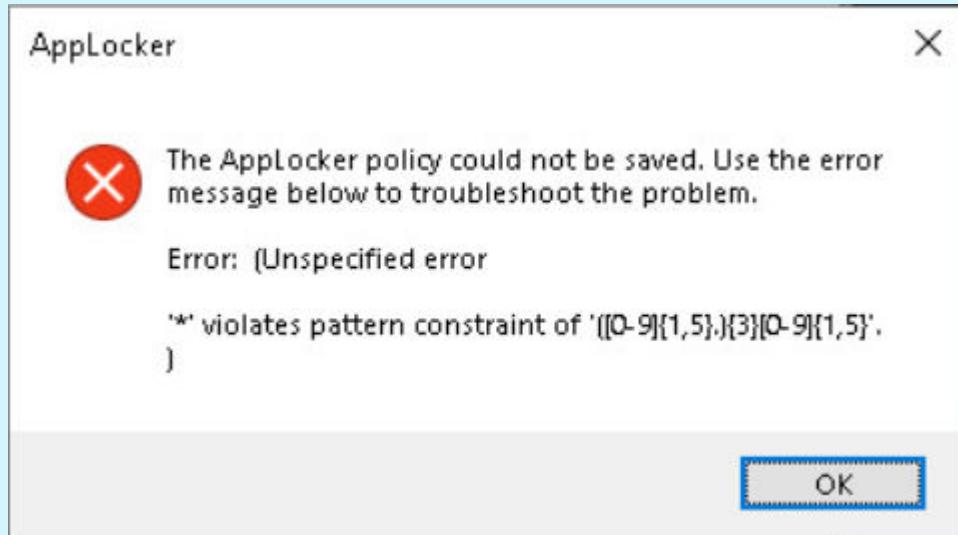
Click Create to close the wizard and create the rules.

**⚠ Some folders and files could not be read during rule generation. The wizard has skipped these folders and files.**

[\*\*< Previous\*\*](#) [\*\*Next >\*\*](#) **Create** [\*\*Cancel\*\*](#)



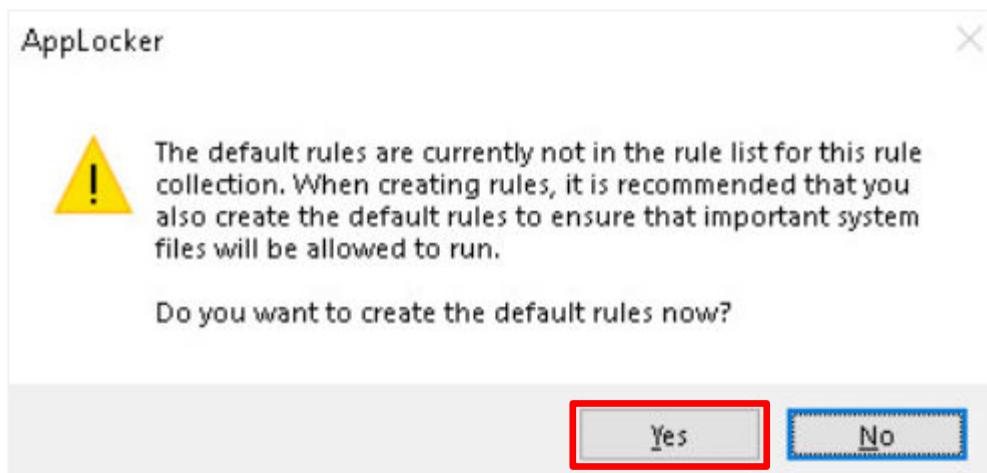
If you get the error popup window:



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**.

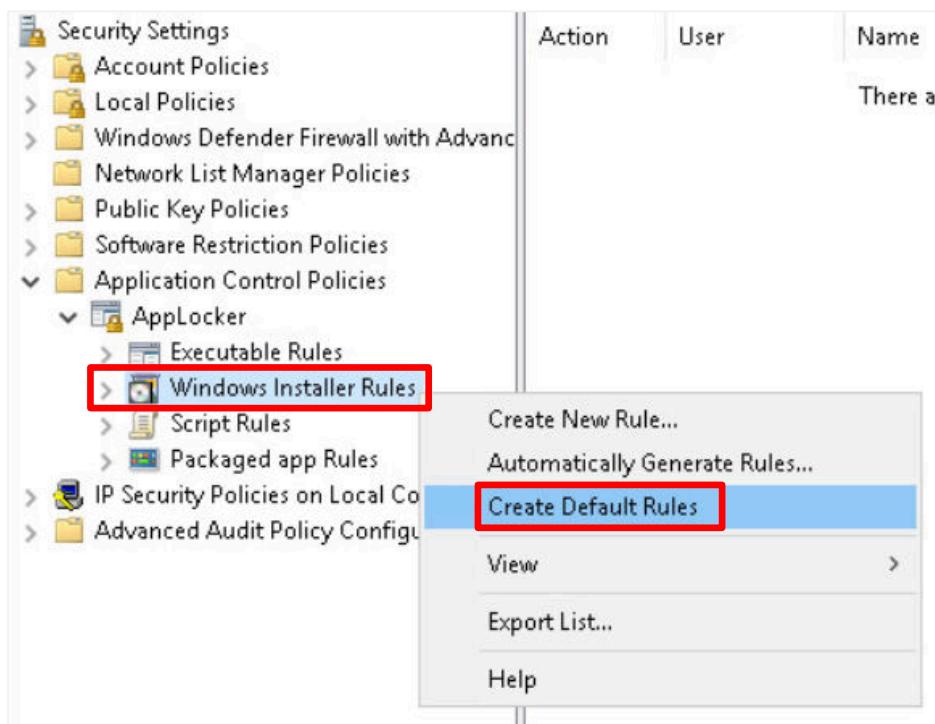
23. On the warning popup window stating, *The default rules are currently not in the rule list for this rule collection*, click on the **Yes** button to create the default rules.



The rules will now be listed in the right panel.

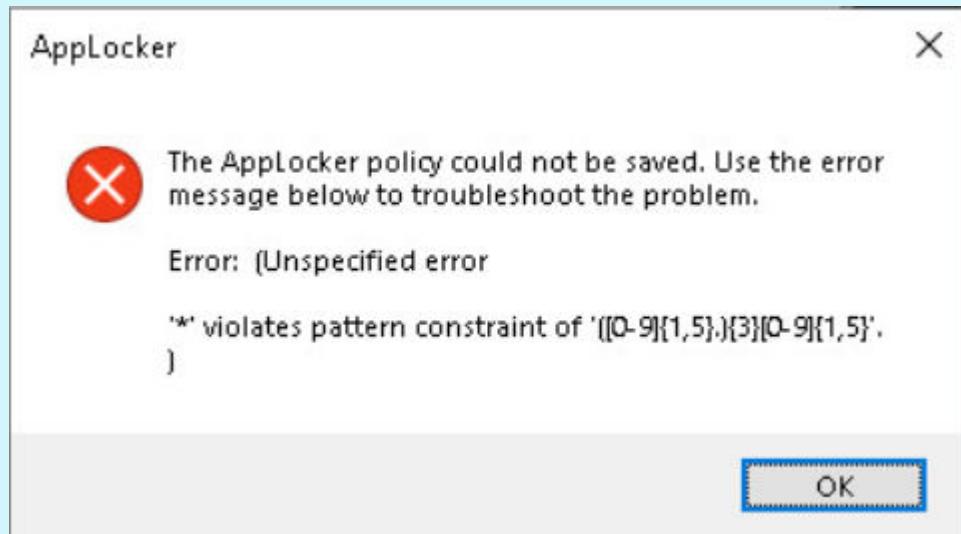
Security Settings	Action	User	Name	Condition
> Account Policies	Allow	Everyone	(Default Rule) All files located in the Pro...	Path
> Local Policies	Allow	Everyone	(Default Rule) All files located in the Wi...	Path
> Windows Defender Firewall with Advanc...	Allow	BUILTIN\Administrators	(Default Rule) All files	Path
> Network List Manager Policies	Allow	Everyone	Program Files: CAPINFO.Signed by O=...	Publisher
> Public Key Policies	Allow	Everyone	Program Files: dftest.exe, mmdbresolv...	File Hash
> Software Restriction Policies	Allow	Everyone	Program Files: DUMPCAP signed by O=...	Publisher
> Application Control Policies	Allow	Everyone	Program Files: EDITCAP signed by O=W...	Publisher
> AppLocker	Allow	Everyone	Program Files: MERGECAP signed by O...	Publisher
> Executable Rules	Allow	Everyone	Program Files: RAWSHARK signed by O...	Publisher
> Windows Installer Rules	Allow	Everyone	Program Files: REORDERCAP signed by ...	Publisher
> Script Rules	Allow	Everyone	Program Files: TEXT2PCAP signed by O...	Publisher
> Packaged app Rules	Allow	Everyone	Program Files: TSHARK signed by O=W...	Publisher
> IP Security Policies on Local Computer	Allow	Everyone	Program Files: WIRESHARK signed by O...	Publisher
> Advanced Audit Policy Configuration	Allow	Everyone	Program Files: MICROSOFT® WINDOW...	Publisher
	Allow	Everyone	Program Files: MICROSOFT (R) WINDO...	Publisher
	Allow	Everyone	Program Files: guestproxycerttool.exe, r...	File Hash
	Allow	Everyone	Program Files: VMWARE TOOLS signed ...	Publisher
	Allow	Everyone	Program Files: VMWARE WORKSTATIO...	Publisher
	Allow	Everyone	Program Files: CommAmqpListener.exe...	File Hash
	Allow	Everyone	Program Files: VERACRYPT signed by O...	Publisher
	Allow	Everyone	Program Files: tftpd64.exe, uninstall.exe	File Hash
	Allow	Everyone	Program Files: PUTTY SUITE signed by ...	Publisher
	Allow	Everyone	Program Files: NPCAP signed by O=INS...	Publisher
	Allow	Everyone	Program Files: Uninstall.exe	File Hash
	Allow	Everyone	Program Files: FIREFOX signed by O=M...	Publisher
	Allow	Everyone	Program Files: INTERNET EXPLORER sig...	Publisher
	Allow	Everyone	Program Files: GIT signed by O=JOHAN...	Publisher
	Allow	Everyone	Program Files: unins000.exe	File Hash

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**.

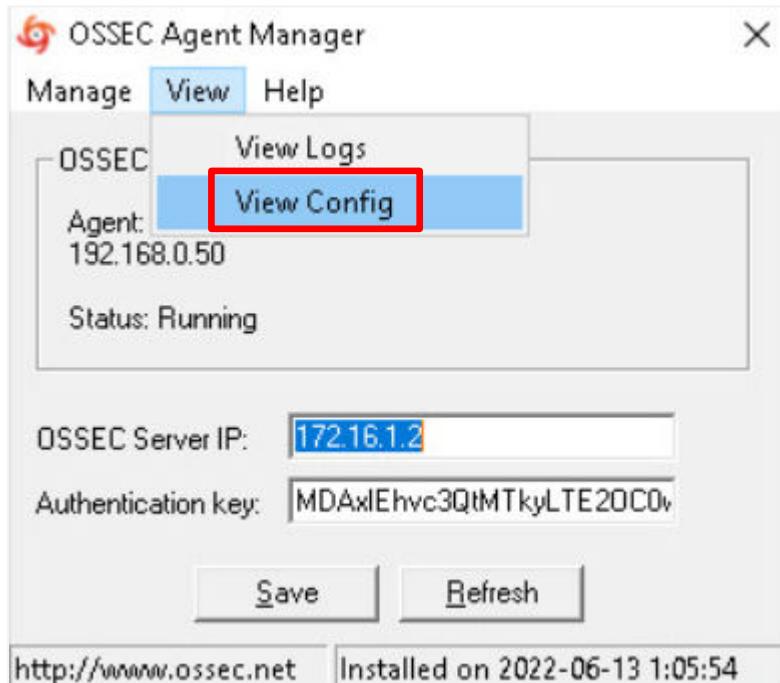
Action	User	Name
Allow	Everyone	(Default Rule) All digitally signed Windows Installer files
Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%
Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files

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 *AlienVault 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*.

A screenshot of a Notepad window titled "ossec.conf - Notepad". The window contains the configuration file for the OSSEC Win32 Agent. The content starts with a comment block: ``. The Notepad window has a standard menu bar with File, Edit, Format, View, and Help.

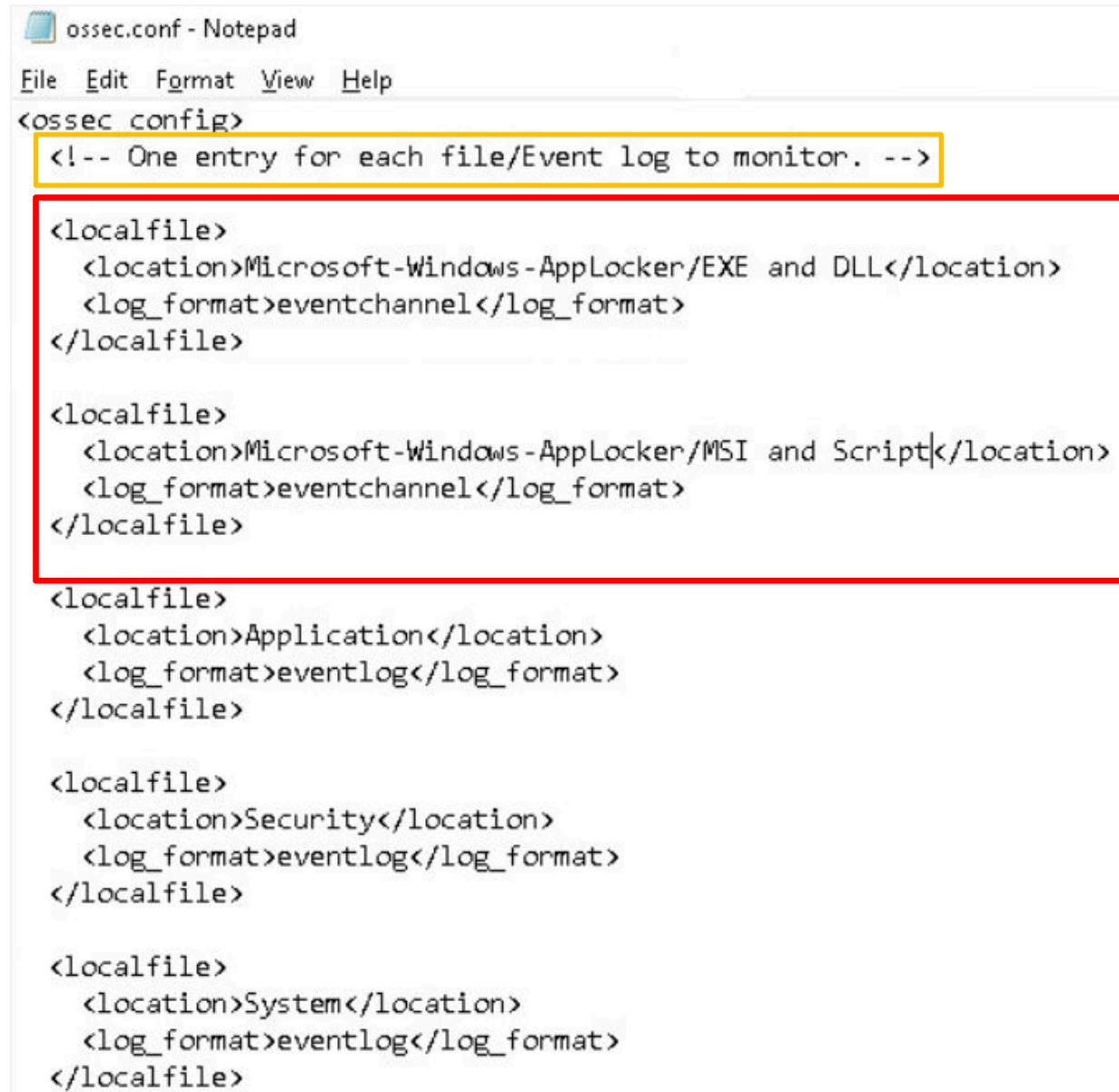
27. Scroll down to the <ossec\_config> below the line

<!-- 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>
```



```
ossec.conf - Notepad
File Edit Format View Help
<ossec config>
  <!-- One entry for each file/Event log to monitor. -->

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

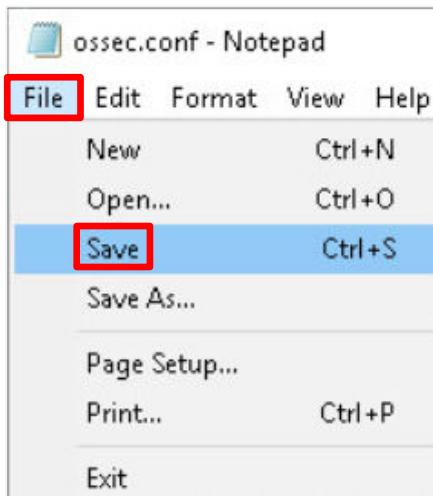
    <localfile>
      <location>Microsoft-Windows-AppLocker/MSI and Script</location>
      <log_format>eventchannel</log_format>
    </localfile>

    <localfile>
      <location>Application</location>
      <log_format>eventlog</log_format>
    </localfile>

    <localfile>
      <location>Security</location>
      <log_format>eventlog</log_format>
    </localfile>

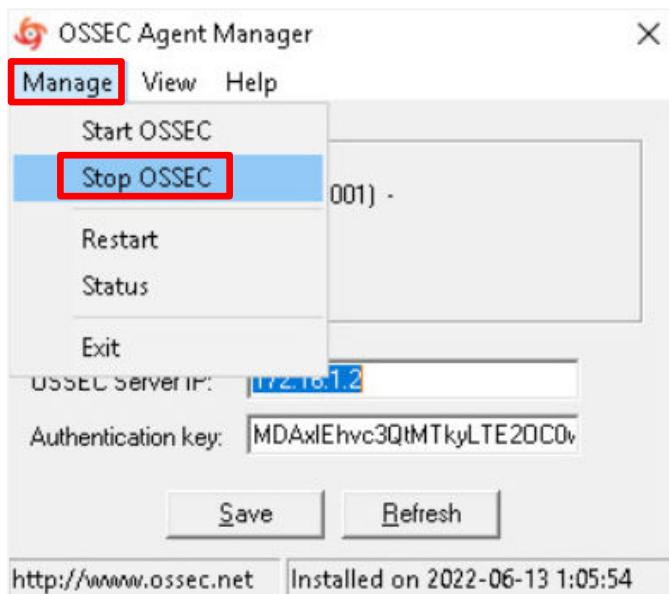
    <localfile>
      <location>System</location>
      <log_format>eventlog</log_format>
    </localfile>
```

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

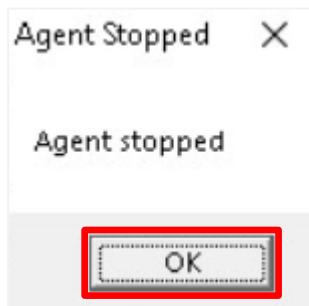


29. Close **Notepad**.

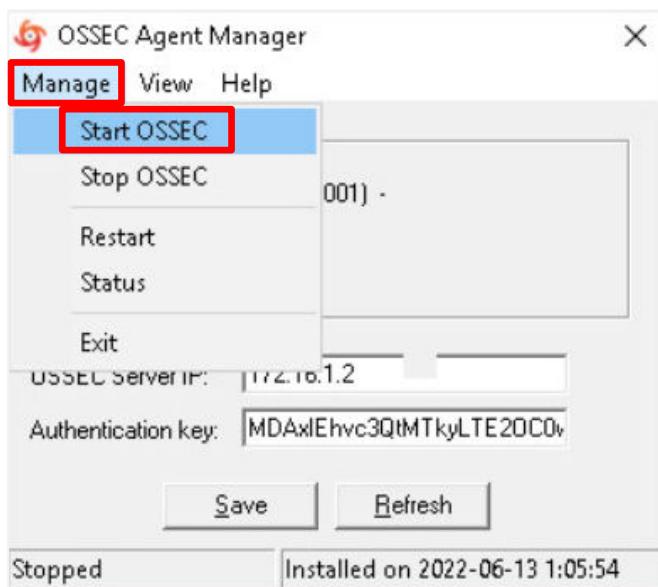
30. On the *OSSEC Agent Manager* window, click on **Manage>Stop OSSEC**.



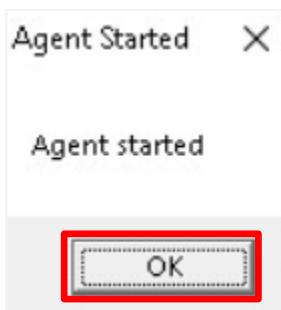
31. On the *Agent Stopped* popup, click **OK**.



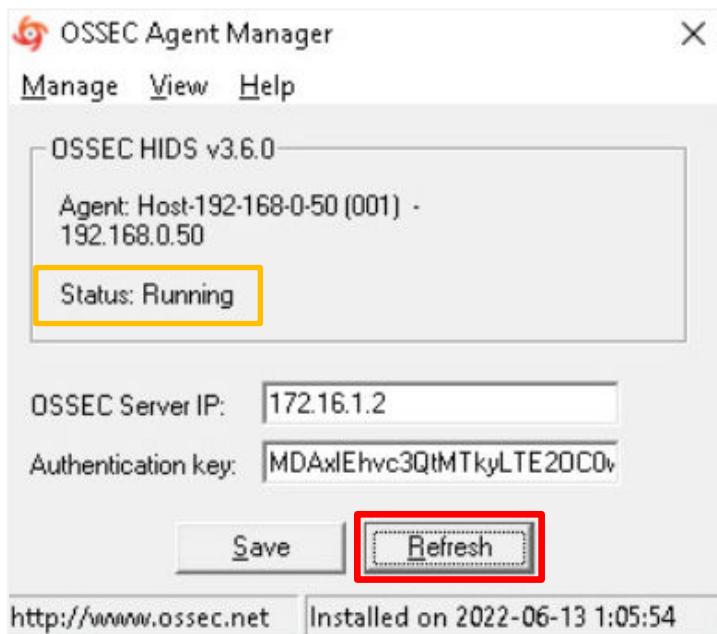
32. On the *OSSEC Agent Manager* window, click on **Manage>Start OSSEC**.



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

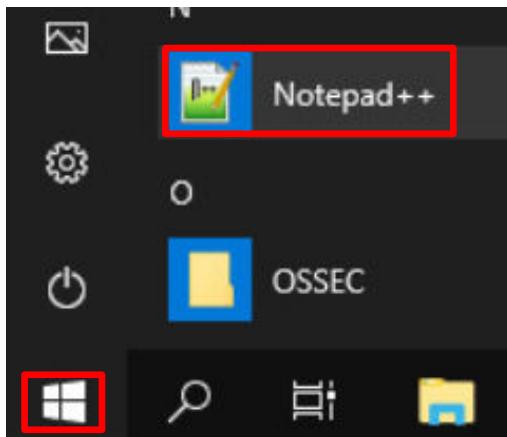
1. Set the focus to the **MintOS** computer.
2. You should still be on the *DETECTION* page under *HIDS CONTROL*. In the *ACTIONS* section, click **RESTART** under *HIDS service is UP*.

The screenshot shows the 'DETECTION' page under 'HIDS CONTROL'. The top navigation bar includes 'OVERVIEW', 'AGENTS', 'AGENTLESS', 'EDIT RULES', 'CONFIG', and 'HIDS CONTROL', with 'HIDS CONTROL' highlighted by a red box. Below this, there are three tabs: 'HIDS CONTROL' (selected), 'HIDS LOG', and 'ALERTS LOG'. The main area is titled 'ACTIONS' and contains four items:

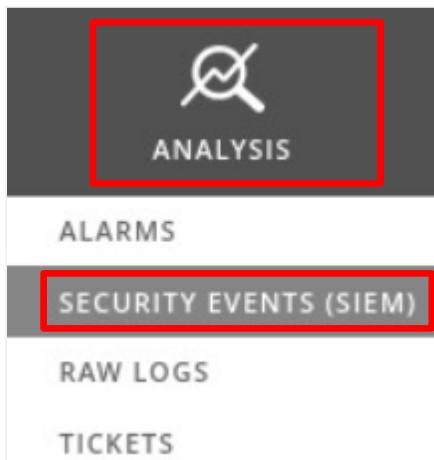
- Client-syslog is NOT running**: Buttons: 'ENABLE' (blue)
- Agentless is running**: Buttons: 'DISABLE' (blue)
- Debug is disabled**: Buttons: 'ENABLE' (blue)
- HIDS service is UP**: Buttons: 'STOP' (blue) and 'RESTART' (highlighted with a red box)

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

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



- Close **Notepad++**.
- Return focus to the **MintOS** computer.
- 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**.

The screenshot shows the **SECURITY EVENTS (SIEM)** interface. The **REAL-TIME** tab is selected. The search bar contains **192.168.0.50**. To its right is a dropdown menu set to **Src or Dst IP**, and a **GO** button. Below the search area, under **SHOW EVENTS**, the **Last Day** radio button is selected. Under **DATA SOURCES**, the dropdown menu is set to **AlienVault HIDS**. At the bottom, there are filters for **userdata1** and a dropdown menu for **Userdata1 field**.

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
<b>AlienVault HIDS: AppLocker allowed a program to execute</b>	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	<b>MED (1)</b>

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

EVENTS    GROUPED    TIMELINE

SHOW 50 ENTRIES

SHOW TREND GRAPH Off

DISPLAYING 1 TO 2 OF 2 EVENTS.

<input type="checkbox"/> EVENT NAME	<input type="checkbox"/> DATE GMT-4:00
AlienVault HIDS: AppLocker allowed a program to execute	2022-09-12 13:03:43

This will show the *Event Details*.

Event details

AlienVault HIDS: AppLocker allowed a program to execute

DATE	2022-09-12 13:03:43 GMT-4:00	CATEGORY	Policy
ALIENVAULT SENSOR	OSSIM [172.16.1.2]	SUB-CATEGORY	Check Passed
DEVICE IP	192.168.0.50 [eth0]	DATA SOURCE NAME	AlienVault HIDS-windows
EVENT TYPE ID	110020	DATA SOURCE ID	7006
UNIQUE EVENT ID#	32bc11ed-be6a-0050-5699-afaedb339e44	PRODUCT TYPE	Operating System
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
1	5	MED (1)	0

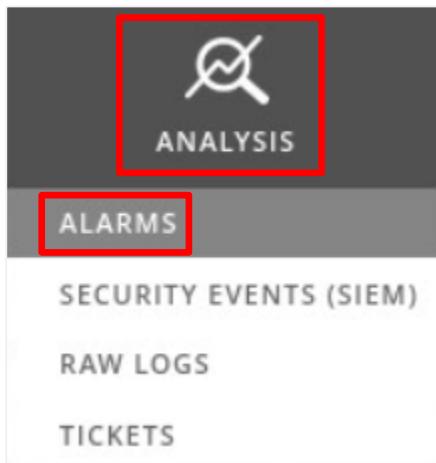
**12. Scrolling down the page will show the details about which application was run, which user ran the application, and the computer on which the application was run.**

FILENAME	USERNAME
%PROGRAMFILES%\NOTEPAD++\NOTEPAD++.EXE	Administrator
USERDATA5	
WIN-E3AIDIHECNG	

**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**.

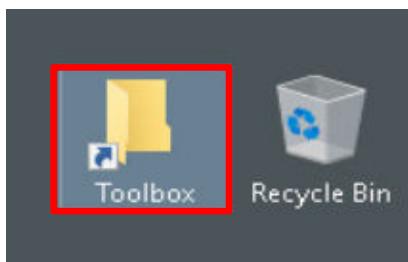


15. Scroll down to the bottom of the page, and you will see the alarm entry.

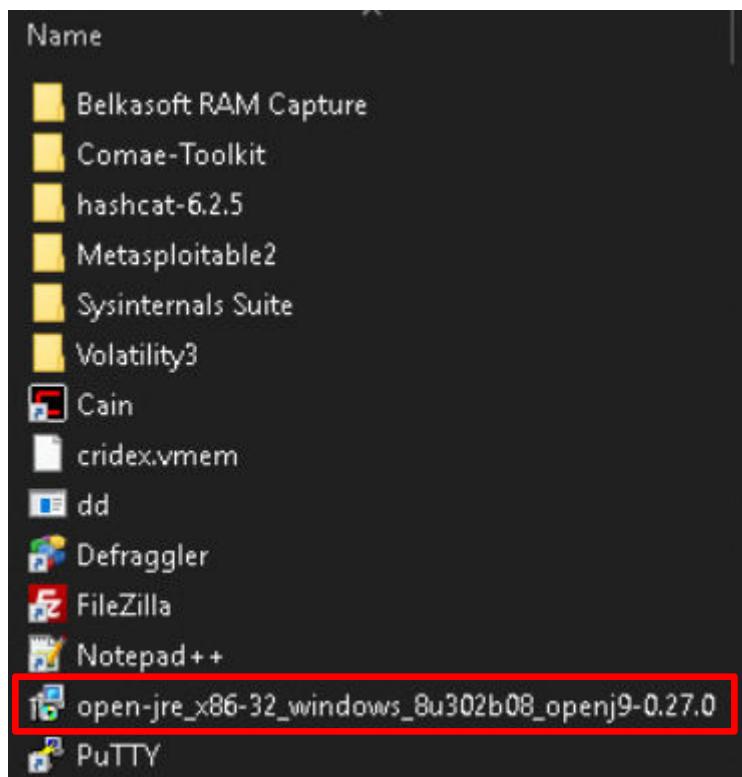
DATE	▼ STATUS	Intent & Strategy	Method	Risk
2022-06-15 03:23:53	open	AlienVault HIDS: AppLocker allowed a program to execute		LOW (1)

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

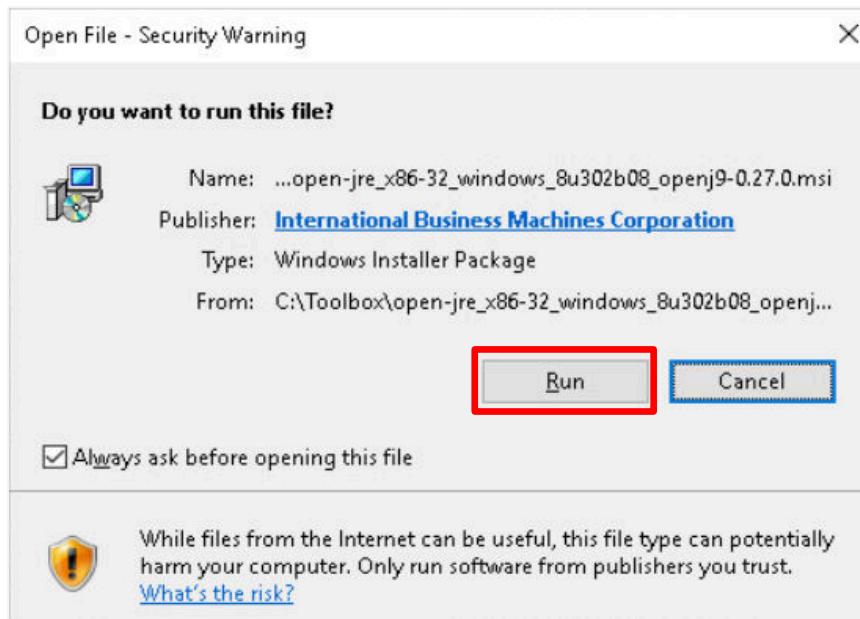
16. Set the focus on the **WinOS** computer.
17. Double-click on the **Toolbox** folder on the *desktop*.



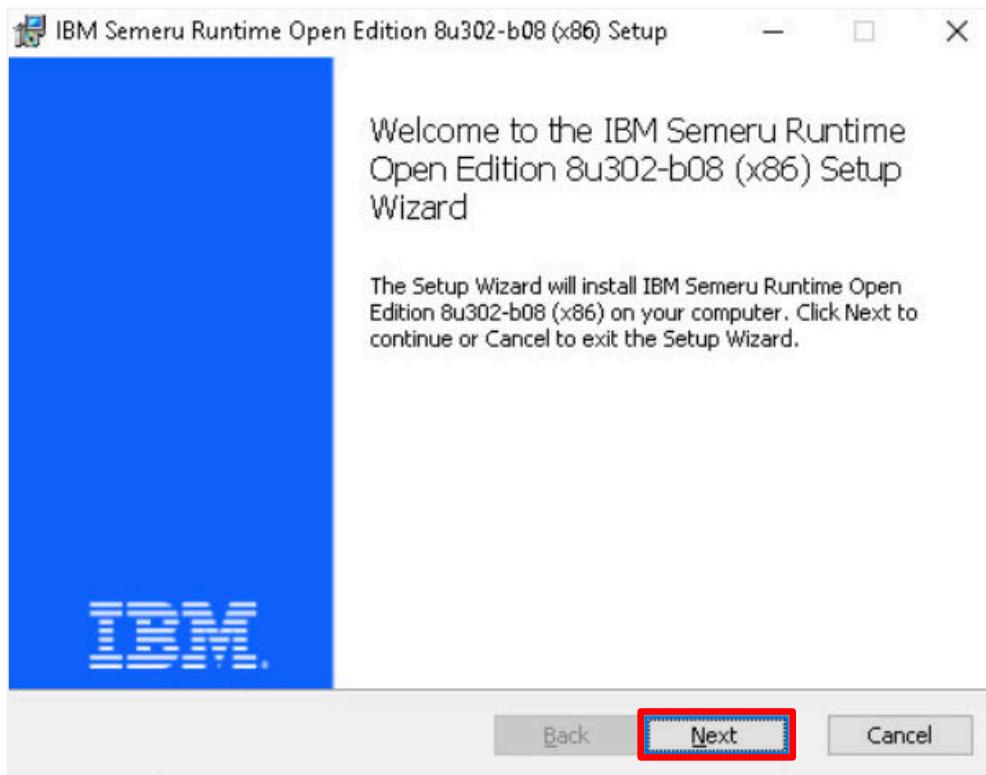
18. In the *Toolbox* folder, find the **open-jre\_x86-32\_windows\_8u302b08** application and double-click to install.



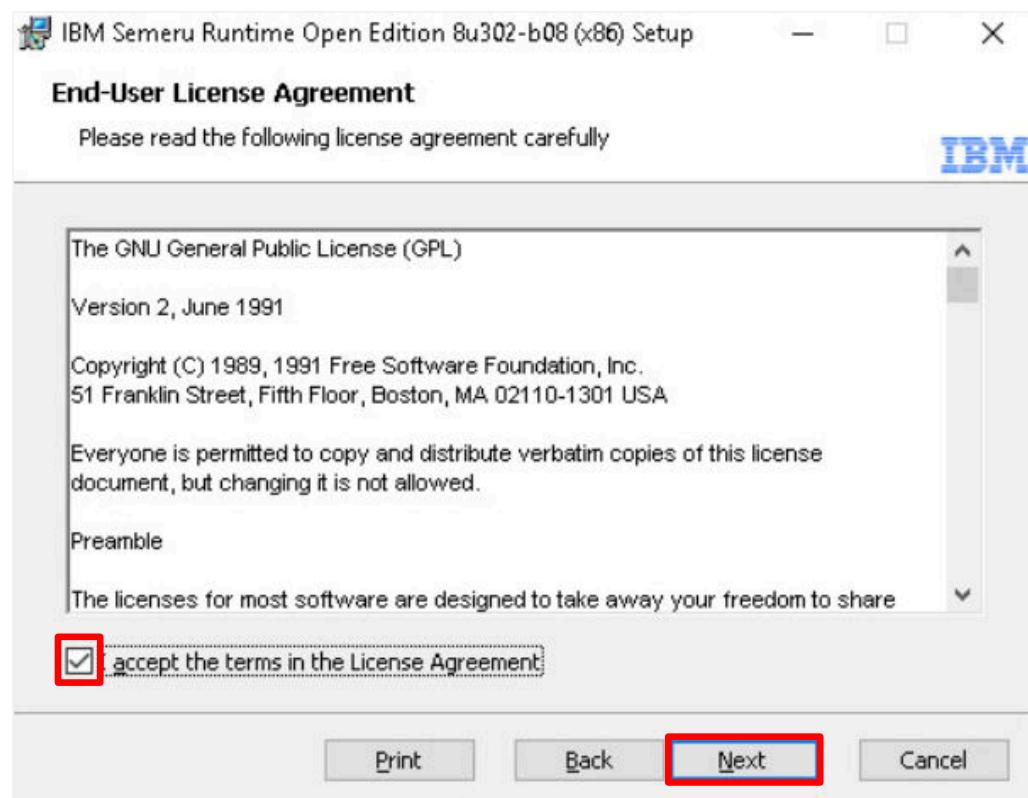
19. On the *Open File – Security Warning* window, click **Run**.



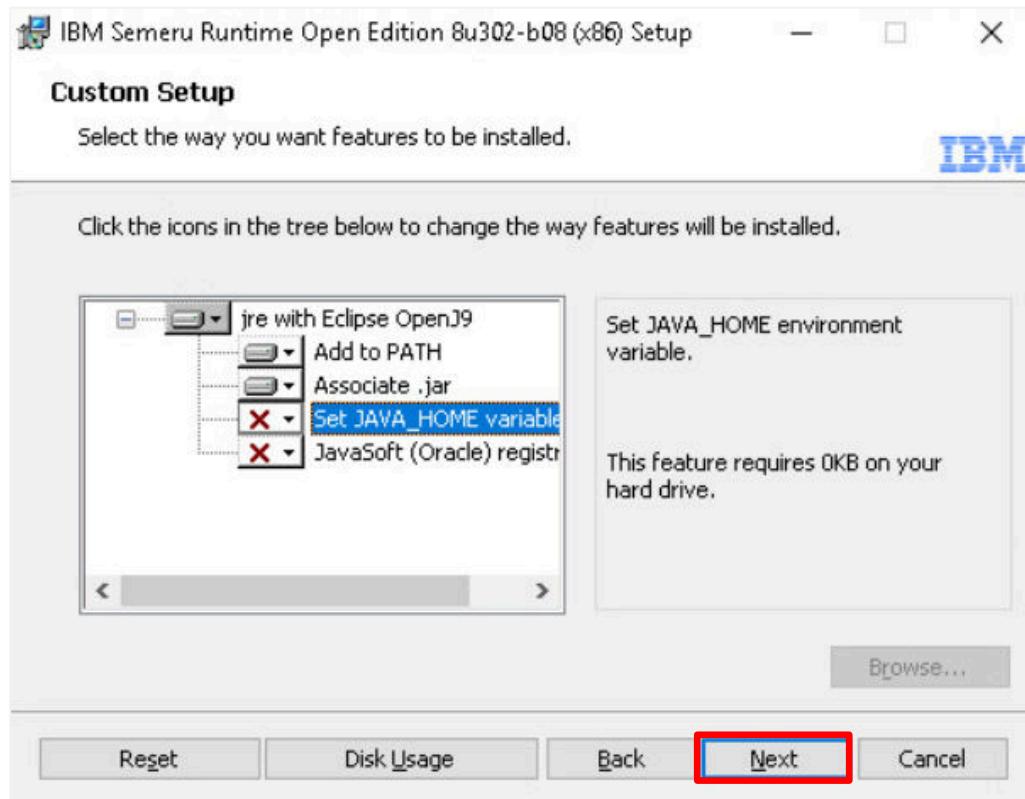
20. On the *Welcome* window, click **Next**.



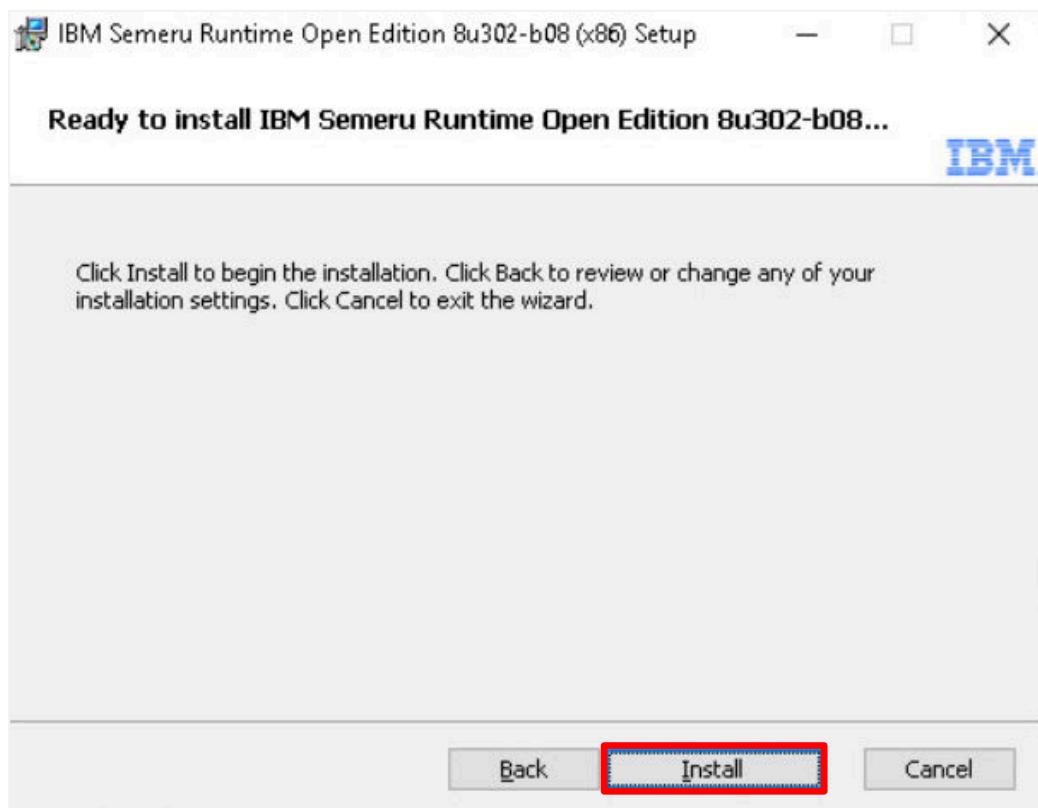
21. On the *License Agreement* window, click the **I accept the terms in the License Agreement** checkbox and click **Next**.



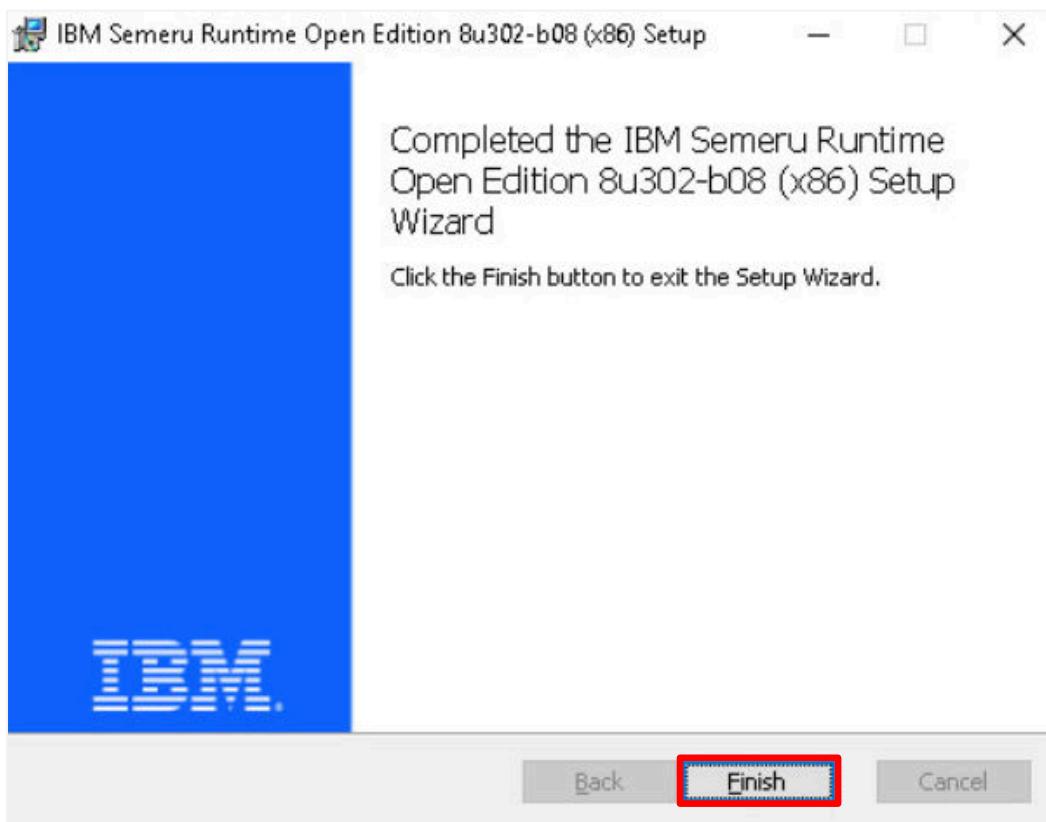
22. On the *Custom Setup* window, accept the defaults and click **Next**.



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

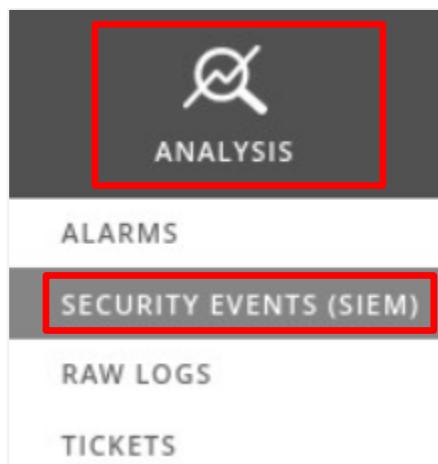


24. On the *Completed* window, click **Finish**.



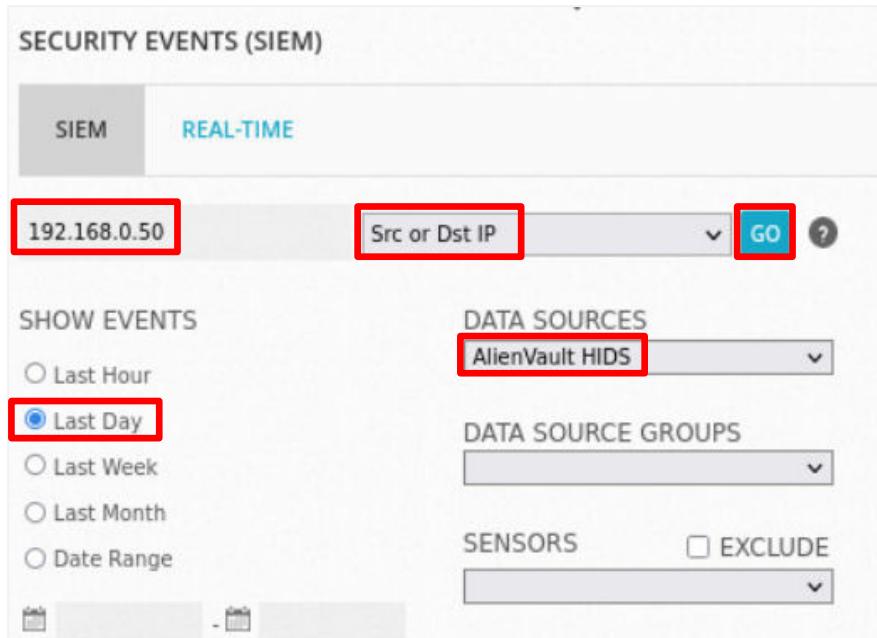
25. Set the focus back to the **MintOS** computer.

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**.



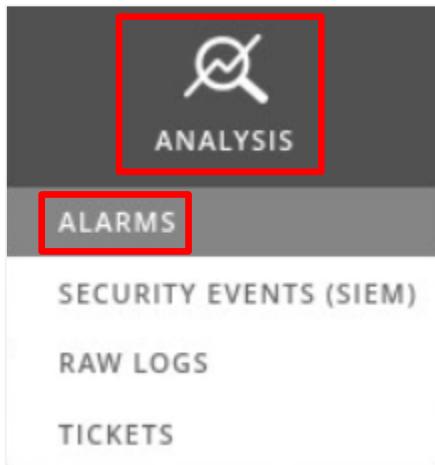
The screenshot shows the 'SECURITY EVENTS (SIEM)' page. At the top, there are two tabs: 'SIEM' (selected) and 'REAL-TIME'. Below the tabs, there is a search bar with the IP address '192.168.0.50' and a dropdown menu set to 'Src or Dst IP'. To the right of the search bar is a blue 'GO' button. Under the search bar, there are two sections: 'SHOW EVENTS' and 'DATA SOURCES'. In 'SHOW EVENTS', the 'Last Day' radio button is selected. In 'DATA SOURCES', the dropdown menu is set to 'AlienVault HIDS'. There are also sections for 'DATA SOURCE GROUPS', 'SENSORS', and an 'EXCLUDE' dropdown.

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*

EVENT NAME	DATE GMT-4:00
AlienVault HIDS: Application Installed.	2022-06-15 04:00:27
AlienVault HIDS: AppLocker allowed an MSI or script to execute	2022-06-15 04:00:22

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



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

DATE	▼	STATUS	◆	INTENT & STRATEGY	◆	METHOD	◆	RISK	◆
2022-06-15 04:00:22		open		AlienVault HIDS: AppLocker allowed an MSI or script to execute				LOW (1)	

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

## 2.5 Compile and Generate HIDS Reports

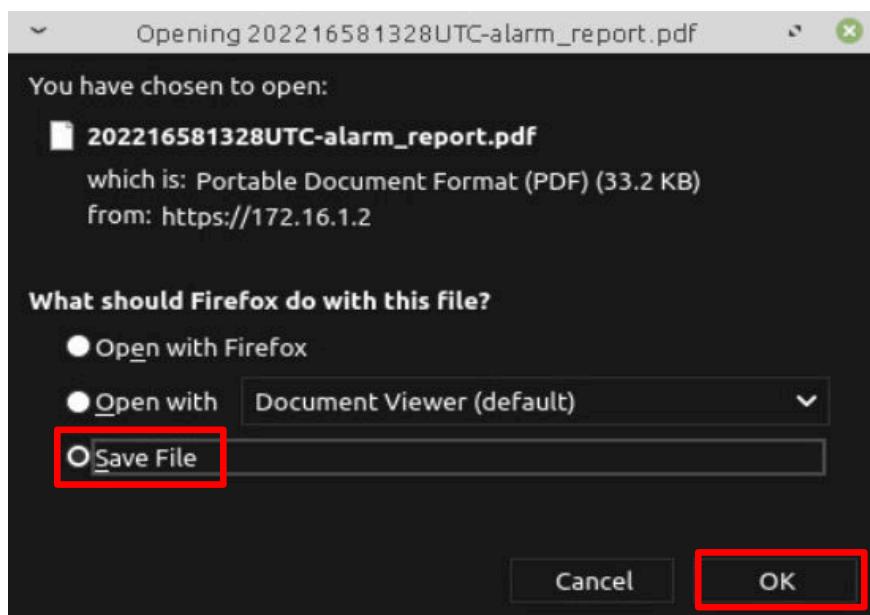
1. Set the focus to the MintOS computer.
2. Hover over the **REPORTS** button on the menu bar and click on **OVERVIEW**.



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.

REPORT NAME	REPORT OPTIONS	ACTIONS
<b>Alarms Report</b>	Date Range 2022-05-07 - 2022-06-06	<b>Download PDF</b> <b>Send by e-mail</b>

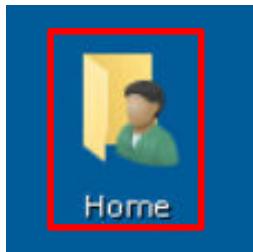
4. When the report is complete, make sure the **Save File** radio button is selected on the *What should Firefox do with this file?* popup window and click the **OK** button.



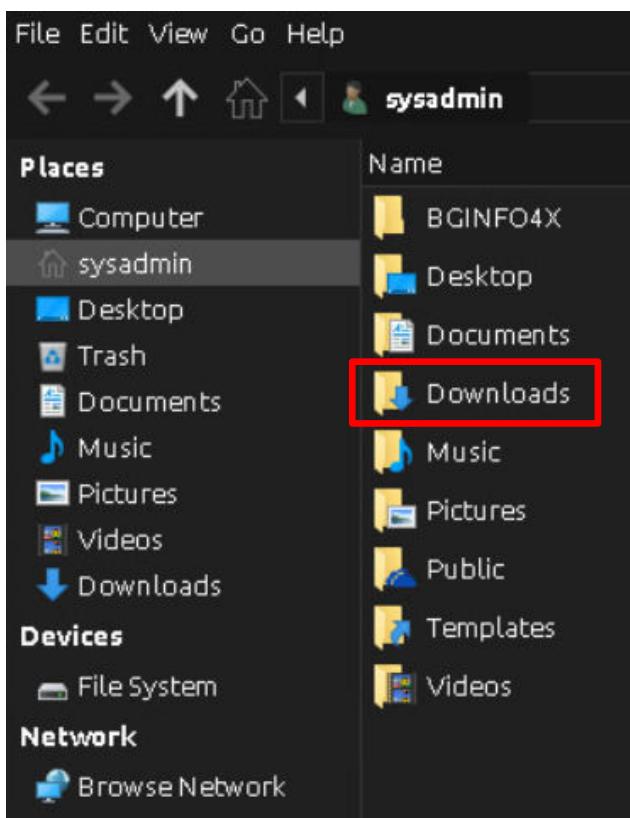
5. Minimize the web browser.

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

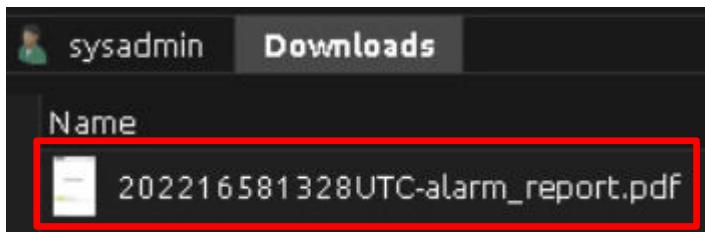
- Double-click on the **Home** folder on the *MintOS* desktop.



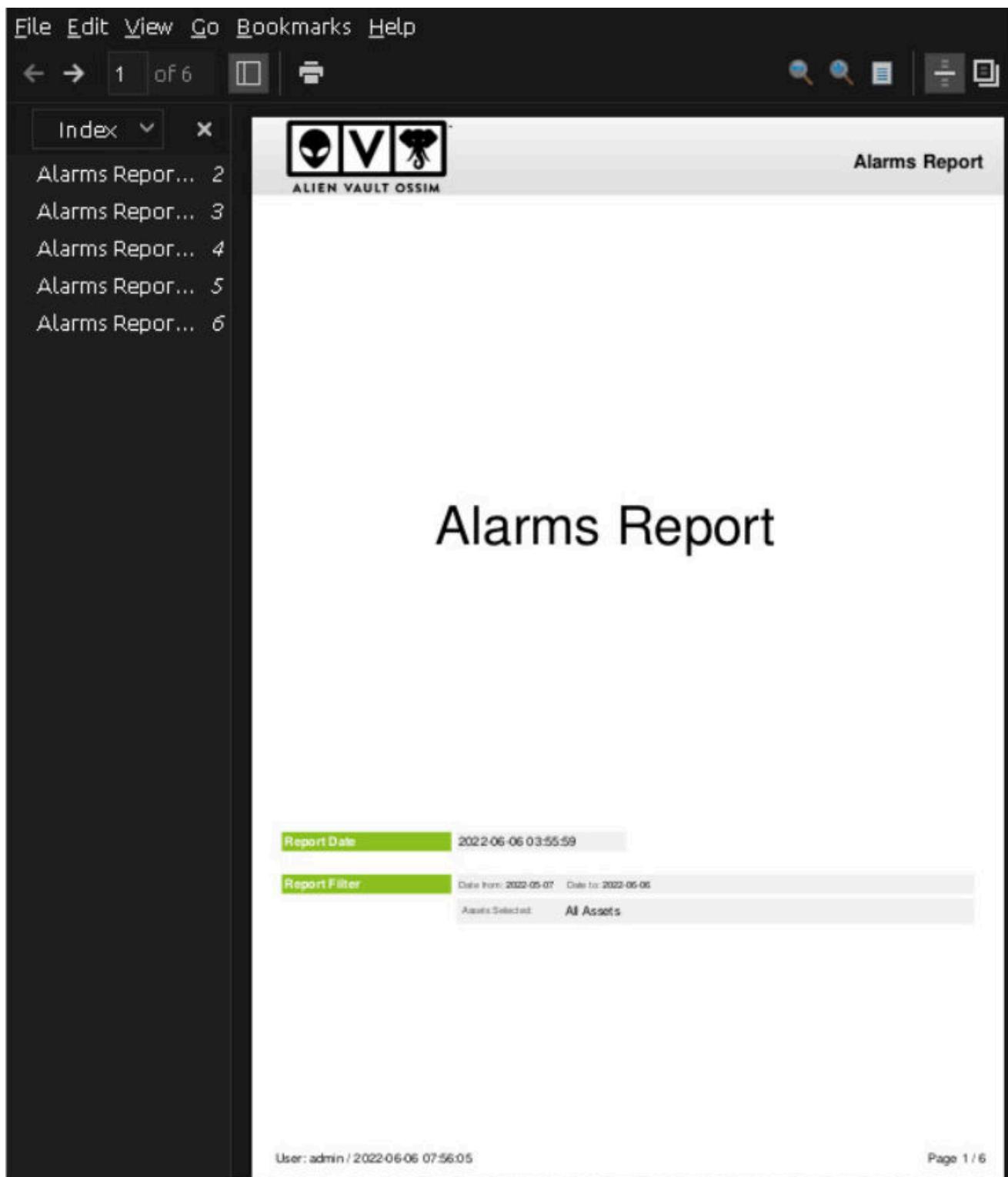
- In the **sysadmin** window, double-click on the **Downloads** folder.



- 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.



The screenshot shows a web-based report interface for AlienVault OSSIM. At the top, there's a navigation bar with links for File, Edit, View, Go, Bookmarks, and Help. Below the navigation is a toolbar with icons for back, forward, search, and print. On the left, a sidebar titled "Index" lists six reports, each starting with "Alarms Repor...". The main content area features the "ALIEN VAULT OSSIM" logo at the top right. The title "Alarms Report" is centered below the logo. At the bottom of the main content area, there are two green buttons: "Report Date" showing "2022-06-06 03:55:59" and "Report Filter" showing "Date from: 2022-05-07 Date to: 2022-06-06 Assets Selected: All Assets". At the very bottom of the page, it says "User: admin / 2022-06-06 07:56:05" and "Page: 1 / 6".

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