



Course: CYB301
Security Defense and Response
(Canadian Context)

Lab 9: Software & Hardware Development Security and
SIEM

Coordinator and Instructor: Muhammad
Siddiqui

Student: Saiprasad Raman (23074624)

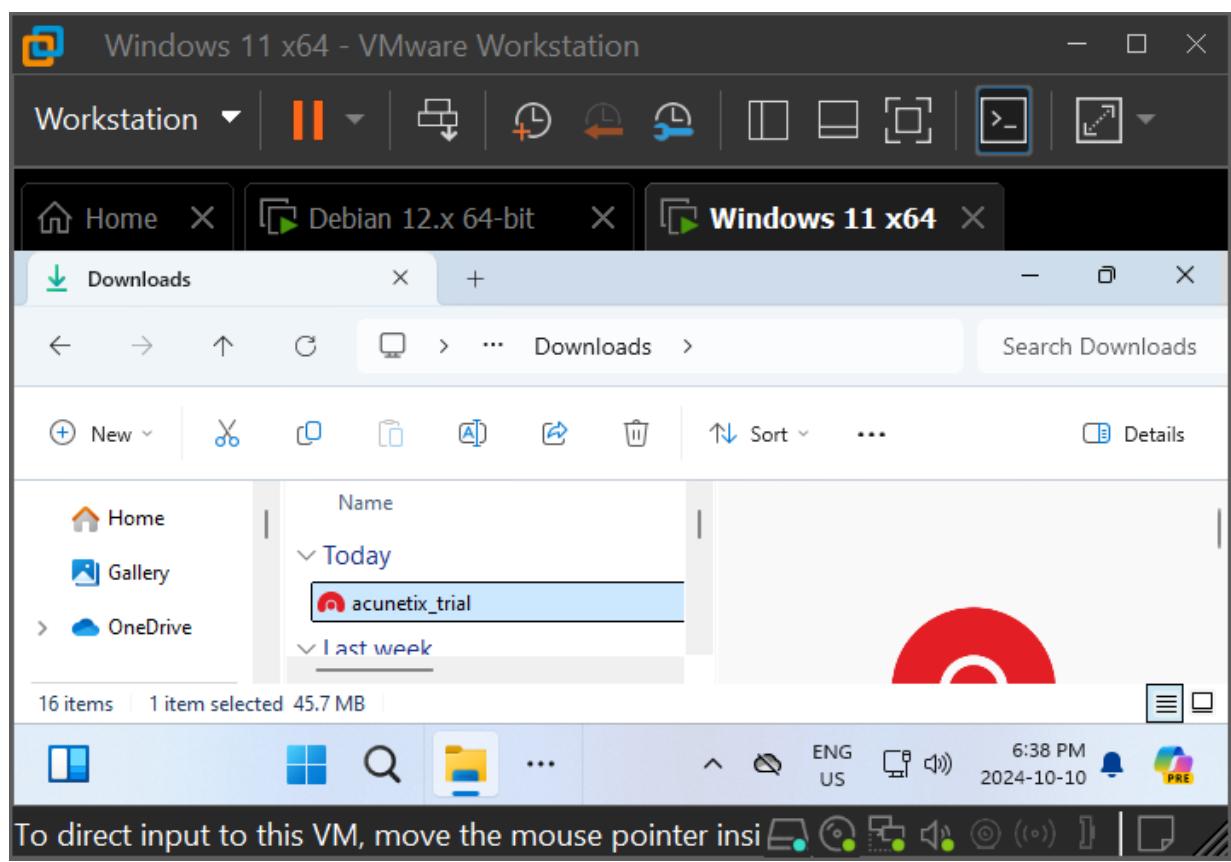
Activity 1: Review an Application Using the OWASP Application Security Architecture.

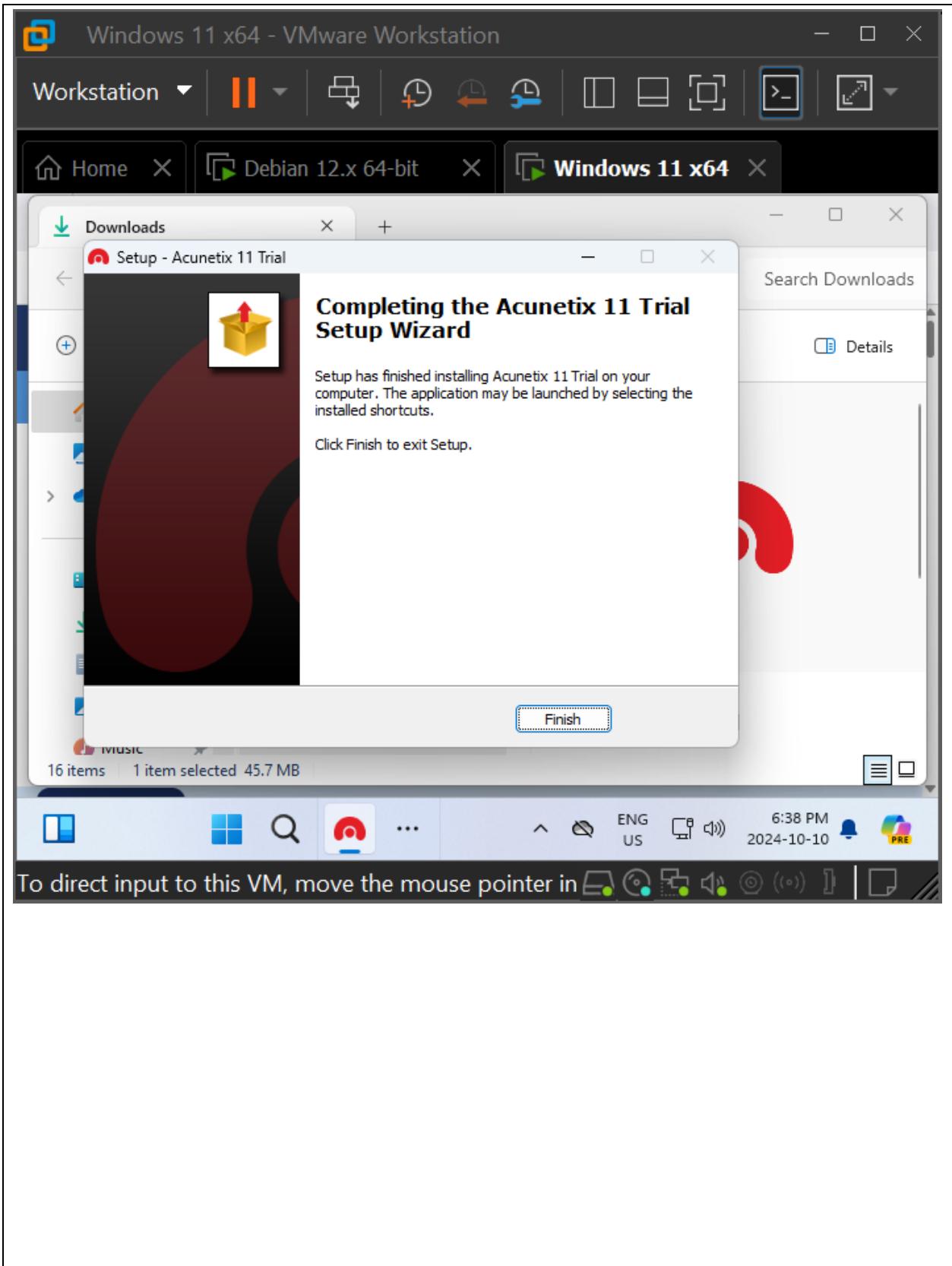
Cheat Sheet

In this exercise, you will use the Acunetix web vulnerability scanner to scan a sample site and then review the data generated.

Part 1: Download and install the Acunetix scanner.

Acunetix provides their Web Vulnerability scanner as a 14-day limited term trial download. You can download it at www.acunetix.com/vulnerability-scanner/download/





Part 2: Select an application and scan it.

When you download the Acunetix scanner, you will receive an email listing Acunetix-hosted vulnerable sites. Select one of these sites and use the vulnerability scanner to scan it. Once it is complete, review the report that was generated by the scan.

The screenshot shows the Acunetix web interface running in a VMware Workstation window. The browser tab is titled "Windows 11 x64 - VMware Workstation". The main page displays a "Scan Stats & Info" card with the following details:

Scan Duration	Requests	Avg. Response Time	Locations
4m 4s	4,551	113ms	19

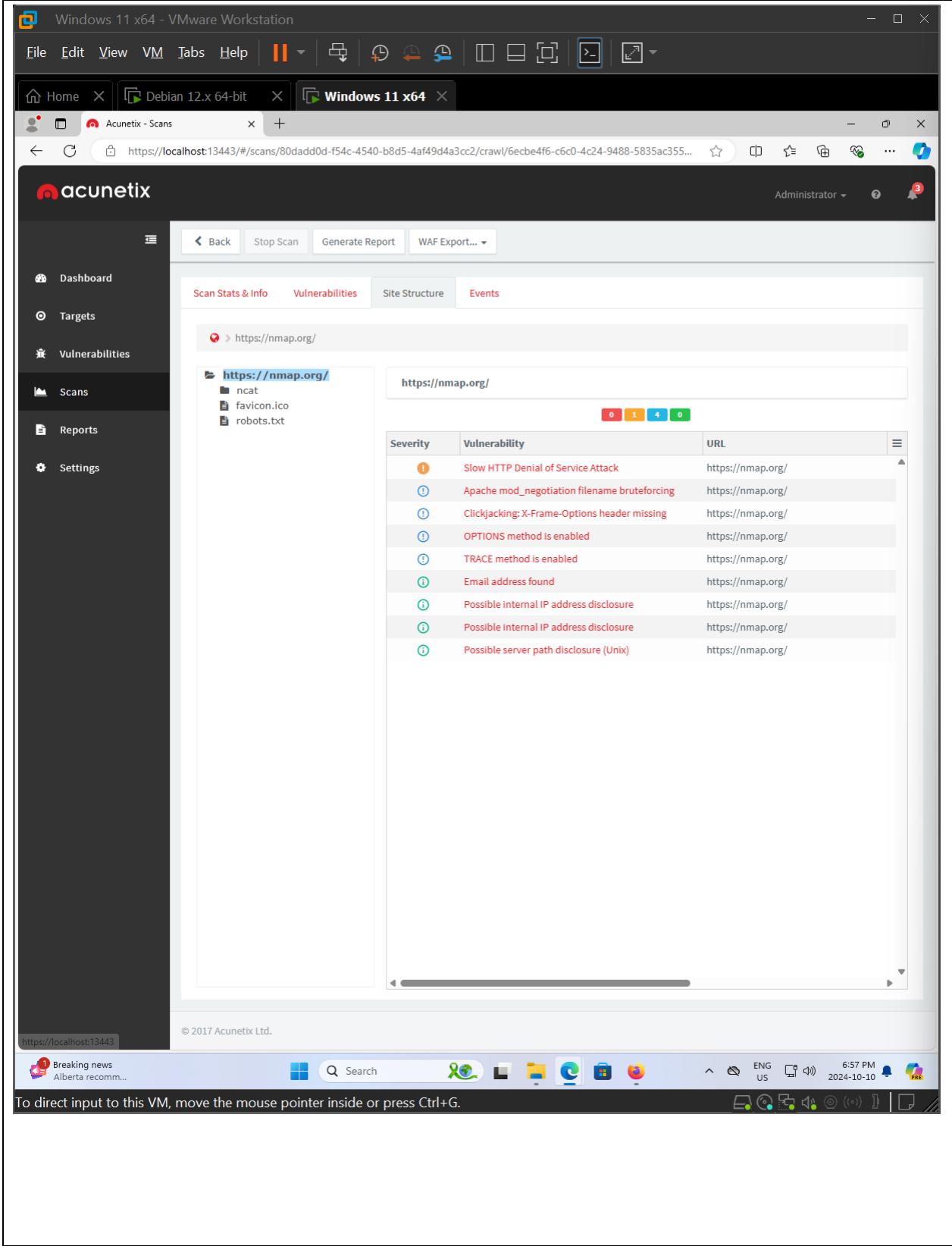
Below this, there are sections for "Target Information" and "Latest Alerts". The "Target Information" table includes:

Address	Server	Operating System	Identified Technologies	Responsive
nmap.org	Apache 2.x	Unix	—	Yes

The "Latest Alerts" section lists five findings:

Alert Type	Description	Date
Slow HTTP Denial of Service Attack	Oct 10, 2024 6:46:02 PM	
Possible internal IP address disclosure	Oct 10, 2024 6:46:24 PM	
Possible internal IP address disclosure	Oct 10, 2024 6:46:26 PM	
Possible server path disclosure (Unix)	Oct 10, 2024 6:46:29 PM	
Email address found	Oct 10, 2024 6:48:54 PM	

At the bottom left, a note says "To direct input to this VM, move the mouse pointer inside or press Ctrl+G." The bottom right corner shows the VMware status bar with "6:58 PM 2024-10-10".



Part 3: Analyze the scan results.

Review the scan results and answer the following questions.

1. What is the most critical vulnerability? How can it be remediated?

Ans.

Vulnerability: The web server is vulnerable with exposure to path while not having any authentication in place.

Remediation: 1. Using strong passwords to authenticate them.

2. Enable HTTPS protocol to encrypt the information
3. Update the softwares.

The screenshot shows a web browser window titled "Windows 11 x64 - VMware Workstation". The address bar indicates the user is on a local file path: "C:/Users/Sairprasad%20aman/Downloads/bd2b6160-ee07-42f8-958e-d34048e6465c.pdf". The main content area displays a security alert titled "Possible server path disclosure (Unix)". The alert states: "One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks." It also notes: "This alert may be a false positive, manual confirmation is required." Below this, there are two tables: one for CVSS2 and one for CVSS3. The CVSS2 table includes fields like Base Score, Access Vector, and Exploitability. The CVSS3 table includes fields like Target Distribution, Attack Vector, and Integrity Impact. A section for CWE lists "CWE-200" under "Affected item". The bottom of the page contains a section titled "(18.1.4) Privacy and protection of personally identifiable information" with a note about ensuring privacy according to relevant legislation and regulation where applicable. The status bar at the bottom of the browser window shows the date and time as "2024-10-10 7:02 PM".

4. What is the most common vulnerability (which occurs most often)? Is there a coding change you would recommend to the developers of this application to prevent it?

Ans. HTTP TRACE method is enabled on the web server which enables cross-domain vulnerabilities.

This could be prevented by turning it TRACE off in the Apache web server by adding TraceEnable directive into the httpd.conf and setting the value to off or by creating a mod_rewrite rule to disable http methods.

The screenshot shows a Windows 11 desktop environment within a VMware Workstation window. A browser window is open, displaying an alert message. The alert states: "TRACE method is enabled" and "HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method." It also notes: "This alert belongs to the following categories: 12.5.1". Below the alert, there is a table with CVSS2 details:

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
-------	---

Below the CVSS2 table, there is another table with CWE and Parameter details:

CWE	CWE-16
Parameter	Variations

At the bottom of the browser window, there is a status bar with the text: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

5. How would you protect this application if you were not able to change the code?

Ans.

1. Create a strong password for the web server
2. Change the protocol from HTTP to HTTPS.
3. Enable Multi Factor Authentication.
4. Create a NAT system in the server to stop the disclosure of the internal IP addresses.

Activity 2: Learn About Web Application Exploits from WebGoat.

OWASP in partnership with Mandiant provides the OWASP Broken Web Applications project virtual machine. This VM includes very vulnerable web applications as a VMware VM, including WebGoat, OWASP's web application vulnerability learning environment.

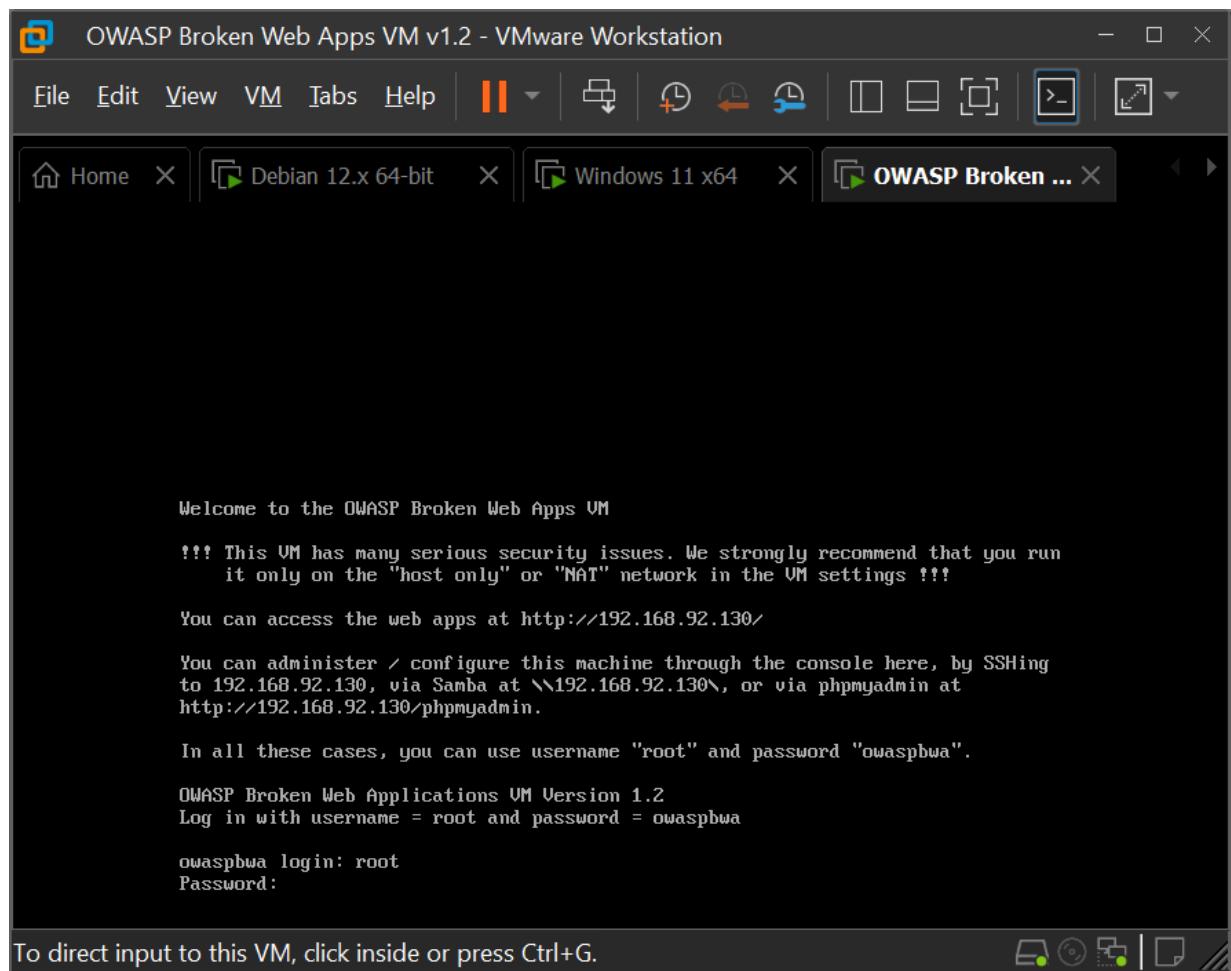
Step 1: Download the VMware VM.

Go to <https://sourceforge.net/projects/owaspbwa/files/1.2/>

Step 2: Run the VMware VM and start WebGoat.

Run the virtual machine using VMware —you can use the free vSphere Hypervisor from www.vmware.com/products/vsphere-hypervisor.html, or the 30-day demo of Workstation Player from www.vmware.com/products/player/playerpro-evaluation.html, if not previously downloaded/using.

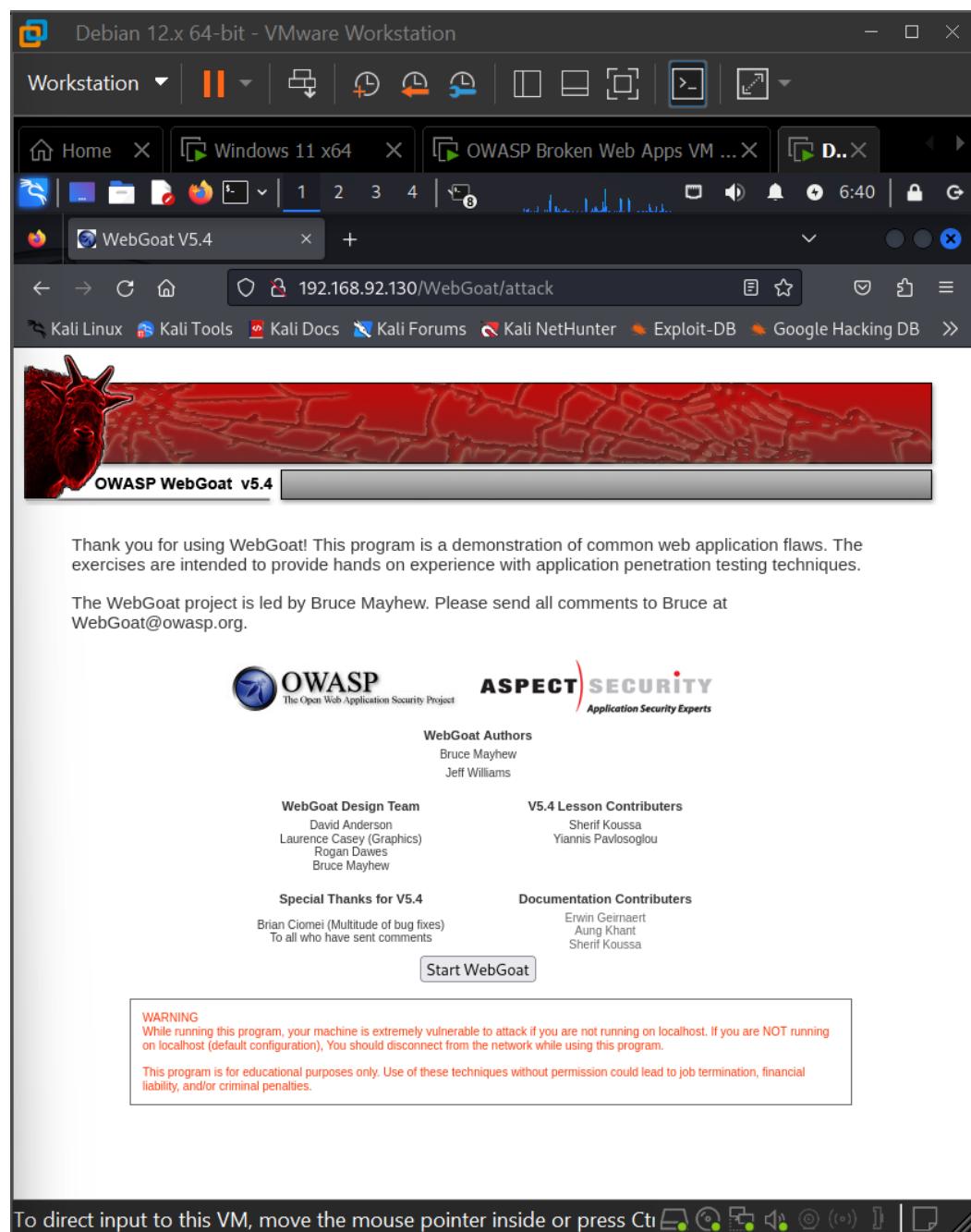
Once the VM starts, log in as root with the password **owaspbwa** and run **ifconfig** to determine your system's IP address.

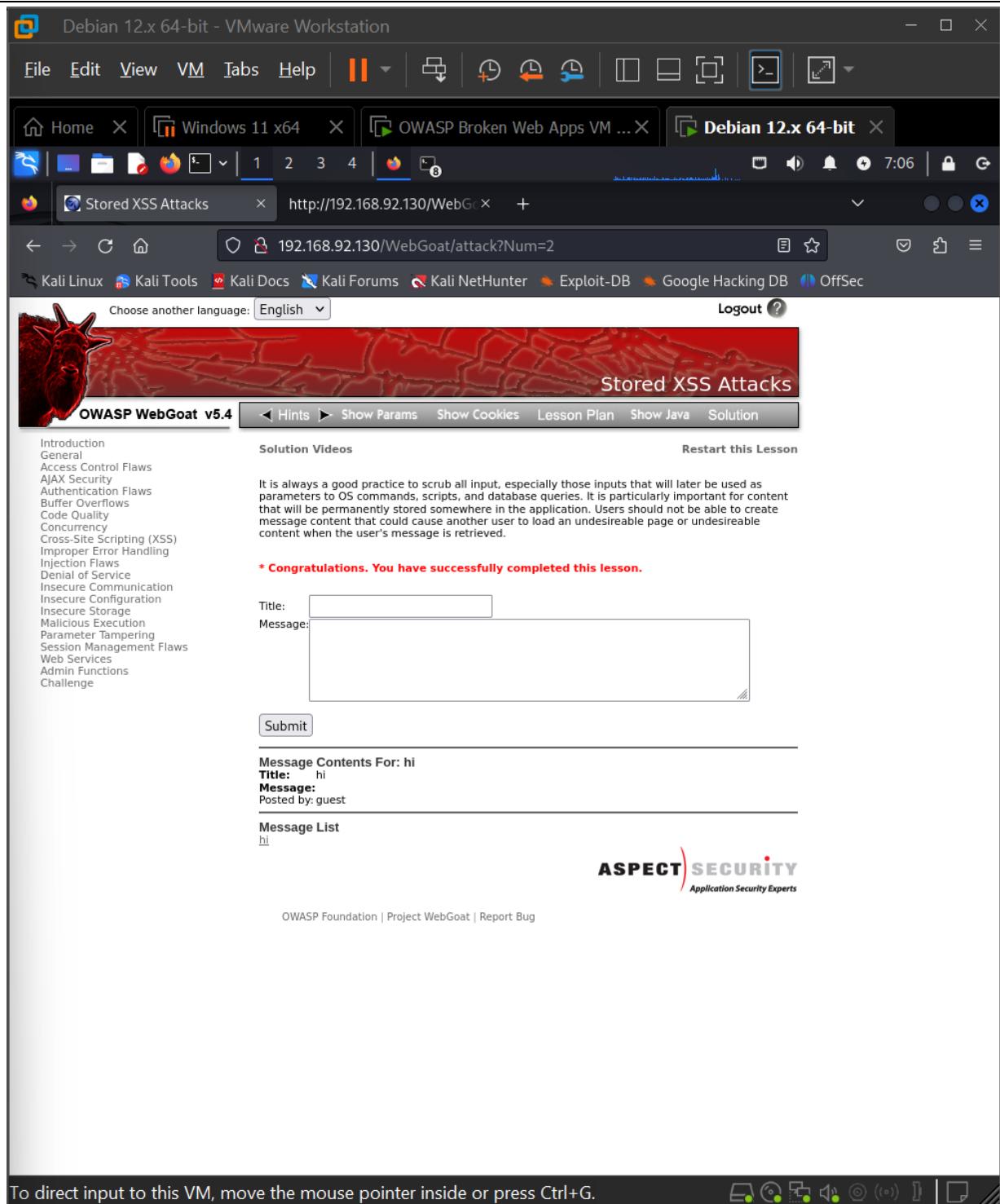


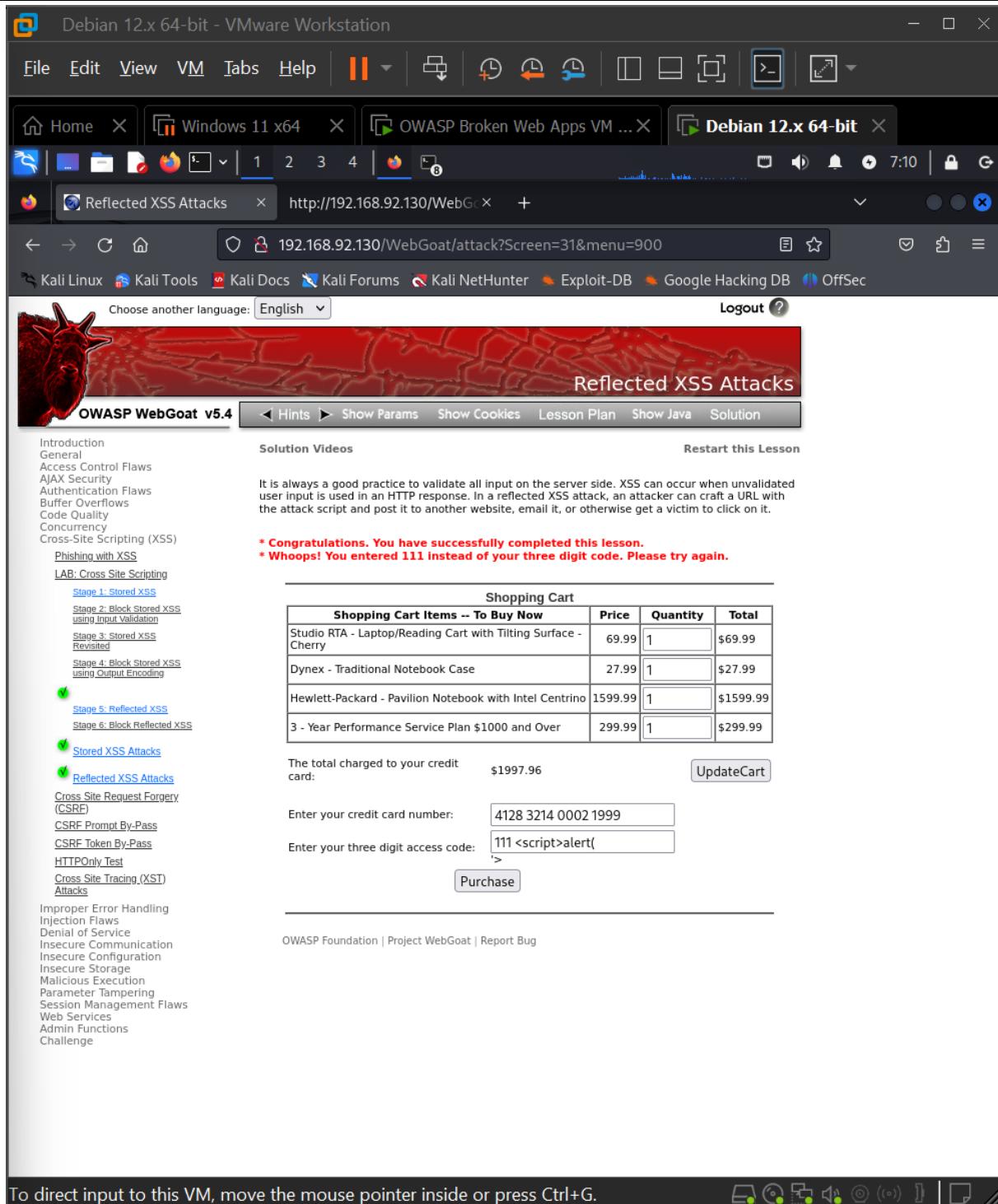


Step 3: Succeed with an attack.

WebGoat includes a multitude of vulnerable web application modules. Select one (or more!) and follow the instructions to attack the application. **Take the screenshot after the successful attack.** If you need help, review the WebGoat lesson plans and solutions at [https://github.com/WebGoat/WebGoat/wiki/\(Almost\)-Fully-Documented-Solution-\(en\)](https://github.com/WebGoat/WebGoat/wiki/(Almost)-Fully-Documented-Solution-(en)), or visit YouTube, where you will find numerous videos that show step-by-step guides to the solutions.





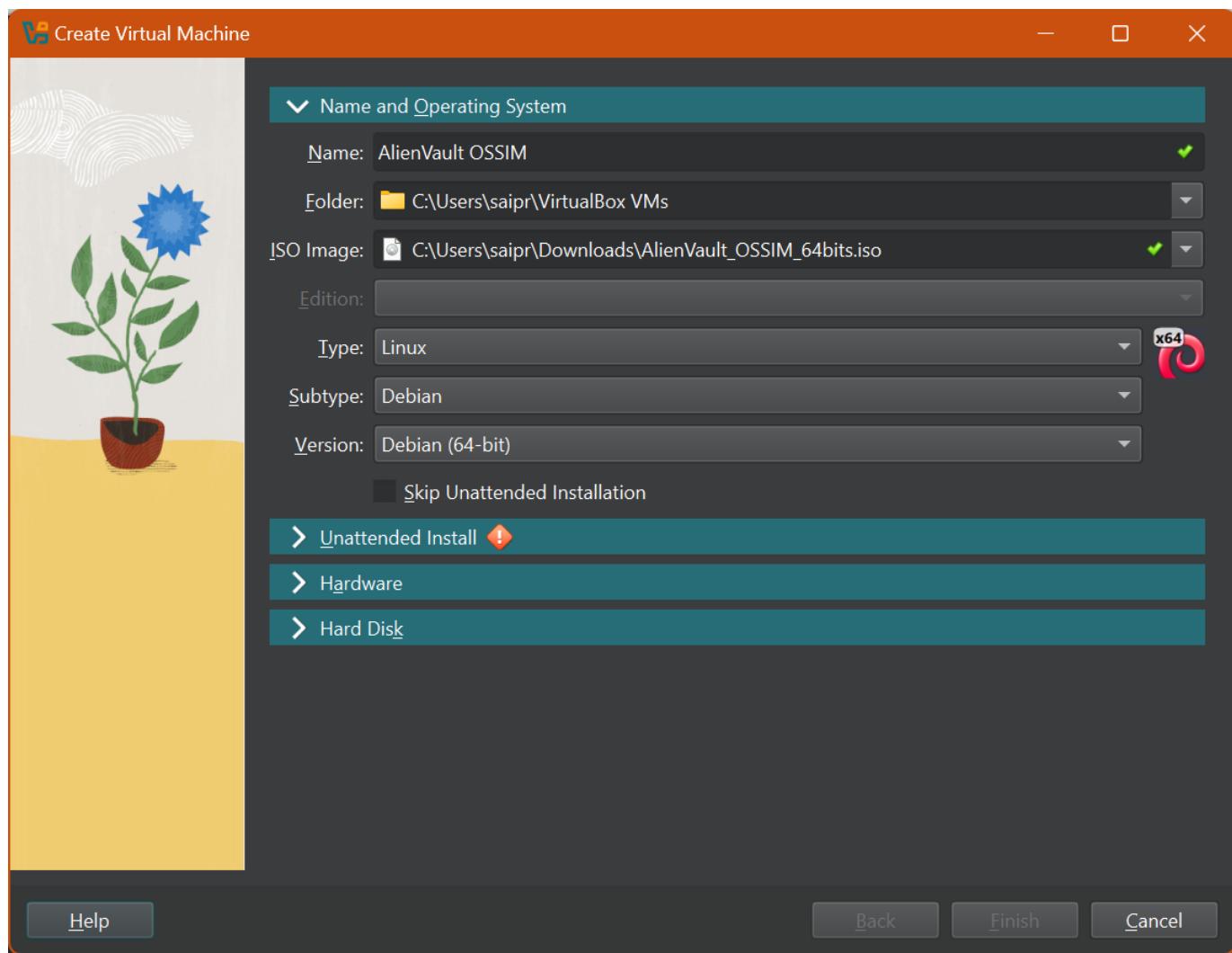


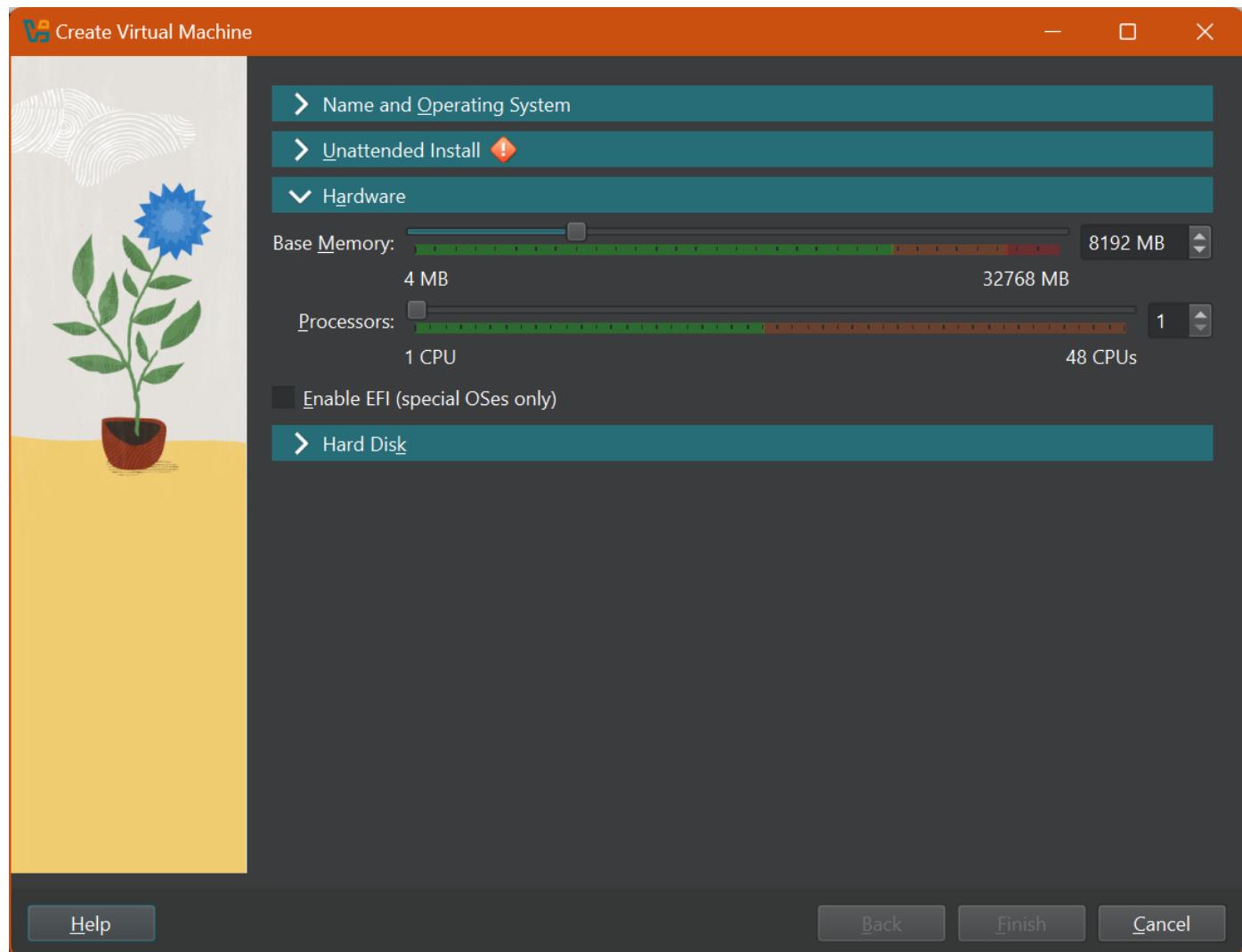
Activity 3: SIEM (Alienvault / Security Onion) - Oracle VirtualBox

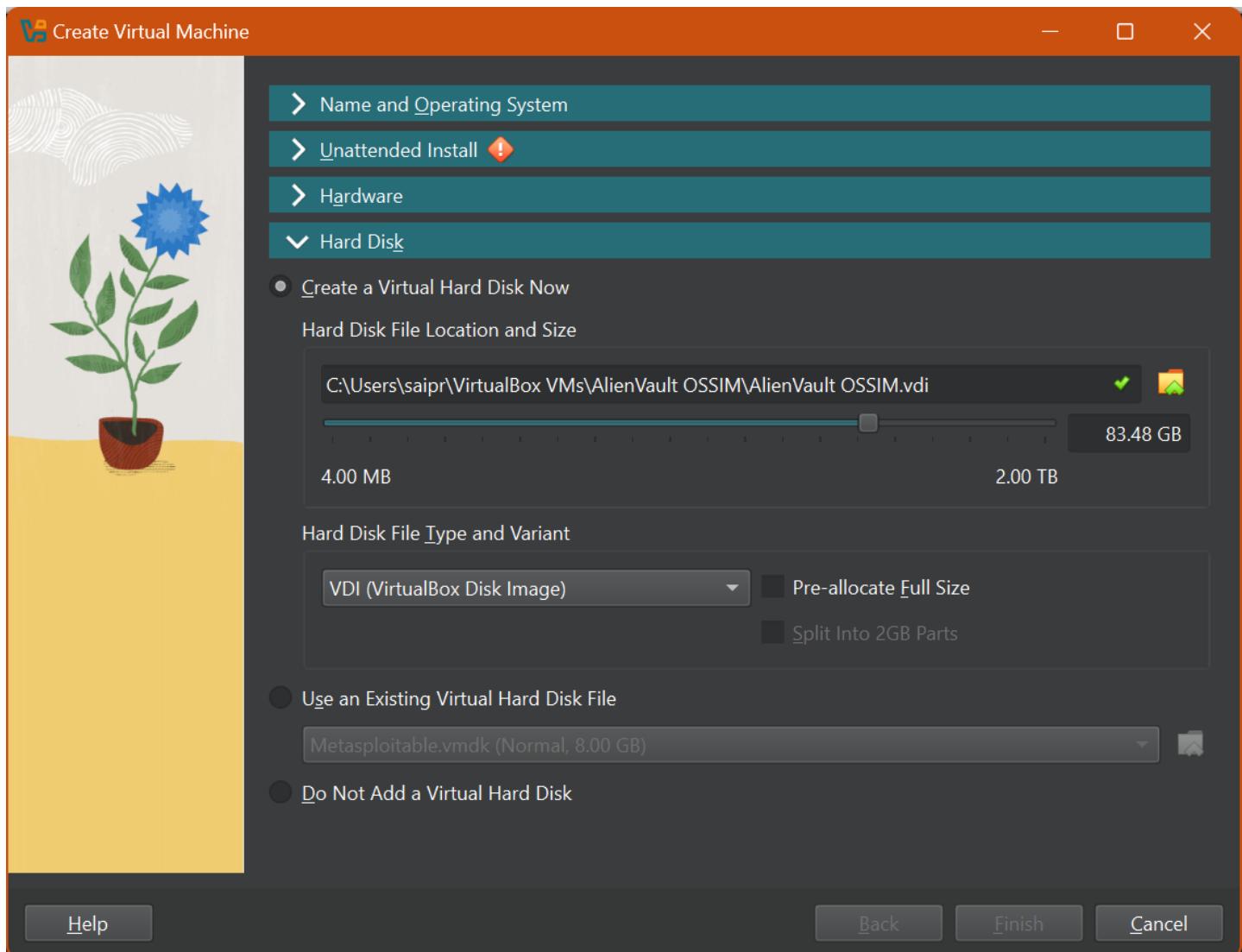
In this activity, we will use Oracle Virtual box to install SIEM (Alienvault OSSIM). You are required to download AlienVault OSSIM from the following link:

<https://cybersecurity.att.com/products/ossim>

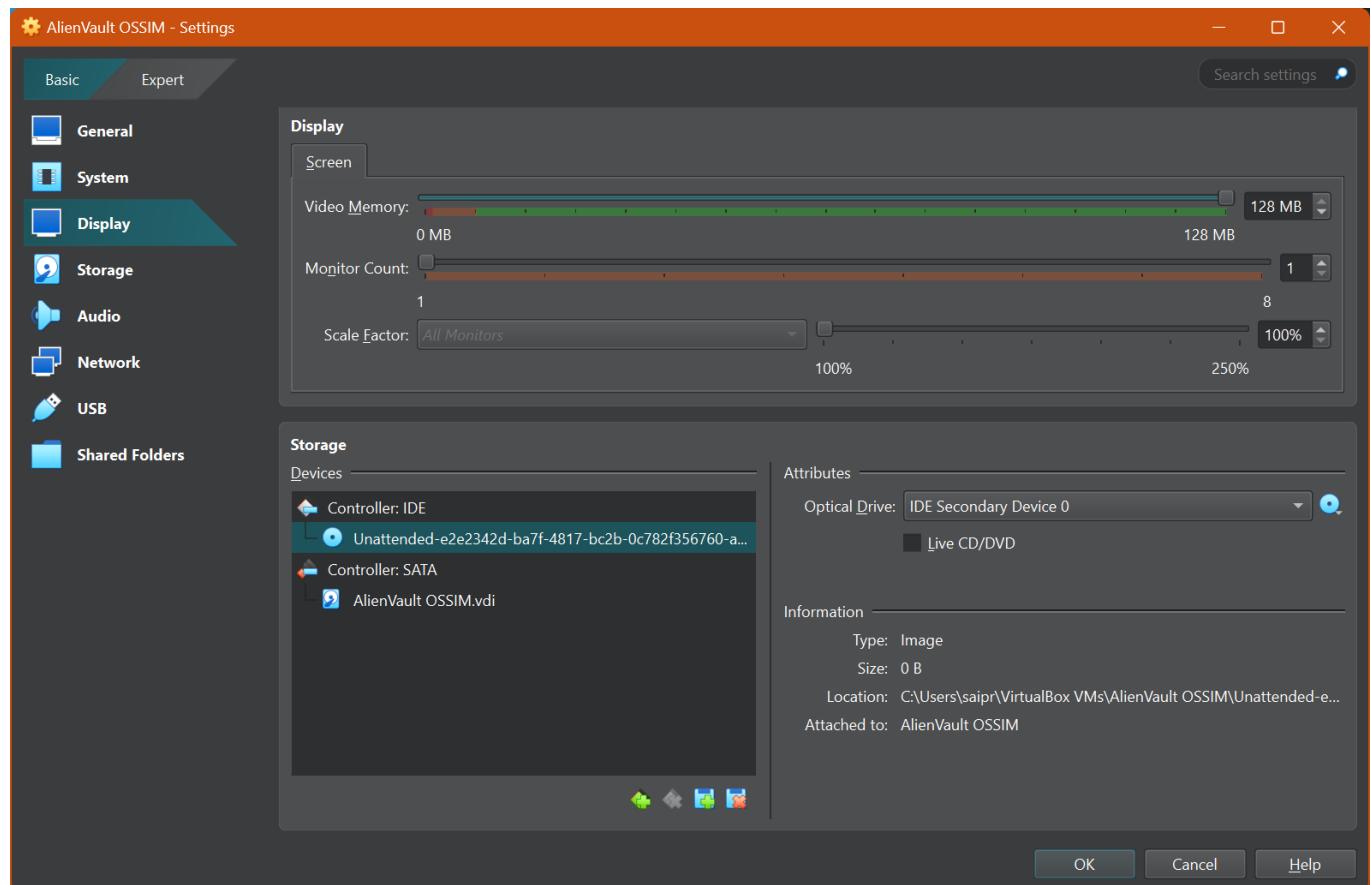
- Launch VirtualBox
- Create a New VM
 - **Name:** AlienVault OSSIM
 - **Type:** Linux
 - **Version:** Debian (64-bit)
 - **Memory Size (RAM):** 8192 MB (Allocate 8 GB)
 - **Hard Disk File Type:** VDI (VirtualBox Disk Image)
 - **Storage on physical hard disk:** Dynamically allocated



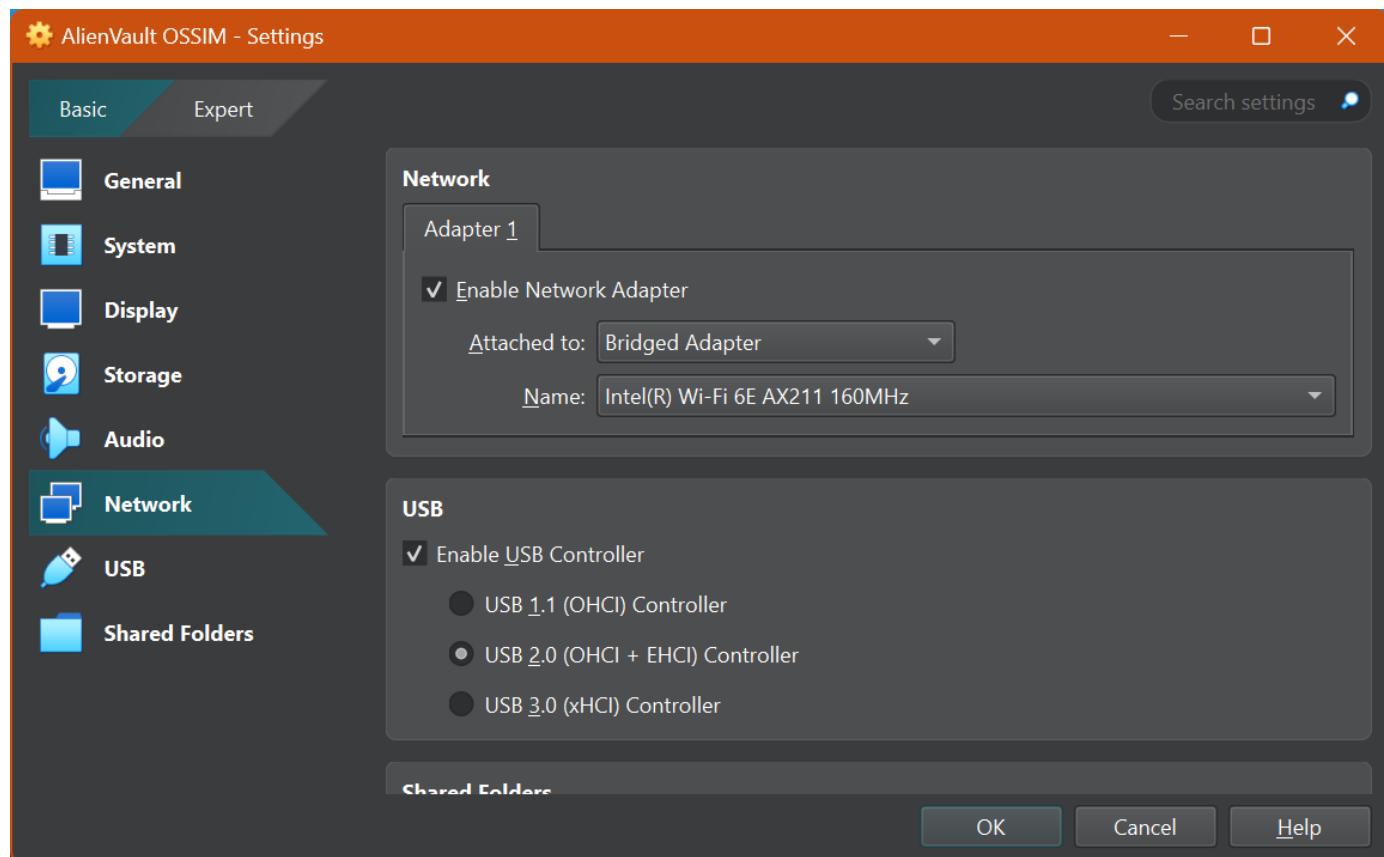




- Go to settings of AlienVault OSSIM VM:
 - **Display:** 128MB (for AlienVault Splash Screen, 128 MB is required)
 - **Storage:**
 - Controller: IDE
- Empty: Attach the AlienVault OSSIM iso file

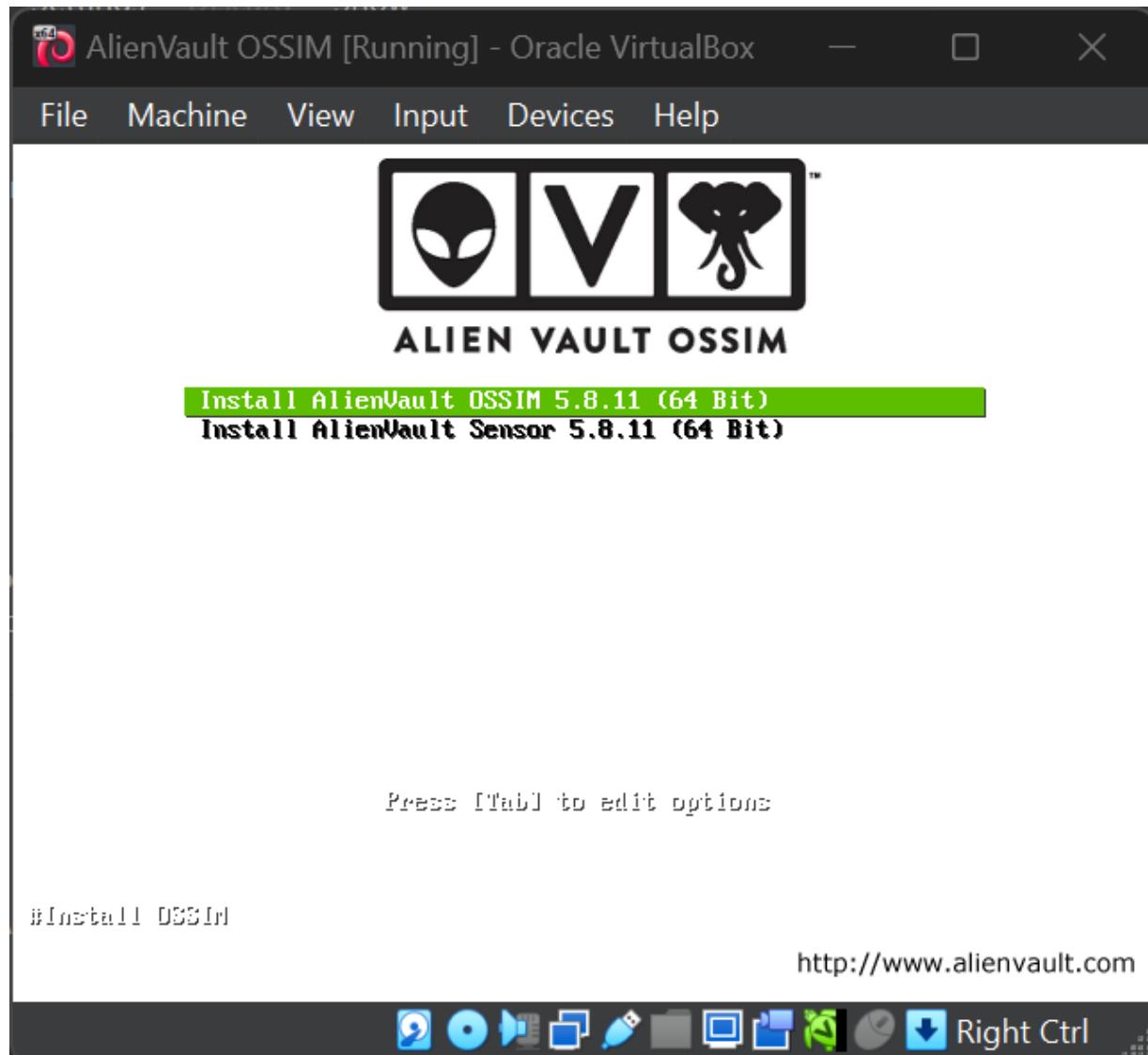


- **Network:** Bridged Adapter ○ Click **OK**.

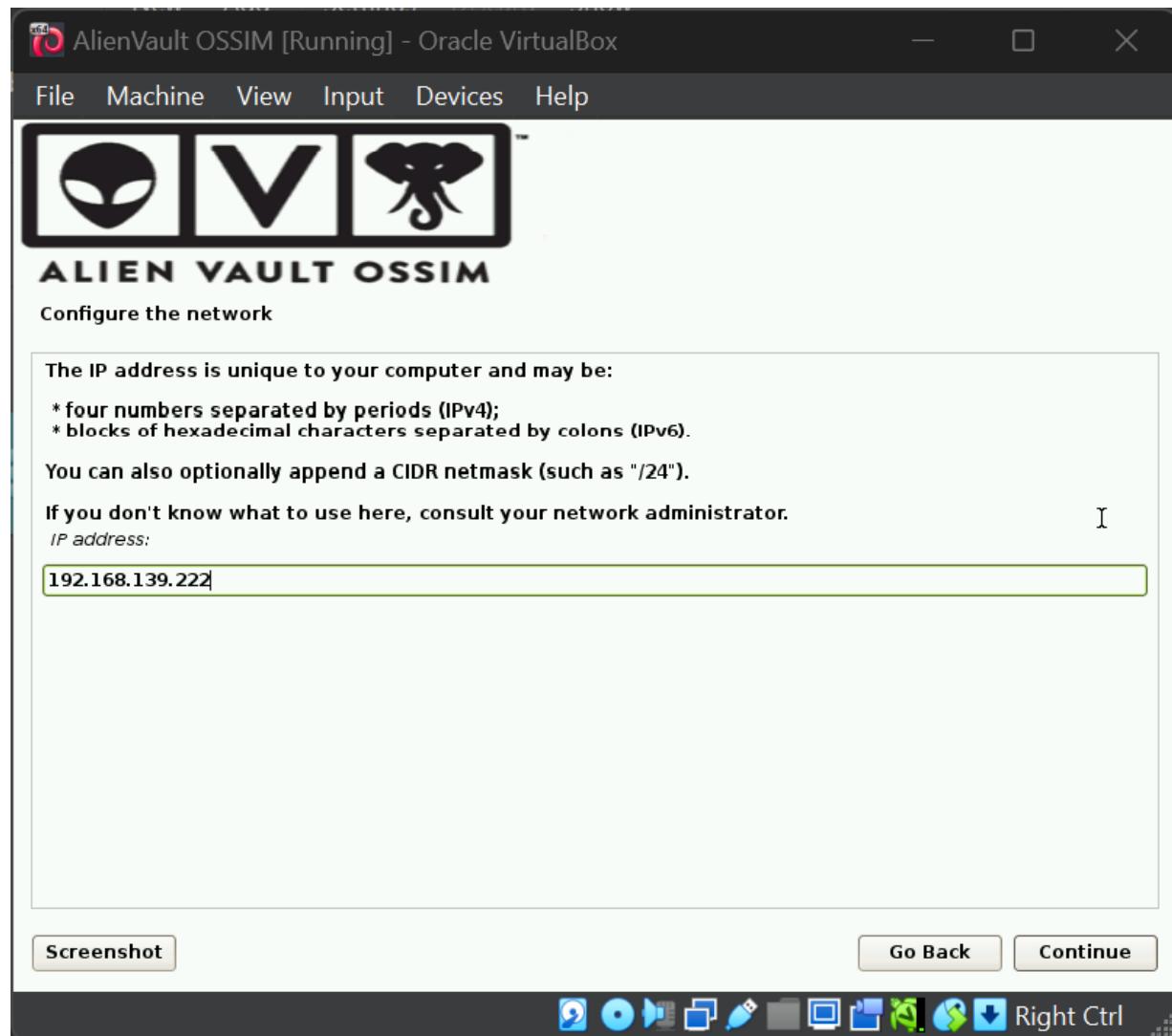


Start to install the AlienVault OSSIM VM ◦ Click on first option: **Install AlienVault OSSIM (64 Bit)**

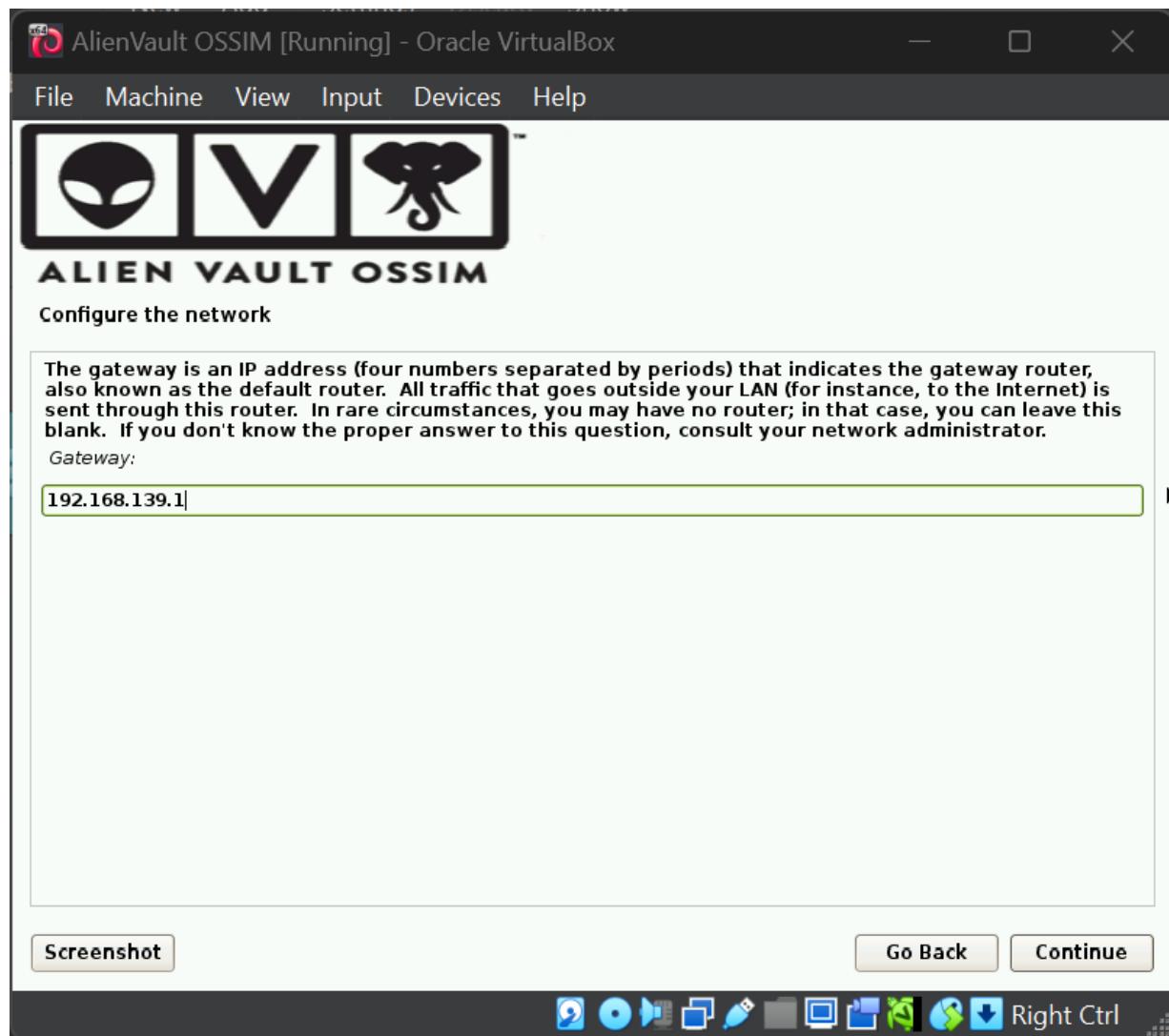
Note: Do not click on second option “Install AlienVault Sensor,” because the First Option AlienVault OSSIM is installed in head office and then AlienVault Sensor is installed in branch offices.



- **Select a language:** English ○ **Select your location:** Canada ○ **Configure the Keyboard:** American English
- **Configure the network:** Provide only un-used static IP address from your network, because AlienVault OSSIM does not take IP from DHCP.

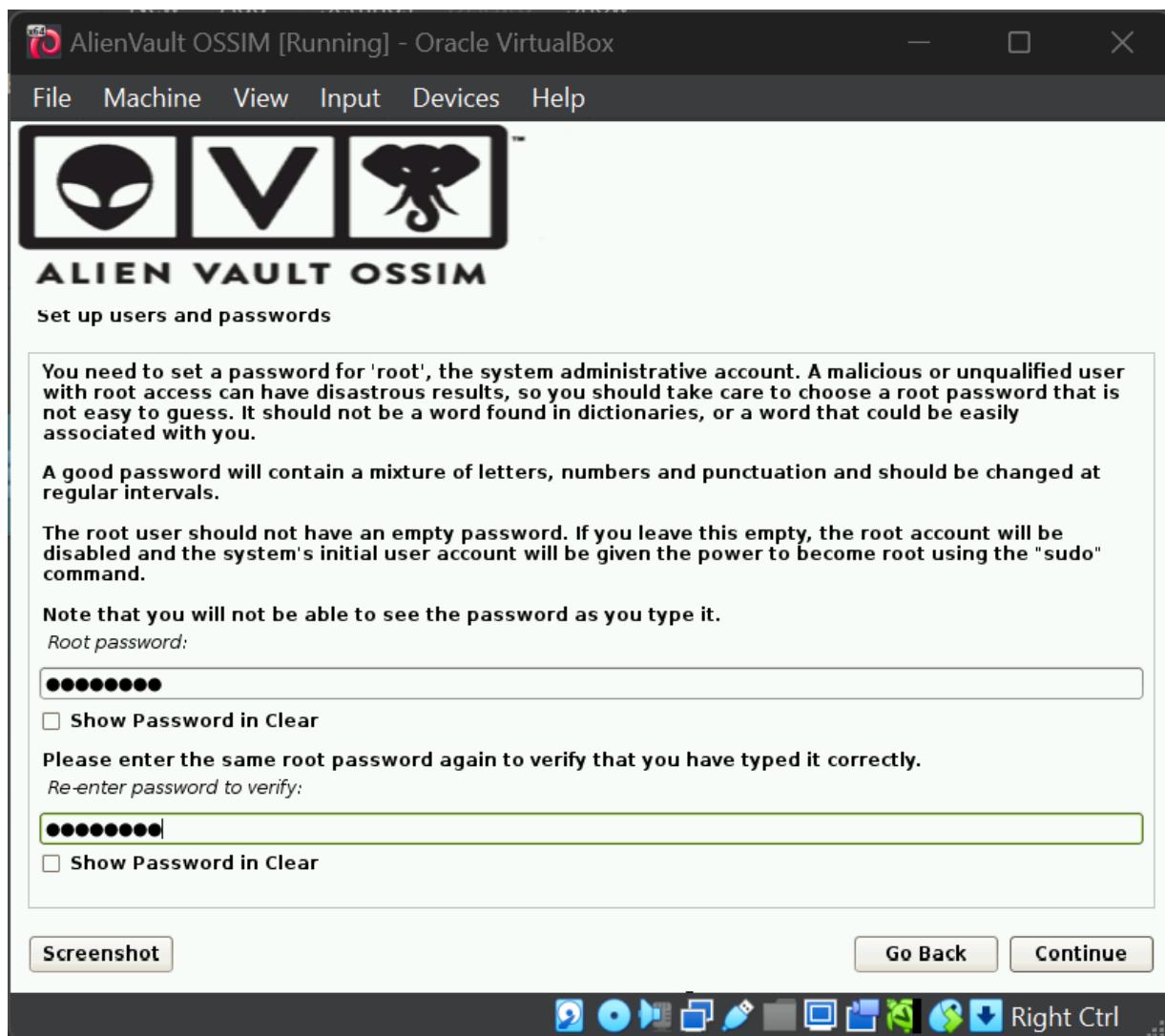


- **Subnet Mask:** (Keep the default) ○ **Gateway:** (Keep the default) ○ **DNS Server:** (Keep the default)

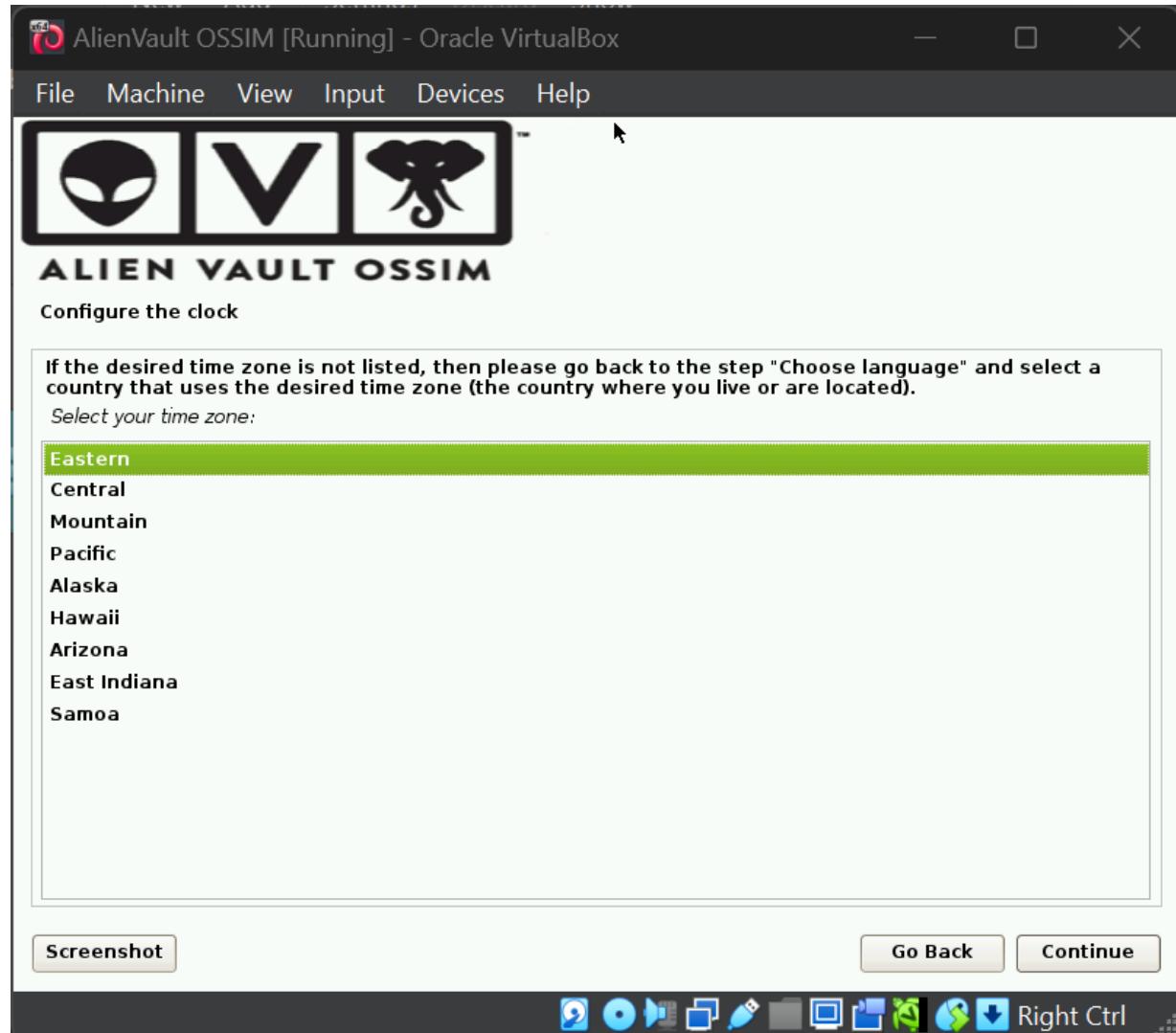


- Set up users and passwords:

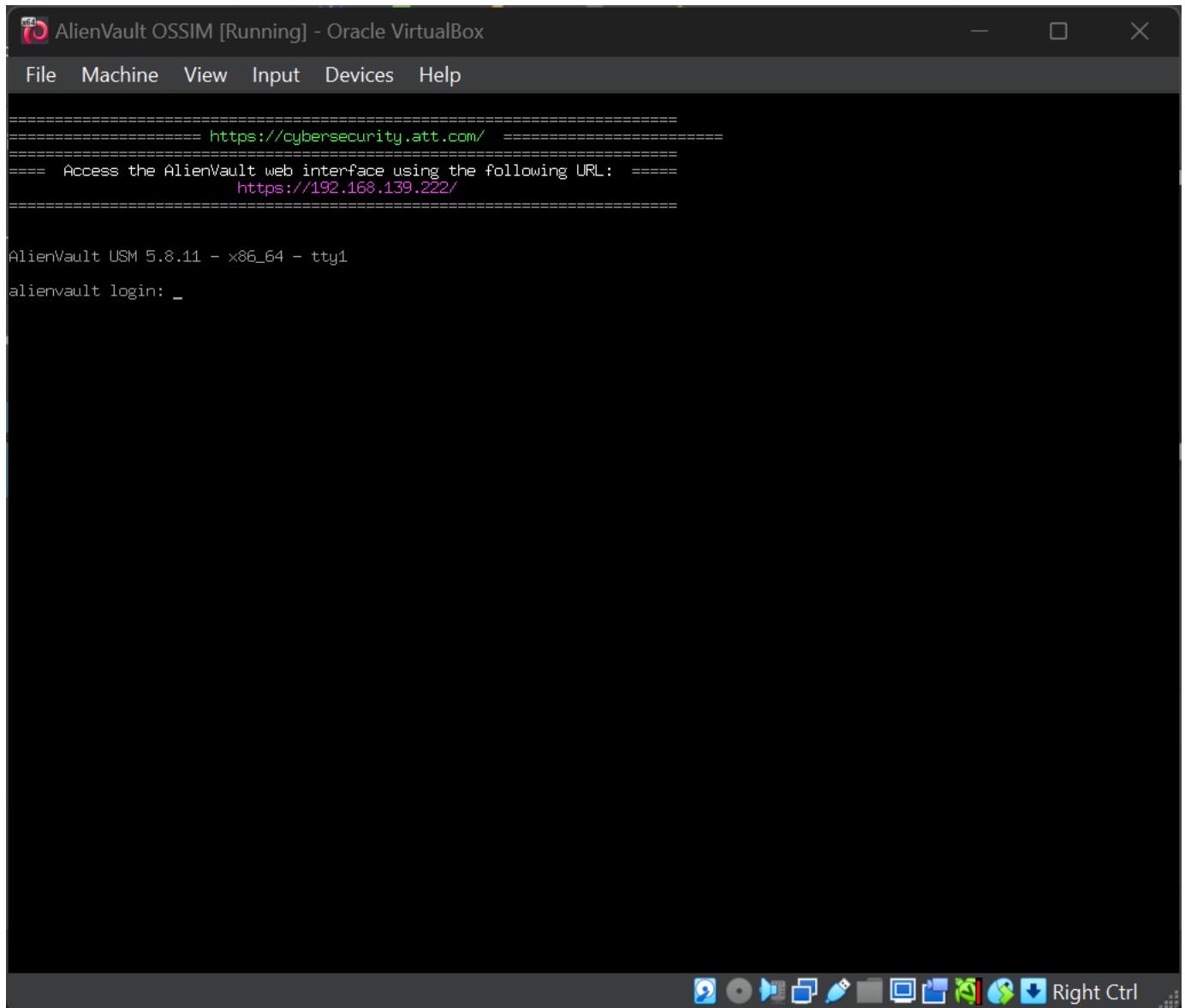
- Root Password: Alien123
- Re-enter Password: Aline123



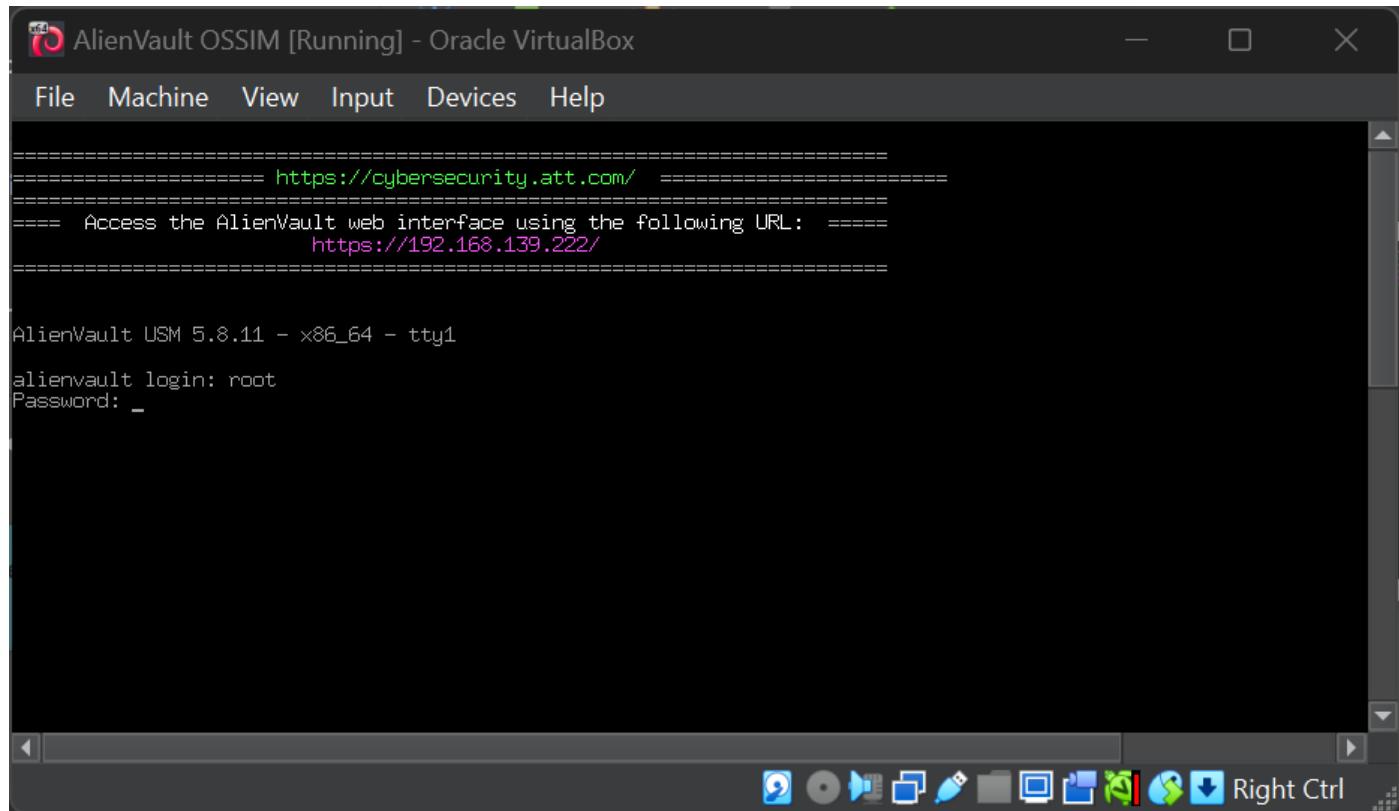
- o Configure the clock: Eastern



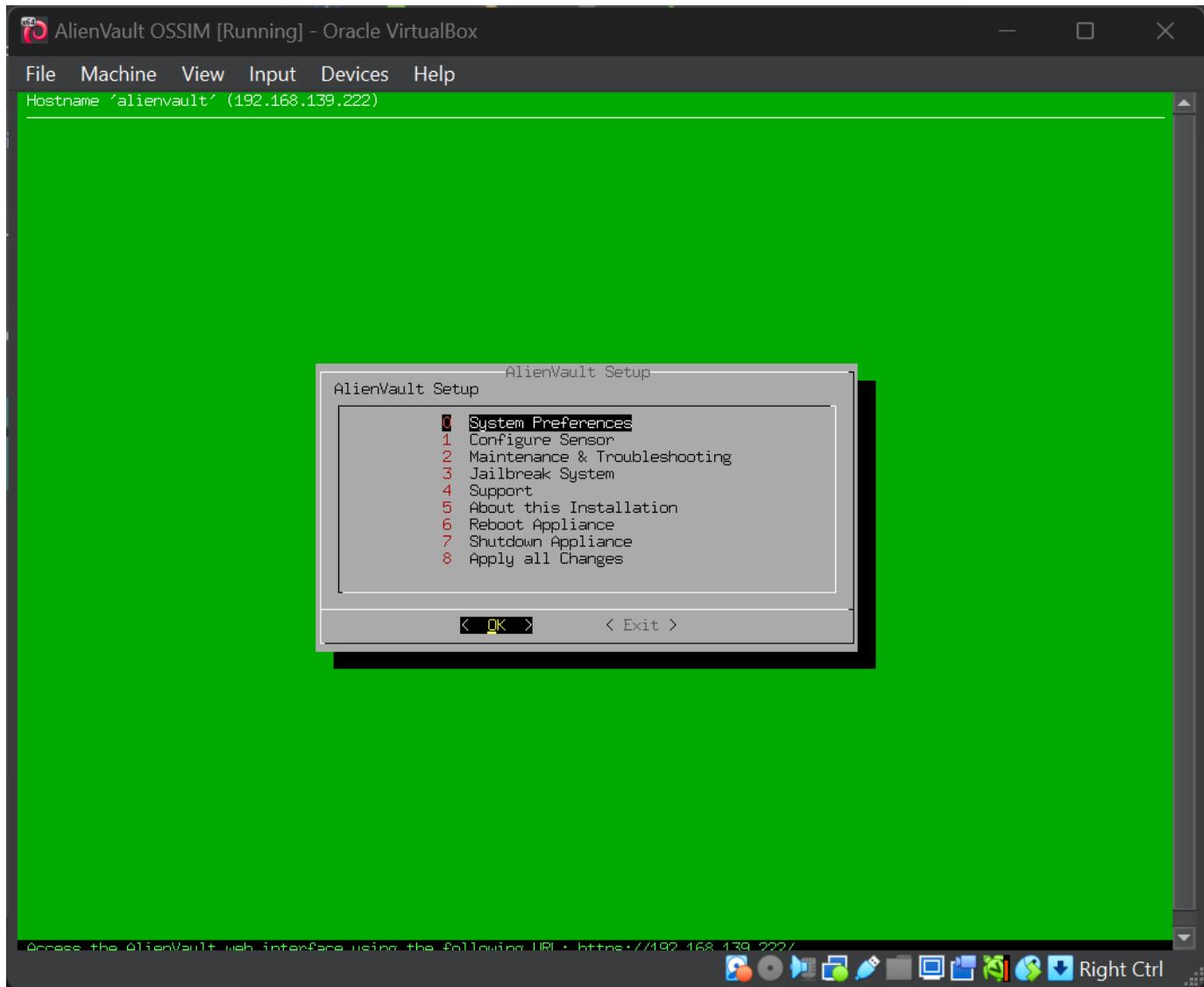
After the successful installation (it may take long time, sometimes hours), you will be able to see a black Debian screen.



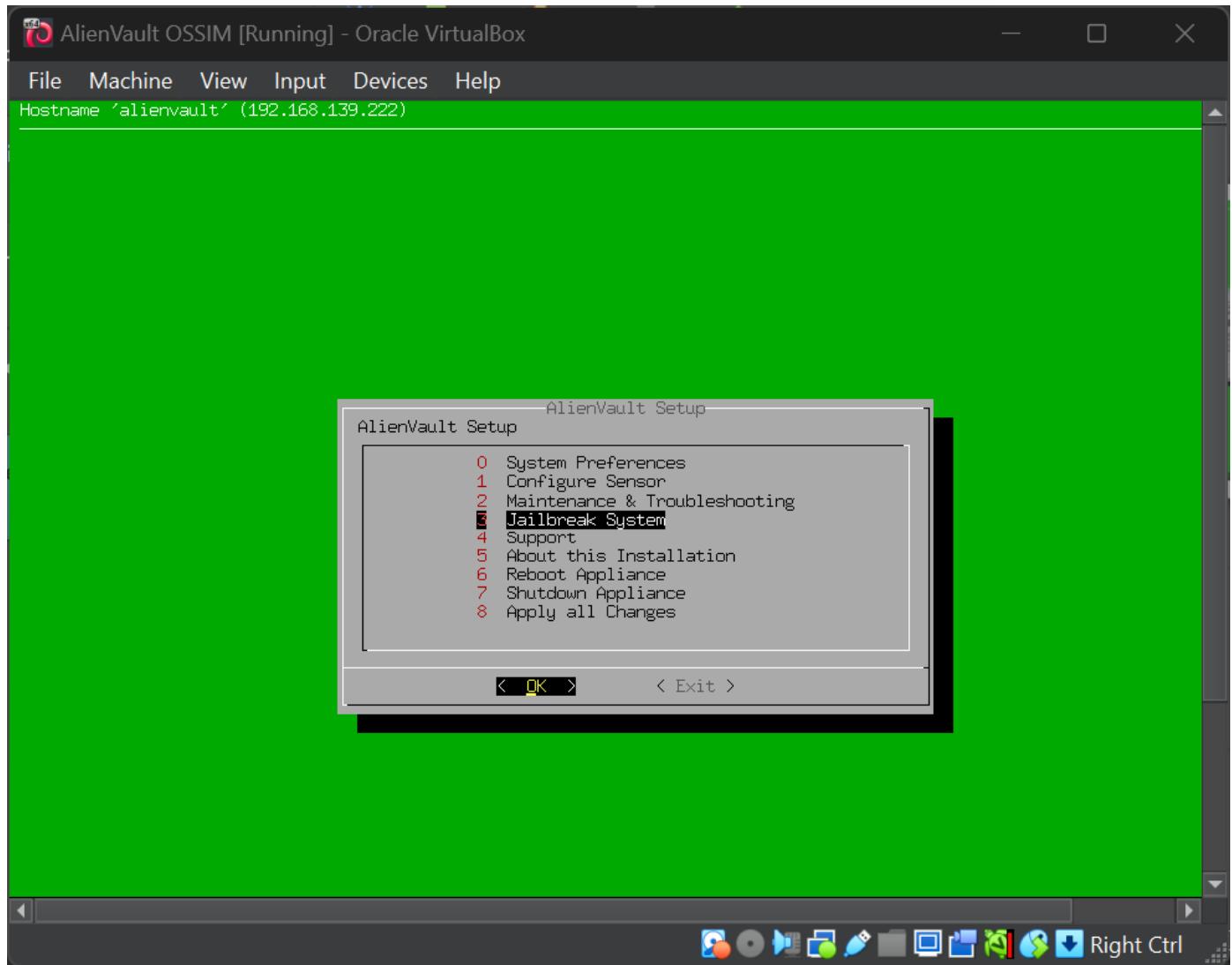
- Log in as **root** and use the password **Alien123**.



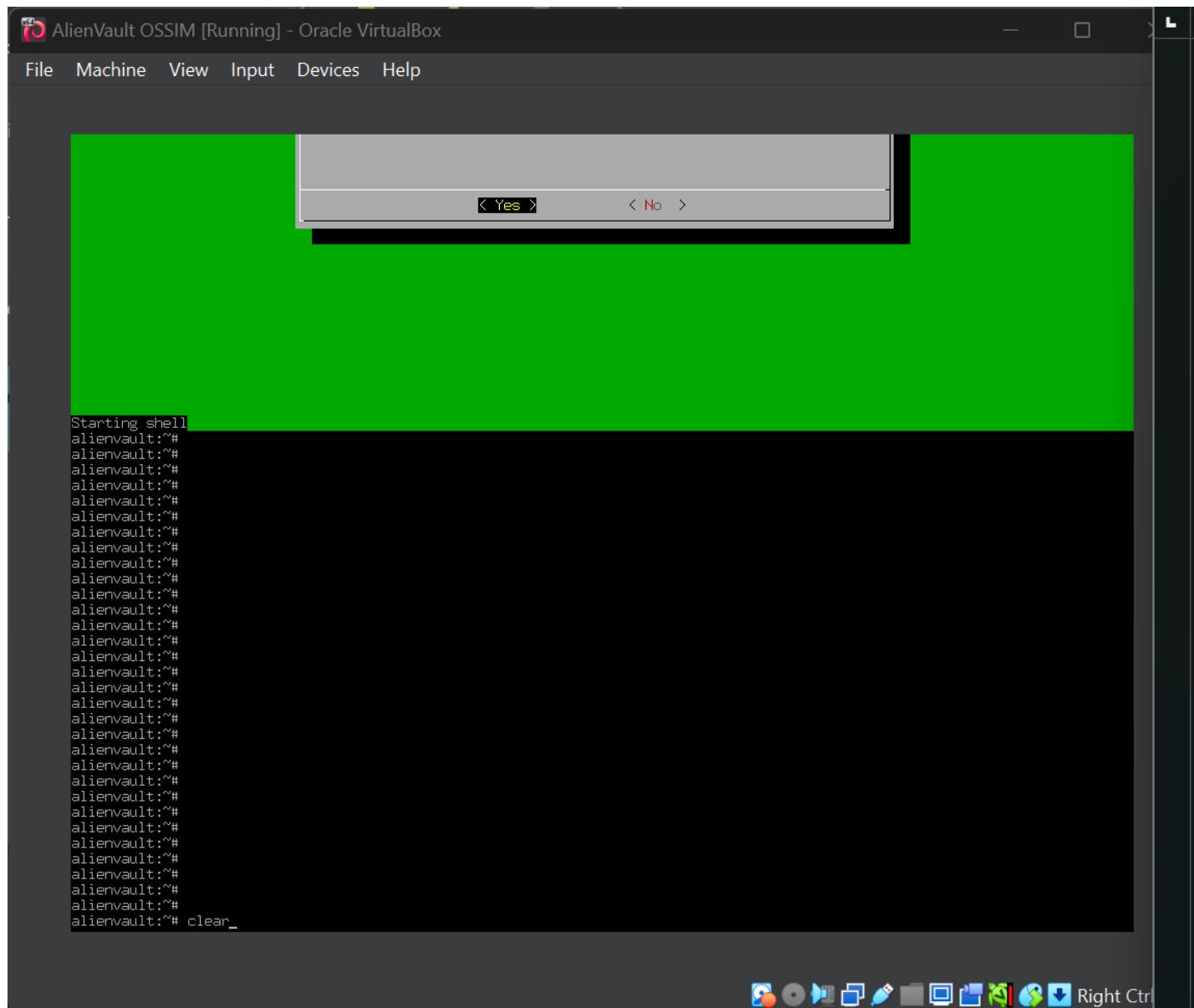
- A small menu driven window will appear.



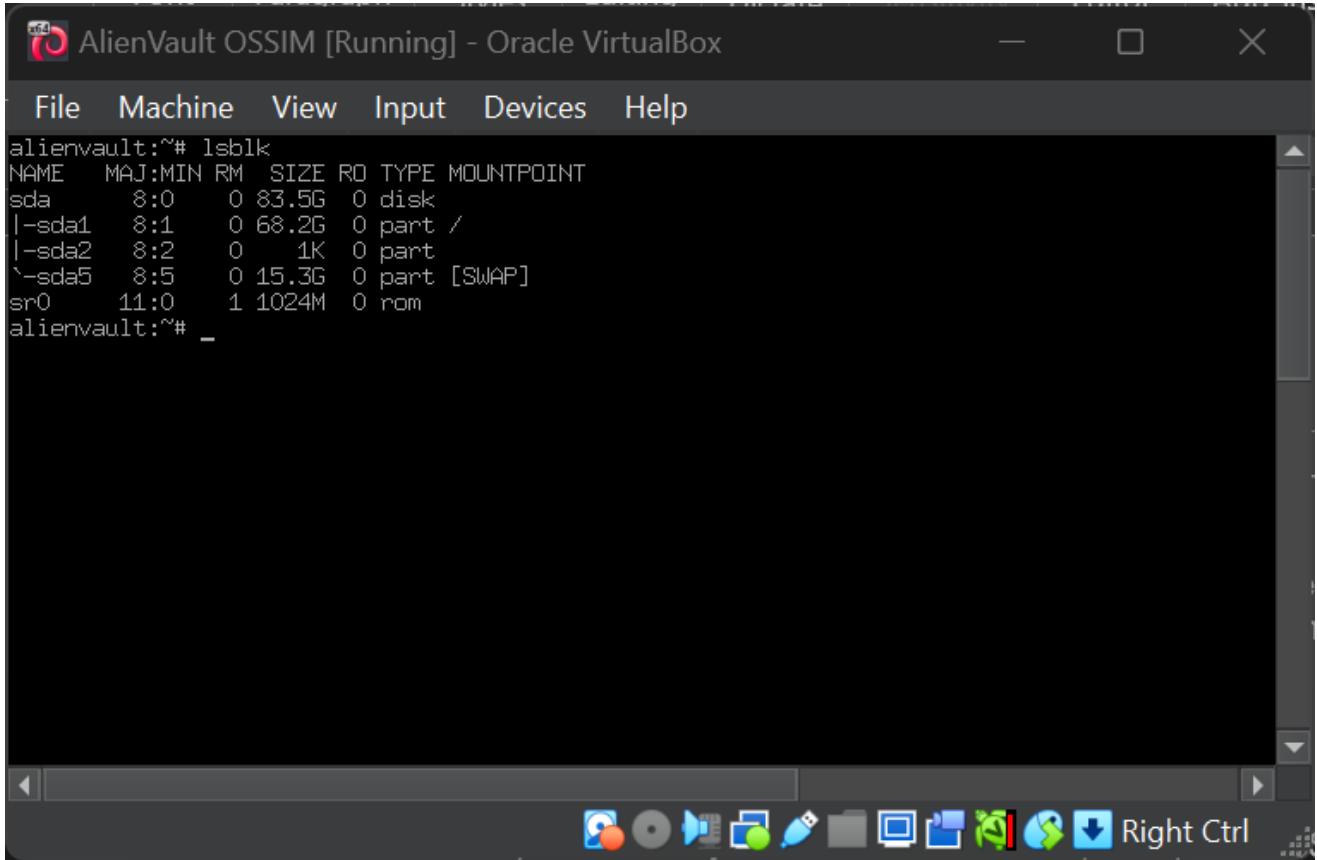
- Select 4th Option: Jailbreak System.



- Continue?: **Yes** ○ Type **clear** (in the bottom-left corner of the screen to clear the screen).

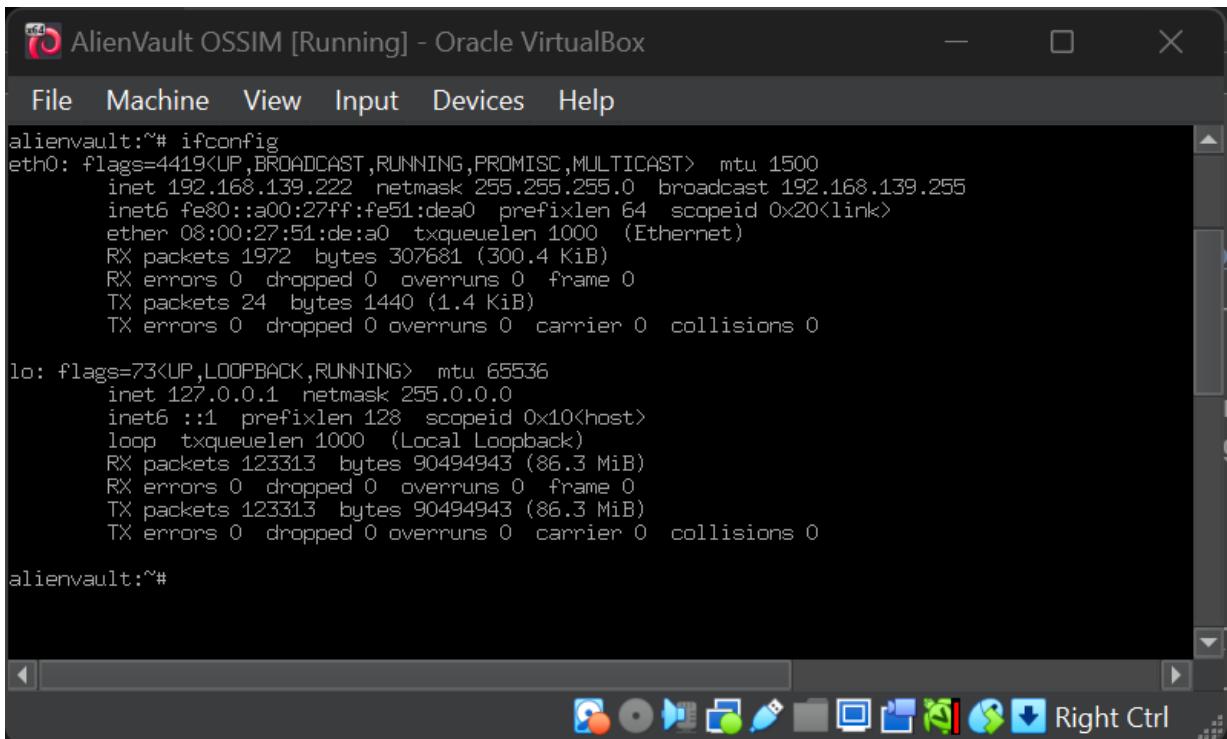


- Type **lsblk** (you should be able to see sda : 80G disk).



```
alienvault:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0 83.5G  0 disk 
|---sda1  8:1    0 68.2G  0 part /
|---sda2  8:2    0   1K  0 part 
`---sda5  8:5    0 15.3G  0 part [SWAP]
sr0     11:0   1 1024M  0 rom 
alienvault:~#
```

- Type **ifconfig** (note the inet ip address).

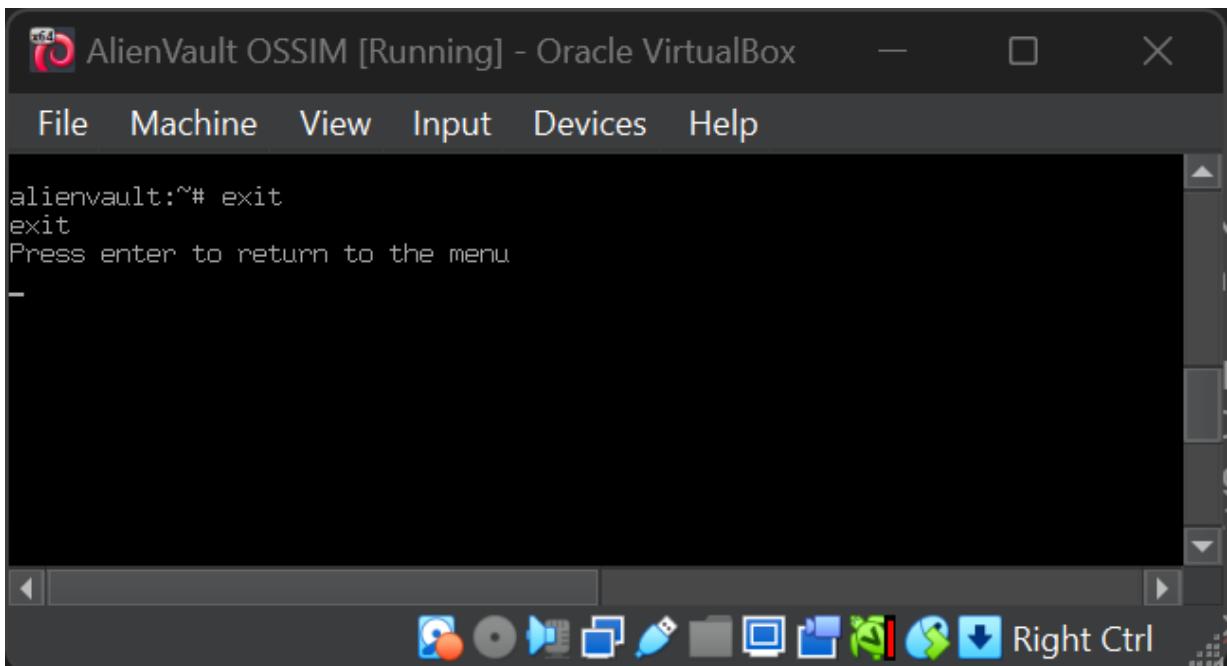


```
AlienVault OSSIM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
alienvault:~# ifconfig
eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
        inet 192.168.139.222 netmask 255.255.255.0 broadcast 192.168.139.255
              inet6 fe80::a00:27ff:fe51:dea0 prefixlen 64 scopeid 0x20<link>
                ether 08:00:27:51:de:a0 txqueuelen 1000 (Ethernet)
                  RX packets 1972 bytes 307681 (300.4 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 24 bytes 1440 (1.4 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                loop txqueuelen 1000 (Local Loopback)
                  RX packets 123313 bytes 90494943 (86.3 MiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 123313 bytes 90494943 (86.3 MiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

alienvault:~#
```

- Type **exit**.



```
AlienVault OSSIM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
alienvault:~# exit
exit
Press enter to return to the menu
-
```

- Launch Google Chrome browser on your host machine (not on VM).
- Type the ip address at URL as <https://192.168.139.222> (the IP address that you noted down after the ifconfig command above).
- Click **Advanced**, and then click **proceed to 192.168.139.222**.

Welcome

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.

If you need more information about AlienVault, please visit [AlienVault.com](#).

Administrator Account Creation

Create an account to access your AlienVault product.

** Asterisks indicate required fields*

FULL NAME *	<input type="text"/>
USERNAME *	<input type="text" value="admin"/>
PASSWORD *	<input type="password"/>
CONFIRM PASSWORD *	<input type="password"/>
E-MAIL *	<input type="text"/>
COMPANY NAME	<input type="text"/>

START USING ALIENVault

○ **Administrator Account Creation:**

- **Full Name:** (Your full name)
- **USERNAME:** (Admin) Do not change
- **Password:** Ossim_123
- **Confirm Password:** Ossim_123
- **Email:** (Your triOS college email address)
- **Company Name:** triOS College
- **Location:** Toronto **(Take the screenshot)**

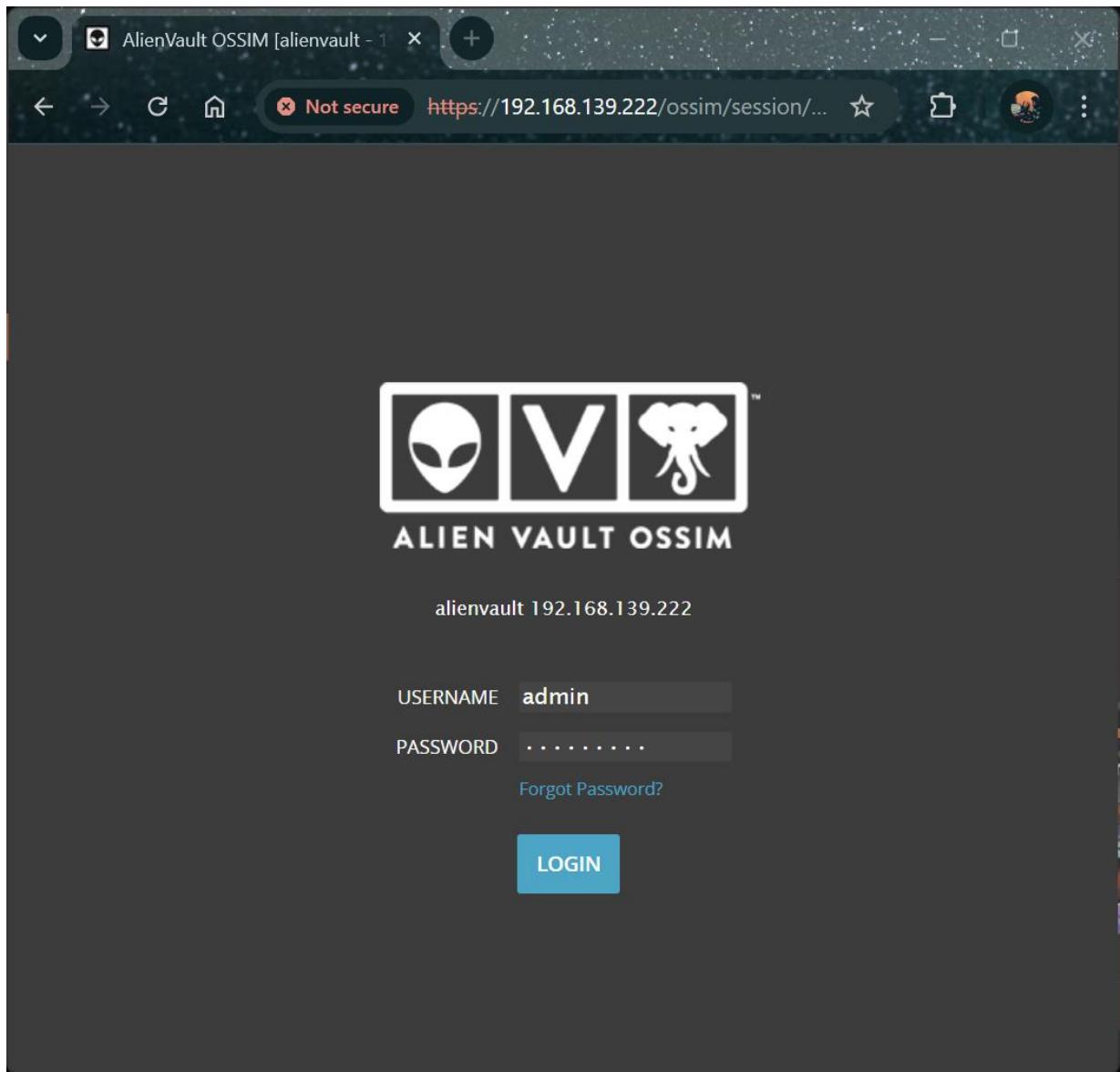
(Now click **Start Using AlienVault.**)

The screenshot shows a web browser window titled "AlienVault OSSIM [alienvault - 1]". The URL in the address bar is <https://192.168.139.222/ossim/session/login.php>. The page has a dark header with the AlienVault logo and the text "ALIEN VAULT OSSIM". The main content area has a "Welcome" heading and a message about creating an administrator user account. Below this is a section titled "Administrator Account Creation" with a sub-instruction to "Create an account to access your AlienVault product." A note states "* Asterisks indicate required fields". The form fields are as follows:

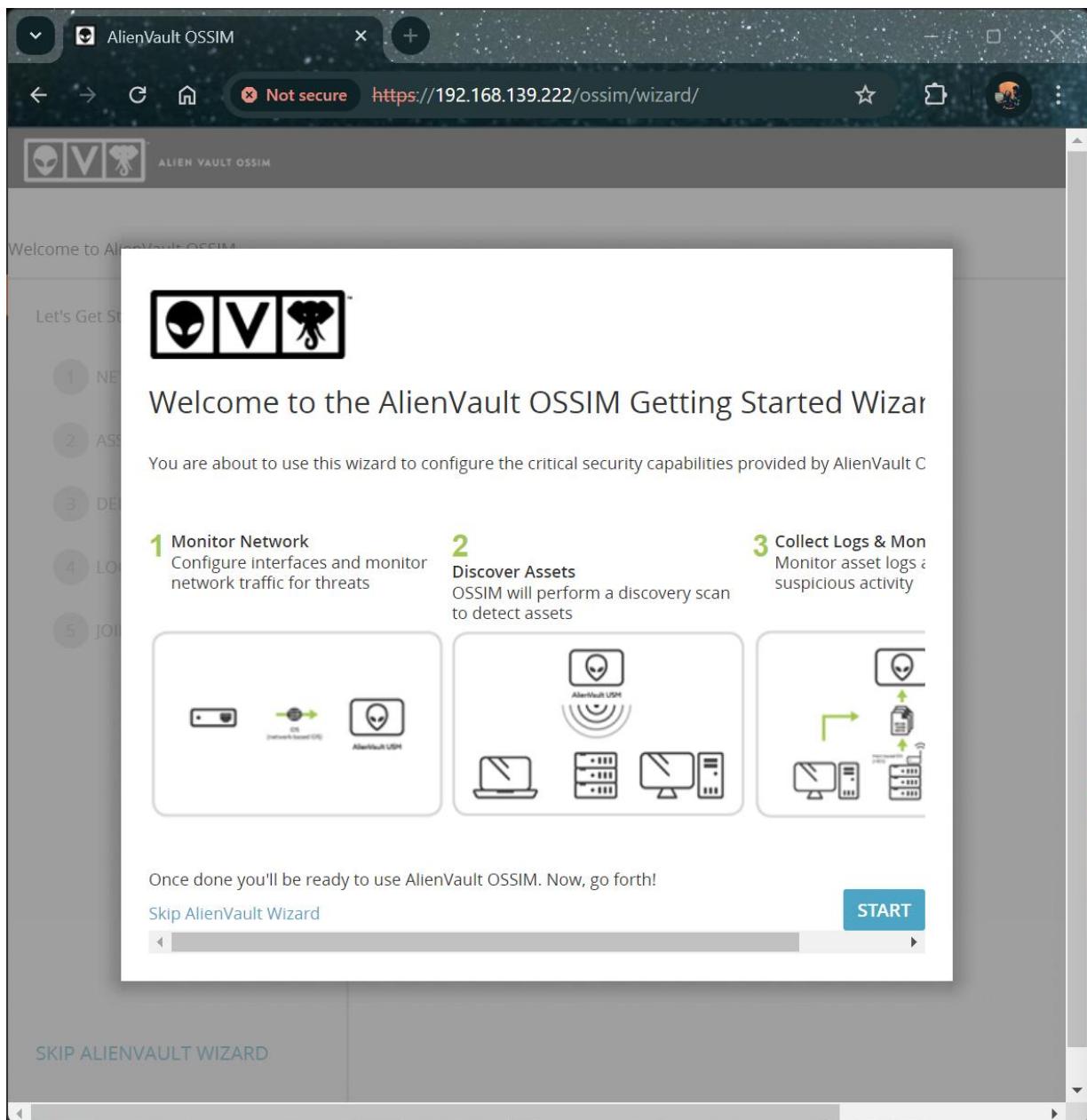
FULL NAME *	Saiprasad Raman
USERNAME *	admin
PASSWORD * very strong
CONFIRM PASSWORD * very strong
E-MAIL *	saiprasadraman15@gmail.com
COMPANY NAME	trios College

A blue button at the bottom center reads "START USING ALIENVault".

o **USERNAME:** admin o **Password:** Ossim_123



- On the Welcome to AlienVault OSSIM Getting Started Wizard, click **START**.



- **Network Interface:** Click **Next**.

Welcome to AlienVault OSSIM

Let's Get Started

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	192.168.139.222	-

Information

- Management:** The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- Network Monitoring:** Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See [Instructions](#) on how to setup a network tap or span.
- Log Collection & Scanning:** Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- Not in Use:** Use this option if you do not want to use one of the network interfaces.

NEXT

- **Asset Discovery:** Add assets manually, if you do not find other VMs.
 - **Hostname:** (Hostname of the other VM)
 - **IP address:** (IP address of the other VM)
 - **Select an Asset Type:** Windows/Linux/Network Device
- Click **Add**. It should be able to find your AlienVault along with other VM as well.

Welcome to AlienVault OSSIM

Let's Get Started

- 1 NETWORK INTERFACES
- 2 ASSET DISCOVERY**
- 3 DEPLOY HIDS
- 4 LOG MANAGEMENT
- 5 JOIN OTX

Scan & Add Assets

In order to begin monitoring your environment we must first find the assets in your network. There are three (3) ways you can add assets to monitor: you can scan your network using network ranges, import a CSV of assets in your network, or you can add assets manually.

Add Asset Manually

Kali Linux	10.0.2.4	Linux	+ ADD
alienvault	192.168.139.222	Linux	X
Host-192-168-137-88	192.168.137.88	Select an Asset Type	X
Host-192-168-139-210	192.168.139.210	Windows	X

SCAN NETWORKS IMPORT FROM CSV

HOSTNAME ▾ IP TYPE

alienvault 192.168.139.222 Linux X Delete

Host-192-168-137-88 192.168.137.88 Select an Asset Type X Delete

Host-192-168-139-210 192.168.139.210 Windows X Delete

SHOWING 1 TO 3 OF 3 ASSETS

FIRST PREVIOUS 1 NEXT LAST

SKIP ALIENVAULT WIZARD BACK NEXT

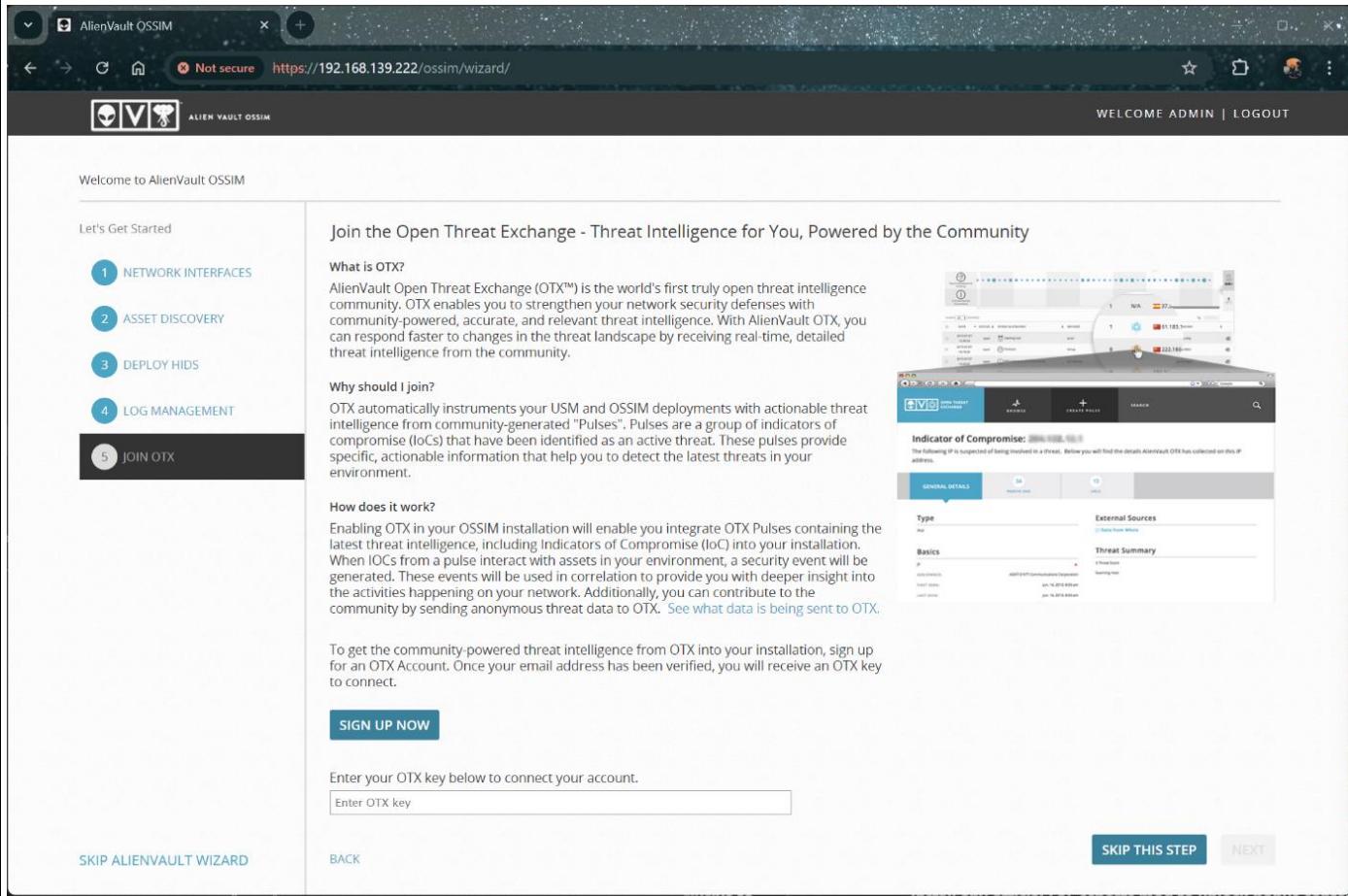
- Deploy HIDS: Click **Next**.

The screenshot shows the AlienVault OSSIM wizard interface. The title bar says "AlienVault OSSIM" and the address bar shows "http://192.168.139.222/ossim/wizard/". The main menu on the left lists "Let's Get Started" with five steps: 1. NETWORK INTERFACES, 2. ASSET DISCOVERY, 3. DEPLOY HIDS (which is highlighted in black), 4. LOG MANAGEMENT, and 5. JOIN OTX. The central panel is titled "Deploy HIDS to Servers" and contains a note about deploying HIDS to perform file integrity monitoring, rootkit detection, and log collection. It specifies that for Windows machines, the agent will be installed locally, while for Unix/Linux environments, remote HIDS monitoring will be configured. Below this, there are tabs for "WINDOWS (1)" and "UNIX / LINUX (1)". A note below the tabs says "Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored; it will be used to deploy an agent to the selected assets." There are fields for "Username" and "Password", and an optional "Domain (Optional)" field. To the right, under "Deploy to the following hosts:", there is a tree view showing "Local_192_168_139_0_24" with a checked checkbox for "Host-192-168-139-210". At the bottom left are "SKIP ALIENVAULT WIZARD" and "BACK" buttons, and at the bottom right is a large blue "NEXT" button.

- Log Management: Click **Skip this Step**.
(You are required to have a corporate managed network device at this level.)

The screenshot shows the AlienVault OSSIM wizard interface. The title bar reads "AlienVault OSSIM" and "Not secure https://192.168.139.222/ossim/wizard/". The top right has "WELCOME ADMIN | LOGOUT". The main area is titled "Welcome to AlienVault OSSIM". On the left, a sidebar lists "Let's Get Started" with steps 1 through 5: 1) NETWORK INTERFACES, 2) ASSET DISCOVERY, 3) DEPLOY HIDS, 4) LOG MANAGEMENT (which is highlighted in dark grey), and 5) JOIN OTX. The main content area is titled "Set up Log Management" and contains the following text: "During the asset discovery scan we found 0 network devices on your network. Confirm the vendor, model, and version of the device shown. Click the 'Enable' button to enable the data source plugin for each device." Below this, a red message states: "There are no network devices found. Return to the asset discovery step by clicking back to either discover or add network devices." At the bottom right are buttons for "SKIP THIS STEP" (in blue) and "NEXT" (in grey).

- Join OTX: Click **Skip this step**, then click **Finish**.



The screenshot shows the AlienVault OSSIM wizard interface at step 5, titled "JOIN OTX". The left sidebar lists steps 1 through 5, with step 5 highlighted in black. The main content area has three sections: "What is OTX?", "Why should I join?", and "How does it work?". It includes a "SIGN UP NOW" button and a field to enter an OTX key. To the right, there are two screenshots of the AlienVault OTX platform. The top one shows a dashboard with various threat intelligence metrics. The bottom one shows a detailed view of an "Indicator of Compromise" (IOC) for an IP address, displaying general details, external sources, and threat summary.

Welcome to AlienVault OSSIM

Let's Get Started

- 1 NETWORK INTERFACES
- 2 ASSET DISCOVERY
- 3 DEPLOY HIDS
- 4 LOG MANAGEMENT
- 5 JOIN OTX

Join the Open Threat Exchange - Threat Intelligence for You, Powered by the Community

What is OTX?
AlienVault Open Threat Exchange (OTX™) is the world's first truly open threat intelligence community. OTX enables you to strengthen your network security defenses with community-powered, accurate, and relevant threat intelligence. With AlienVault OTX, you can respond faster to changes in the threat landscape by receiving real-time, detailed threat intelligence from the community.

Why should I join?
OTX automatically instruments your USM and OSSIM deployments with actionable threat intelligence from community-generated "Pulses". Pulses are a group of indicators of compromise (IoCs) that have been identified as an active threat. These pulses provide specific, actionable information that help you to detect the latest threats in your environment.

How does it work?
Enabling OTX in your OSSIM installation will enable you integrate OTX Pulses containing the latest threat intelligence, including Indicators of Compromise (IoC) into your installation. When IOCs from a pulse interact with assets in your environment, a security event will be generated. These events will be used in correlation to provide you with deeper insight into the activities happening on your network. Additionally, you can contribute to the community by sending anonymous threat data to OTX. See what data is being sent to OTX.

To get the community-powered threat intelligence from OTX into your installation, sign up for an OTX Account. Once your email address has been verified, you will receive an OTX key to connect.

SIGN UP NOW

Enter your OTX key below to connect your account.

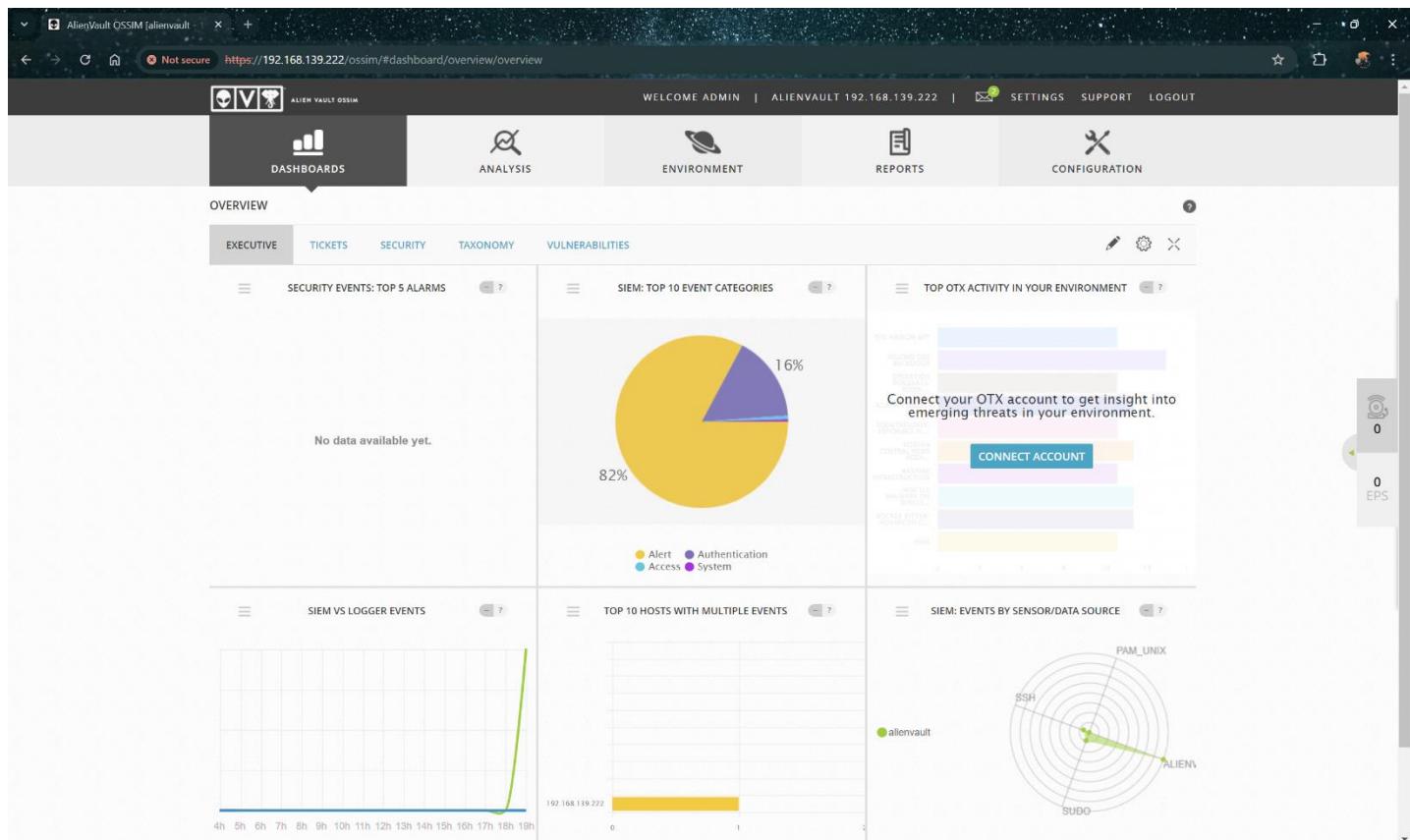
Enter OTX key

SKIP ALIENVULT WIZARD **BACK** **NEXT** **SKIP THIS STEP**

The screenshot shows a web browser window for AlienVault OSSIM. The URL is <https://192.168.139.222/ossim/wizard/>. The page title is "Welcome to AlienVault OSSIM". On the left, there's a sidebar titled "Let's Get Started" with five numbered steps: 1. NETWORK INTERFACES, 2. ASSET DISCOVERY, 3. DEPLOY HIDS, 4. LOG MANAGEMENT, and 5. JOIN OTX (which is highlighted with a dark background). The main content area has a heading "Don't Worry, You Can Join the AlienVault Open Threat Exchange at Any Time!" followed by the text: "You've chosen not to join the Open Threat Exchange at this time. You can join the AlienVault OTX community through your AlienVault OSSIM web interface at any time." Below this, it says "Click 'Finish' to start using AlienVault OSSIM". At the bottom of the main area are "SKIP ALIENVAULT WIZARD" and "BACK" buttons, and a "FINISH" button on the right.

Take a tour of AlienVault OSSIM.

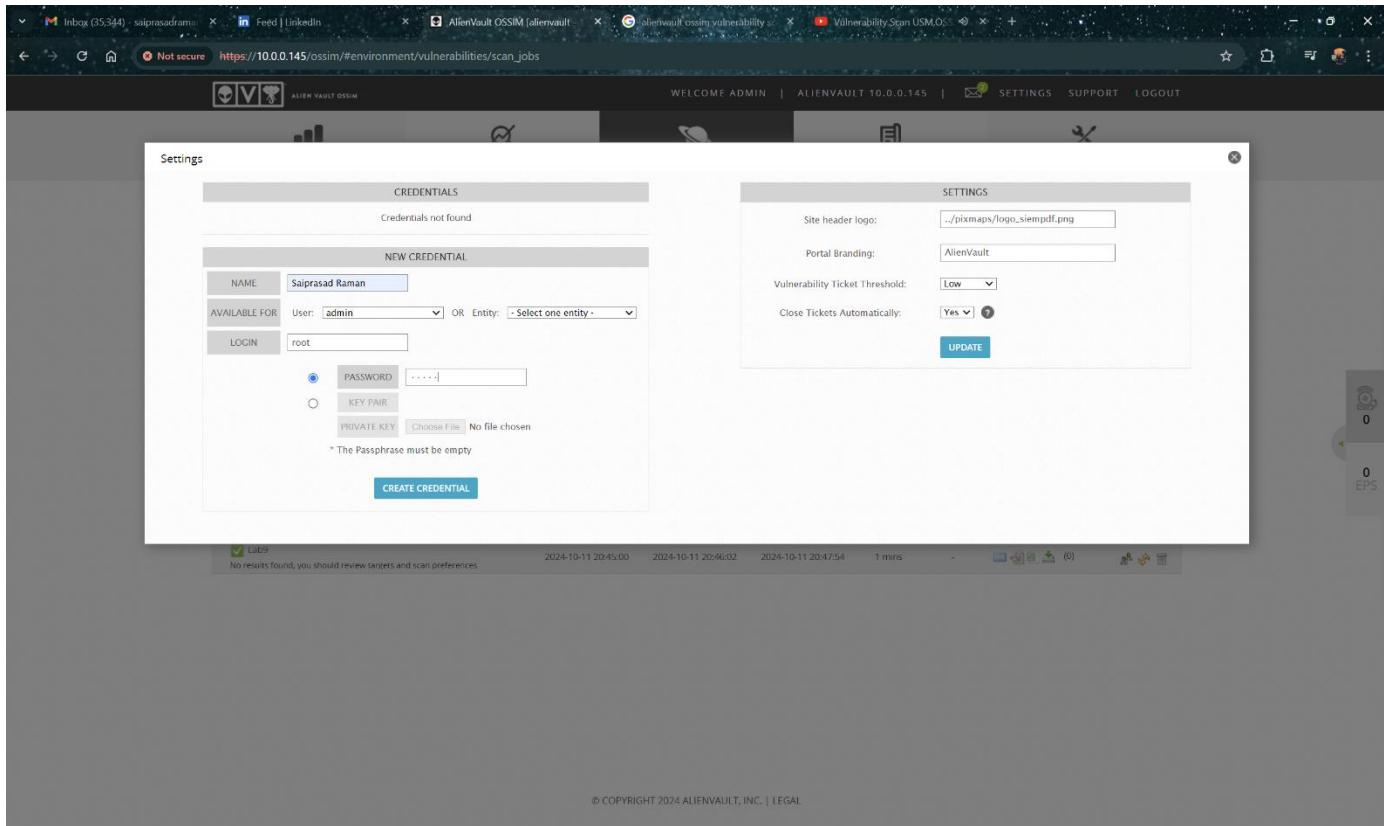
- See the Dashboard of AlienVault.



- Click on **Environment**, a dropdown menu will open, click **vulnerabilities**.

The screenshot shows the AlienVault OSSIM web interface. At the top, there is a navigation bar with links for DASHBOARDS, ANALYSIS, ENVIRONMENT (which is highlighted with a dark background), REPORTS, and CONFIGURATION. Below the navigation bar, there is a sub-menu for VULNERABILITIES with options for OVERVIEW, SCAN JOBS, and THREAT DATABASE. The main content area has two sections: 'BY SEVERITY' and 'TOP 10 HOSTS'. Both sections display a message 'No results found'. On the right side, there is a sidebar with icons for PROFILES, SETTINGS, and a camera icon labeled '0 EPS'. At the bottom, there is a search bar with placeholder text 'Asset Vulnerability Details', a radio button for 'Host/Net', and a 'FIND' button. A note says 'No results found: Click here to run a Vulnerability Scan now'. The footer contains copyright information: '© COPYRIGHT 2024 ALIENVULT, INC. | LEGAL'.

- Click **settings** and **add new credentials** for other VM:
- Name: root (or any other host that is in your VM) ○ Login: root ○ Password: (the root password) ○ Click create credential, after the credentials created, **Take the screenshot** and then close the window.



- Click on **Environment**, a dropdown menu will open, click on **Assets & Groups**.
- Select the other VM from Assets by clicking the checkmark on the left side of other VM hostname and then clicking **Actions** (a drop-down menu will open).
 - You can run Asset Scan and/or Vulnerability scan.

Note: “Deploy HIDS agent” is only for Windows-based systems and not for Linux.

HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCHE
Host-192-168-139-210	192.168.139.210		Windows XP/2000	2	

- After vulnerability scan is completed (it may take 20+ minutes for deep scan), click **REPORTS**, then click **Overview**, then scroll down to Vulnerabilities Report, click on **View Report**.
- Download the report and submit it along with this lab.

The screenshot shows the AlienVault OSSIM web interface. At the top, there's a navigation bar with tabs for DASHBOARDS, ANALYSIS, ENVIRONMENT, REPORTS (which is currently selected), and SETTINGS. Below this is a sub-navigation bar with sections for OVERVIEW, REPORT NAME, REPORT OPTIONS, and ACTIONS. The main content area displays several report cards:

- Alarms Report**: Includes checkboxes for Title Page, Top 10 Attacker Host, Top 10 Attacked Host, Top 10 Used Ports, Top 15 Alarms, and Top 15 Alarms by Risk. It also has a Date Range selector set from 2024-09-12 to 2024-10-12, and buttons for Download PDF and Send by e-mail.
- Asset Details**: A form for entering Host Name/IP/Network with a "View Report" button.
- Availability Report**: A form for selecting a Section (Trends) with a "View Report" button.
- Business & Compliance ISO PCI Report**: Includes checkboxes for Title Page, Threat overview, Business real impact risks, C.I.A Potential impact, PCI-DSS 2.0, PCI-DSS 3.0, Trends, ISO27002 Potential impact, and ISO27001. It has a Date Range selector set from 2024-09-12 to 2024-10-12, and buttons for Download PDF and Send by e-mail.
- Geographic Report**: A form for selecting a Date Range from 2024-09-12 to 2024-10-12, with buttons for Download PDF and Send by e-mail.
- SIEM Events +**: Includes checkboxes for Title Page, Top 10 Attacker Host, and Top 10 Attacked Host. It has a Date Range selector set from 2024-09-12 to 2024-10-12, and buttons for Download PDF and Send by e-mail.

