Course: CYB301

Security Defense and Response

(Canadian Context)

Lab 9: Software & Hardware Development Security and SIEM

Coordinator and Instructor: Muhammad Siddiqui

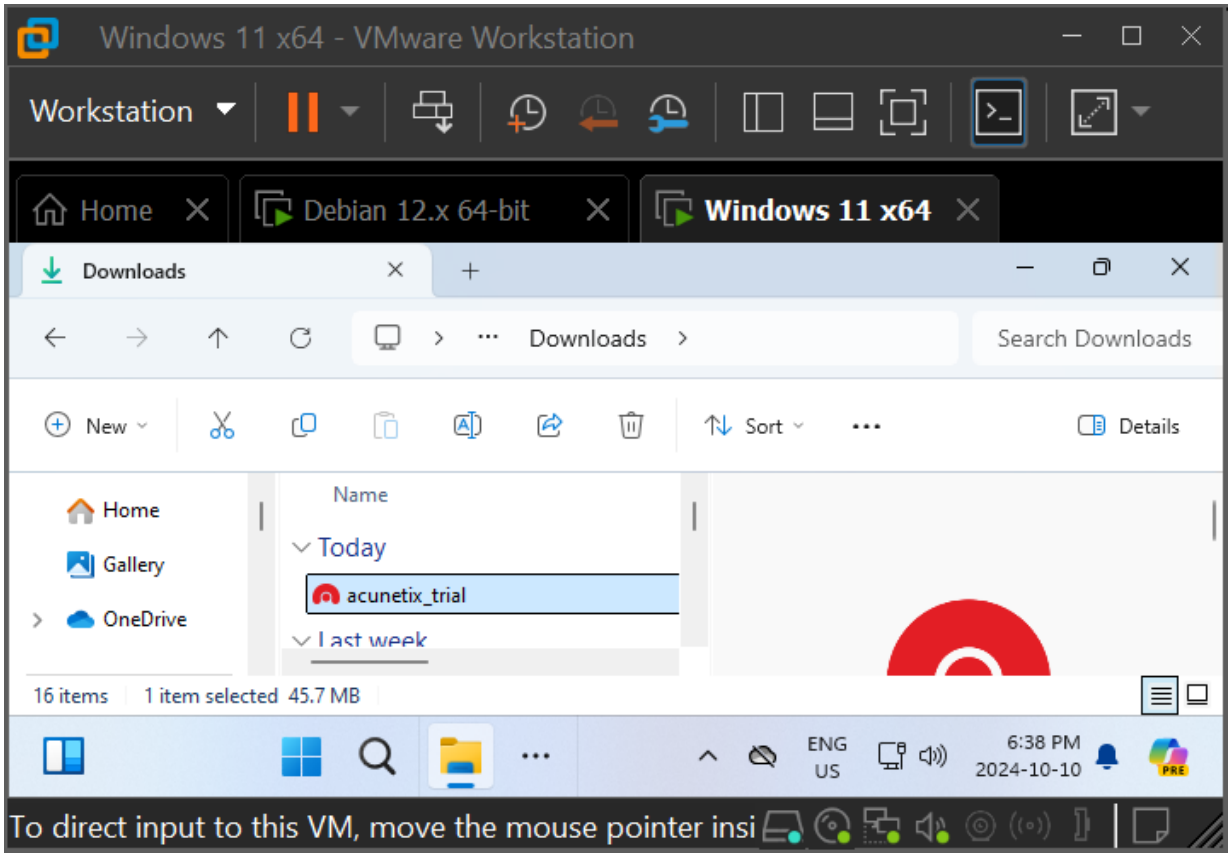
Student: Saiprasad Raman (23074624)

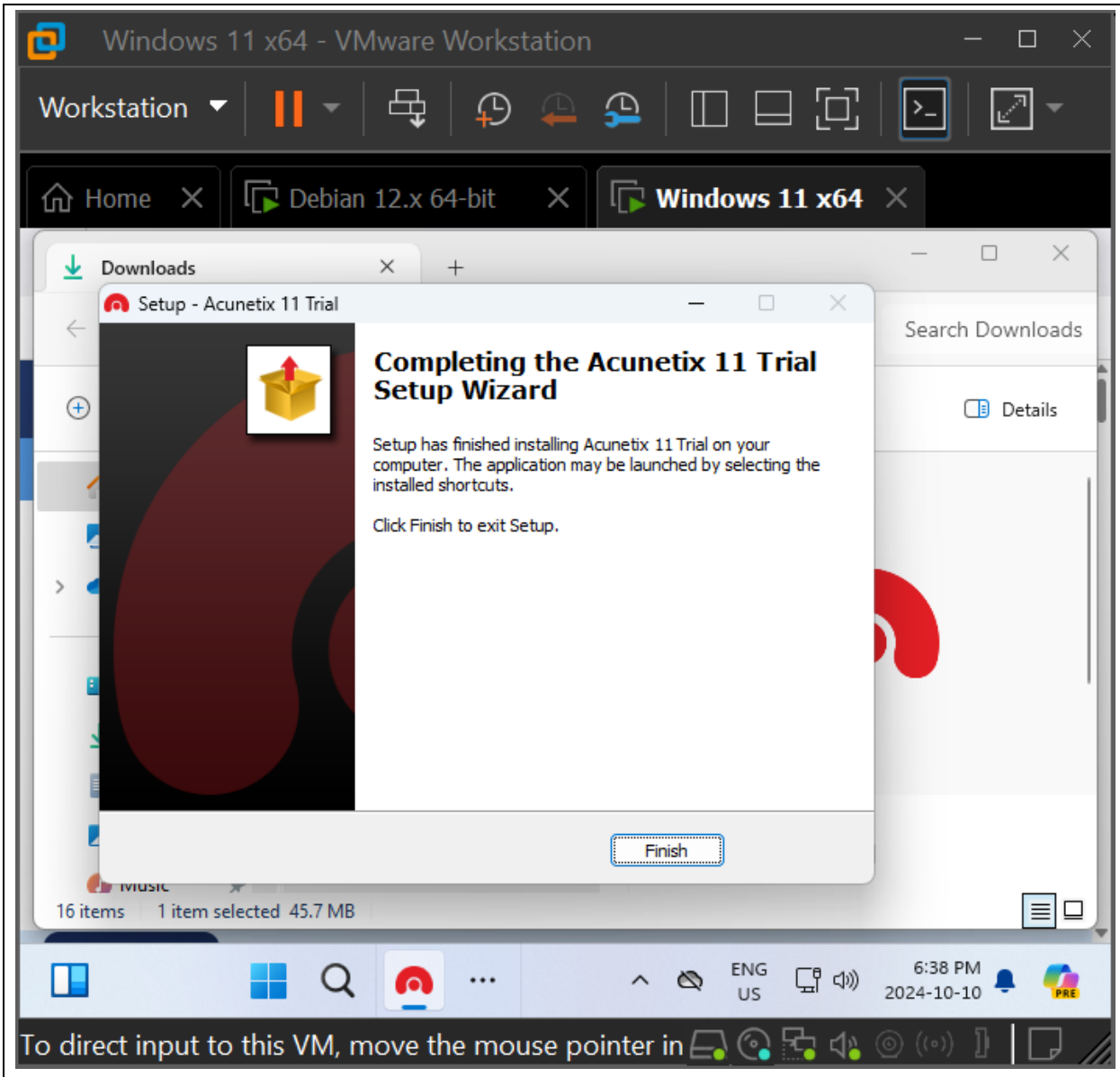
Activity 1: Review an Application Using the OWASP Application Security Architecture.
Cheat Sheet

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.

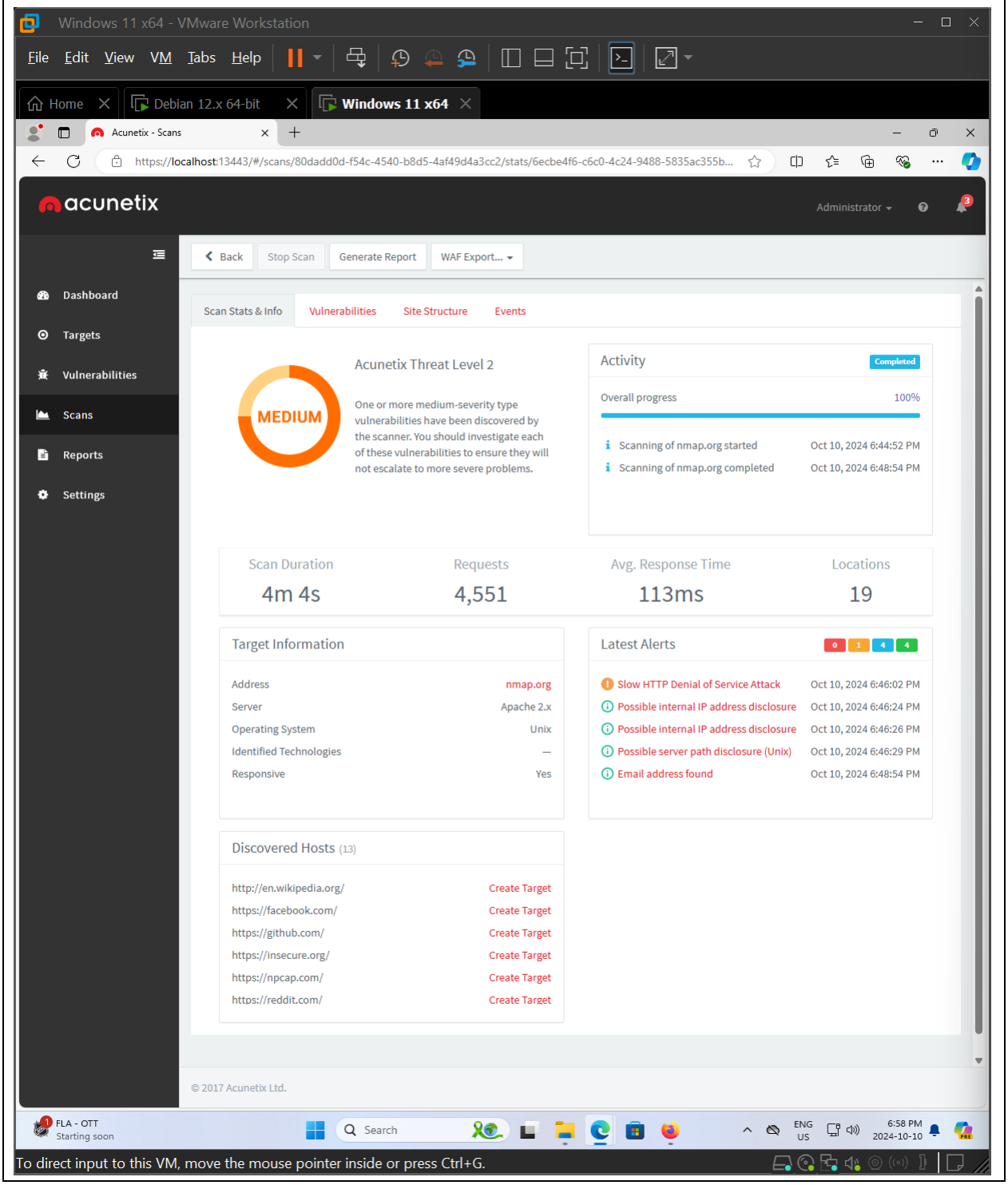
Acunetix provides their Web Vulnerability scanner as a 14-day limited term trial download. You can download it at www.acunetix.com/vulnerability-scanner/download/

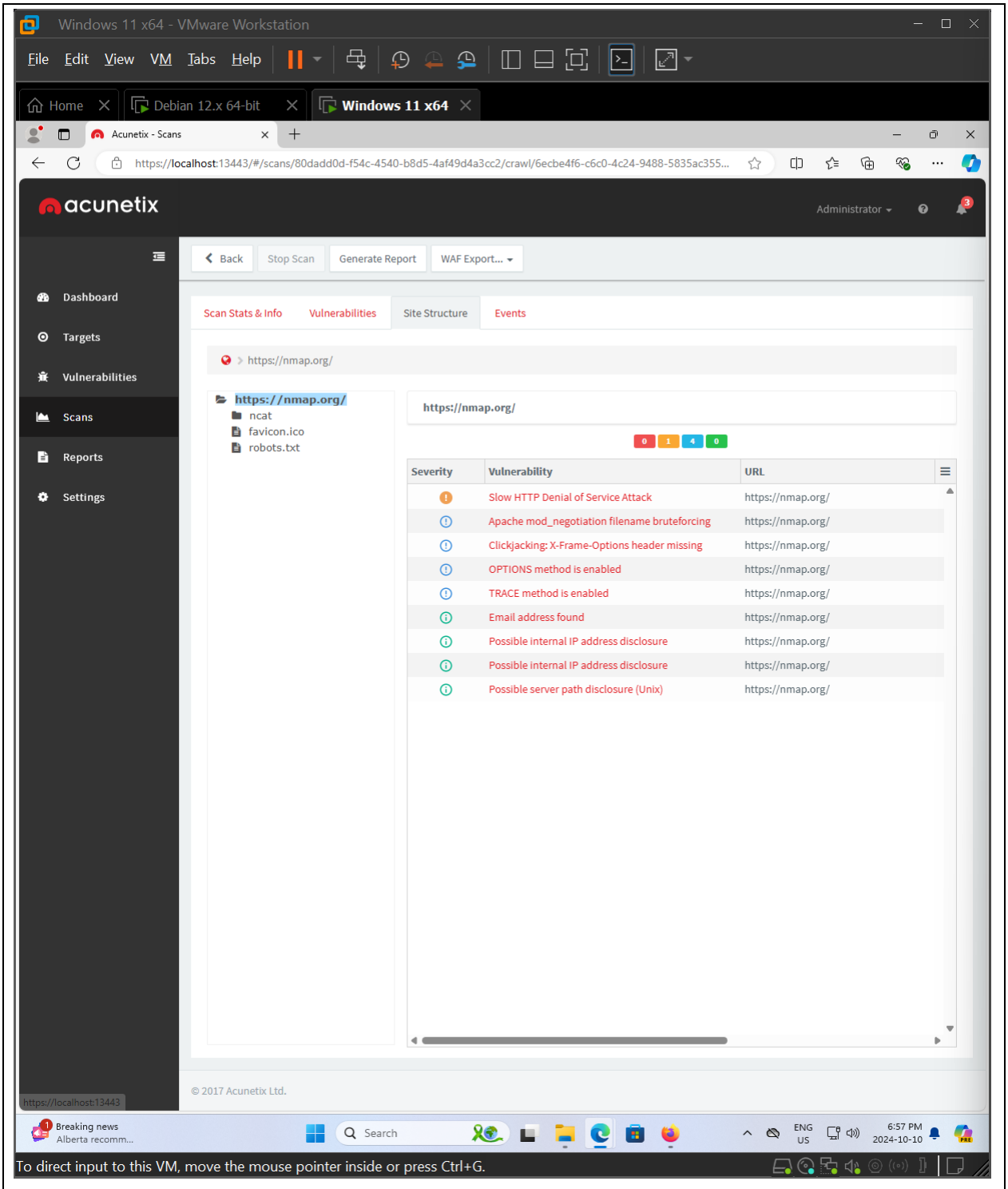



Windows 11 x64 - VMware Workstation
Workstation
Home
Debian 12.x 64-bit
Windows 11 x64
Downloads
Search Downloads
Details
Setup - Acunetix 11 Trial
Completing the Acunetix 11 Trial Setup Wizard
Setup has finished installing Acunetix 11 Trial on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Finish
16 items
1 item selected 45.7 MB
ENG
US
6:38 PM
2024-10-10
To direct input to this VM, move the mouse pointer in

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.




Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 12.x 64-bit
Windows 11 x64
Acunetix - Scans
https://localhost:13443/#/scans/80dadd0d-f54c-4540-b8d5-4af49d4a3cc2/crawl/6ecbe4f6-c6c0-4c24-9488-5835ac355...
acunetix
Administrator
Back
Stop Scan
Generate Report
WAF Export...
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Scan Stats & Info
Vulnerabilities
Site Structure
Events
https://nmap.org/
https://nmap.org/
ncat
favicon.ico
robots.txt
0 1 4 0
Severity
Vulnerability
URL
Slow HTTP Denial of Service Attack https://nmap.org/
Apache mod_negotiation filename bruteforcing https://nmap.org/
Clickjacking: X-Frame-Options header missing https://nmap.org/
OPTIONS method is enabled https://nmap.org/
TRACE method is enabled https://nmap.org/
Email address found https://nmap.org/
Possible internal IP address disclosure https://nmap.org/
Possible internal IP address disclosure https://nmap.org/
Possible server path disclosure (Unix) https://nmap.org/
© 2017 Acunetix Ltd.
https://localhost:13443
Breaking news
Alberta recomm...
Search
ENG
US
6:57 PM
2024-10-10
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Part 3: Analyze the scan results.

Review the scan results and answer the following questions.

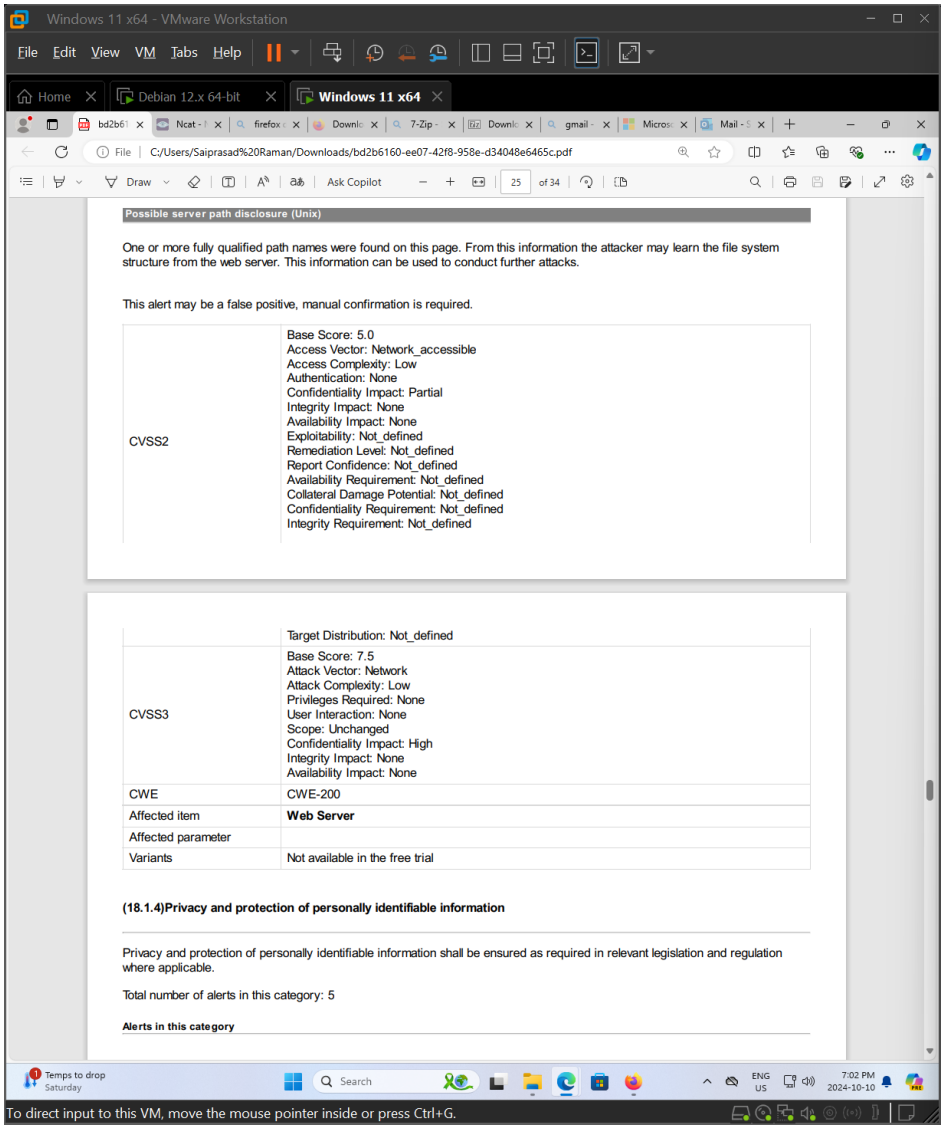
1. What is the most critical vulnerability? How can it be remediated?

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.

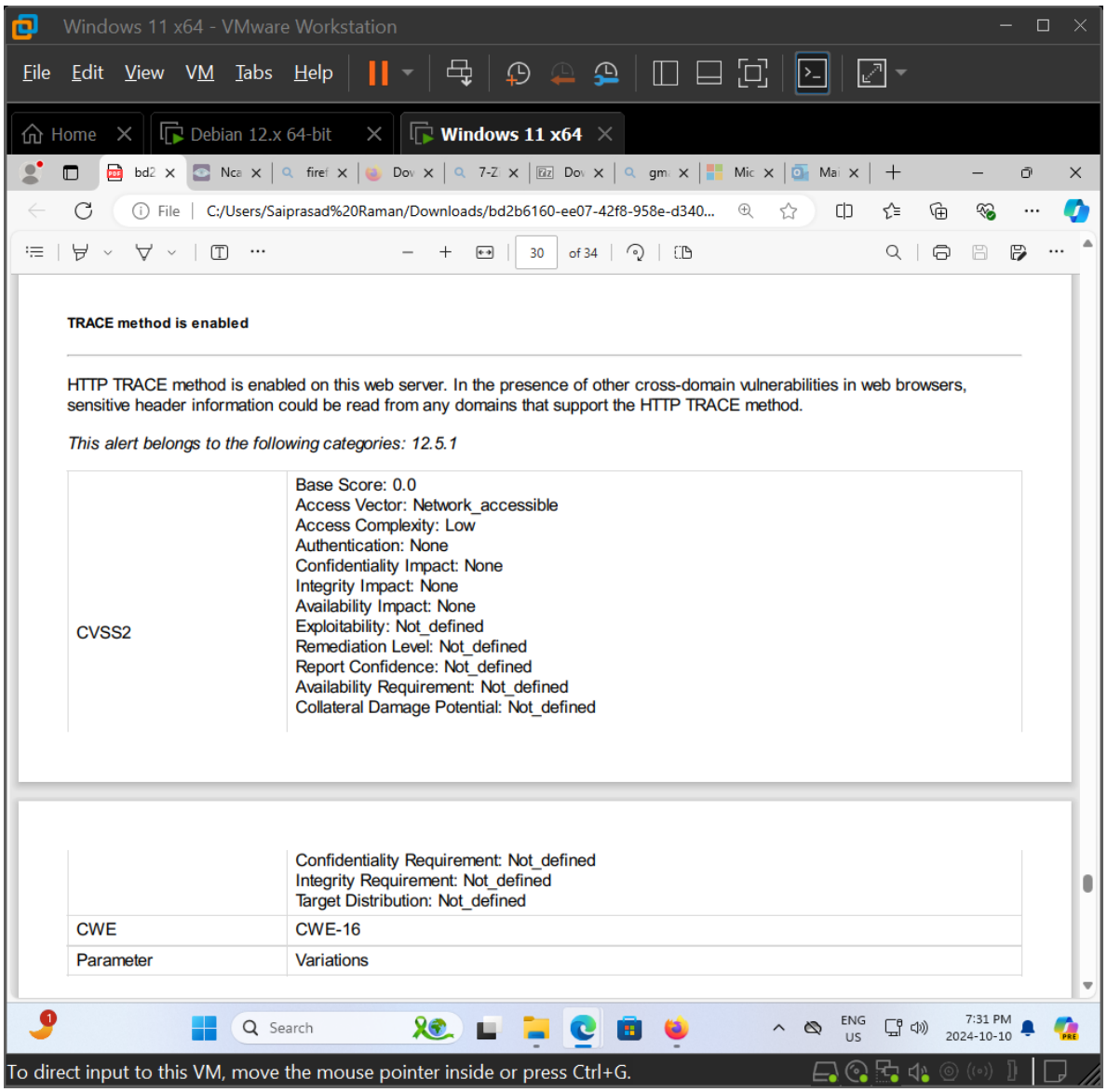
2. Enable HTTPS protocol to encrypt the information
3. Update the softwares.



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.



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

Ans.

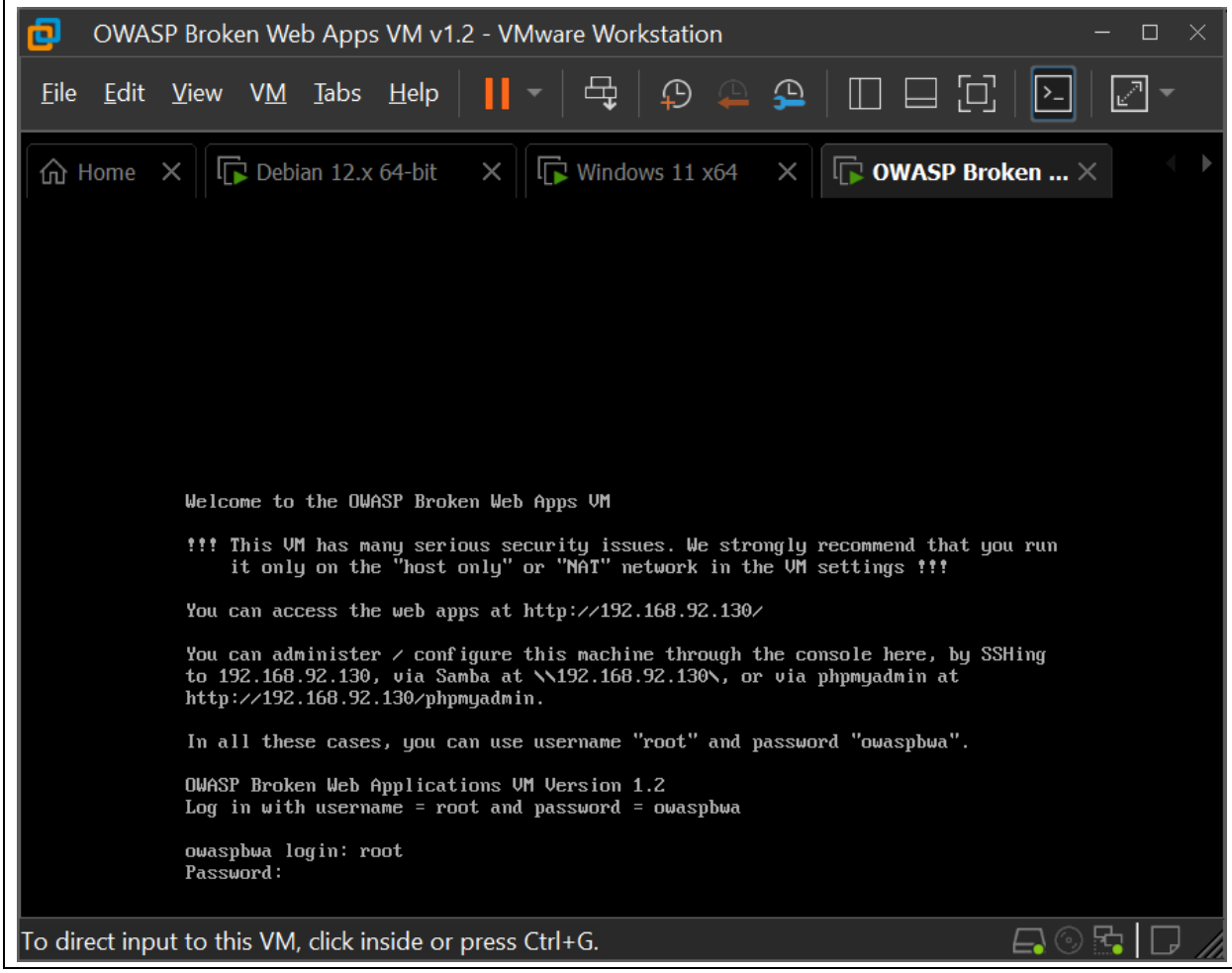
1. Create a strong password for the web server
2. Change the protocol from HTTP to HTTPS.
3. Enable Multi Factor Authentication.
4. Create a NAT system in the server to stop the disclosure of the internal IP addresses.

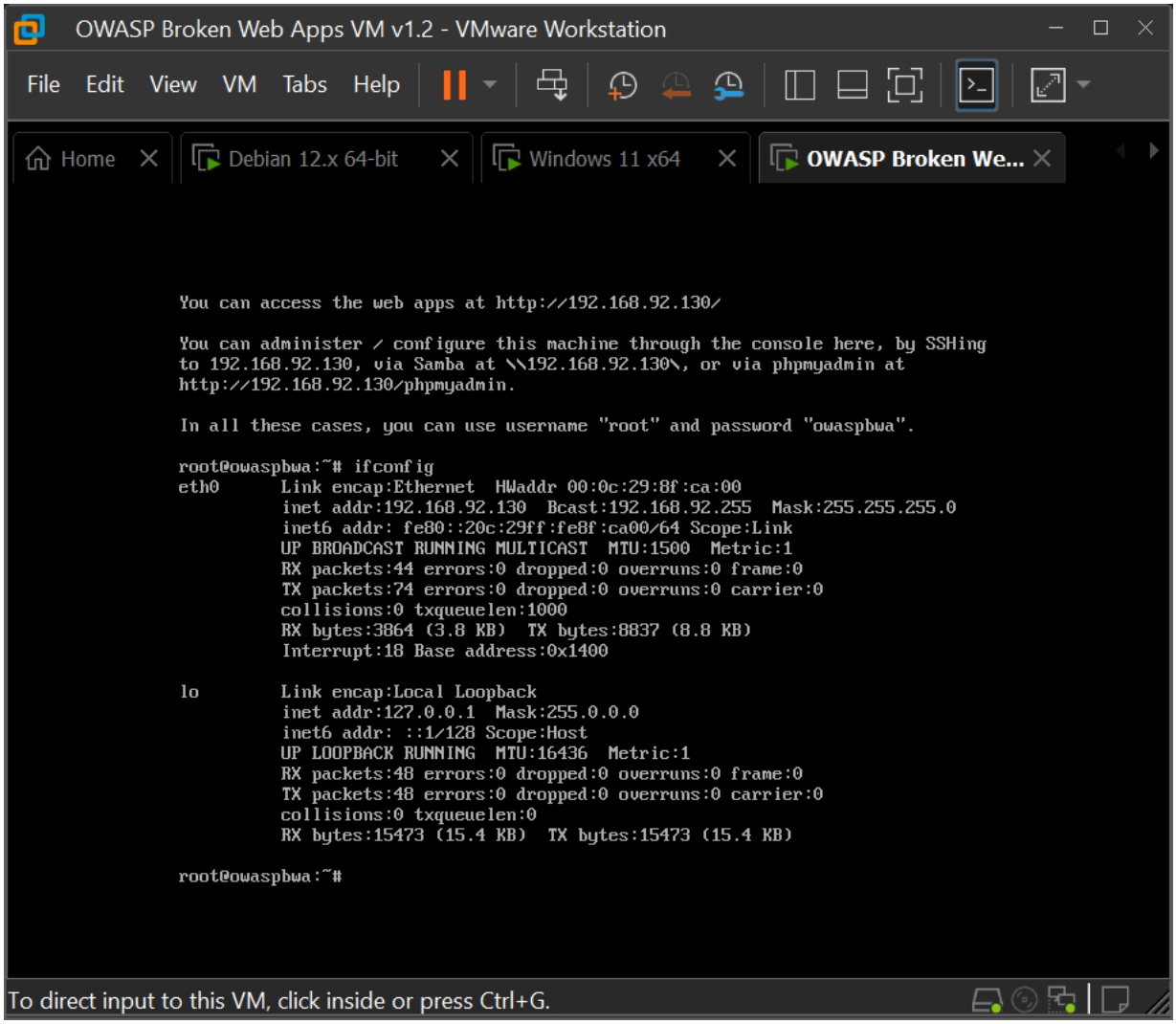
Activity 2: Learn About Web Application Exploits from WebGoat.

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/

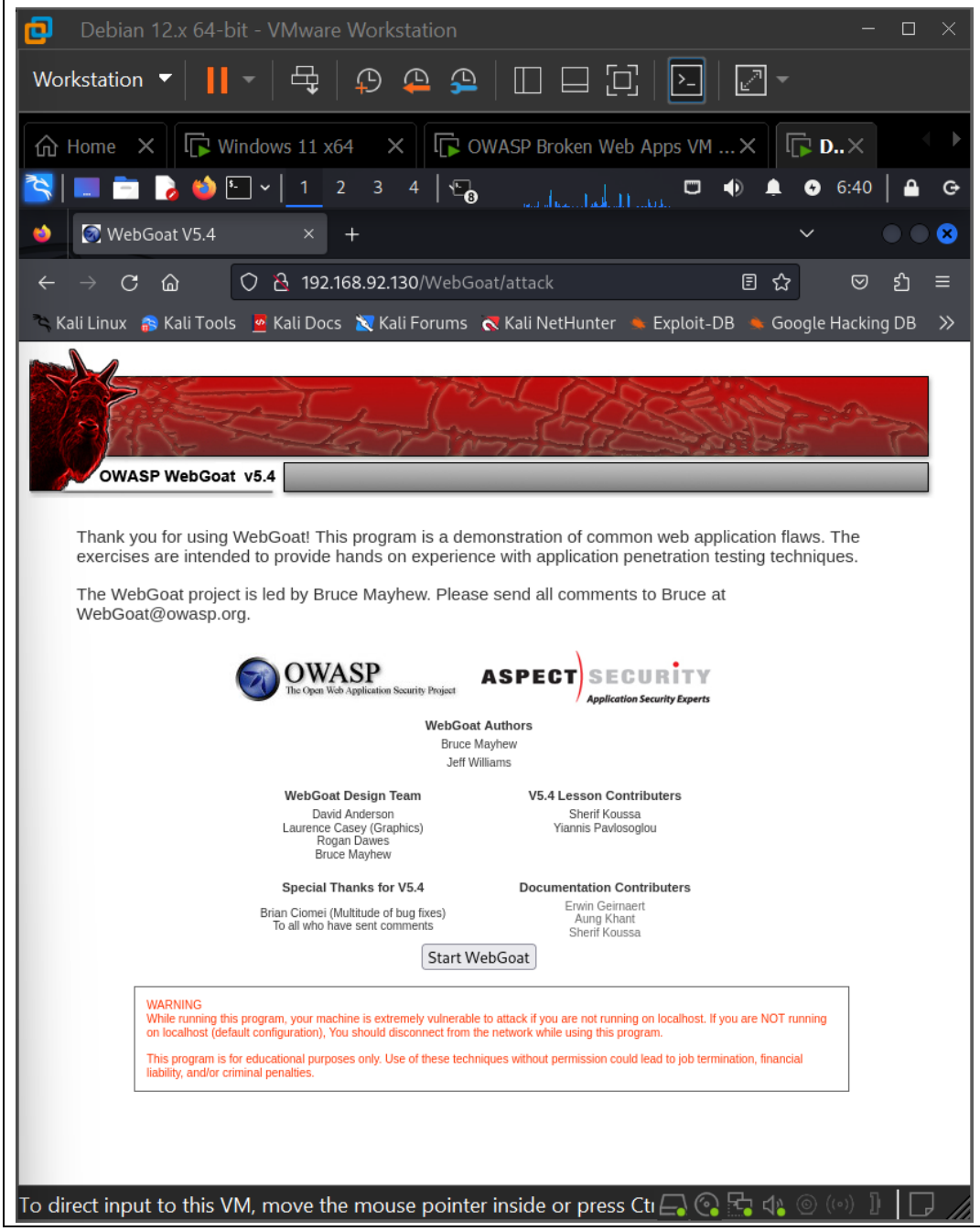
Step 2: Run the VMware VM and start WebGoat.
Run the virtual machine using VMware —you can use the free vSphere Hypervisor from www.vmware.com/products/vsphere-hypervisor.html, or the 30-day demo of Workstation Player from www.vmware.com/products/player/playerpro-evaluation.html, if not previously downloaded/using. Once the VM starts, log in as root with the password **owaspbwa** and run **ifconfig** to determine your system's IP address.

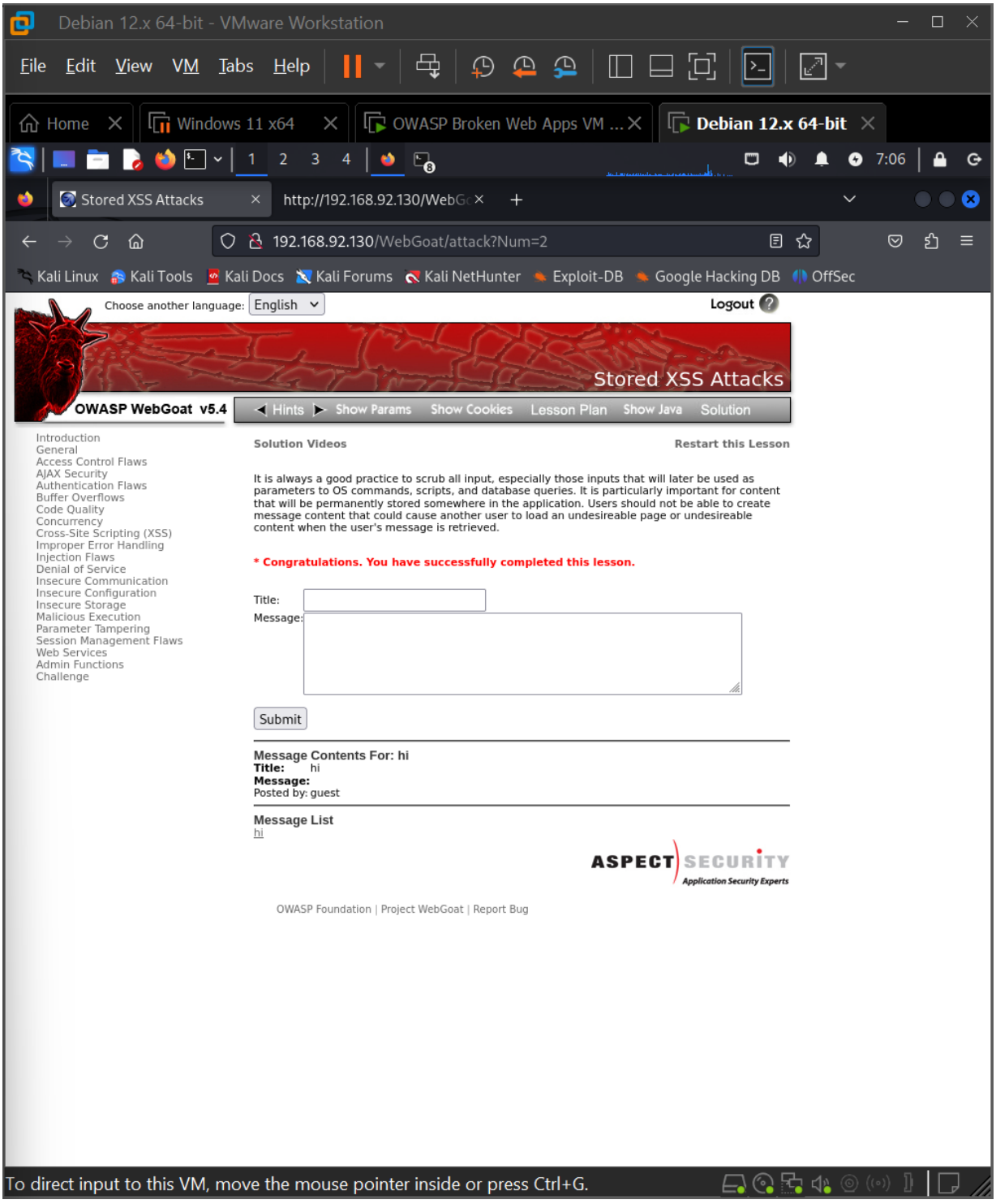


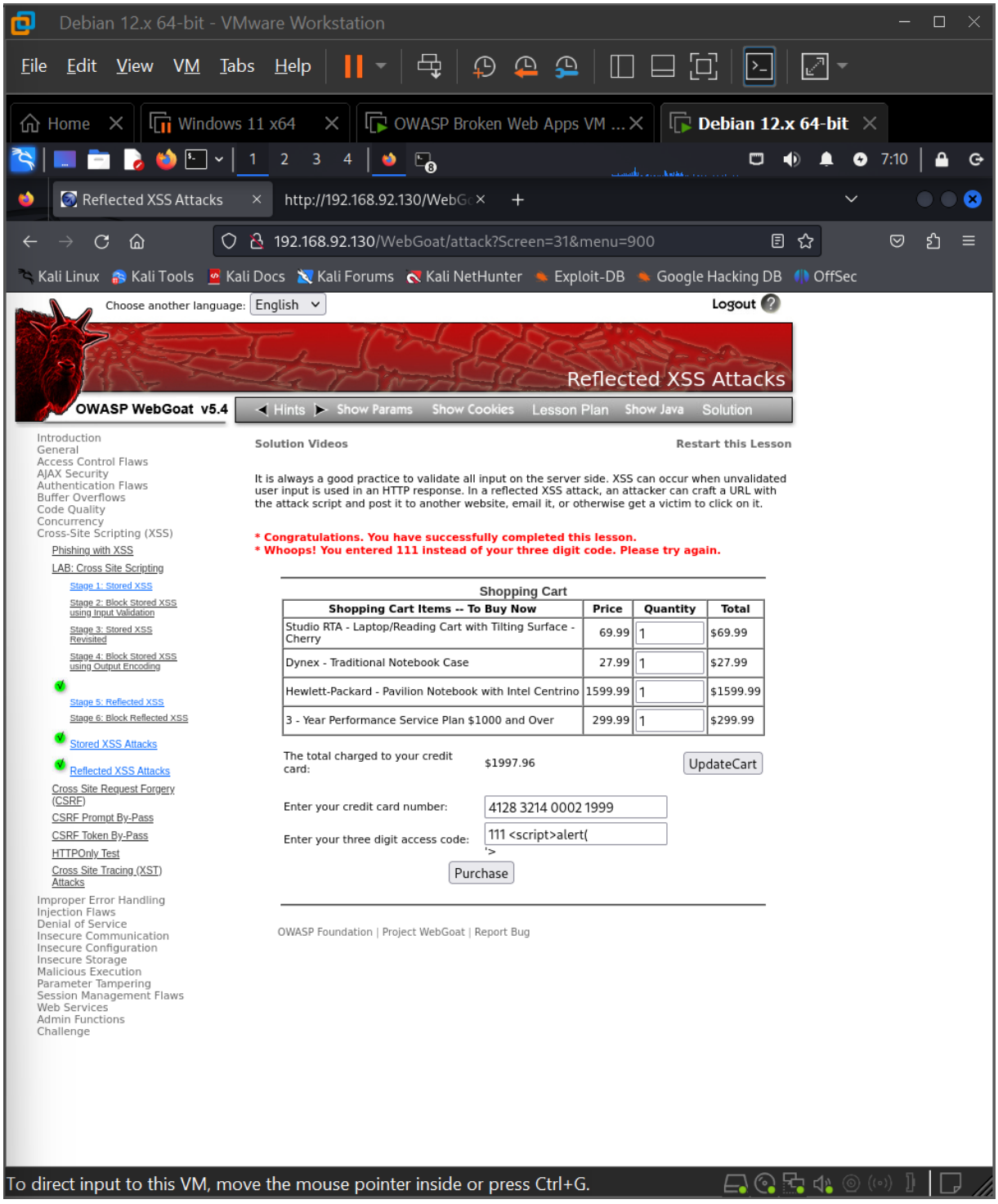

OWASP Broken Web Apps VM v1.2 - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 12.x 64-bit
Windows 11 x64
OWASP Broken We...
You can access the web apps at http://192.168.92.130/
You can administer / configure this machine through the console here, by SSHing
to 192.168.92.130, via Samba at \\192.168.92.130\, or via phpmyadmin at
http://192.168.92.130/phpmyadmin.
In all these cases, you can use username "root" and password "owaspbwa".
root@owaspbwa:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:8f:ca:00
inet addr:192.168.92.130 Bcast:192.168.92.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe8f:ca00/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:44 errors:0 dropped:0 overruns:0 frame:0
TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3864 (3.8 KB) TX bytes:8837 (8.8 KB)
Interrupt:18 Base address:0x1400
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:48 errors:0 dropped:0 overruns:0 frame:0
TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:15473 (15.4 KB) TX bytes:15473 (15.4 KB)
root@owaspbwa:~#
To direct input to this VM, click inside or press Ctrl+G.

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), or visit YouTube, where you will find numerous videos that show step-by-step guides to the solutions.



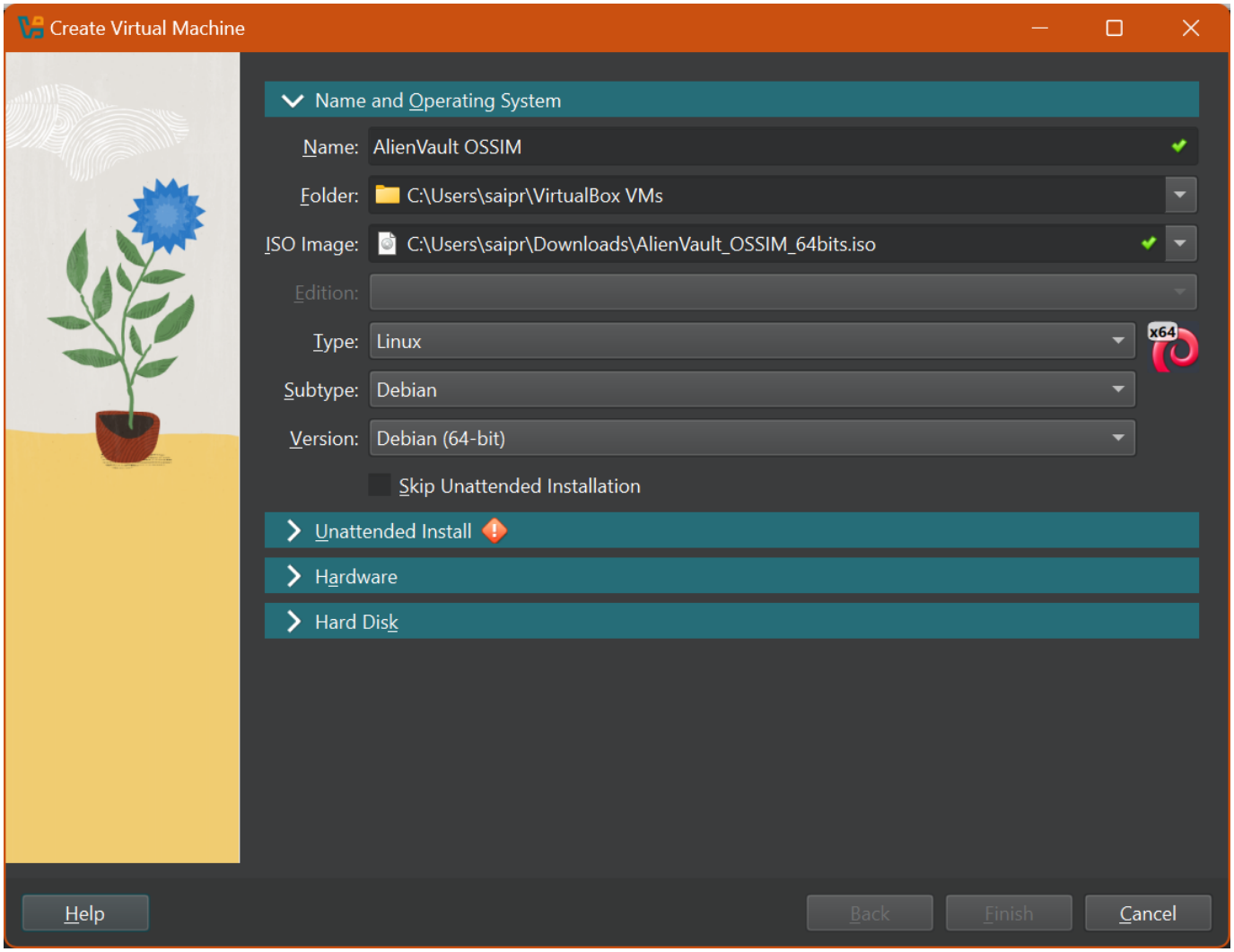

Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 11 x64
OWASP Broken Web Apps VM ...
Debian 12.x 64-bit
Stored XSS Attacks
http://192.168.92.130/WebG
192.168.92.130/WebGoat/attack?Num=2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Choose another language: English
Logout
Stored XSS Attacks
OWASP WebGoat v5.4
Hints Show Params Show Cookies Lesson Plan Show Java Solution
Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions
Challenge
Solution Videos
Restart this Lesson
It is always a good practice to scrub all input, especially those inputs that will later be used as parameters to OS commands, scripts, and database queries. It is particularly important for content that will be permanently stored somewhere in the application. Users should not be able to create message content that could cause another user to load an undesireable page or undesireable content when the user's message is retrieved.
* Congratulations. You have successfully completed this lesson.
Title:
Message:
Submit
Message Contents For: hi
Title: hi
Message:
Posted by: guest
Message List
hi
ASPECT SECURITY
Application Security Experts
OWASP Foundation | Project WebGoat | Report Bug
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

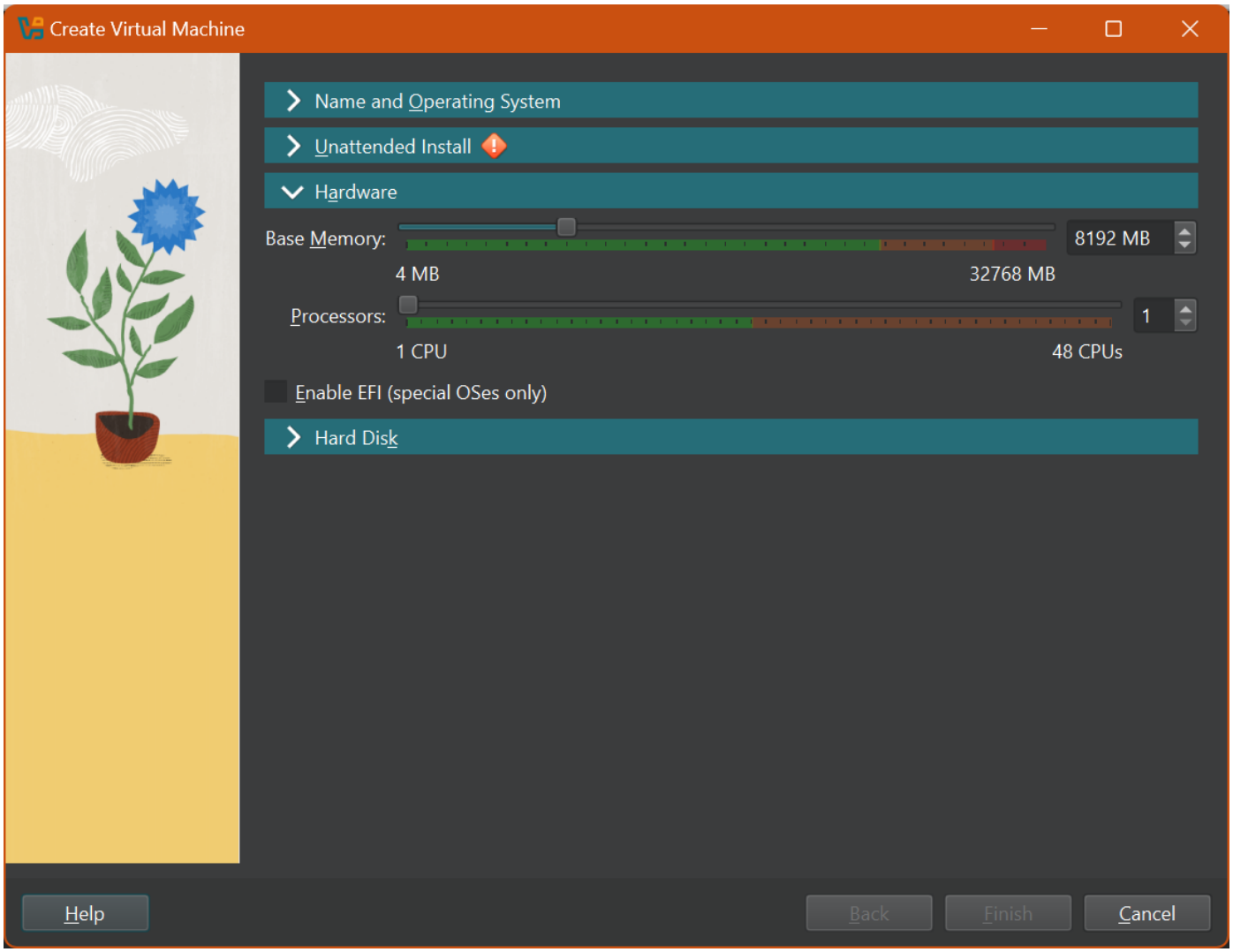

Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 11 x64
OWASP Broken Web Apps VM ...
Debian 12.x 64-bit
Reflected XSS Attacks
http://192.168.92.130/WebGo
192.168.92.130/WebGoat/attack?Screen=31&menu=900
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Choose another language: English
Logout
Reflected XSS Attacks
OWASP WebGoat v5.4
Hints Show Params Show Cookies Lesson Plan Show Java Solution
Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Phishing with XSS
LAB: Cross Site Scripting
Stage 1: Stored XSS
Stage 2: Block Stored XSS using Input Validation
Stage 3: Stored XSS Revisited
Stage 4: Block Stored XSS using Output Encoding
Stage 5: Reflected XSS
Stage 6: Block Reflected XSS
Stored XSS Attacks
Reflected XSS Attacks
Cross Site Request Forgery (CSRF)
CSRF Prompt By-Pass
CSRF Token By-Pass
HTTPOnly Test
Cross Site Tracing (XST) Attacks
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions
Challenge
Solution Videos
Restart this Lesson
It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input is used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.
* Congratulations. You have successfully completed this lesson.
* Whoops! You entered 111 instead of your three digit code. Please try again.
Shopping Cart
Shopping Cart Items -- To Buy Now
Price
Quantity
Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry
69.99
1
$69.99
Dynex - Traditional Notebook Case
27.99
1
$27.99
Hewlett-Packard - Pavilion Notebook with Intel Centrino
1599.99
1
$1599.99
3 - Year Performance Service Plan $1000 and Over
299.99
1
$299.99
The total charged to your credit card:
$1997.96
UpdateCart
Enter your credit card number:
4128 3214 0002 1999
Enter your three digit access code:
111 <script>alert(
'>
Purchase
OWASP Foundation | Project WebGoat | Report Bug
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

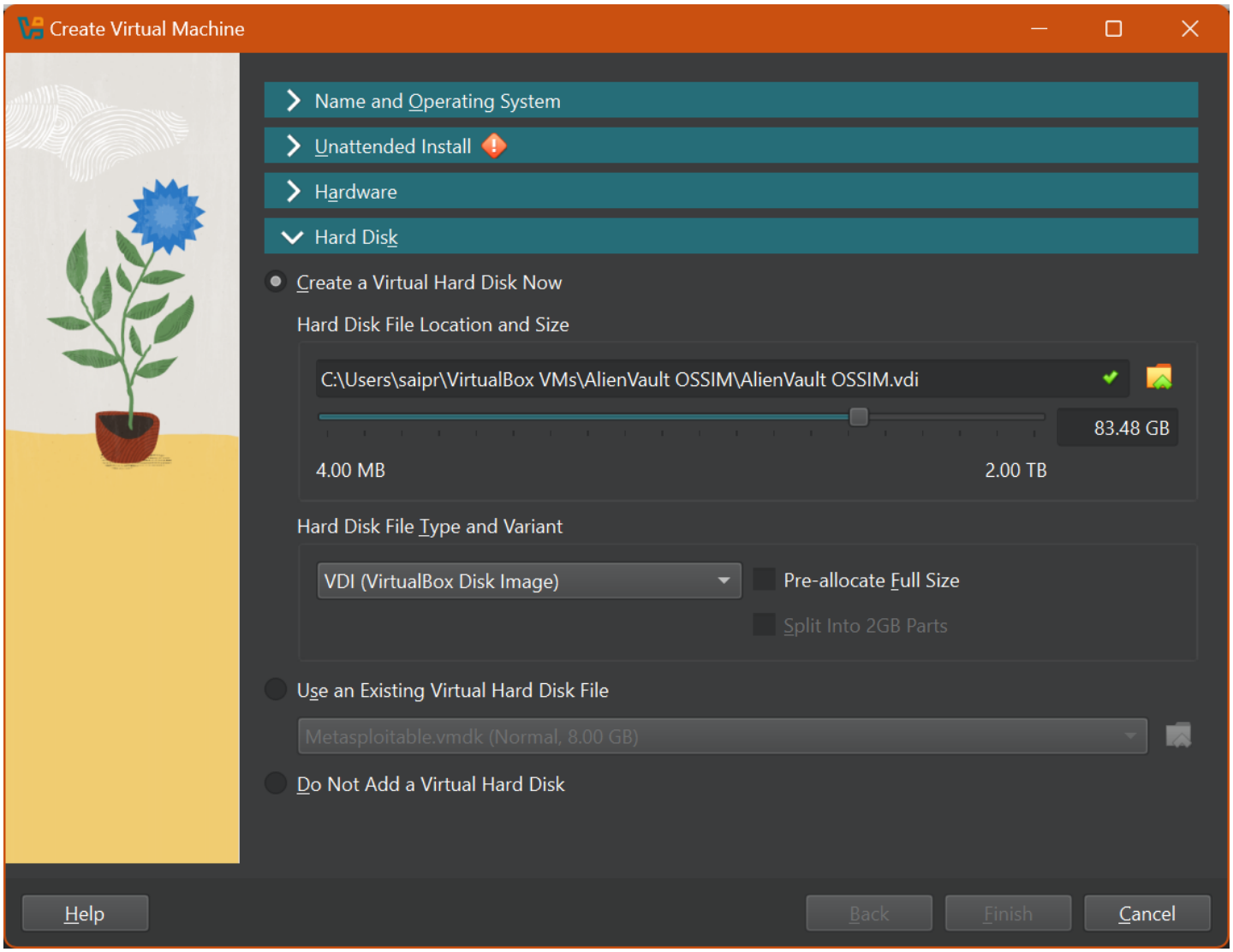
Activity 3: SIEM (Alienvault / Security Onion) - Oracle VirtualBox

In this activity, we will use Oracle Virtual box to install SIEM (Alienvault OSSIM). You are required to download AlienVault OSSIM from th
https://cybersecurity.att.com/products/ossim

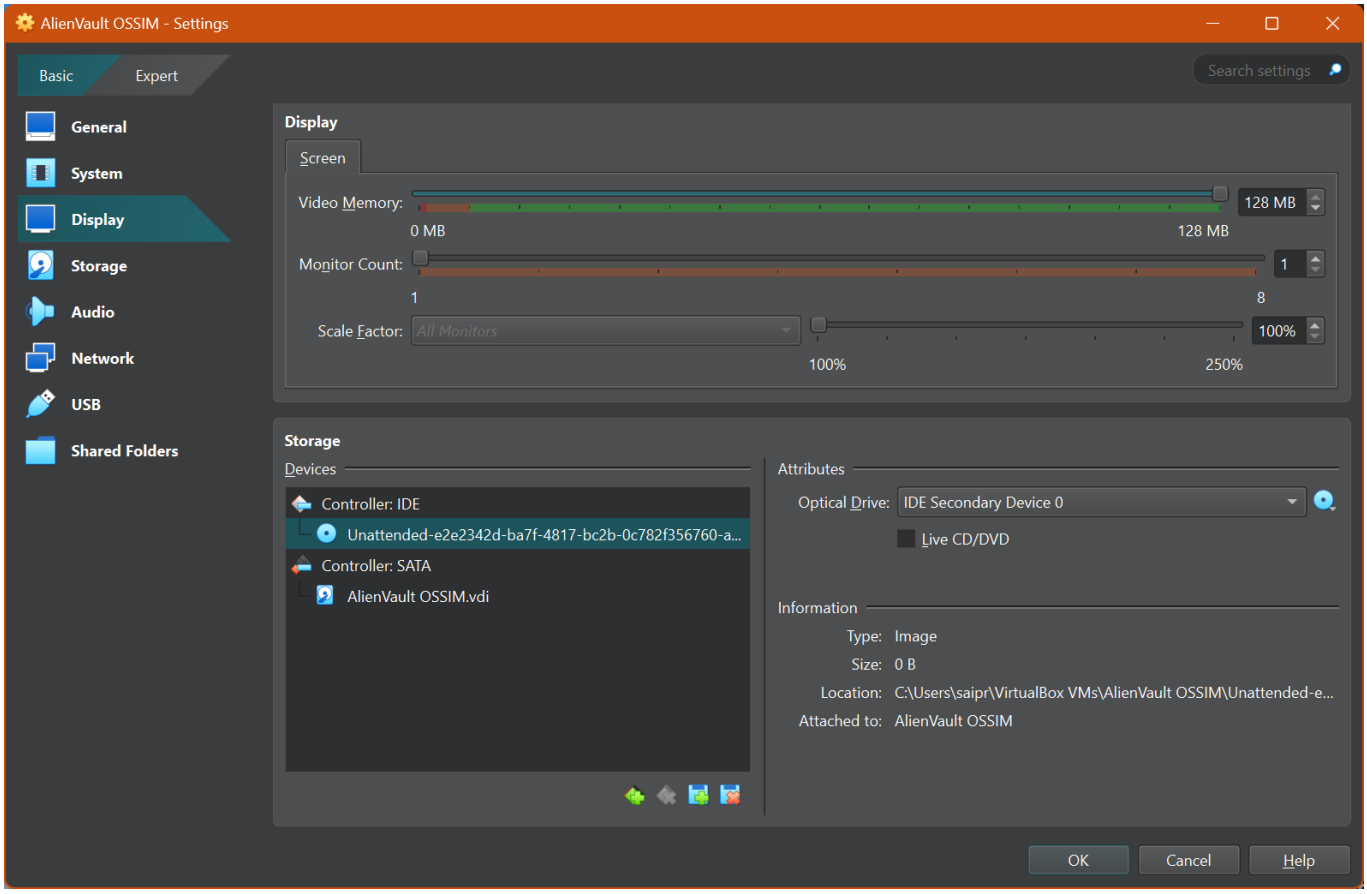
- Launch VirtualBox
- Create a New VM ○ **Name:** AlienVault OSSIM ○ **Type:** Linux ○ **Version:** Debian (64-bit) ○ **Memory Size (RAM):** 8192 MB (A
  a virtual hard disk now ○ **Hard Disk File Type:** VDI (VirtualBox Disk Image) ○ **Storage on physical hard disk:** Dynamically allocat
  GB



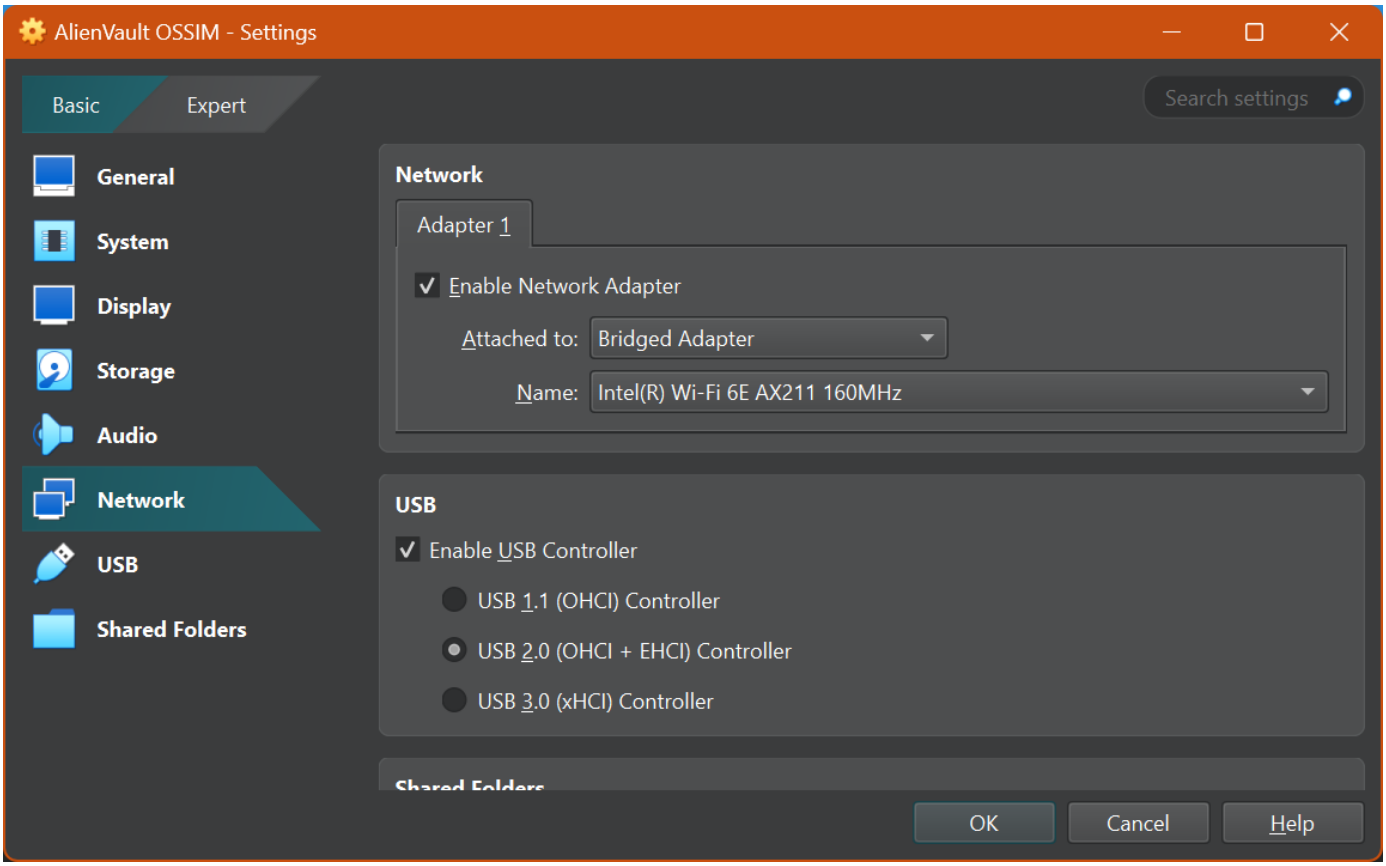

Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory:
8192 MB
4 MB
32768 MB
Processors:
1
1 CPU
48 CPUs
Enable EFI (special OSes only)
Hard Disk
Help
Back
Finish
Cancel


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
C:\Users\saipr\VirtualBox VMs\AlienVault OSSIM\AlienVault OSSIM.vdi
83.48 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split Into 2GB Parts
Use an Existing Virtual Hard Disk File
Metasploitable.vmdk (Normal, 8.00 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Finish
Cancel

- 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

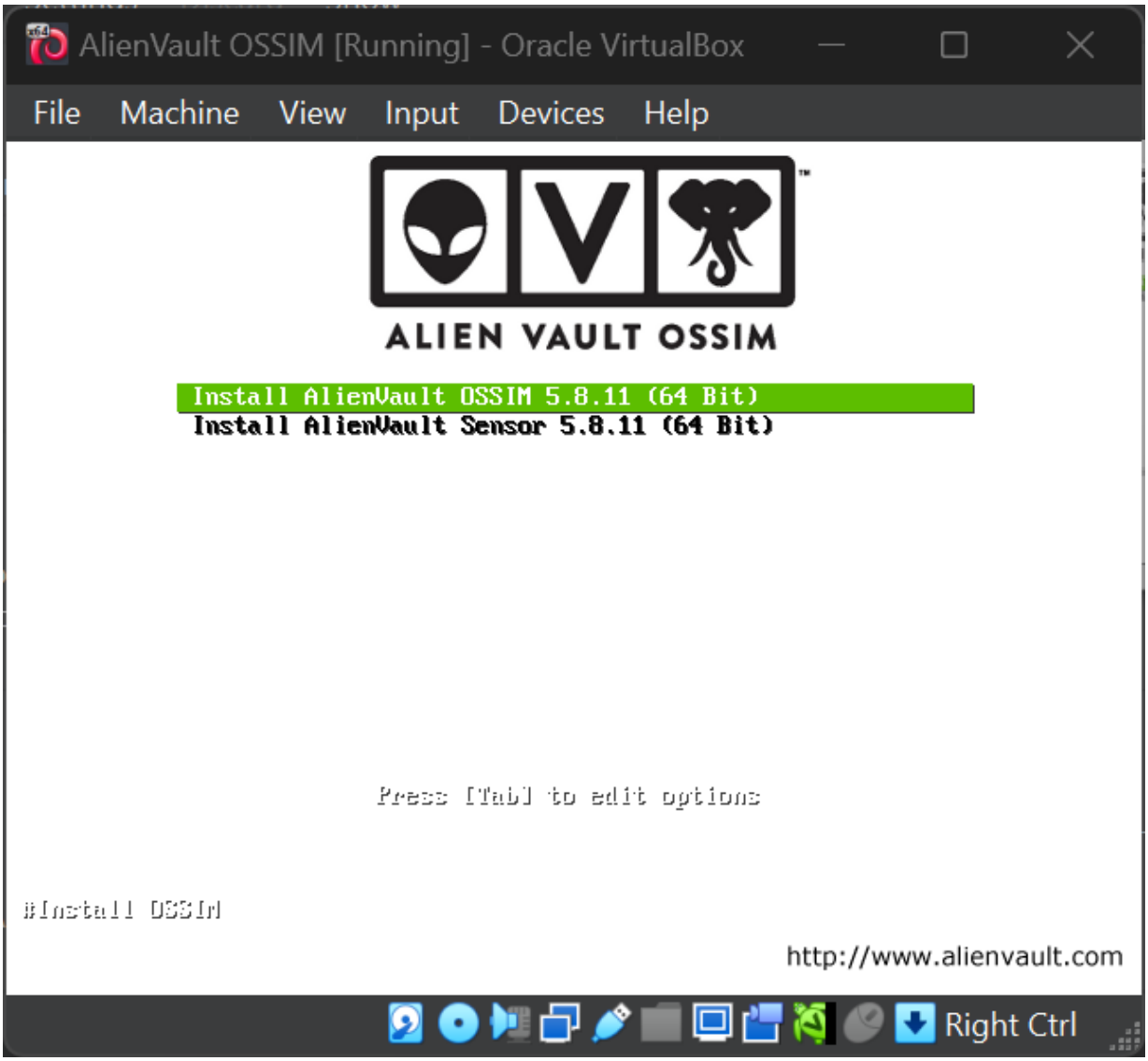


○ **Network:** Bridged Adapter ○ Click **OK.**

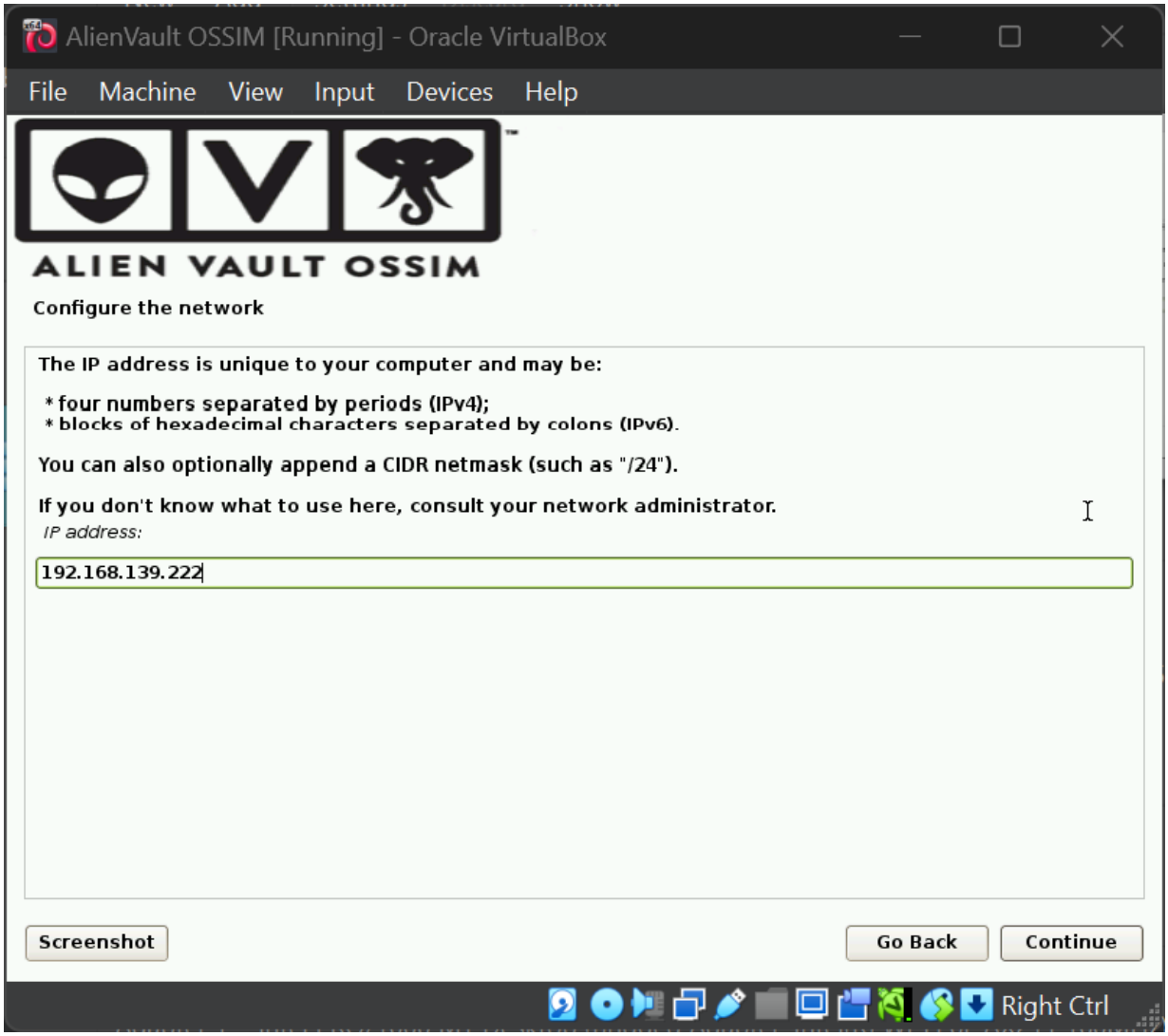


Start to install the AlienVault OSSIM VM ○ Click on first option: **Install AlienVault OSSIM (64 Bit)**

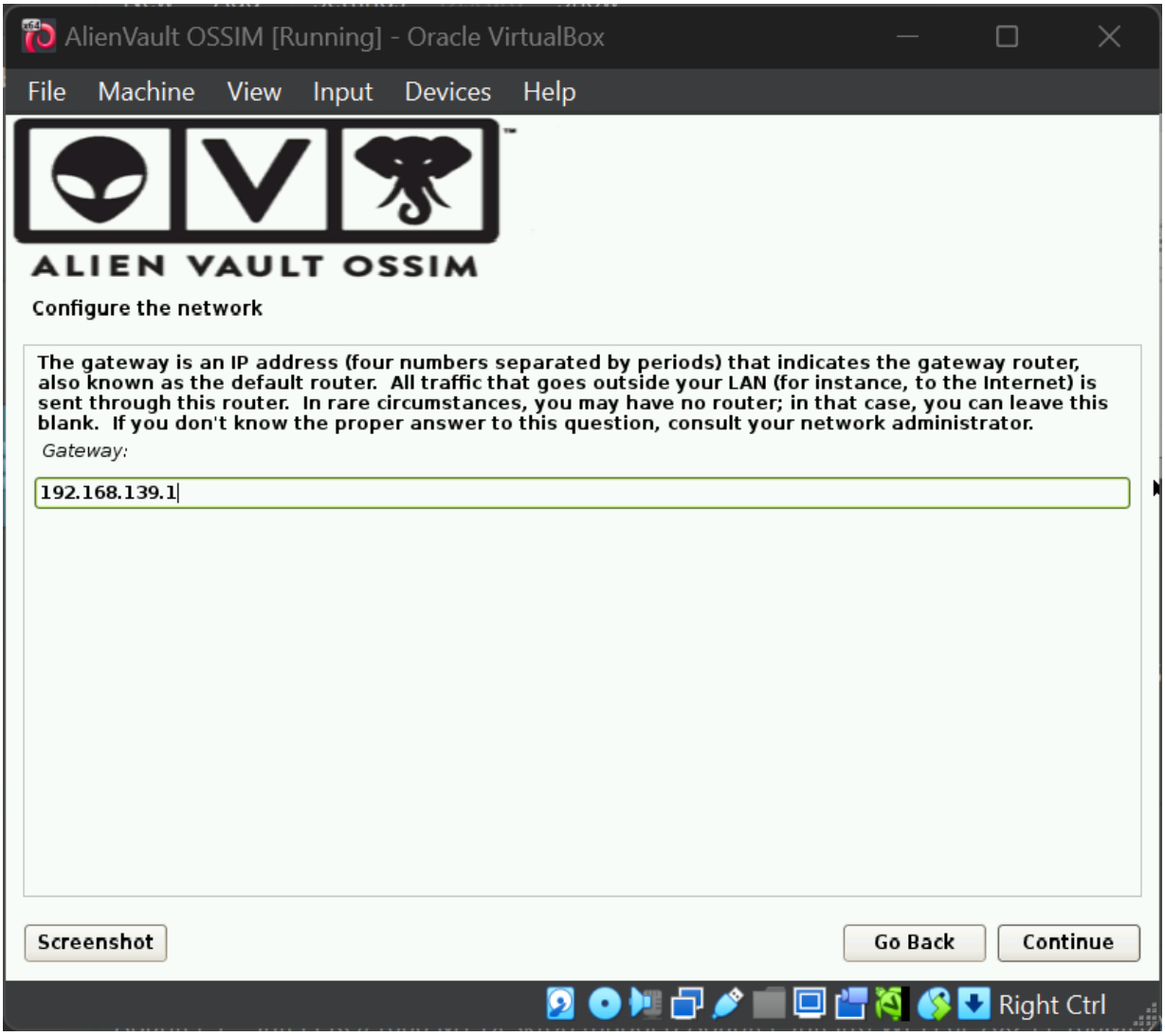
Note: Do not click on second option “Install AlienVault Sensor,” because the First Option AlienVault OSSIM is installed in head office and then AlienVault Sensor is installed in branch offices.



○ **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.

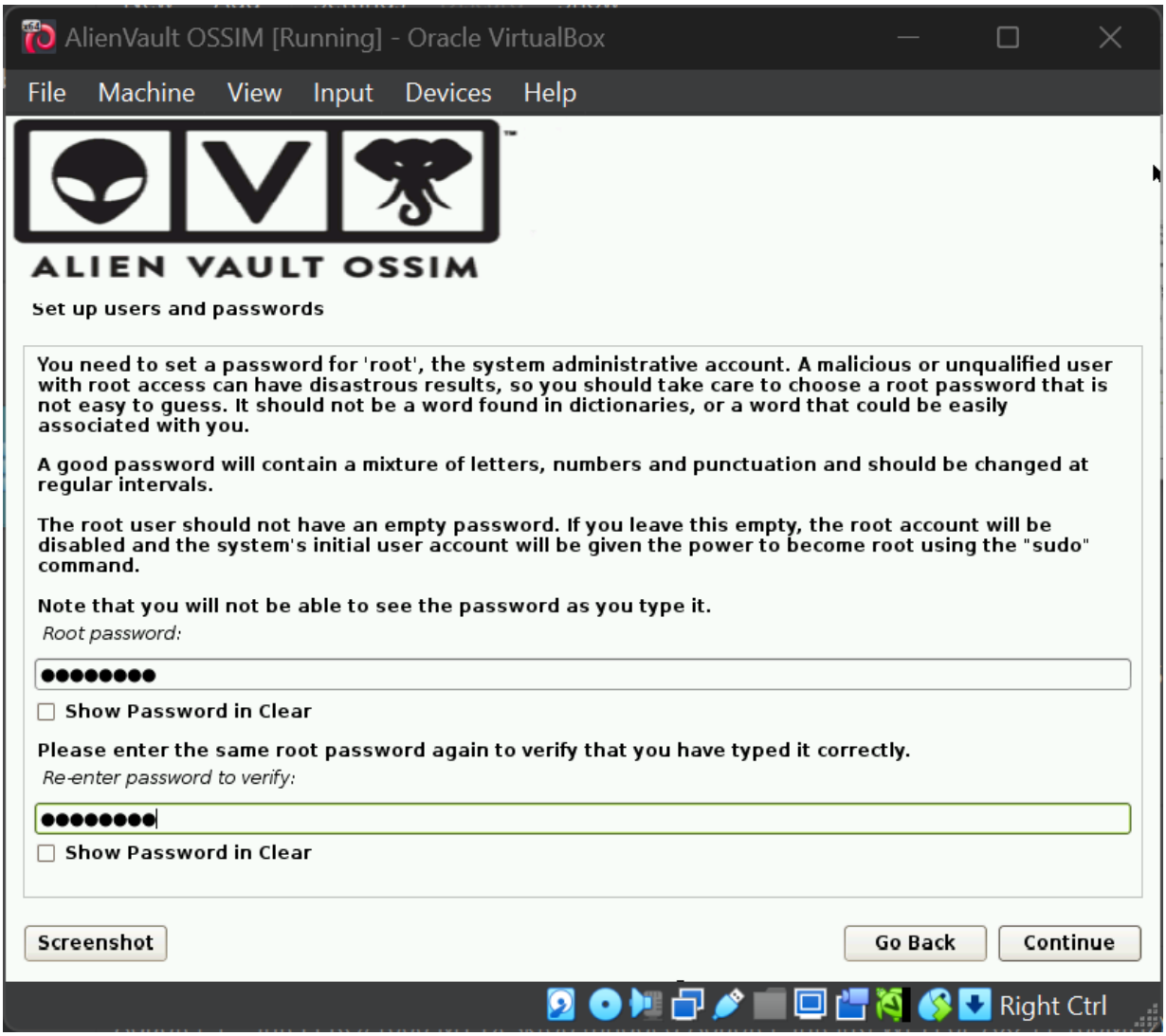


- **Subnet Mask**: (Keep the default) ○ **Gateway**: (Keep the default) ○ **DNS Server:** (Keep the default)

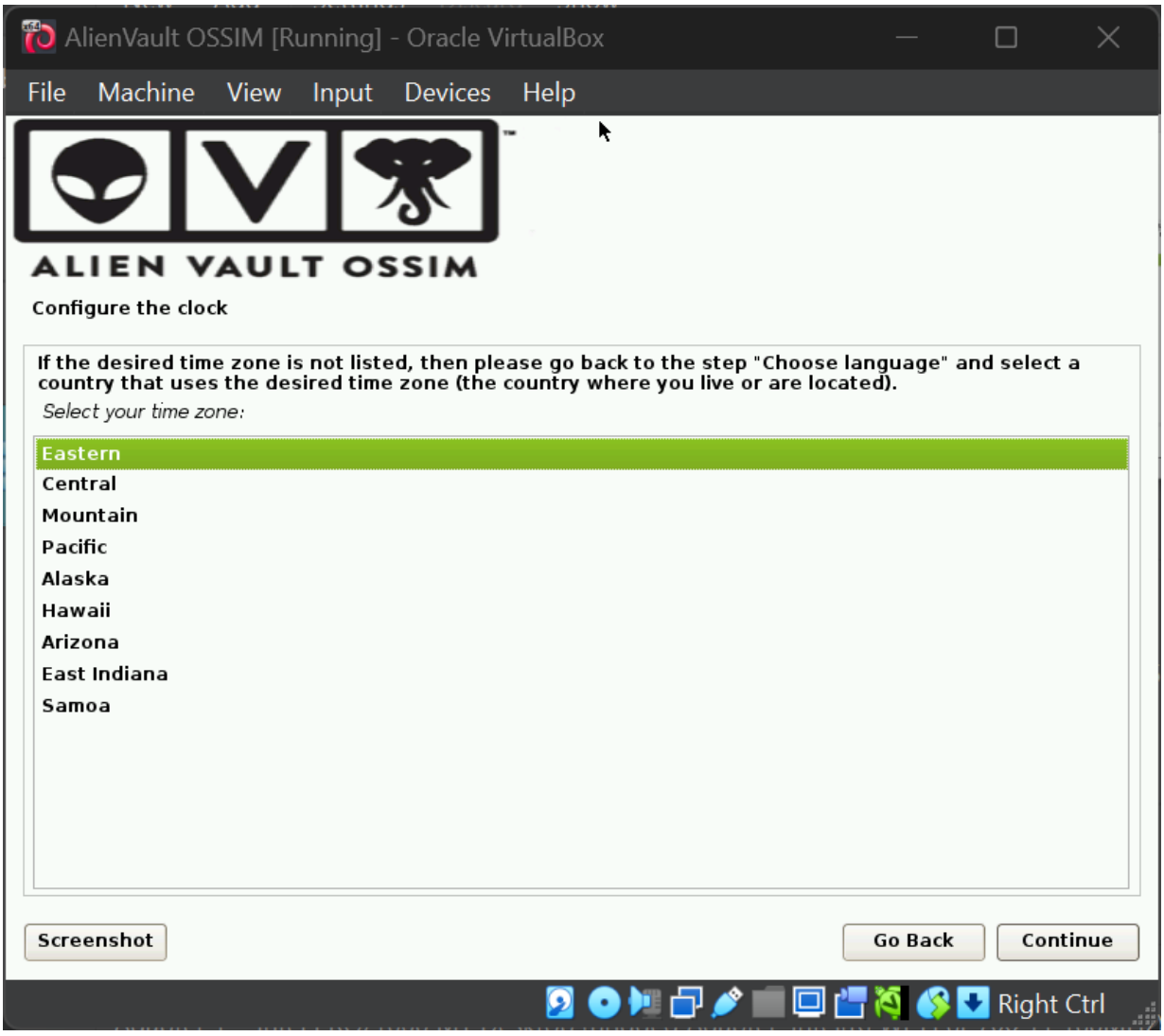


○ **Set up users and passwords:**

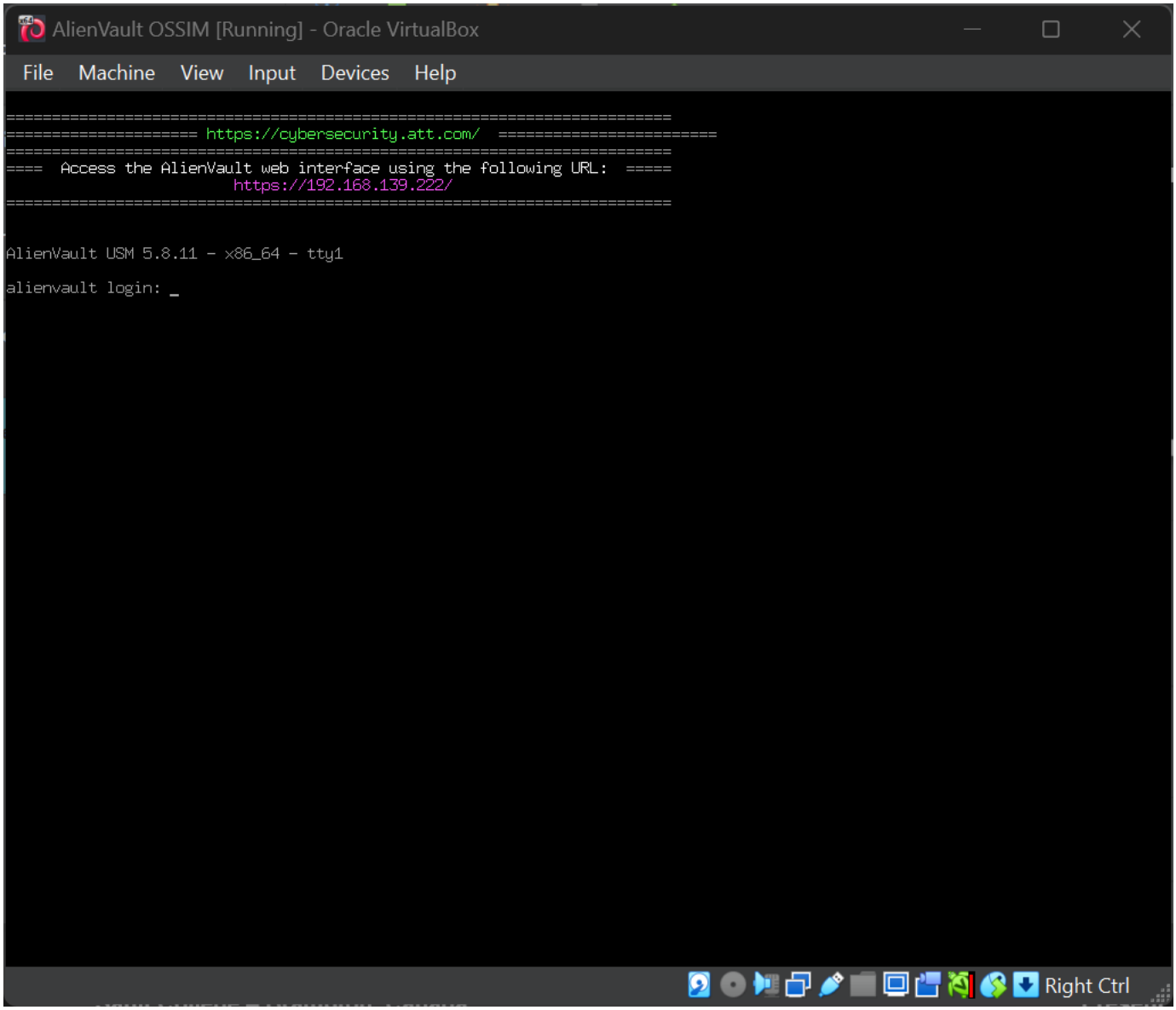
- Root Password: Alien123
- Re-enter Password: Aline123



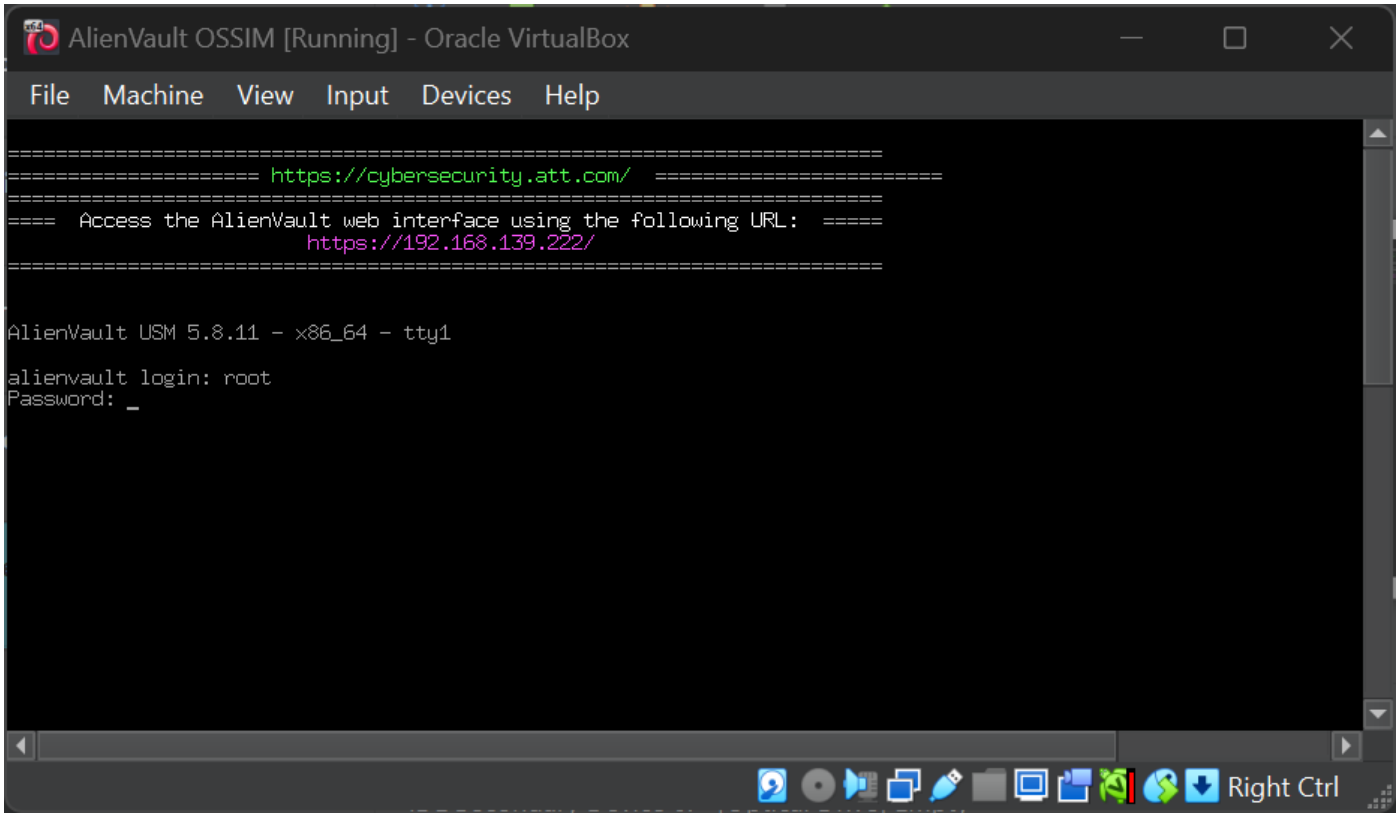
○ **Configure the clock:** Eastern



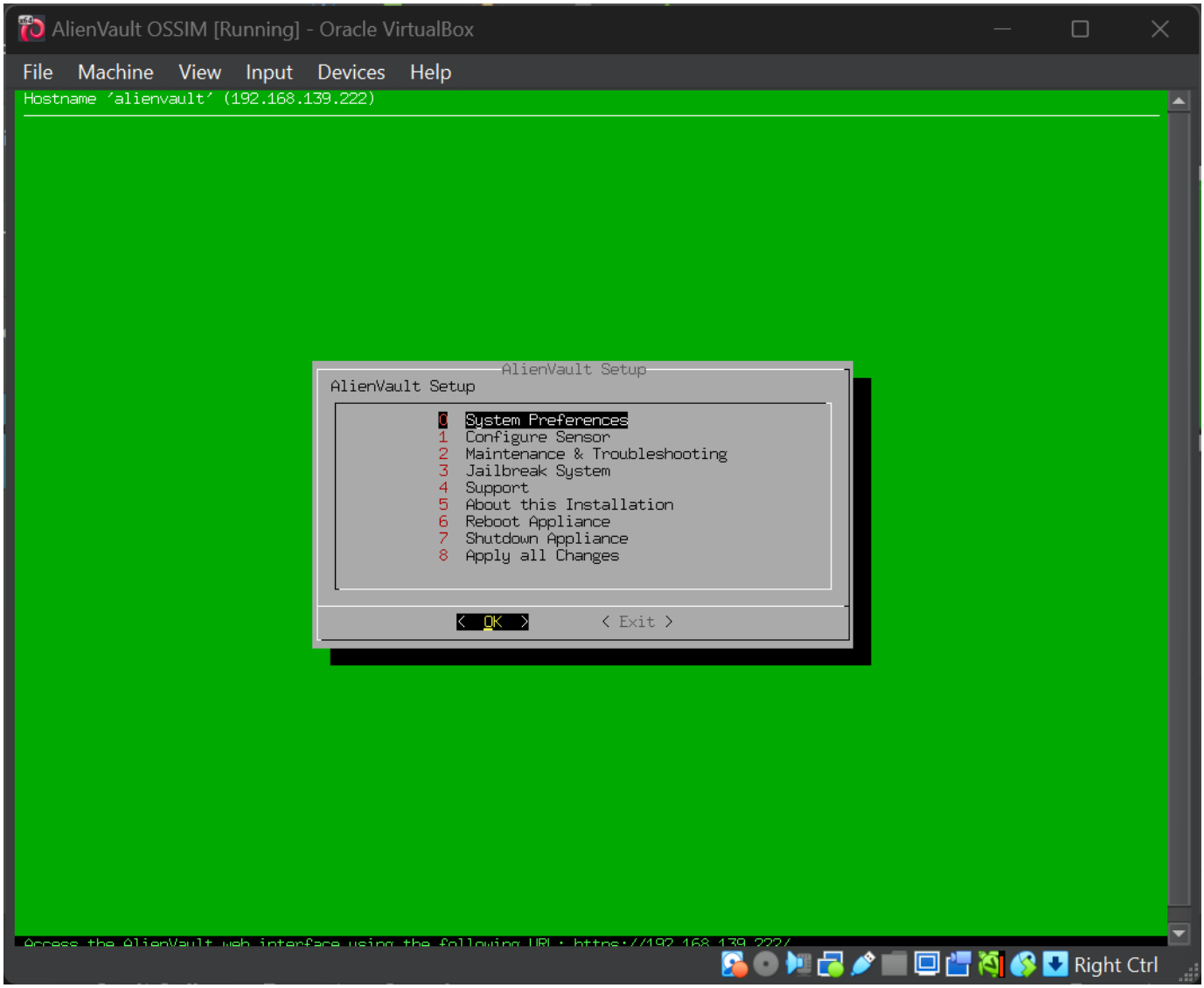
After the successful installation (it may take long time, sometimes hours), you will be able to see a black Debian screen.



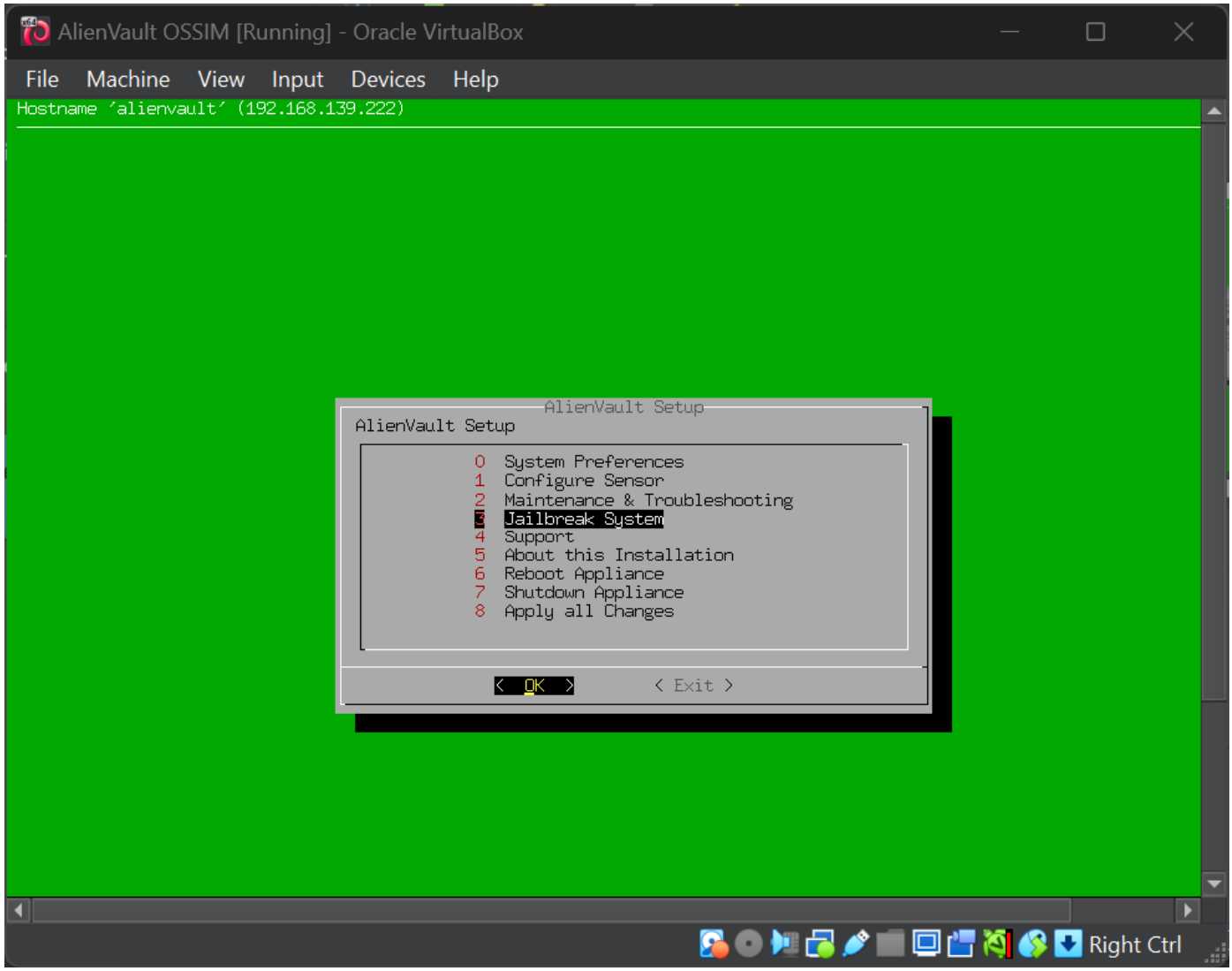
- Log in as **root** and use the password **Alien123.**



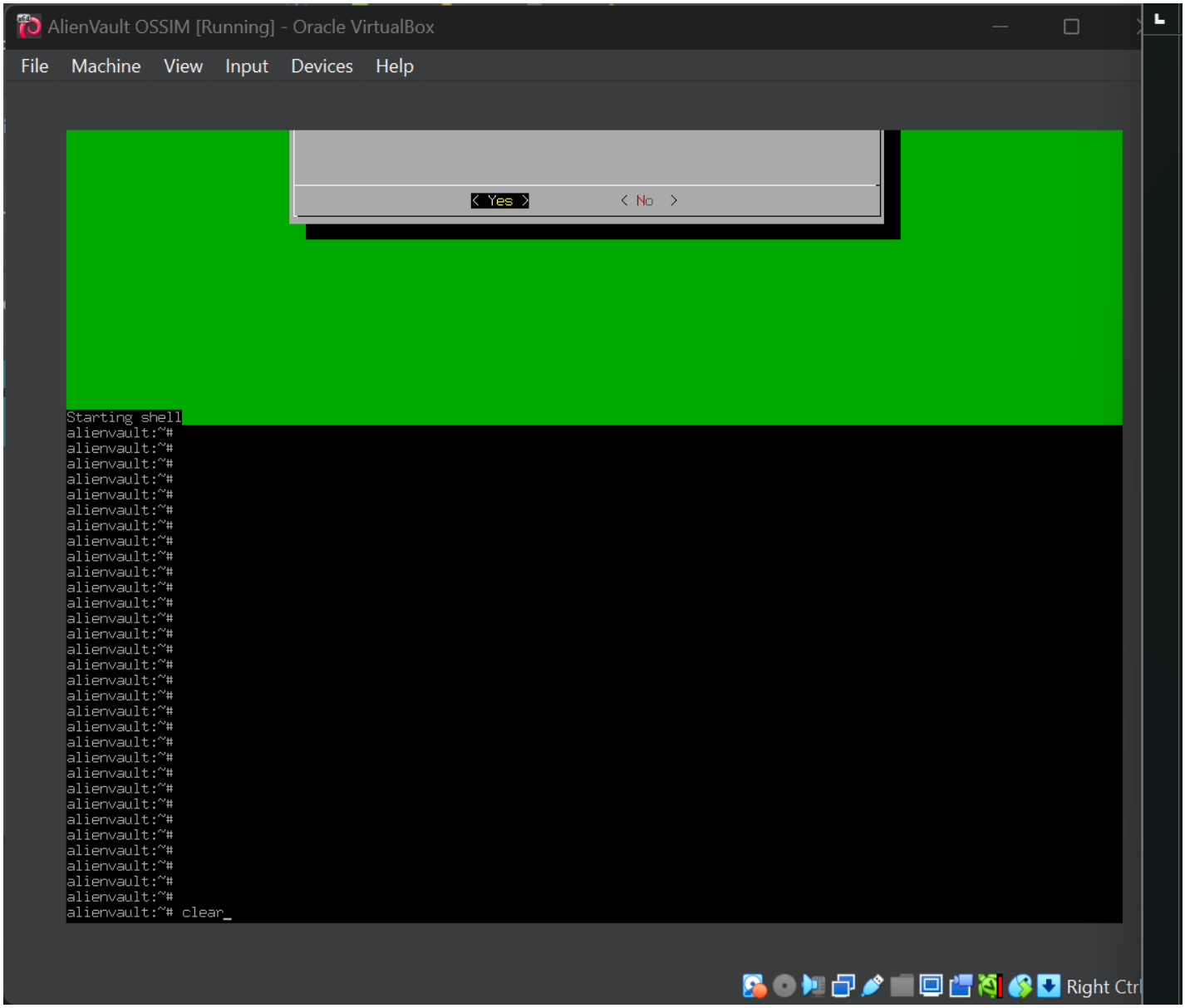
- A small menu driven window will appear.



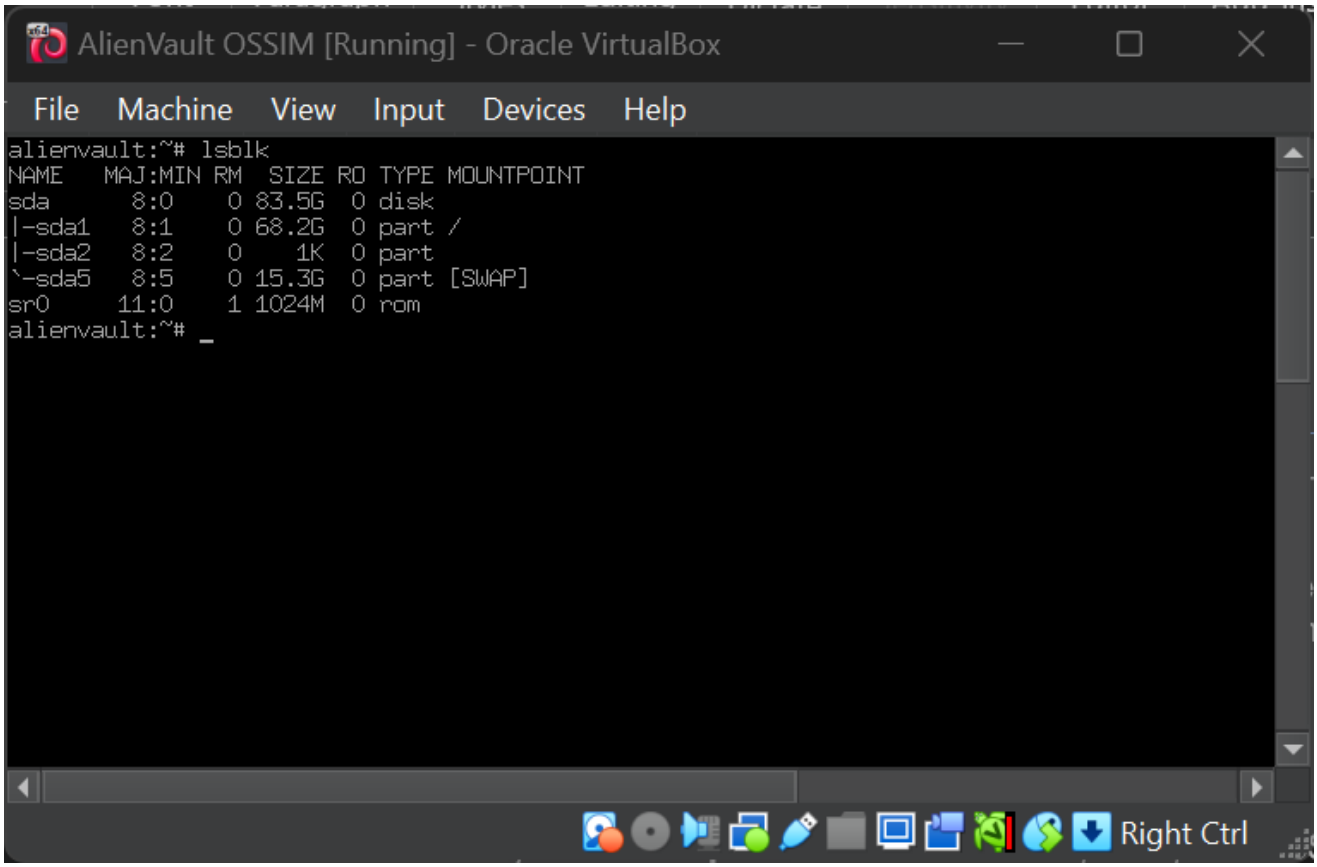
- Select 4th Option: Jailbreak System.



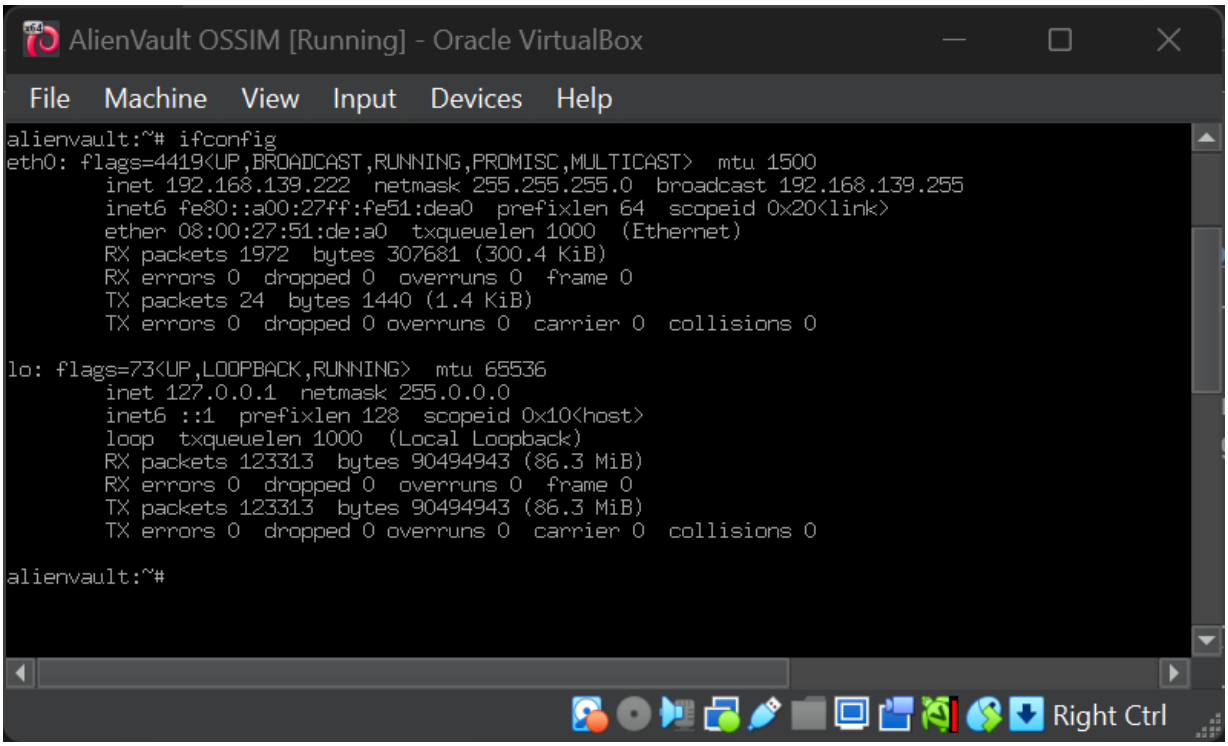
- Continue?: **Yes** ○ Type **clear** (in the bottom-left corner of the screen to clear the screen).



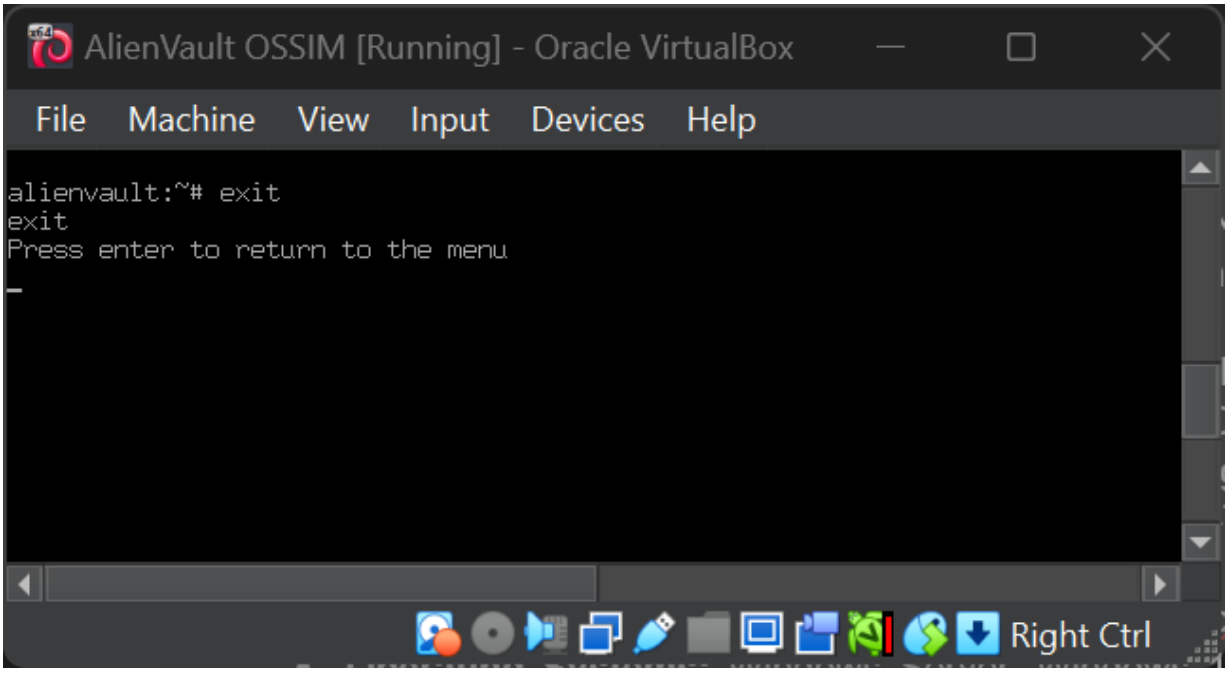
○ Type **lsblk** (you should be able to see sda : 80G disk).



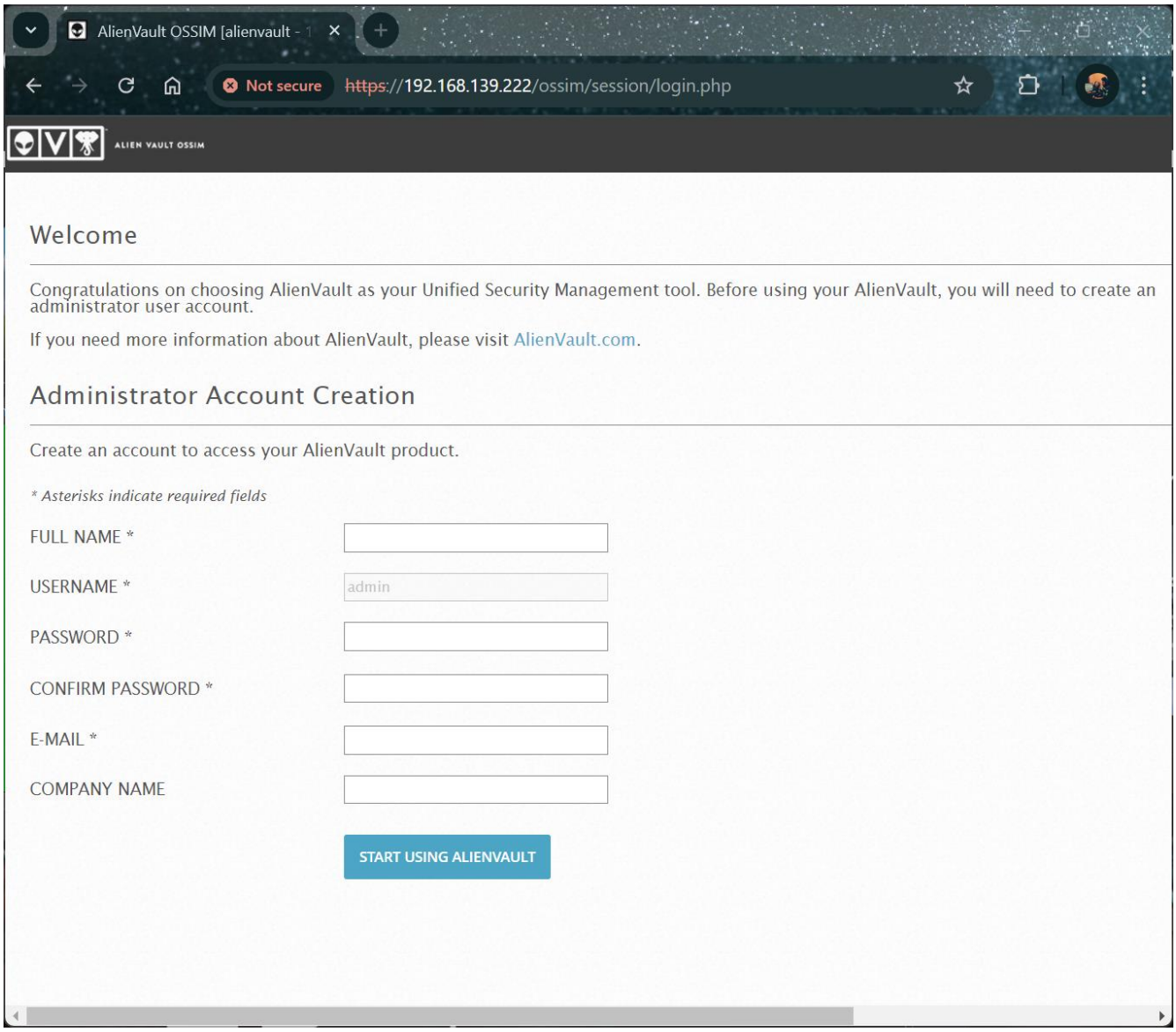
○ Type **ifconfing** (note the inet ip address).



○ Type **exit.**

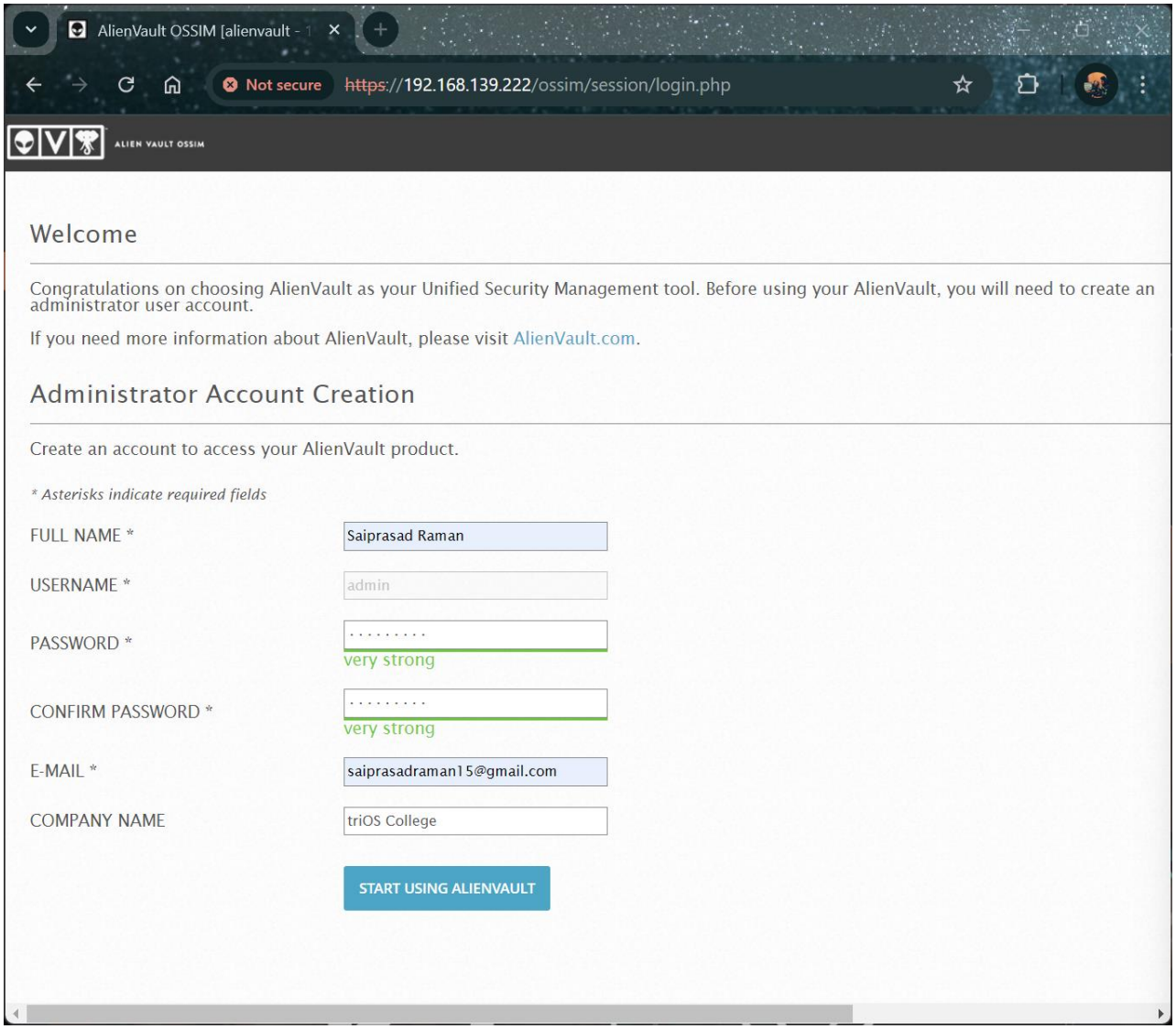


- Launch Google Chrome browser on your host machine (not on VM).
- Type the ip address at URL as https://___.___.___.___ (the IP address that you noted down after the ifconfig command above).
- Click **Advanced,** and then click **proceed to ___.___.___.___**

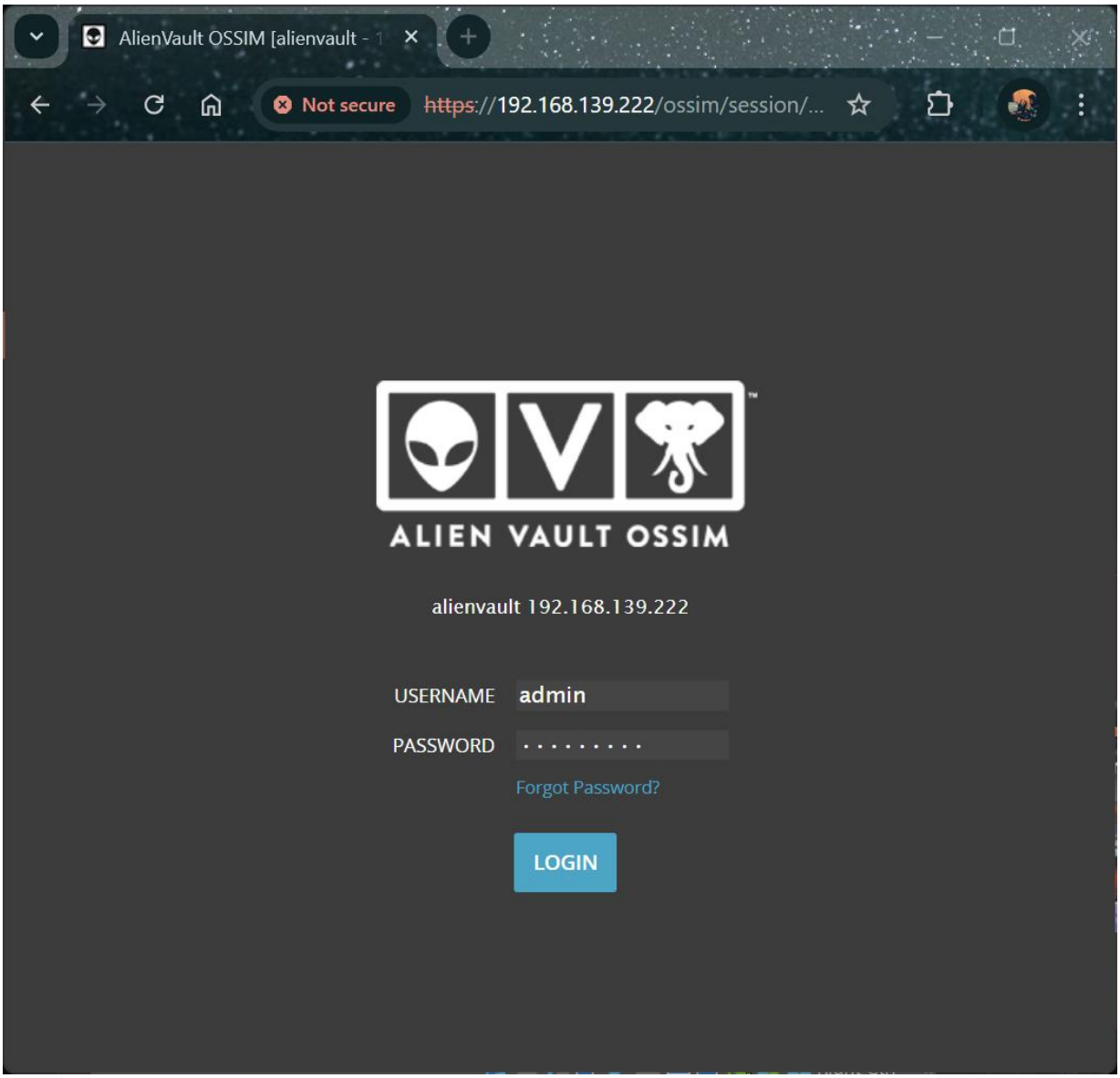


- **Administrator Account Creation:**
  - **Full Name:** (Your full name)
  - **USERNAME:** (Admin) Do not change
  - **Password:** Ossim_123
  - **Confirm Password:** Ossim_123
  - **Email:** (Your triOS college email address)
  - **Company Name:** triOS College
  - **Location:** Toronto **(Take the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

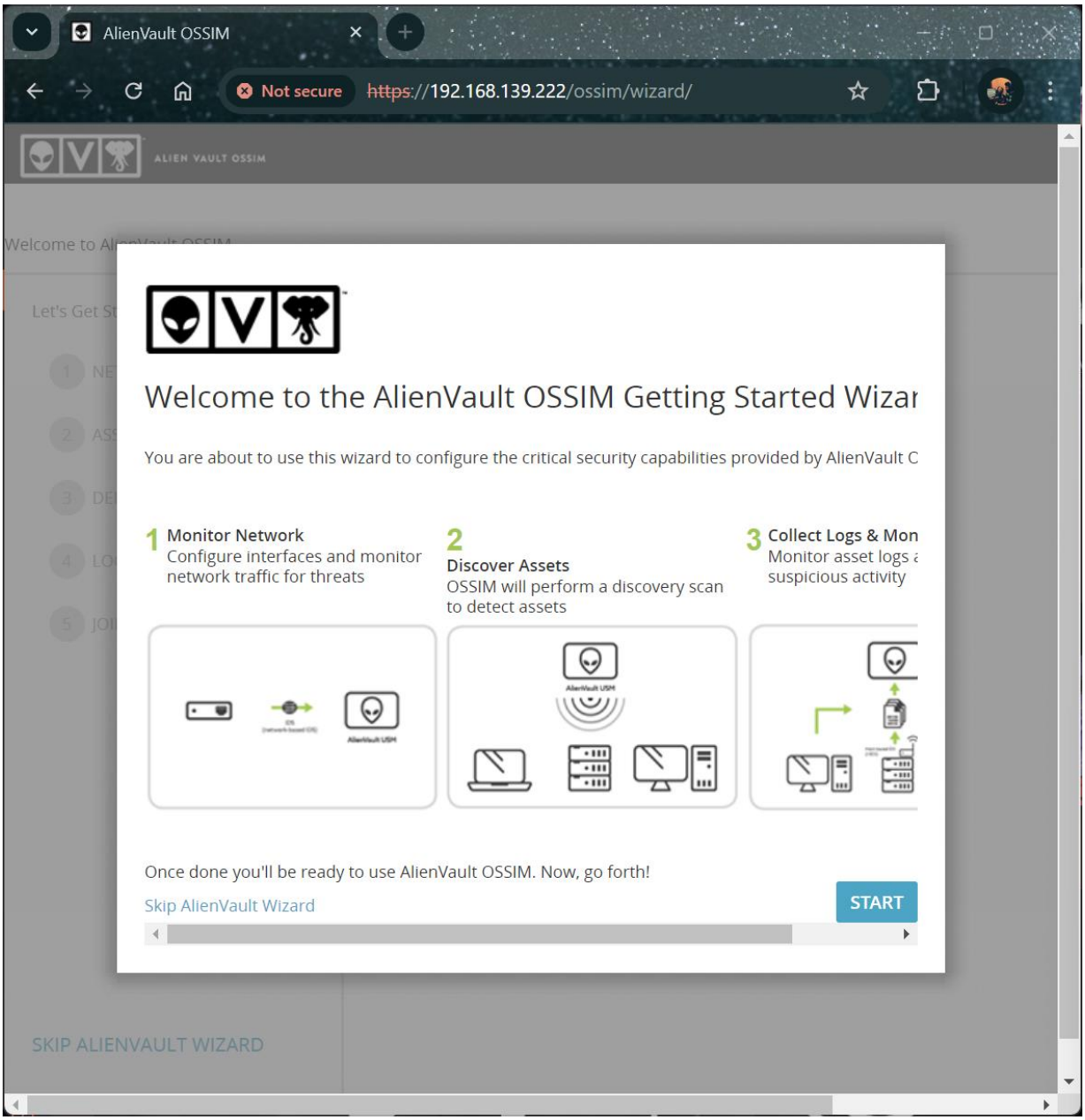
(Now click **Start Using AlienVault.**)



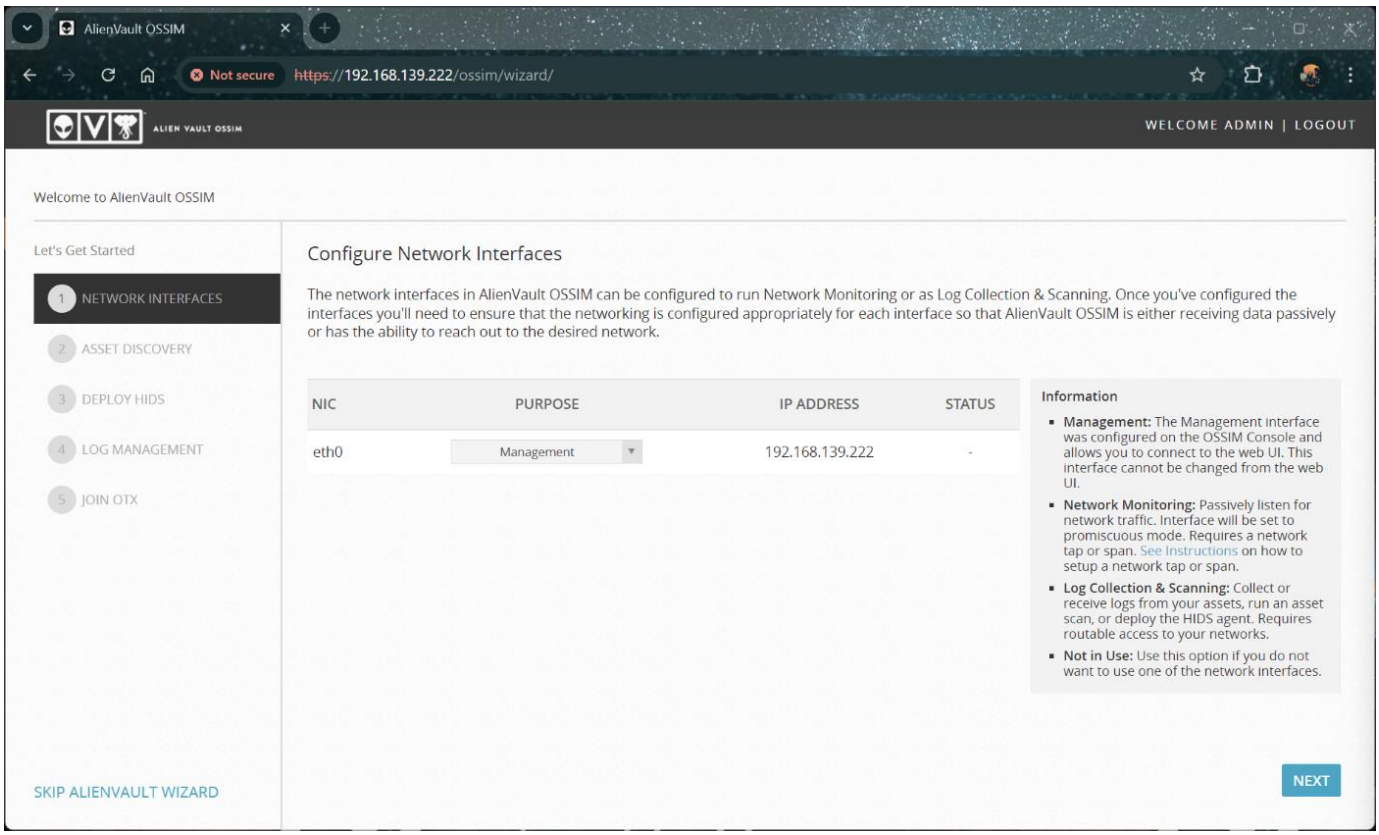
○ **USERNAME:** admin ○ **Password:** Ossim_123



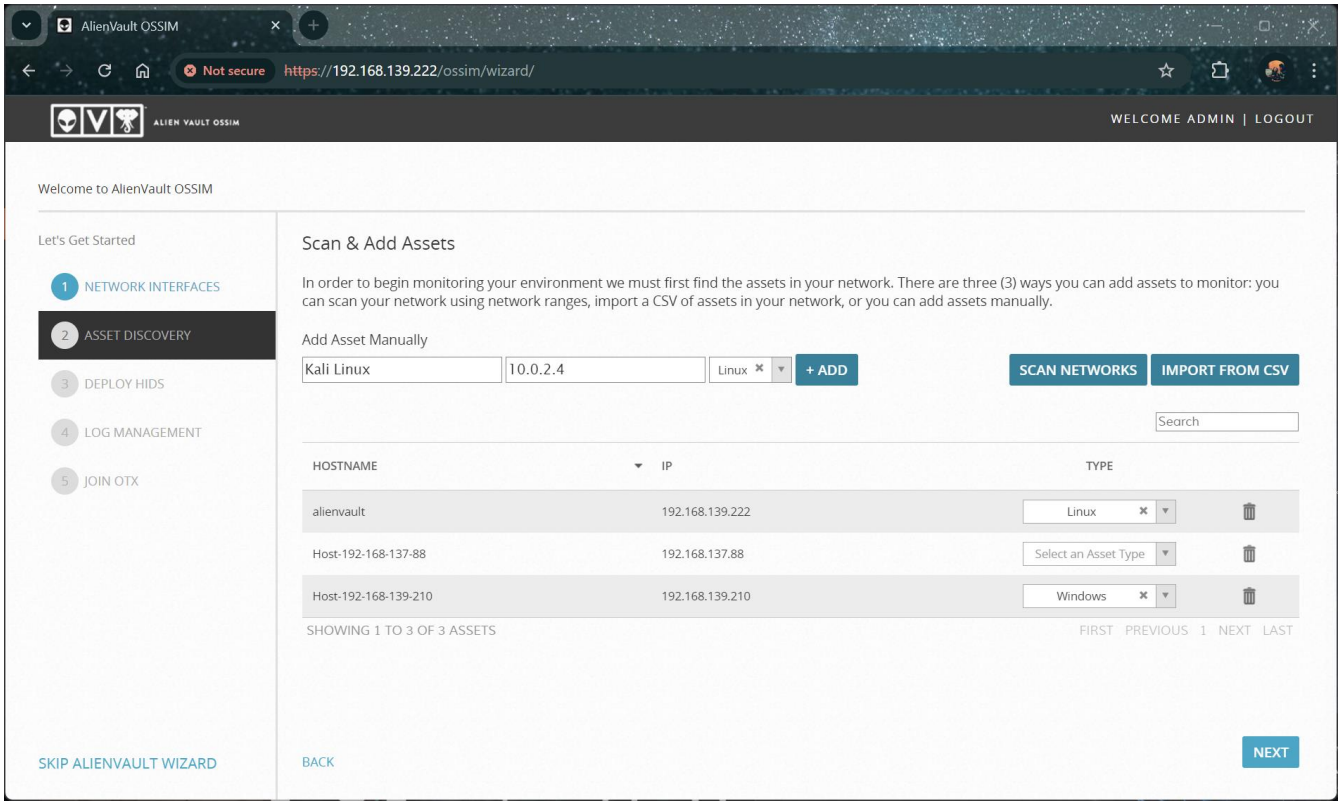
○ On the Welcome to AlienVault OSSIM Getting Started Wizard, click **START.**



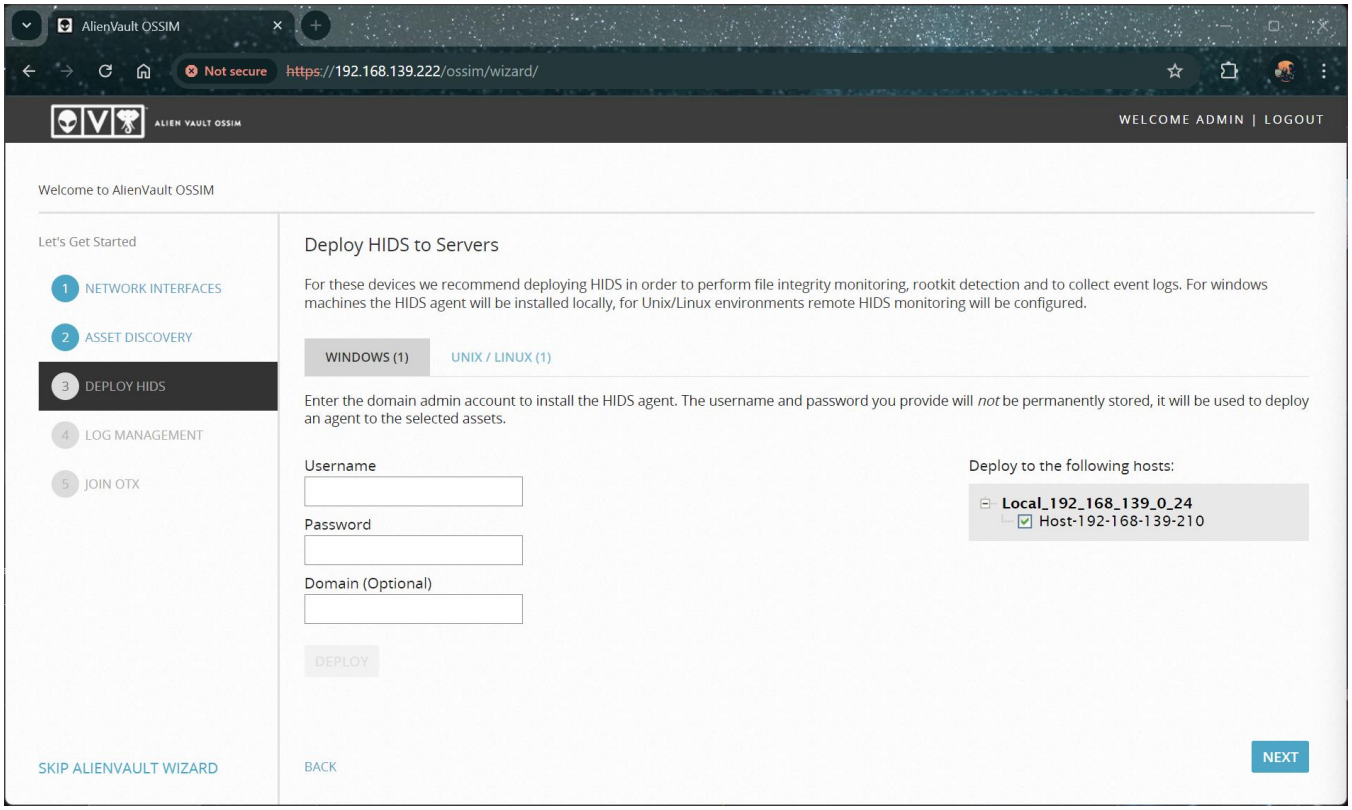
- **Network Interface:** Click **Next**.



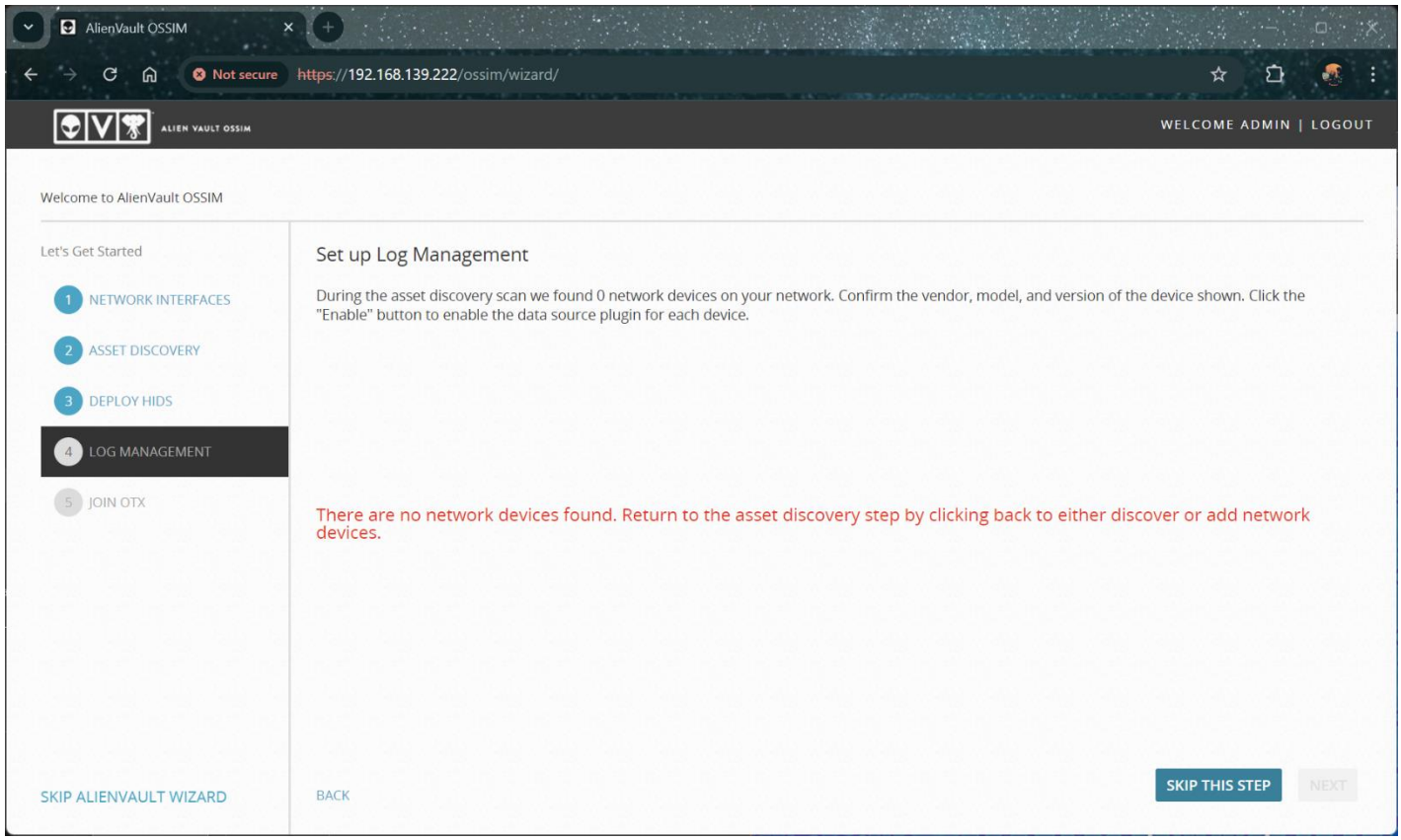
- **Asset Discovery:** Add assets manually, if you do not find other VMs.
  - **Hostname:** (Hostname of the other VM)
  - **IP address:** (IP address of the other VM)
  - **Select an Asset Type:** Windows/Linux/Network Device
- Click **Add**. It should be able to find your AlienVault along with other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



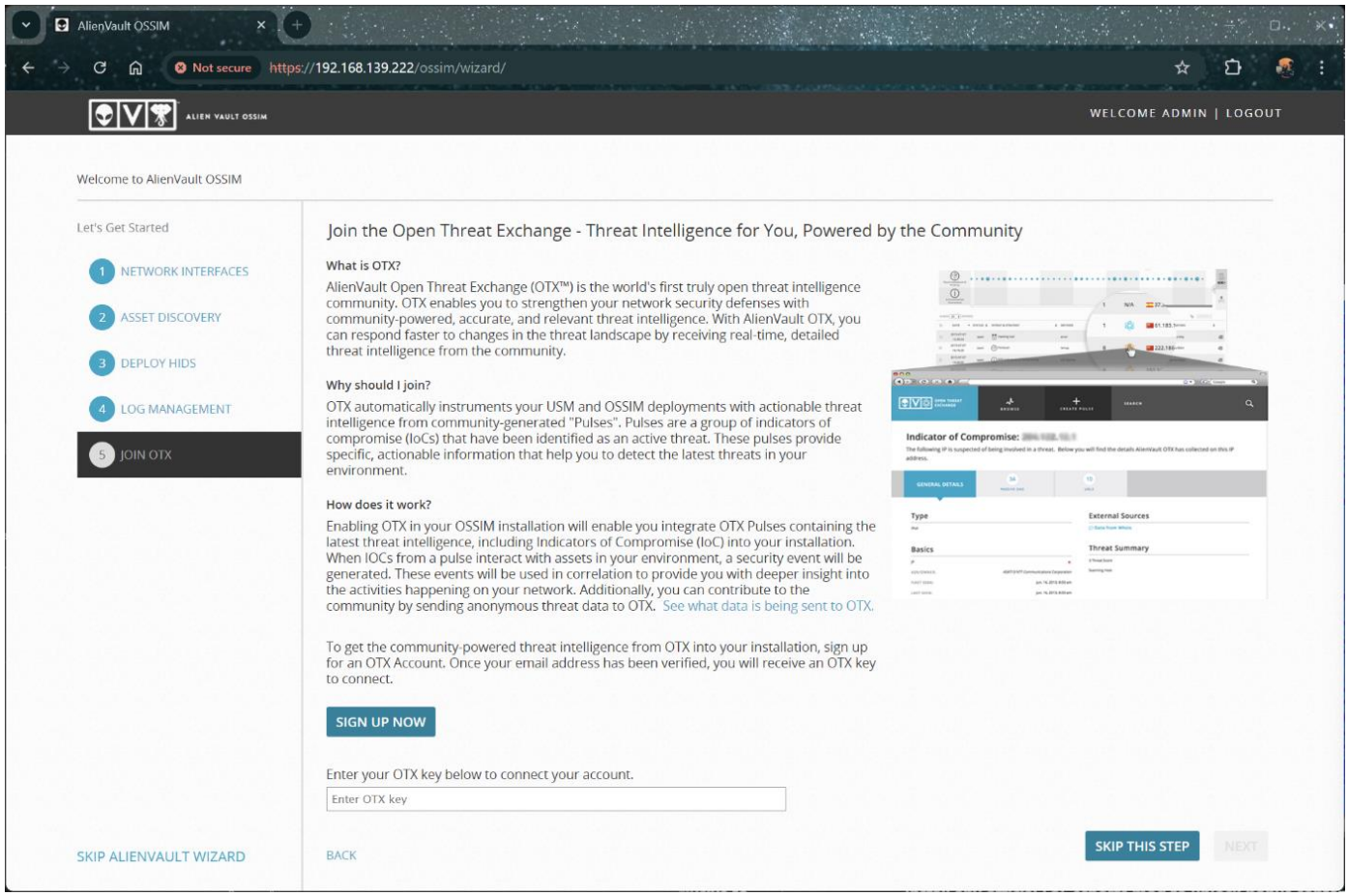
- Deploy HIDS: Click **Next.**

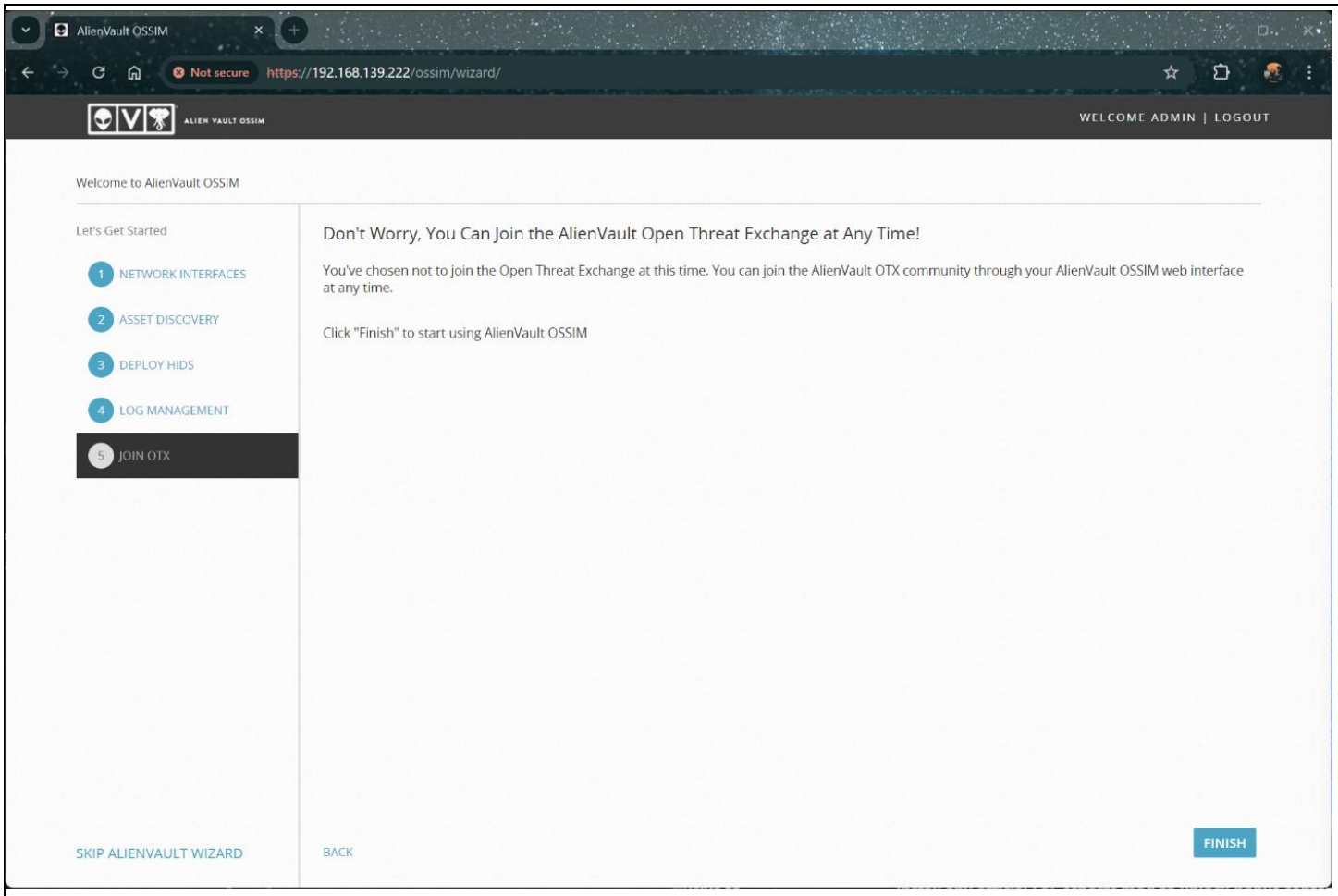


- Log Management: Click **Skip this Step.**
  (You are required to have a corporate managed network device at this level.)



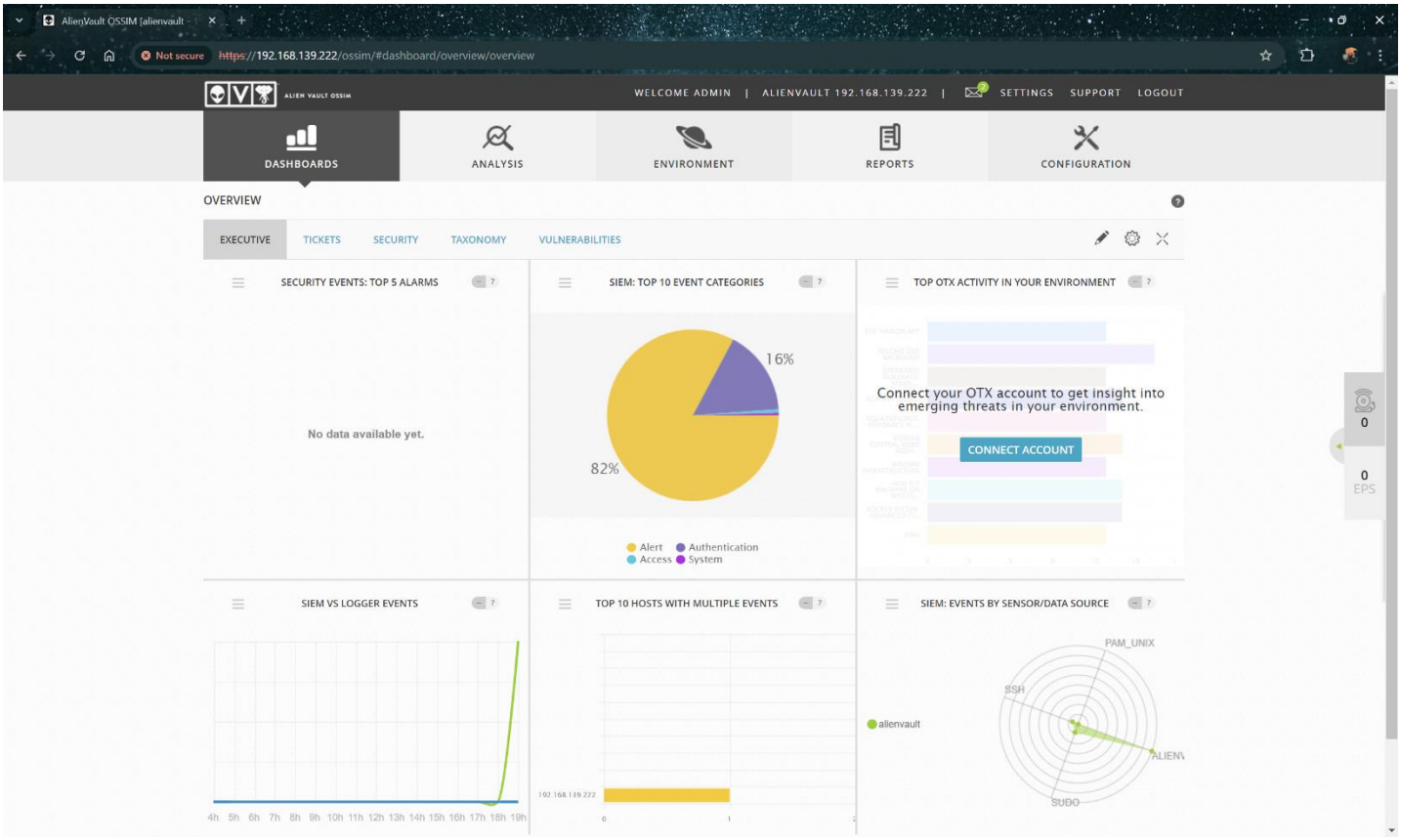
- Join OTX: Click **Skip this step**, then click **Finish**.



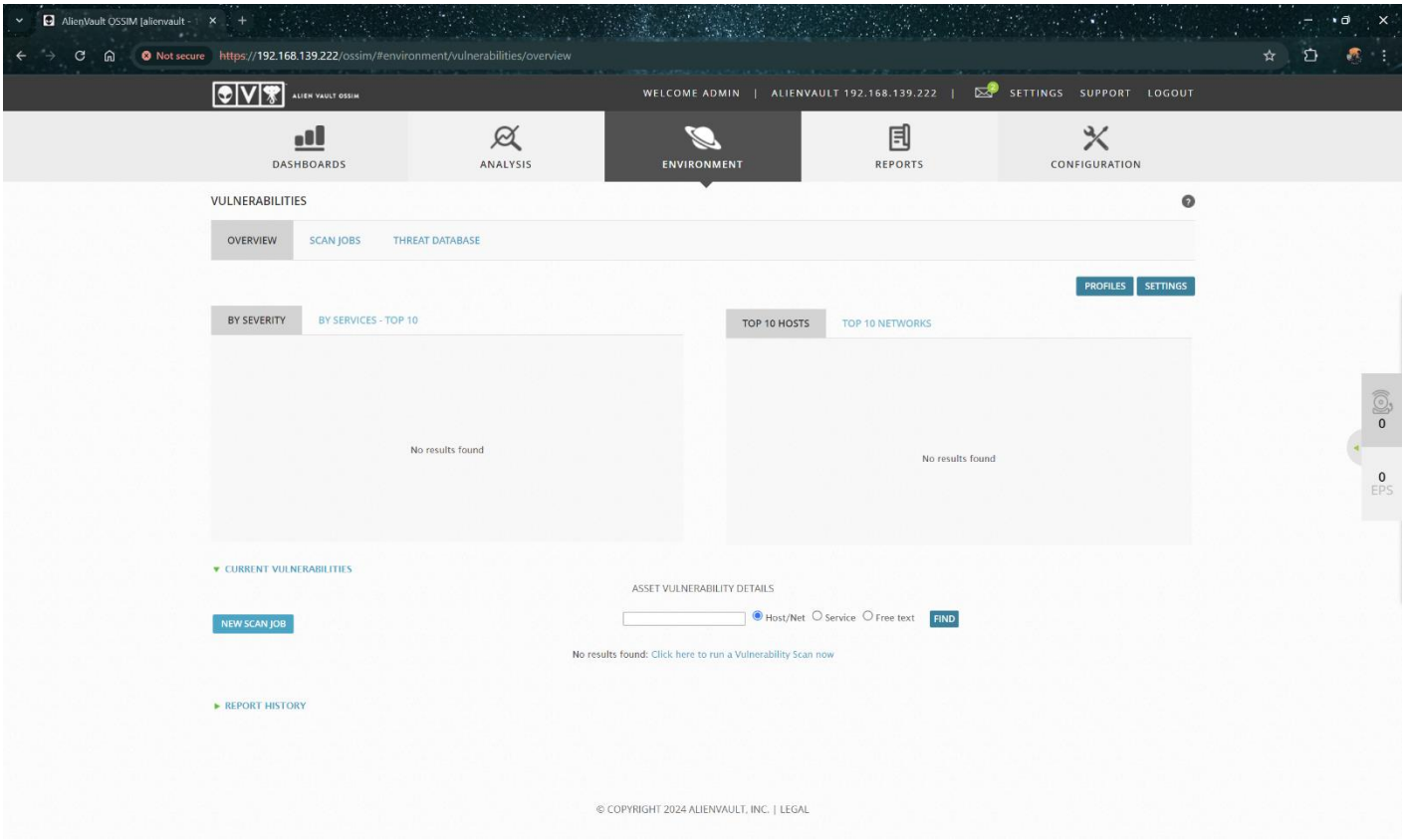

AlienVault OSSIM
Not secure
https://192.168.139.222/ossim/wizard/
ALIEN VAULT OSSIM
WELCOME ADMIN | LOGOUT
Welcome to AlienVault OSSIM
Let's Get Started
1 NETWORK INTERFACES
2 ASSET DISCOVERY
3 DEPLOY HIDS
4 LOG MANAGEMENT
5 JOIN OTX
Don't Worry, You Can Join the AlienVault Open Threat Exchange at Any Time!
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.
Click "Finish" to start using AlienVault OSSIM
SKIP ALIENVAULT WIZARD
BACK
FINISH

Take a tour of AlienVault OSSIM.

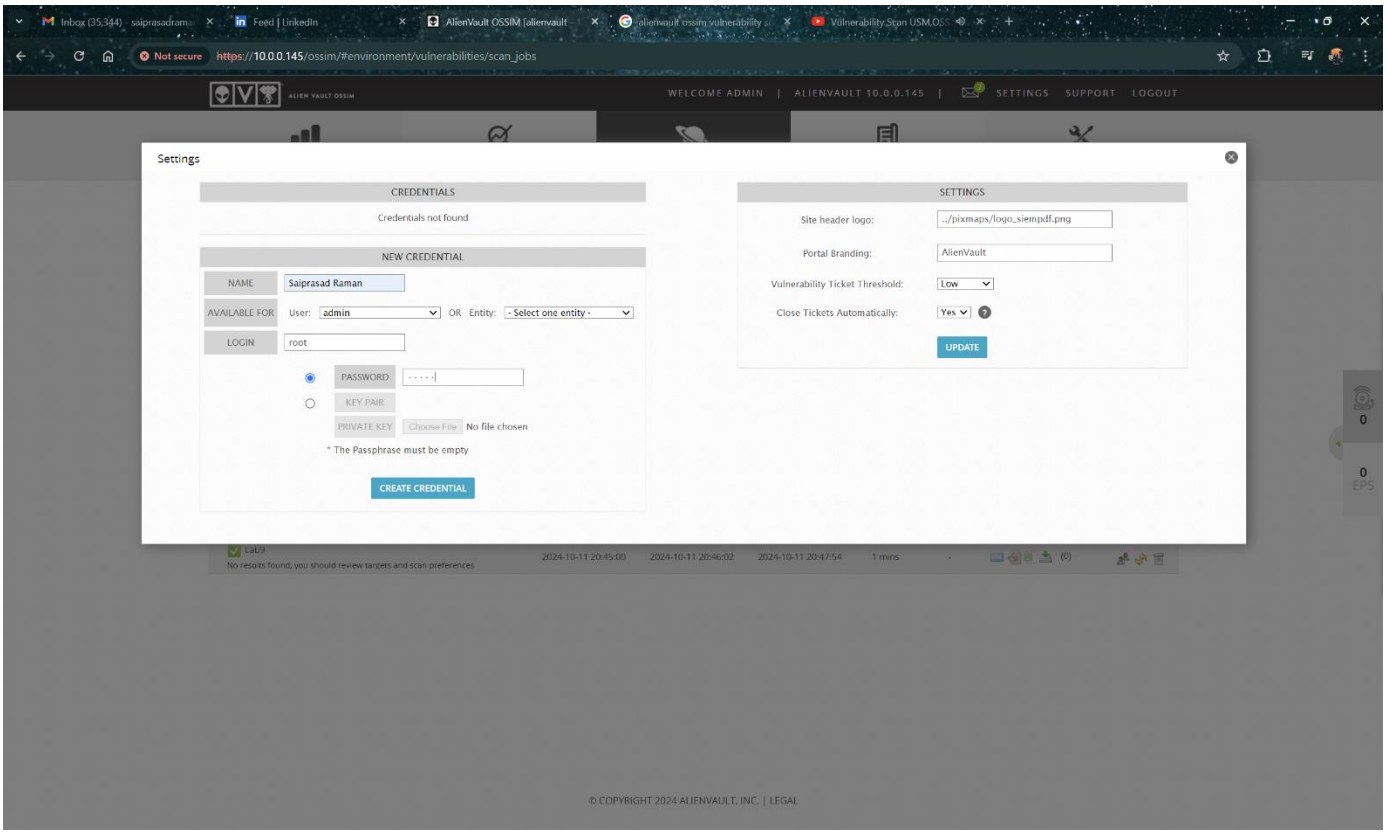
- See the Dashboard of AlienVault.



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

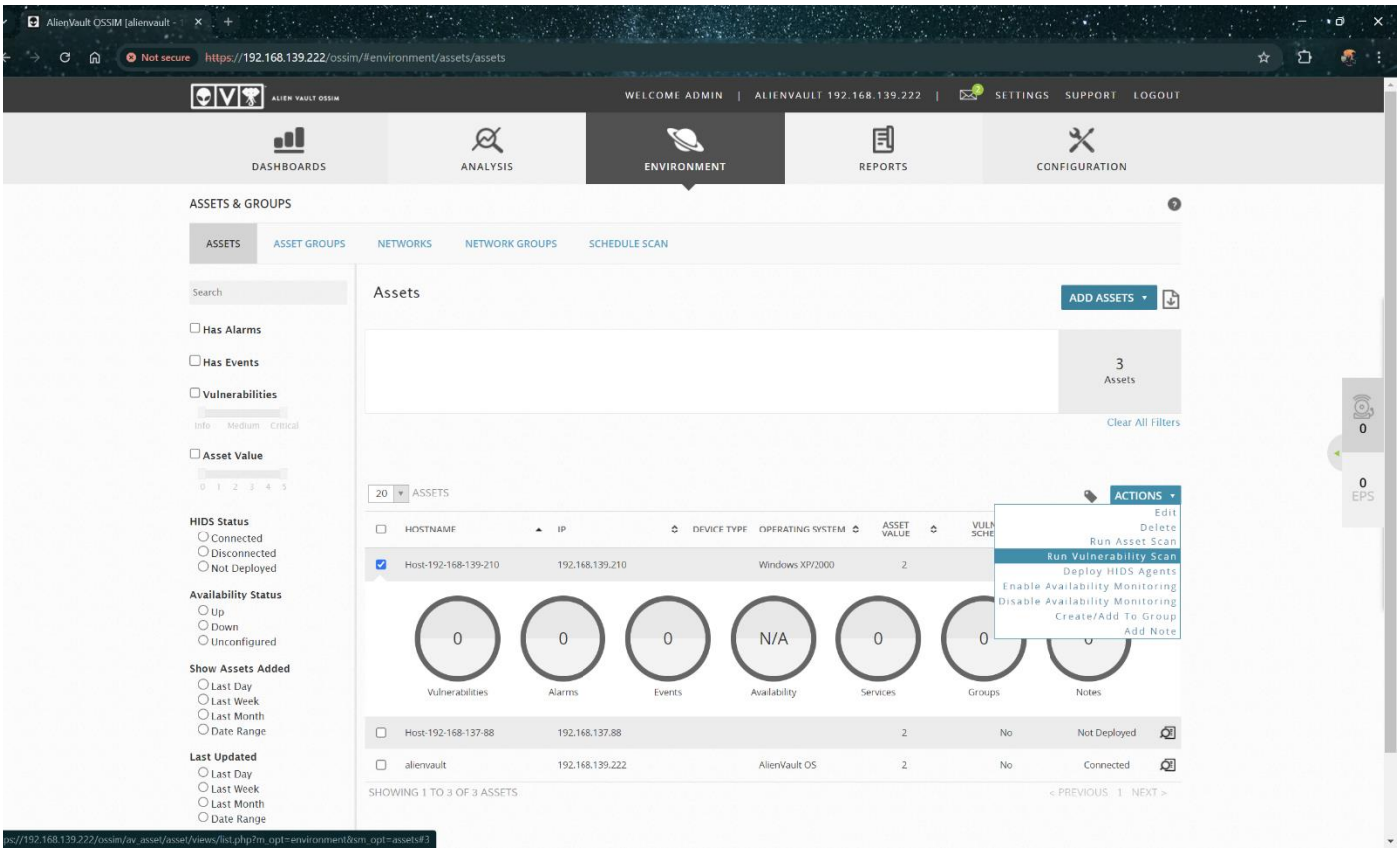


- Click **settings** and **add new credentials** for other VM:
- Name: root (or any other host that is in your VM) ○ Login: root ○ Password: (the root password) ○ Click create credential, after the credentials created, **Take the screenshot** and then close the window.

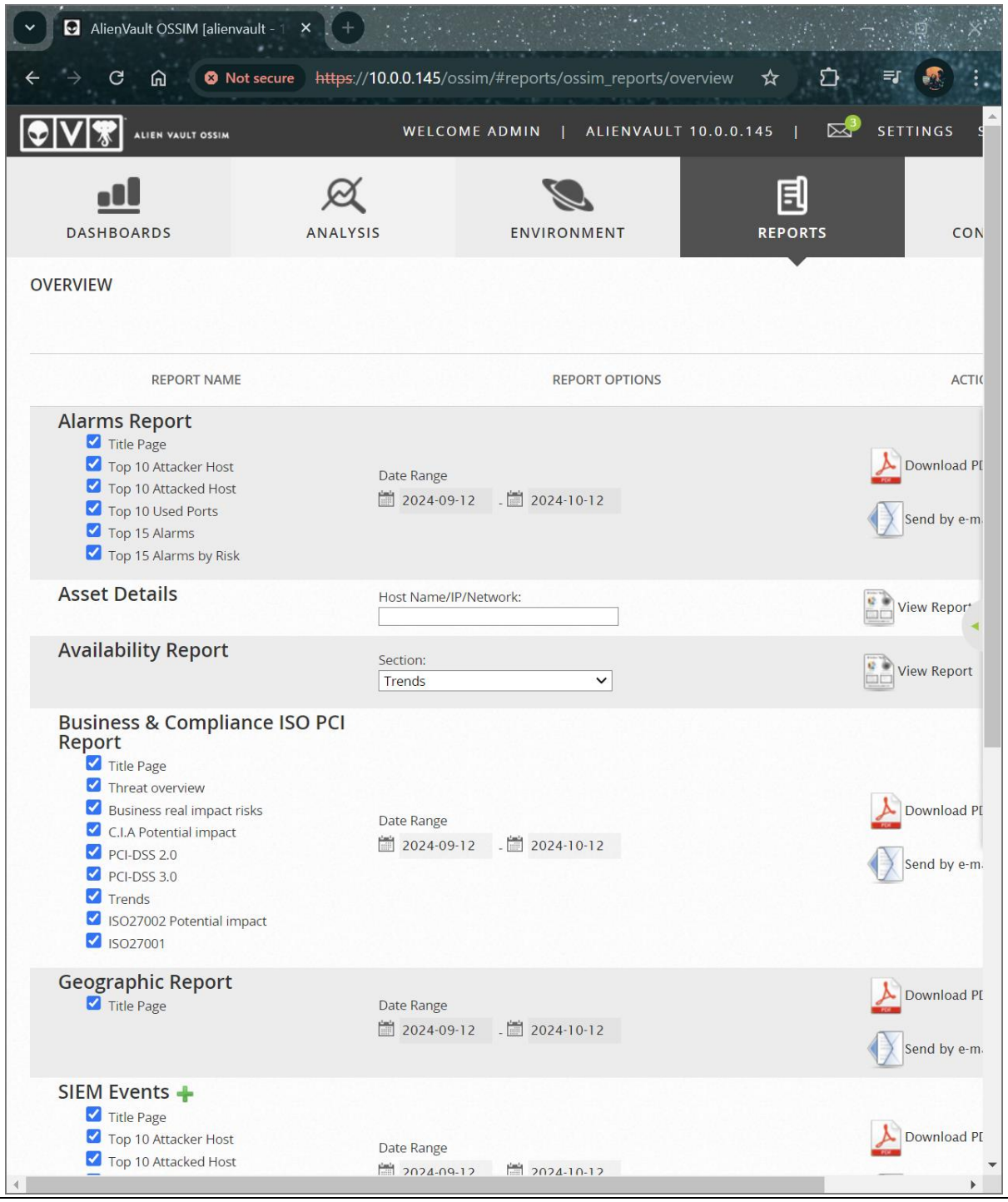


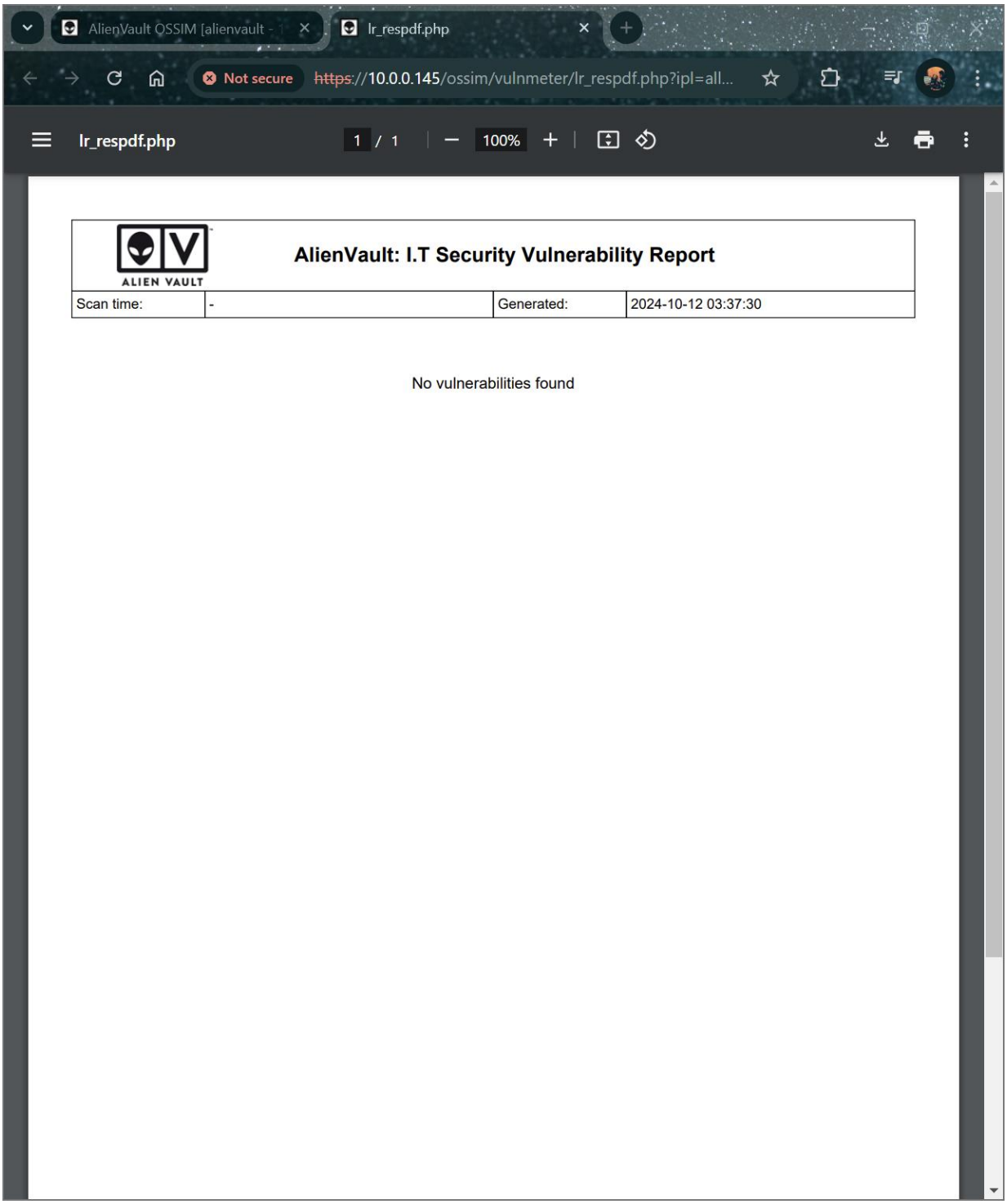
- Click on **Environment**, a dropdown menu will open, click on **Assets & Groups.**
- Select the other VM from Assets by clicking the checkmark on the left side of other VM hostname and then clicking **Actions** (a drop-down menu will open).
    - You can run Asset Scan and/or Vulnerability scan.

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



- 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.




AlienVault OSSIM [alienvault -
lr_respdf.php
Not secure
https://10.0.0.145/ossim/vulnmeter/lr_respdf.php?ipl=all...
lr_respdf.php
1 / 1
100%
AlienVault: I.T Security Vulnerability Report
Scan time:
-
Generated:
2024-10-12 03:37:30
No vulnerabilities found