

Ethically Hacking an E-Commerce Website

Capstone Project

edureka!
a Veranda Enterprise

Problem Statement:

Overview

Congratulations on making it so far! This is the Certification Project for Cyber Security and Ethical Hacking Internship Program, and here we will use all the concepts learned in this course.

Context

Ever since the birth of electronics and computers, people have begun shifting lifestyles to comprehend technology. We are currently at an age where most daily tasks involve using the world wide web or a device to connect to it.

Most of the content on the internet consists of web applications developed by companies and hosted to be shown to a user having an internet connection.

Having this luxury, terrorists and attackers would be intrigued to abuse. A cyber attacker might target a web application, a site, or a place with lots of traffic and user presence.

Here we have a sandboxed e-commerce website that is intentionally vulnerable for you to attack it at any limits you prefer to help you master the skills necessary to become an Ethical Hacker.

Business Requirement

Ethical hacking is legally attacking or hacking into a target to discover hidden vulnerabilities and to test the limits of impact the discovered vulnerability could cause.

Any digital property must not be attacked, but if the owner of the digital property consents, you could legally test the property within bounds.

An *e-commerce* web application consists of all the features a user might use on other sites (social media, movie/media). From the development point of view, the most critical types of software codes and transactions exist in an e-commerce site.

Testing the security of an e-commerce application will give you a broader idea of approaching a different type of site.

The only primary difference between a site like Amazon and the sandboxed site given here is that the sandboxed application is not publicly hosted on the internet.

Even though Amazon is secured, the company has an active security team to discover vulnerabilities.

As an *ethical hacker* practicing on places like the sandboxed site will sharpen your skill in offensively testing a site.

Objective

To break down the given application and hack into it to discover vulnerabilities, all the while understanding the limits and preserving the integrity of a target.

This is almost like the “4th Capture the Flag” challenge, but over here, this is the real deal where the training wheel comes off and directly showcases what a real-life web application would look like

After discovering vulnerabilities documenting the vulnerability in a general report would help people from other technology backgrounds would understand the severity of a vulnerability.

Format of a simple vulnerability report

Title:

Description:

Steps to Reproduce:

Impact:

Example of a report

Title:

Cross-site scripting at (target)

Description:

A *cross-site scripting* vulnerability was found at the endpoint (endpoint) and could be exploited to make a remote user execute web application code.

Steps to reproduce:

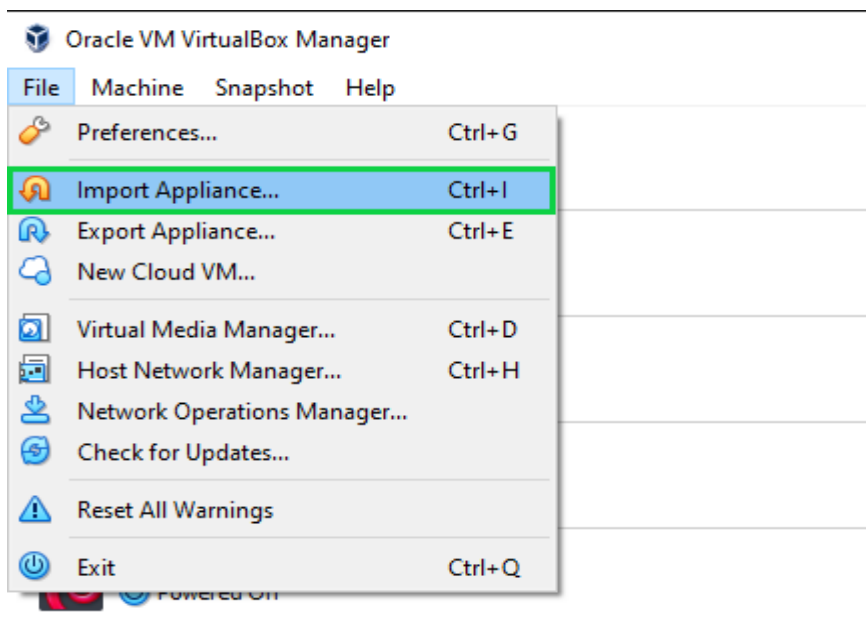
1. Craft vulnerable URL endpoint (target.com/?endpoint=value) with the following payload: `<script>alert(1)</script>`
2. The payload should look like this:
`https://target.com/?endpoint=<script>alert(1)</script>`
3. Send to the victim or execute in the victim session
4. Once the victim clicks the URL, the code will execute

Impact:

An attacker will perform actions as the victim and be capable of stealing the victim's cookies and taking over the victim's account.

Steps and tasks

- Download the Sandbox E-Commerce site virtual box appliance attached in the LMS.
- After successfully downloading, **Import the VirtualBox Appliance** into the VirtualBox.



← Import Virtual Appliance

Appliance to import

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.
















File: C:\Users\ [redacted] \Desktop\Files\JS.ova

Expert Mode Next Cancel

← Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
 Name	JS
 Guest OS Type	 Ubuntu (64-bit)
 CPU	1
 RAM	1024 MB
 DVD	<input checked="" type="checkbox"/>
 USB Controller	<input checked="" type="checkbox"/>
 Sound Card	<input checked="" type="checkbox"/> ICH AC97
 Network Adapter	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
 Storage Controller (IDE)	PIIX4
 Storage Controller (IDE)	PIIX4
 Storage Controller (SATA)	AHCI
 Virtual Disk Image	JS-disk001.vmdk
 Base Folder	C:\Users\ [redacted] \VirtualBox VMs
 Primary Group	/

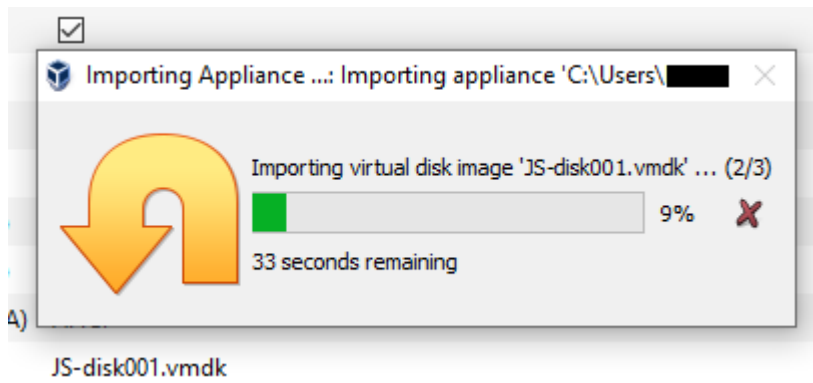
Machine Base Folder: C:\Users\ [redacted] \VirtualBox VMs

MAC Address Policy: Include all network adapter MAC addresses

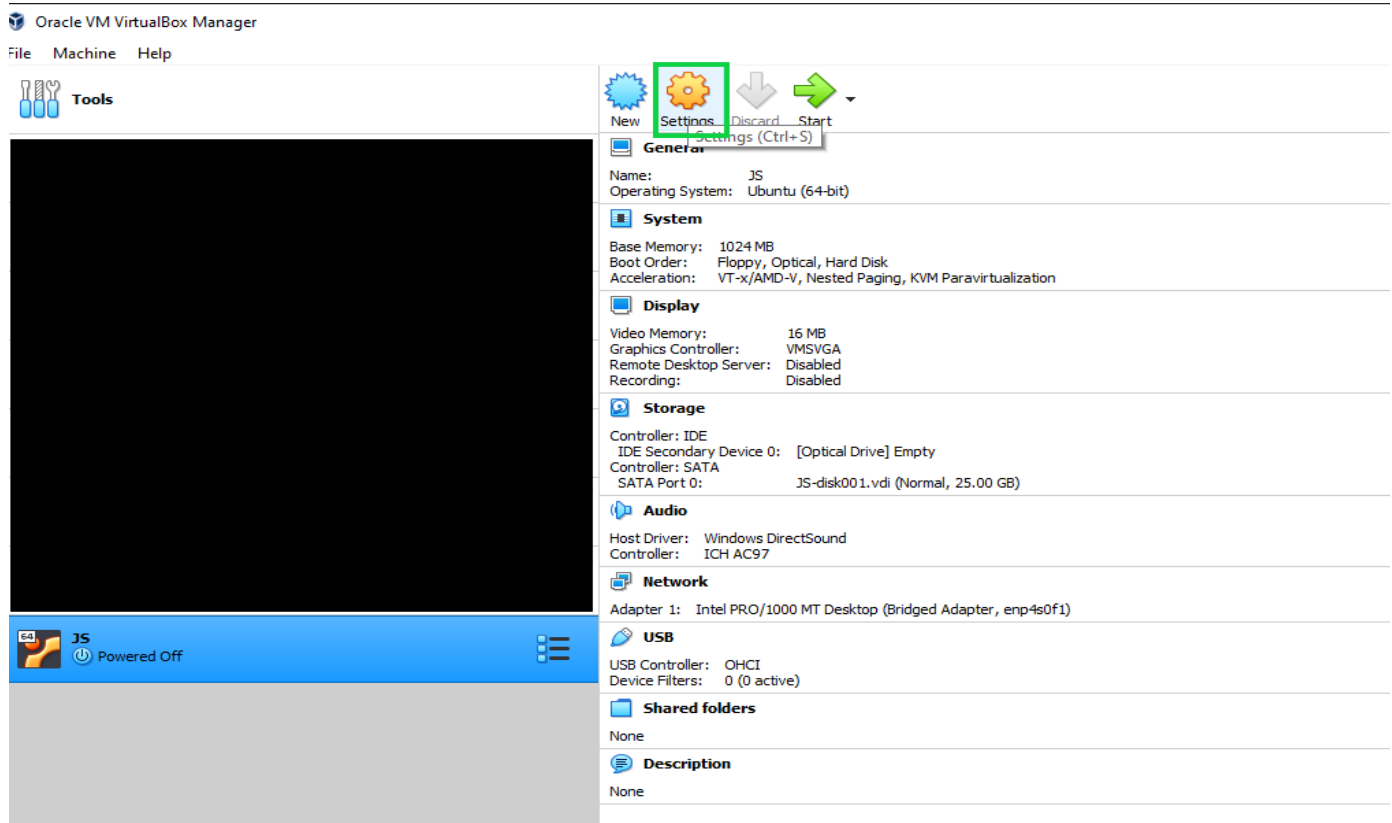
Additional Options: ☒ Import hard drives as VDI

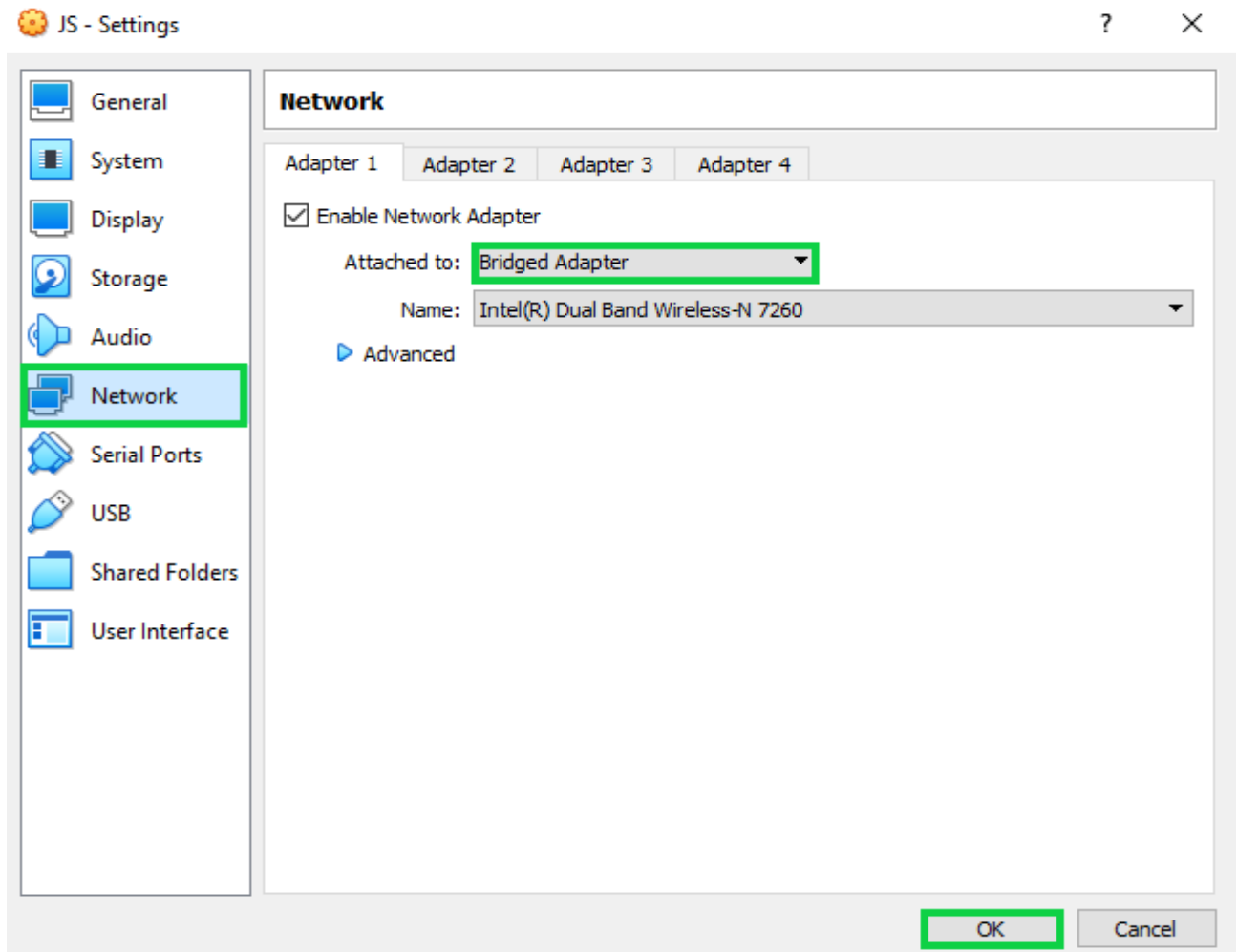
Appliance is not signed

Restore Defaults Import Cancel

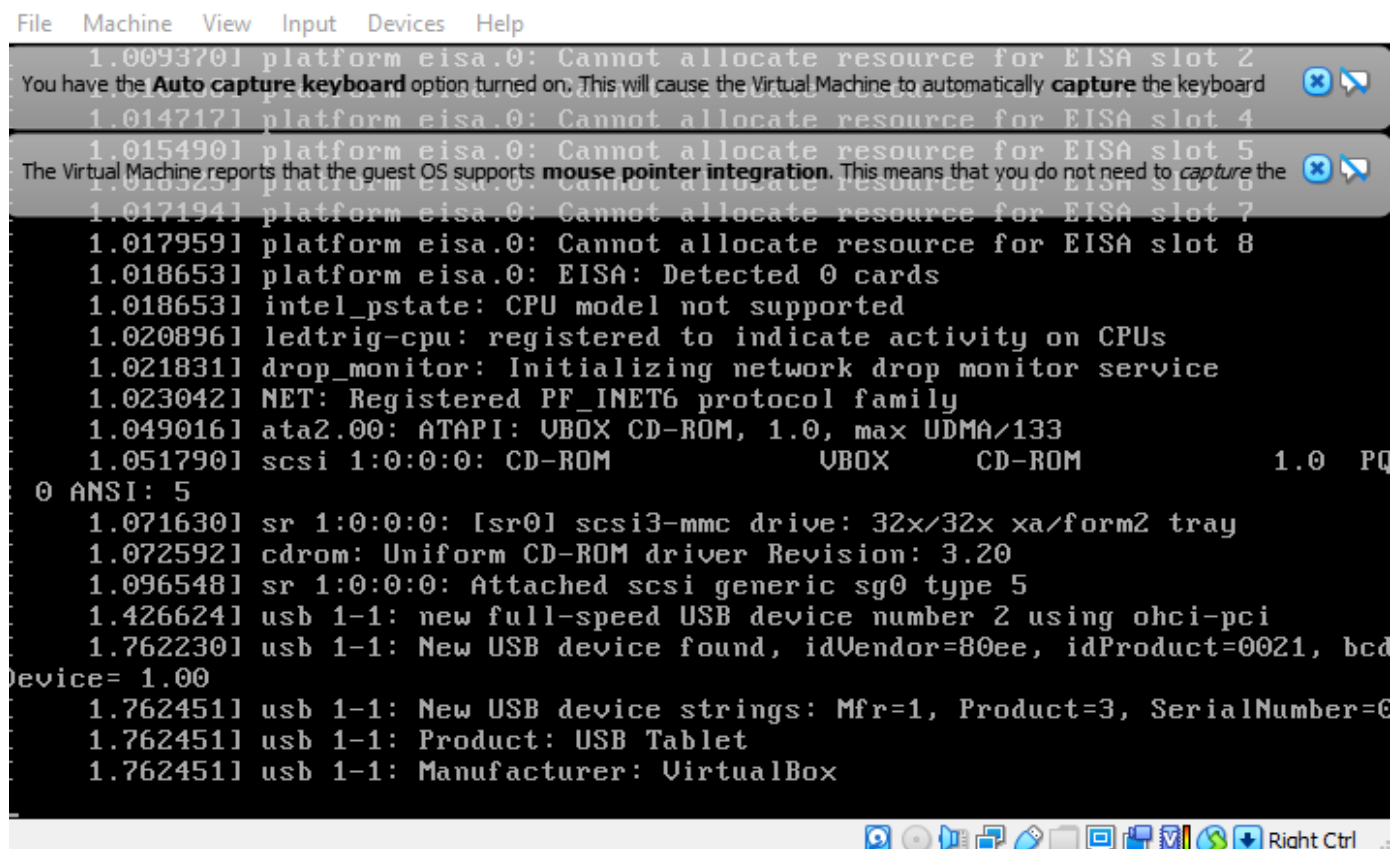
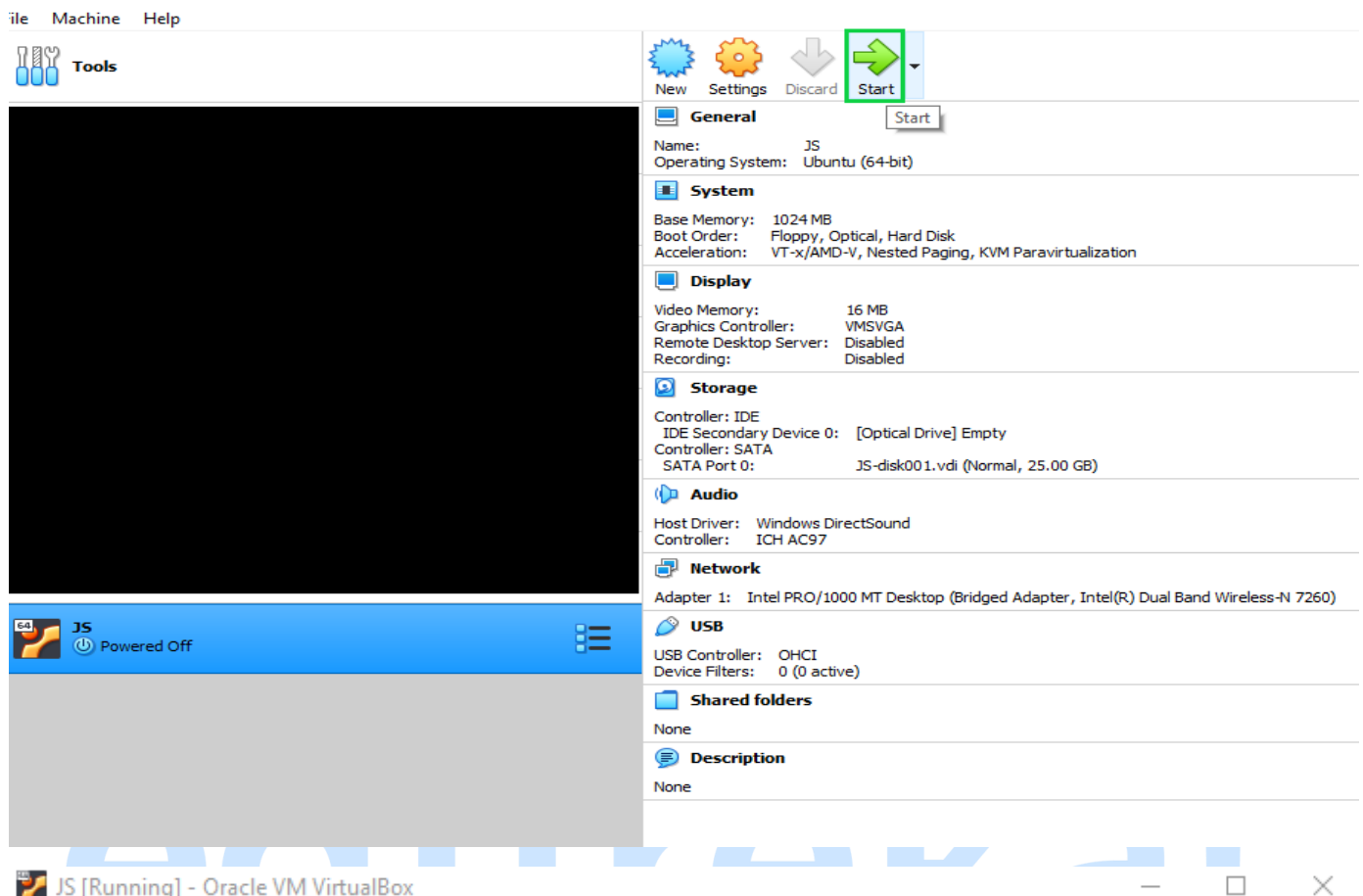


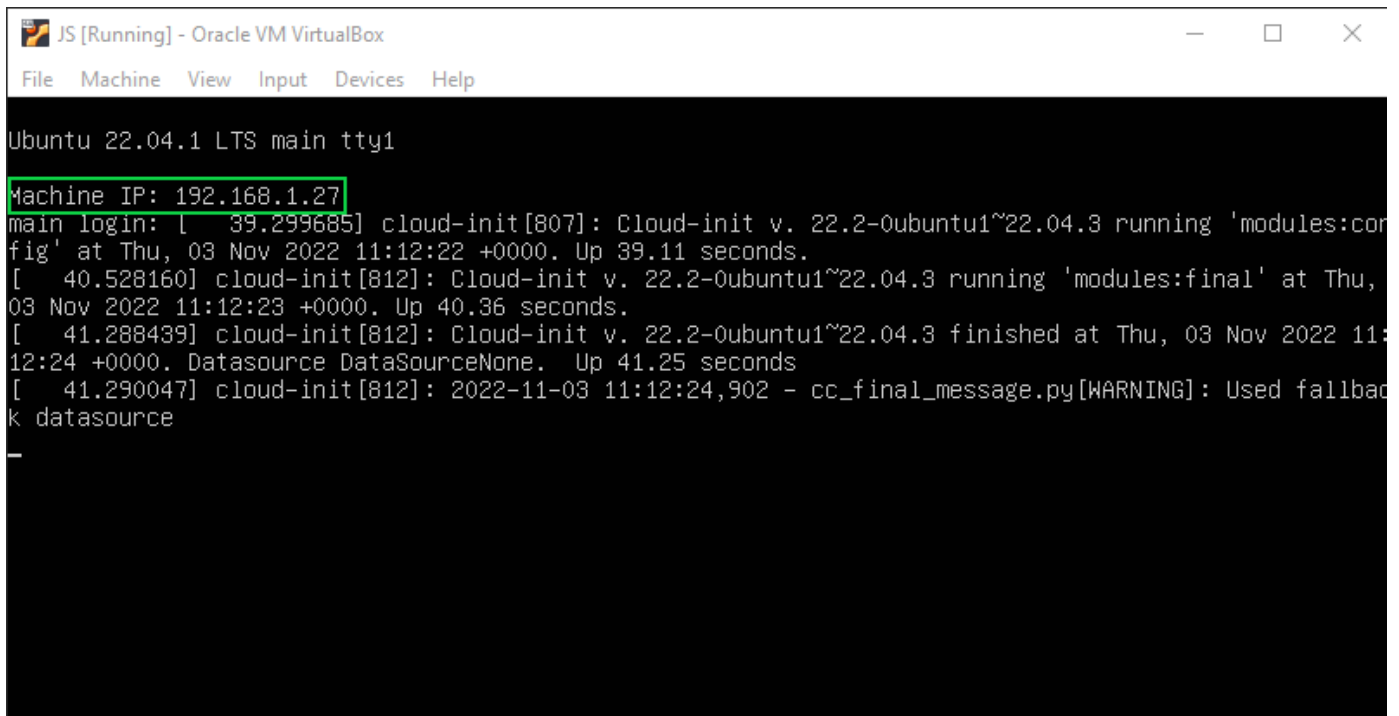
- When the import is successful, go to **Settings** and set the network adapter to **Bridged Adapter**.





- Start the machine and wait for the machine to boot up and for the “Machine IP:” to appear.





```
JS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 22.04.1 LTS main tty1
Machine IP: 192.168.1.27
main login: [ 39.299685] cloud-init[807]: Cloud-init v. 22.2-0ubuntu1~22.04.3 running 'modules:con
fig' at Thu, 03 Nov 2022 11:12:22 +0000. Up 39.11 seconds.
[ 40.528160] cloud-init[812]: Cloud-init v. 22.2-0ubuntu1~22.04.3 running 'modules:final' at Thu,
03 Nov 2022 11:12:23 +0000. Up 40.36 seconds.
[ 41.288439] cloud-init[812]: Cloud-init v. 22.2-0ubuntu1~22.04.3 finished at Thu, 03 Nov 2022 11:
12:24 +0000. Datasource DataSourceNone. Up 41.25 seconds
[ 41.290047] cloud-init[812]: 2022-11-03 11:12:24,902 - cc_final_message.py[WARNING]: Used fallback
k datasource
```

Use **Nmap** to scan and find the e-commerce site and start hacking away.

edureka!
a Veranda Enterprise