HyperionDev

Capstone Project - Case Study for Local VM

Task

Visit our website

Introduction

In this task, you will be required to understand a scenario and then use acquired knowledge from previous tasks to exploit a victim's machine with little knowledge of the network. This will allow you to think quickly, put theory into practice, and enhance your problem-solving skills.

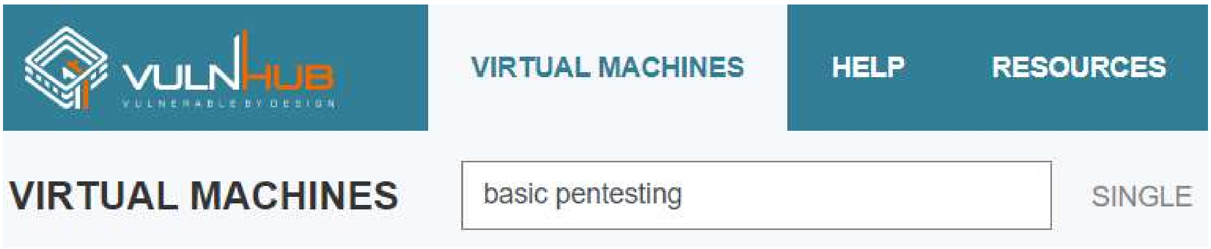
Overview

In this capstone task, you will have the opportunity to hack into another machine. You will install a virtual machine, "Basic Pentesting 1", which acts as the victim's machine. You will then use Kali Linux to gather information on the target and find ways to exploit the machine based on the information you have gathered. The task includes finding exploitable services running on open ports to gain entry into the internal network to print the password file. All the assessments will be carried out on Kali Linux using the tools indicated below.

Virtual machine installation

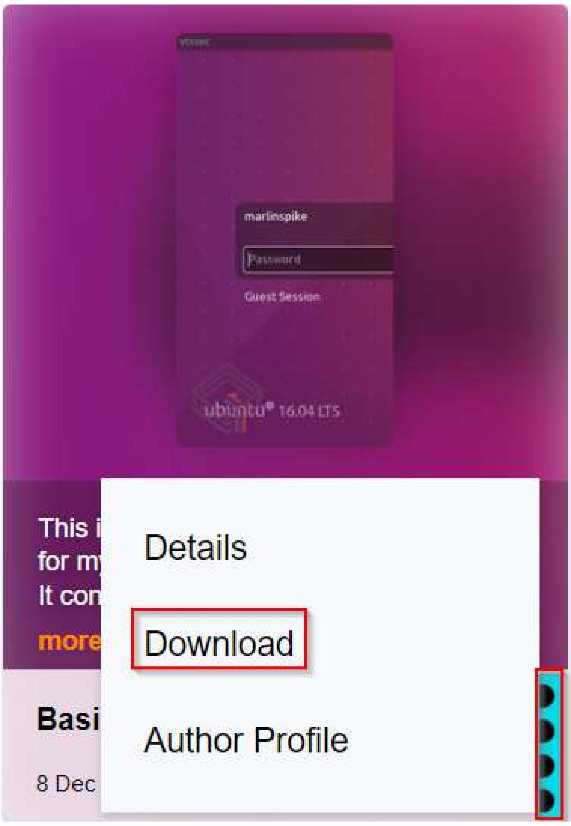
1. Go to **[Vulnerable By Design ~ VulnHub](#)**.

2. In the search box, enter "basic pentesting" and hit Enter.

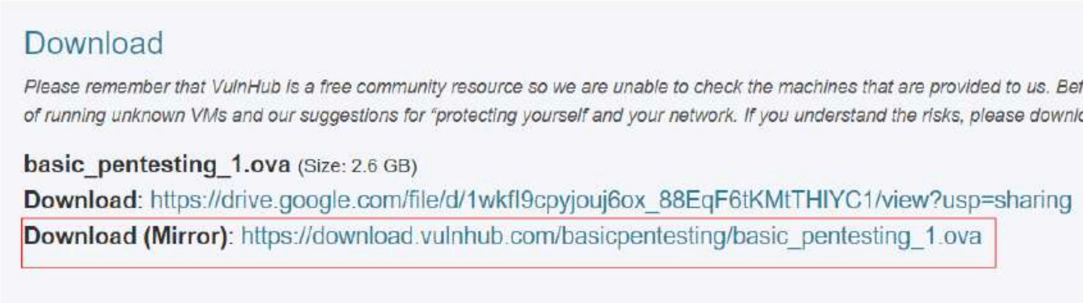


3. Locate and select "Basic Pentesting 1" by **Josiah Pierce** from the search results.

4. Click on the four dots in the lower right corner and choose “Download”.



5. Click on the **Download(Mirror)** link to begin downloading the "basic_pentesting_1.ova" virtual machine file.

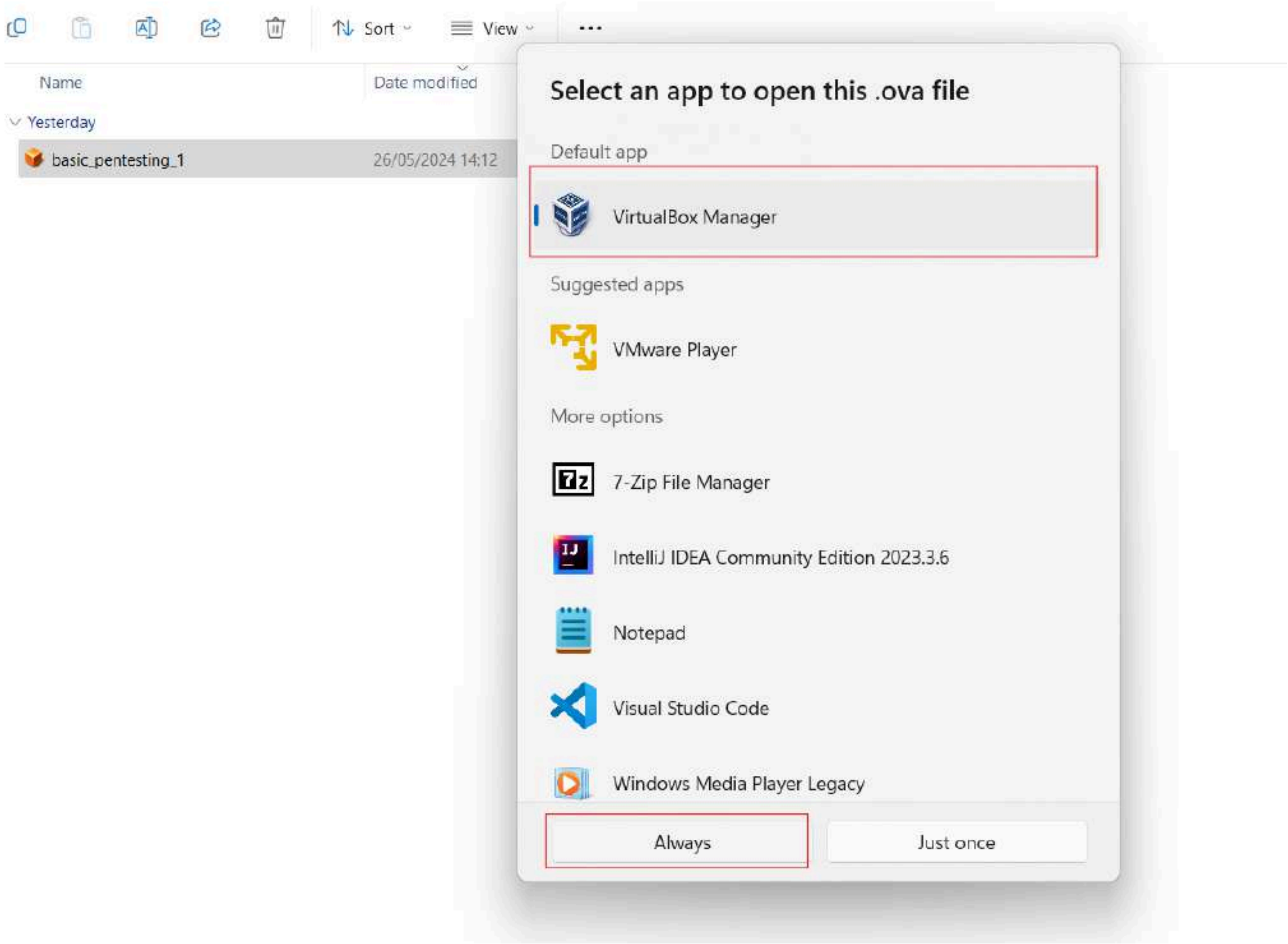


Download

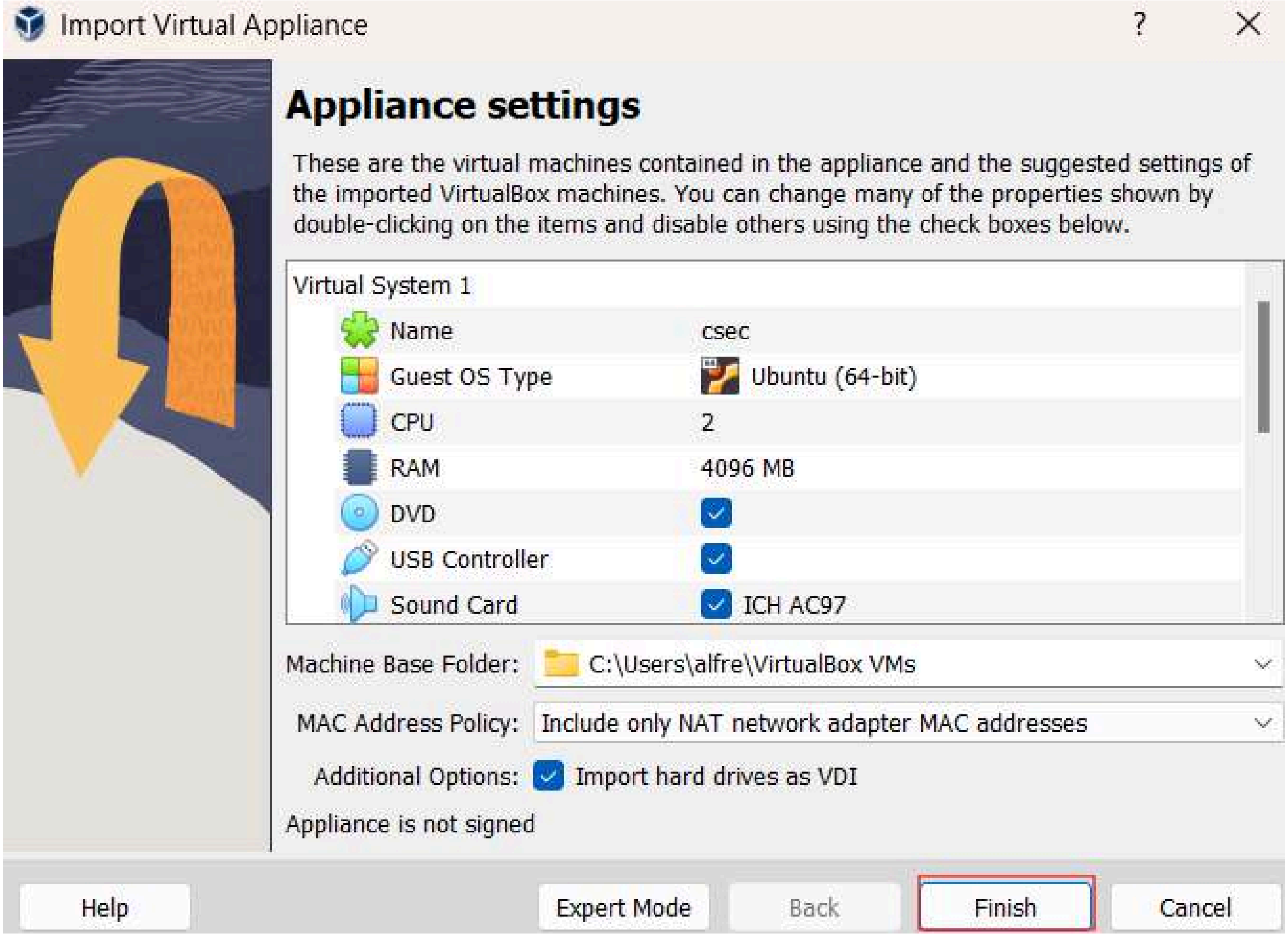
Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Bef
of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please downlo

basic_pentesting_1.ova (Size: 2.6 GB)
Download: https://drive.google.com/file/d/1wkfl9cpyjouj6ox_88EqF6tKMtTHIYC1/view?usp=sharing
Download (Mirror): https://download.vulnhub.com/basicpentesting/basic_pentesting_1.ova

6. Once you have downloaded the machine, navigate to your Downloads folder and locate the downloaded file. Right-click on the file and choose the option to open with VirtualBox. Alternatively, after right-clicking, you can select "Open with" and then choose VirtualBox Manager:



7. After opening the file, a window will appear asking you to change the appliance settings. Simply click "Finish."



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	csec
Guest OS Type	Ubuntu (64-bit)
CPU	2
RAM	4096 MB
DVD	☑
USB Controller	☑
Sound Card	☑ ICH AC97

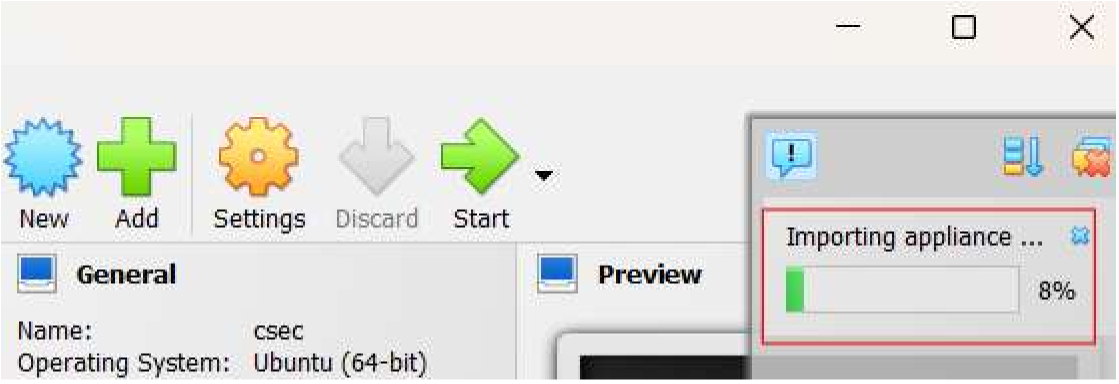
Machine Base Folder: C:\Users\alfre\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

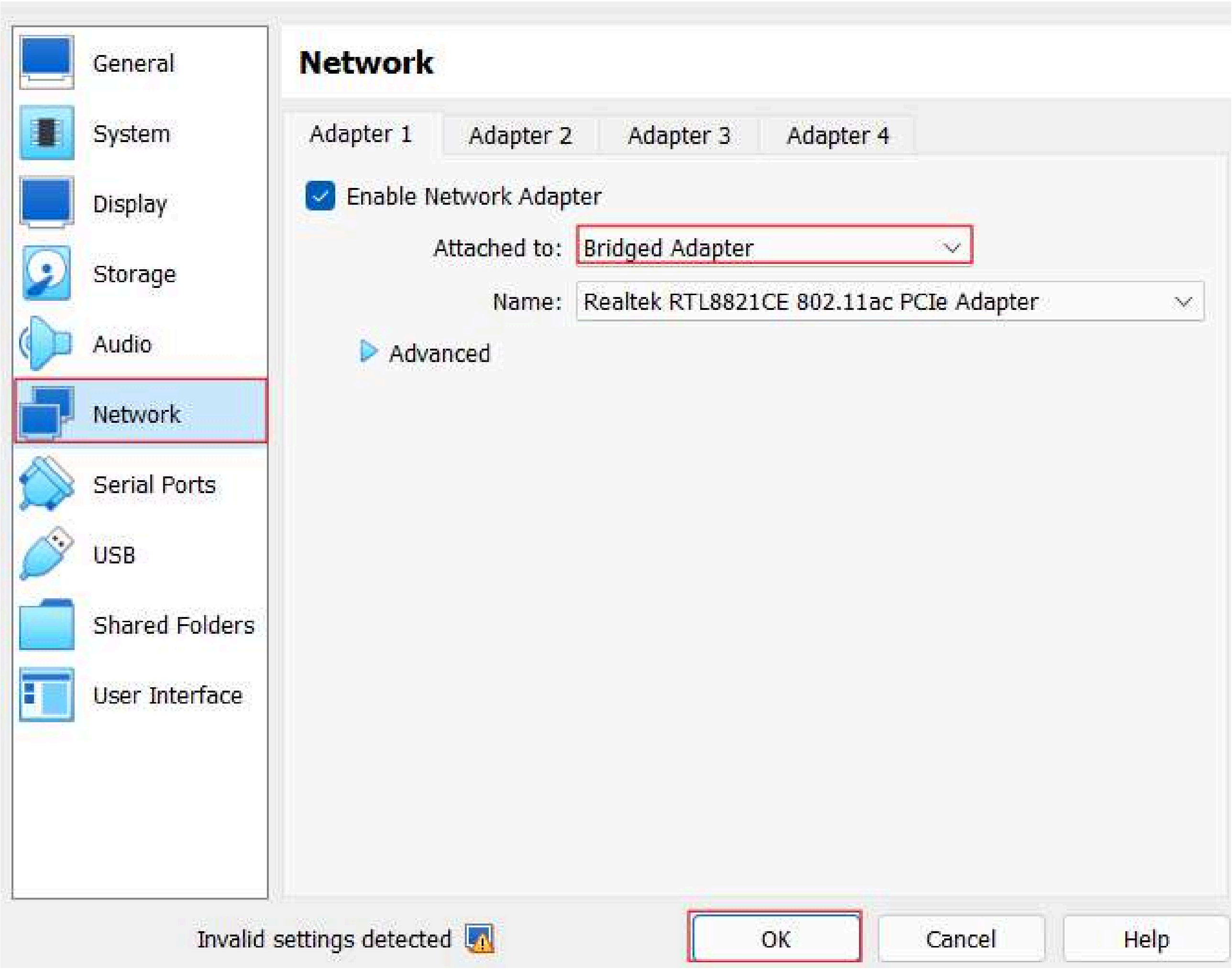
8. After this, the "basic_pentesting_1.ova" machine will begin importing into Oracle VirtualBox. You should see a progress bar indicating that the machine is being imported. Please wait until the import is complete.



Name: csec
Operating System: Ubuntu (64-bit)

Importing appliance ... 8%

9. "Before starting the virtual machine, you'll need to configure some settings. Open the Oracle VM VirtualBox Manager and click on 'Settings.' Then, navigate to the 'Network' section. In the 'Attached to' dropdown menu, select 'Bridged Adapter.'



☑ Enable Network Adapter

Attached to: Bridged Adapter

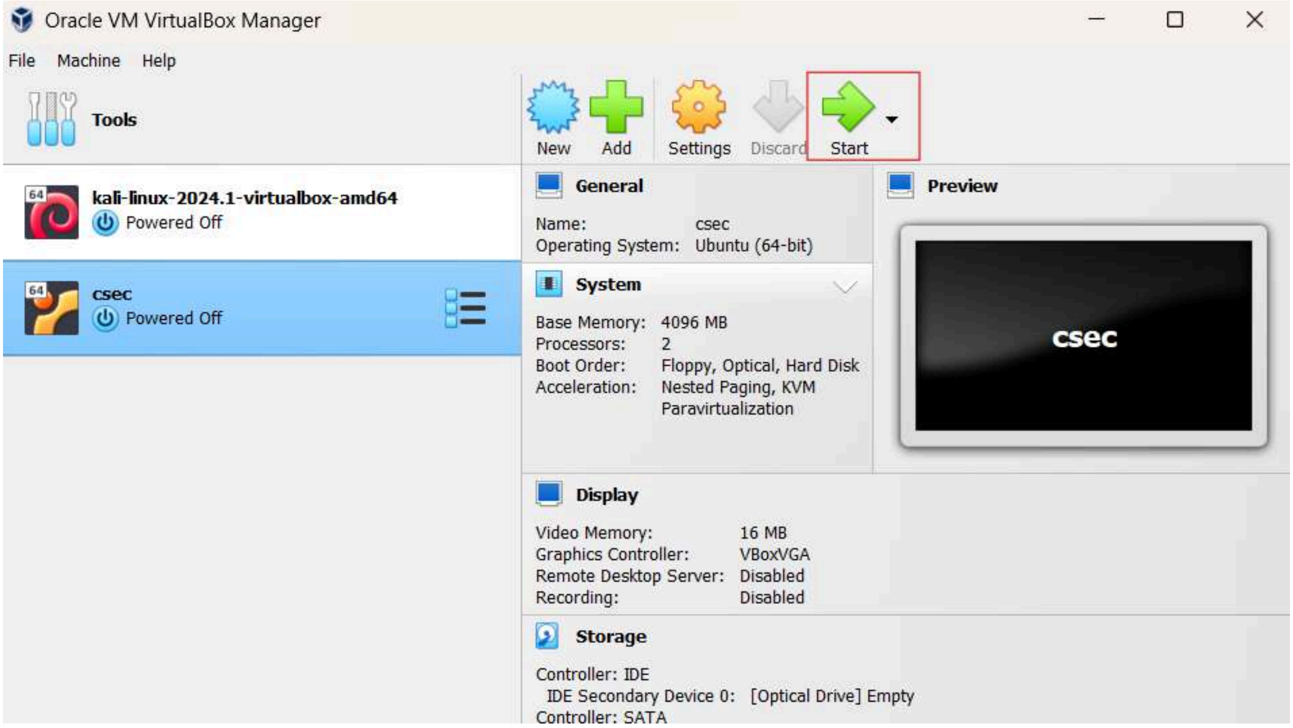
Name: Realtek RTL8821CE 802.11ac PCIe Adapter

Invalid settings detected

Take note

The 'Bridged Adapter' option enables the virtual machine to integrate seamlessly with the host network, granting it a distinct presence on the network and facilitating direct access to other network resources. Alternatively, users may opt for the 'Host-only Adapter,' which establishes a private network limited to communication between the host machine and its virtual machines. Another viable choice is the 'NAT' (Network Address Translation) setting, which affords the virtual machine internet connectivity through the host's network while maintaining isolation from external network resources.

10. Once this process is complete, you can then start the virtual machine.



kali-linux-2024.1-virtualbox-amd64
Powered Off

csec
Powered Off

General

Name: csec
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

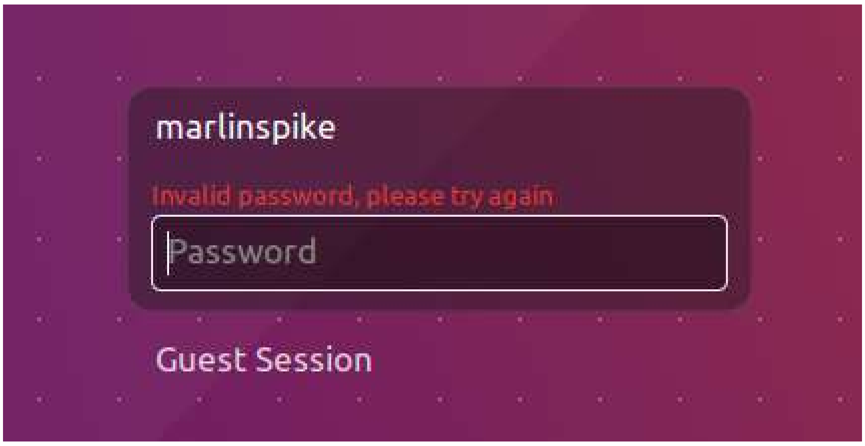
Display

Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA

11. After starting the machine, you will be taken to the login page. If you've made it this far, congratulations! You have successfully installed the Basic Pentesting 1 virtual machine for this capstone project.



marlinspike

Invalid password, please try again

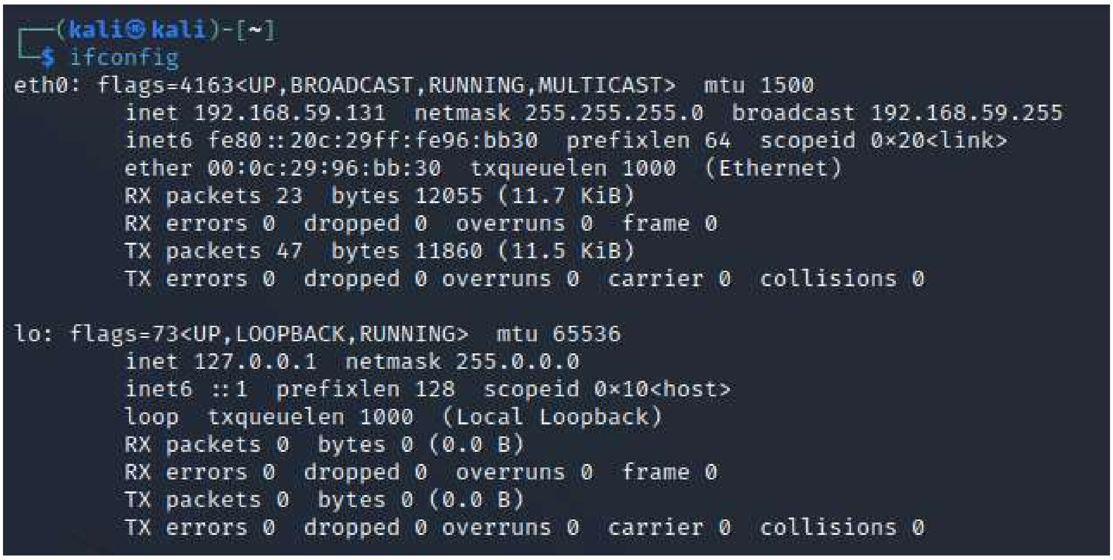
Don't worry about the password just yet; figuring it out is part of your task.

Complete setup

1. Open up a terminal on your Kali Linux machine and run the following command to display your network configuration:

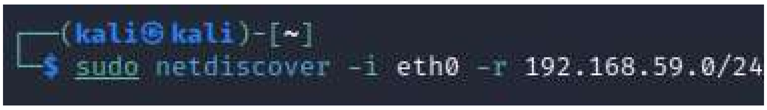
```
ifconfig
```

   After executing the command above, you should see the following output:



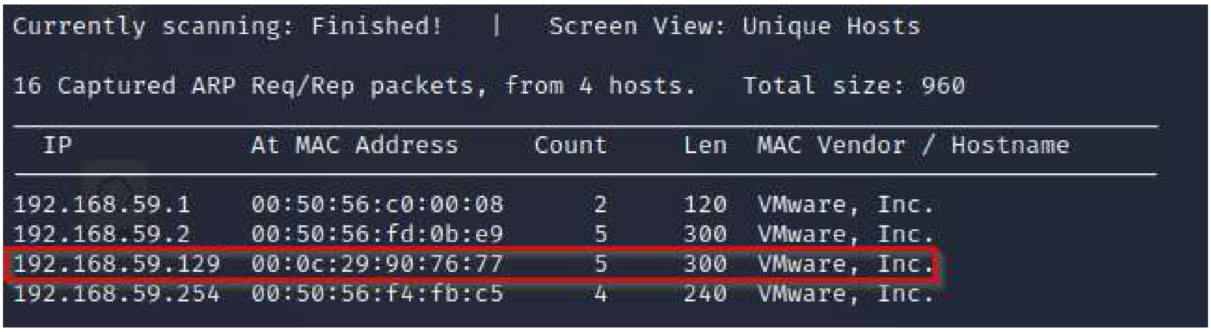
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.59.131  netmask 255.255.255.0  broadcast 192.168.59.255
        inet6 fe80::20c:29ff:fe96:bb30  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:96:bb:30  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 12055 (11.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 11860 (11.5 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Use **netdiscover** to scan your network range and find the IP address of the "Basic Pentesting 1" machine. For example, if your IP address is **192.168.59.131**, your network range is **192.168.59.0/24**.



```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -i eth0 -r 192.168.59.0/24
```

3. Review the output of **netdiscover** to find the IP address assigned to the "Basic_Pentesting_1" VM. The output will list all active devices on the network along with their IP addresses and MAC addresses. Identify the "Basic Pentesting 1" machine by its IP address.



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

16 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 960
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.59.1    00:50:56:c0:00:08      2     120  VMware, Inc.
192.168.59.2    00:50:56:fd:0b:e9      5     300  VMware, Inc.
192.168.59.129  00:0c:29:90:76:77      5     300  VMware, Inc.
192.168.59.254  00:50:56:f4:fb:c5      4     240  VMware, Inc.
```

Case study

You have been hired by the Basic Pentesting Company (Ltd) to test whether there is an issue with their security controls. They have given you their login portal as well as a way to get their IP address. They want to identify if you can gain unauthorised access to the internal network. The client's team will be sending you requests to complete in stages.

You will need the following tools to complete the task:

- Netdiscover
- Nmap
- Metasploit

Practical task

Create a Google document (or another text document that you can later convert to a PDF) called case_study. This assessment will be completed in stages. For each stage, you will be given a scenario of what the client expects of you. Provide your answers for each stage under the appropriate heading.

Stage 1

The client's team wants to know if any potential services are running on ports which could be security threats.

- List the services that are running and include a screenshot of the scan report

Hint: Use Nmap

Stage 2

Do research on all the services found in stage 1 and indicate which service has a backdoor vulnerability.

Hint: Use the search option in Metasploit. Analyse the different services and their versions on the open ports for possible backdoor vulnerabilities. This particular backdoor vulnerability was introduced in a package that affected Linux systems between 28 November and 2 December 2010. Therefore, pay attention to possible outdated versions of services running on open ports.

Stage 3

Open up Metasploit and exploit the “Backdoor” vulnerability to have root accessibility.

- Provide a screenshot to show that you have exploited the vulnerability

Hint: Use `set payload payload/cmd/unix/reverse`

Stage 4

Extract the password file. The password file indicates to the client that you can access the “Basic Pentesting 1” machine because the hash can be cracked to reveal the password. A brute force attack was used to crack the hashed password by searching common passwords such as using a name, password1, and 123456789. The cracked password is **marlinspike**.

- Provide the command for extracting the password file.

- Insert a screenshot of the output after using the above command.

- Login to the Basic Pentesting login portal to provide proof of concept to the client. Provide the username and password for the “Basic Pentesting” machine.

Submission

- Convert your Google doc (or alternative text document) containing your answers to a PDF and upload it.

Important: Be sure to upload all files required for the task submission inside your task folder and then click "Request review" on your dashboard.

Share your thoughts

HyperionDev strives to provide internationally excellent course content that helps you achieve your learning outcomes.

Do you think we’ve done a good job or do you think the content of this task, or this course as a whole, can be improved?

Share your thoughts anonymously using this **form**.