

Defending the Network from a Simulated Attack (3e)

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

Student:

Nick Derleth

Email:

nderle02664@fontbonne.edu

Time on Task:

0 hours, 19 minutes

Progress:

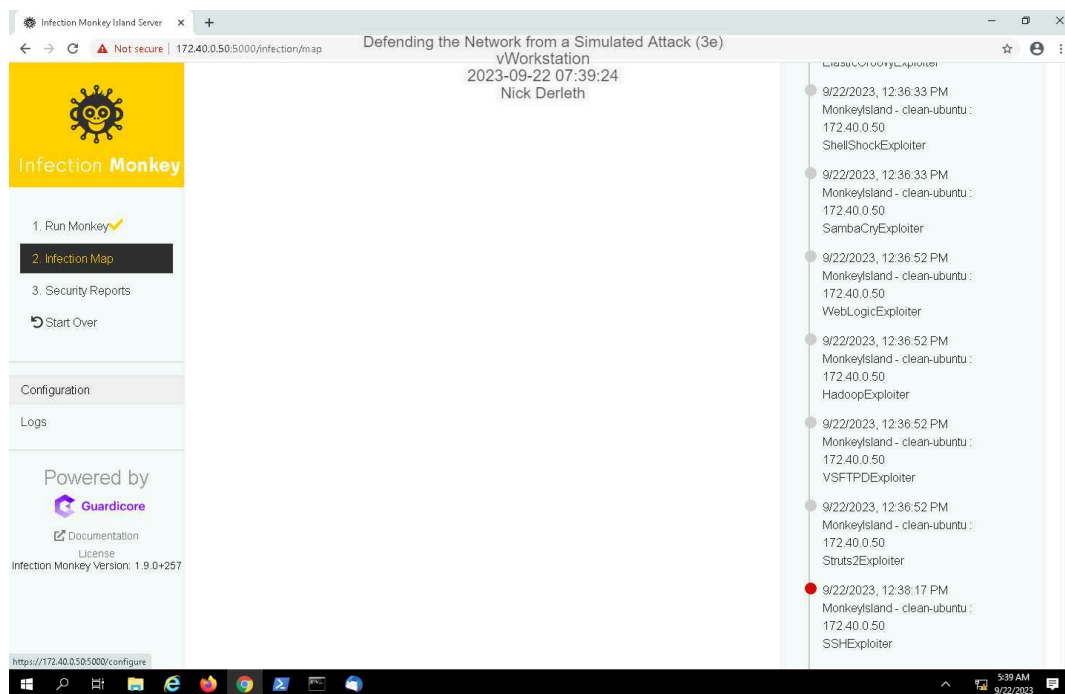
36%

Report Generated: Friday, September 22, 2023 at 8:48 AM

Section 1: Hands-On Demonstration

Part 1: Perform a Simulated Attack with Infection Monkey

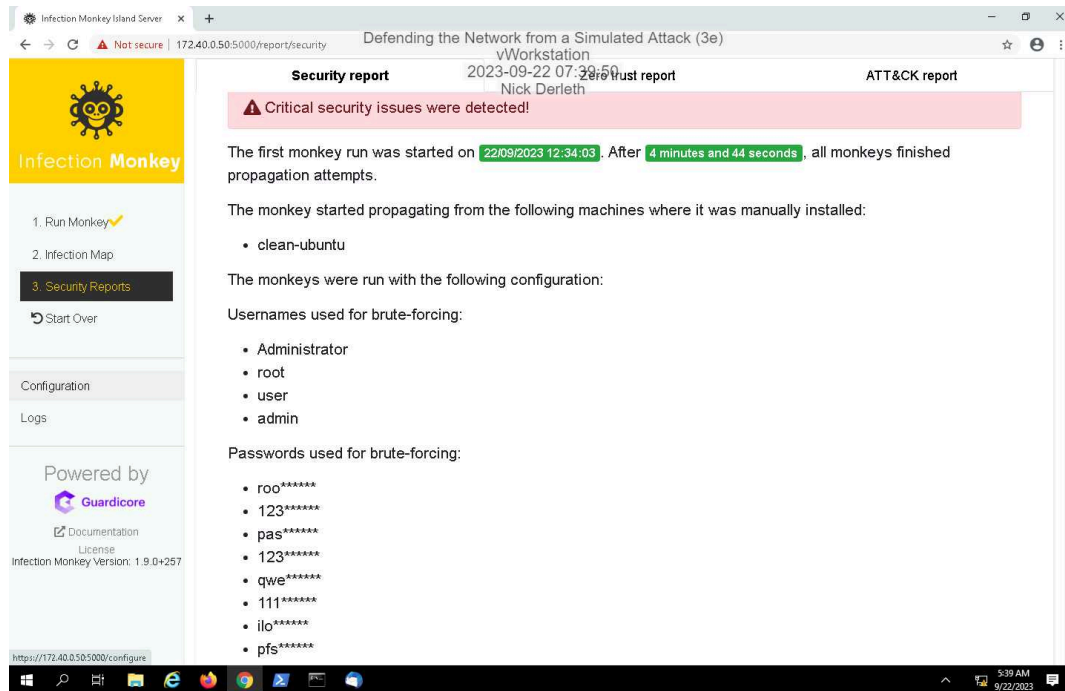
14. **Make a screen capture** showing the **successful exploit of the corporationtechs.com web server from MonkeyIsland.**



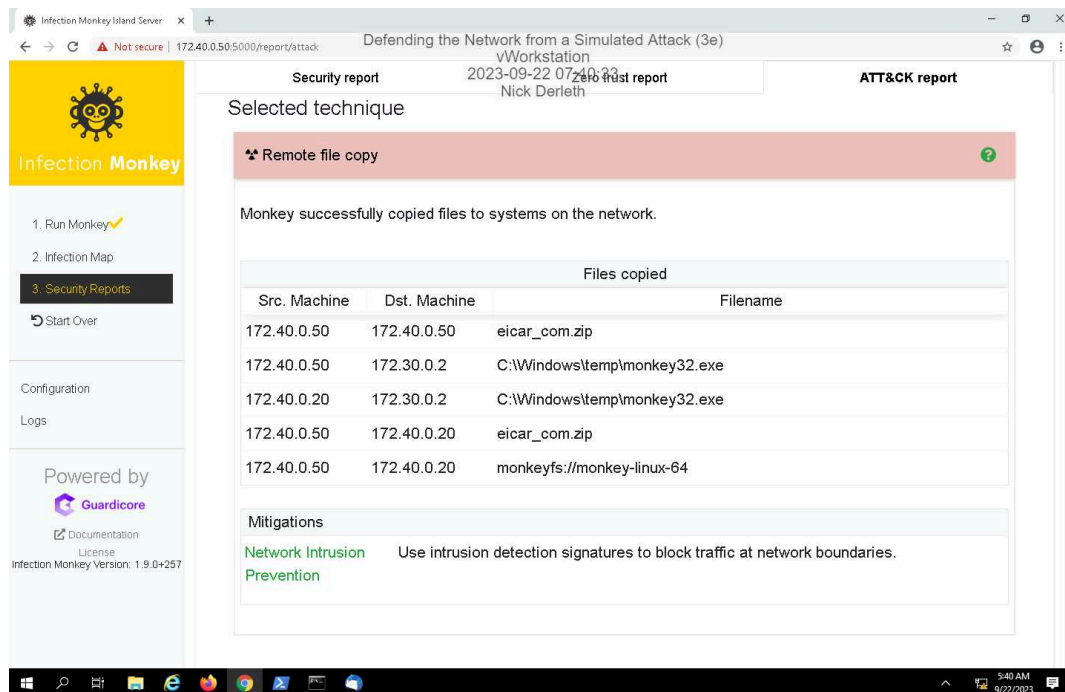
Defending the Network from a Simulated Attack (3e)

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

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



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

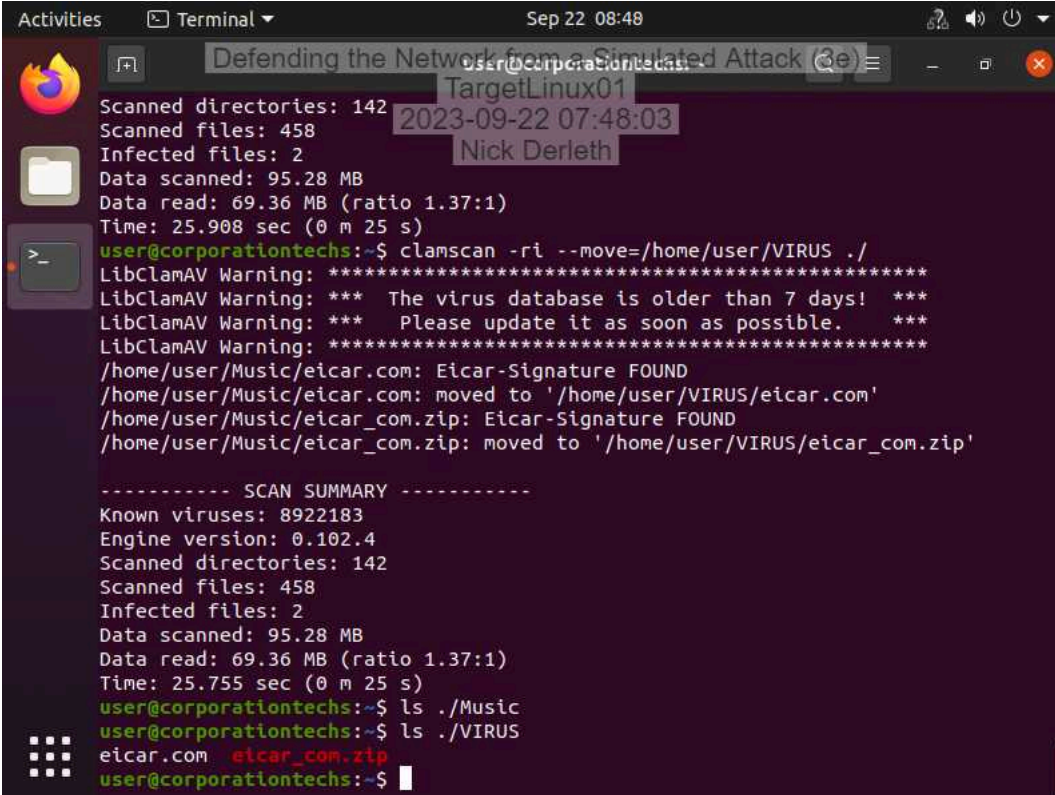


Part 2: Use Antivirus Software to Remove Malicious Files

Defending the Network from a Simulated Attack (3e)

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

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



The image shows a terminal window titled "Defending the Network from a Simulated Attack (3e)" with a user prompt "user@corporationtechs:". The terminal displays the output of a ClamAV scan command. The scan results show 142 directories scanned, 458 files scanned, and 2 infected files. The infected files are eicar.com and eicar_com.zip, both of which were moved to the /home/user/VIRUS directory. The terminal also shows a scan summary and the results of ls commands for the /Music and /VIRUS directories.

```
Scanned directories: 142
Scanned files: 458
Infected files: 2
Data scanned: 95.28 MB
Data read: 69.36 MB (ratio 1.37:1)
Time: 25.908 sec (0 m 25 s)
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: 25.755 sec (0 m 25 s)
user@corporationtechs:~$ ls ./Music
eicar.com  eicar_com.zip
user@corporationtechs:~$ ls ./VIRUS
eicar.com  eicar_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**.

Incomplete

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

Incomplete

Part 2: Patch the Exploited System

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

Incomplete

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

Incomplete

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

Incomplete

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**.

Incomplete

Part 2: Harden the Network Perimeter

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

Incomplete