|  |
| --- |
| Cybersecurity |
| PROJECT 2: PENETRATION TESTING 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](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative](#_4i7ojhp) 10

[Summary Vulnerability Overview 1](#_2xcytpi)3

Vulnerability Findings [1](#_1ci93xb)4

# 

## Contact Information

|  |  |
| --- | --- |
| **Company Name** | Black Hat Cyber Team |
| **Contact Name** | Sean Vanzante |
| **Contact Title** | Ethical Hacker Who Loved This Activity |

## 

## Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Comments** |
| 001 | February 24, 2025 | Sean Vanzante | Conducted Penetration Test on Rekall Inc using a variety of methods and tools to discover, identify and exploit vulnerabilities.  Engagement consisted of the 5 phases of a Pen Test:  #1 – Planning & Reonnaissance  #2 – Scanning  #3 – Exploitation  #4 – Post-Exploitation  #5 – Reporting |

# READ ME / SOURCES CREDIT

# Group project 2 Partner: Nicholas Babcok, Tameem Faizi, Griffin Pelletier, Udoy Dey

# Sources:

# Google AI

# Chat GPT

## 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:

Chart

Description automatically generated with medium confidence

### 

### 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.

* Weak password: although there were some successful attempts to obtain user credentials, some instances of cracking password hashing was not successful
* On first attempts to exploit some web vulnerabilities, not all attempts were successful showing at least a base sense of security
* Number of hosts open through nmap scanning is an acceptable amount
* Drupal service is a secure service

### 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.

* Insecure website due to poor coding practices
* Input validation and sanitization on website
* Weak credentials & authentication: although present in a few cases, it was not always the case that all users / password hashes were found and able to be cracked
* No apparent firewall, or incident detection, prevention and response system in place; need for better detection and monitoring procedures
* Limit Sudo access to apply principle of least privilege and update / upgrade to ensure maximum level of security
* Disable unnecessary services and close / limit port access
* NTLM was replaced by Kerberos in Windows 2000 due to several insecurities, wherever possible, Kerberos authentication should be utilized
* Upgrade, update and / or patch software – Update / Upgrade: Apache Struts, Jserv, Tomcat; Update / patch or replace: SLMail for more secure alternative
* Review world permissions on files and directories to ensure principle of least privilege is implemented

## Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It’s fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

## 

This penetration test assessed the security posture of the target environment, identifying multiple vulnerabilities across network services, web applications, and authentication mechanisms. High-risk findings include exposed services on specific ports, which could allow unauthorized access and on service exploitation. Additionally, reconnaissance strategies using **Nmap and Nessus scans** revealed misconfigurations and potential attack vectors.

The web, linux and windows applications assessment uncovered several critical vulnerabilities, including **SQL injection, cross-site scripting (XSS), local file inclusion (LFI), PHP injection and directory traversal, all** exploiting vulnerable PHP code. Further, sensitive credentials were found embedded in multiple locations and exposed text files on the website, presenting a significant risk of unauthorized access. Once access was gained to the Windows 10 machine, we were able to laterally move into WinDC to gain full and uninhibited access to the Domain Controller.

Nmap scanning tool was used to identify hosts and devices connected to the network and obtain specific information on open ports, operating systems and services. Nessus scanning tool was used to identify known vulnerabilities that could be exploited by attackers.

Metasploit tool used for RCE exploitation to gain access to Windows 10 machine, establish persistence, laterally move into Domain Controller and gain privilege escalation.

Authentication and session management weaknesses were exploited through **brute-force attacks using Burp Suite’s cluster bomb and session hijacking via the sniper module**. The team successfully executed **command-line injection**, gaining remote shell access. Open-source intelligence (OSINT) and **crt.sh reconnaissance** provided additional insight into external threats and certificate management.

Privilege escalation was achieved using **Kiwi credential dumping** to extract credentials from the **Security Accounts Manager (SAM) and cache**, followed by **password cracking with John the Ripper.** Finally, **DCsync was used to impersonate a domain controller**, allowing access to highly sensitive Active Directory (AD) information, demonstrating a complete compromise of domain security.

These findings highlight significant security weaknesses that could be exploited by malicious actors. Immediate remediation is recommended, including **patching vulnerable services, strengthening authentication mechanisms, improving web application security, and enhancing system monitoring and logging** to detect and prevent future attacks.

Vulnerabilies observed have been detailed and documented in the Vulnerability Findings section, which includes screenshots and remediation strategies.

## 

## Summary Vulnerability Overview

|  |  |
| --- | --- |
| **Vulnerability** | **Severity** |
| XSS – Cross-site scripting on php; welcome.php | **High** |
| XSS – Cross-site scripting on php; memory-planner.php | **High** |
| HTTP – About-Rekall.php | **High** |
| LFI – Local File Instrusion | **High** |
| SQL Injection | **Critical** |
| Exposure of sensitive data & lack of proper authentication / encryption | **Critical** |
| Command line injection on Login page | **Critical** |
| Brute force attack | **High** |
| PHP injection | **High** |
| Session management | **High** |
| Directory Traversal | **High** |
| OSINT framework; sensitive information | **Information** |
| Open hosts, ports & their services | **Medium** |
| Open port for host running Drupal service | **Medium** |
| RCE vulnerability with Apache Struts | **Critical** |
| RCE Exploit | **Critical** |
| RCE Exploit | **Critical** |
| RCE Exploit | **Critical** |
| Sudo vulnerability - CVE-2019-14287 / Weak password | **Critical** |
| OSINT framework; sensitive information | **Critical** |
| FTP vulnerability | **High** |
| SLMail vulnerability | **High** |
| Task schedule to gain persistence | **High** |
| Credential Access & Weak Authentication vulnerability | **High** |
| Lateral movement into WinDC & Credential Access | **Critical** |
| Improper authentication and authorization vulnerability | **Critical** |

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

|  |  |
| --- | --- |
| **Scan Type** | **Total** |
| Hosts | 192.168.14.35  34.102.136.180  192.168.13.0 / 24 (subnet scan)  192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  172.22.117.0 / 24 (subnet scan)  172.22.117.10  172.22.117.20 |
| Ports | 21, 22, 80, 106, 110, 443, 5901, 6001, 8009, 8080 |

|  |  |
| --- | --- |
| **Exploitation Risk** | **Total** |
| **Critical** | 11 |
| **High** | 12 |
| **Medium** | 2 |
| **Low** | 1 |

## Vulnerability Findings

|  |  |
| --- | --- |
| **Vulnerability 1** | **Findings** |
| **Title** | XSS – Cross-site scripting on php; welcome.php |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | Reflected XSS payload: <script>alert(‘XSS’);</script> allowed injection of malicious code; code injected into user input: “put your name here” and “leave us a comment” |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation and sanitization; content security policy; trust specific format / extensions. |

|  |  |
| --- | --- |
| **Vulnerability 2** | **Findings** |
| **Title** | XSS – Cross-site scripting on php; memory-planner.php |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | Reflected XSS payload: scrscriptipt allowed injection of malicious script; code injected into user input: “choose your character” |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation and sanitization; content security policy; trust specific format / extensions. |

|  |  |
| --- | --- |
| **Vulnerability 3** | **Findings** |
| **Title** | HTTP; About-Rekall.php |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | Used curl command to connect to IP address 192.168.14.35 through port 80 and gain access through About-Rekall.php page |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation and sanitization; secure coding practices and regular reviews. |

|  |  |
| --- | --- |
| **Vulnerability 4** | **Findings** |
| **Title** | LFI – Local File Instrusion on php; memory-planner.php |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | #1 - Create php script in Linux and upload to memory-planner.php page; user input 1st field “please upload an image:browse”  #2 - Change extension of script to php.jpg and upload to memory-planner.php; user input 2nd field “please upload an image:browse” -- user input would only accept jpg format |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation and sanitization; restrict file access by using dedicated file directory for these types of files; restrict file uploads and inclusions. |

|  |  |
| --- | --- |
| **Vulnerability 5** | **Findings** |
| **Title** | SQL Injection on Login page |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | Directory traversal on Rekall Disclaimer page to gain access to /etc/passwd directory and find user name with home directory; SQL injection using true statement of OR 1=1 to gain access |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation and sanitization; use prepared statements; restrict file uploads and inclusions. |

|  |  |
| --- | --- |
| **Vulnerability 6** | **Findings** |
| **Title** | Exposure of sensitive data & lack of proper authentication / encryption on the Login page |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | #1 Use control “u” to view the html source code on their website; user name and password is exposed.  #2 – adding robots.txt extension in url will open a window with sensitive information. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Remove and do not store sensitive data in the HTML source code. Password encryption using secure hashing algorithms. |

|  |  |
| --- | --- |
| **Vulnerability 7** | **Findings** |
| **Title** | Command line injection on Login page |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | After exploiting the Login page from Vulnerability #6, click “here” on Login page takes you to their networking.php page with reference to vendors.txt file; when using linux code “cat” as command line injection, information on SIEM is exposed: splunk firewall, barracuda cloud, aws load balancer. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation; use library functions that are built-in functions instead of shell commands to execute system commands. |

|  |  |
| --- | --- |
| **Vulnerability 8** | **Findings** |
| **Title** | Brute force attack |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | Using burpsuite tool, captured user name and password through cluster bomb brute force. User name and password validated through website Login. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement strong password policies; use MFA; educate employees about password policies; set limits on failed login attempts. |

|  |  |
| --- | --- |
| **Vulnerability 9** | **Findings** |
| **Title** | PHP injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | Add robots.txt extension in the URL, opens a window showing souvenirs.php. In the URL, add /souvenirs.php after the IP address 192.168.14.35 and a “CALLUSNOW” button appears, click it to show vulnerability. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation and sanitization; content security policy; trust specific format / extensions. |

|  |  |
| --- | --- |
| **Vulnerability 10** | **Findings** |
| **Title** | Session management |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | On Login page, username: melina password: milena (identified from previous exploitat) will enable a “here” button to pop up; click it and you can view a webpage with Admin legal documents – Restricted Area. Using the burpsuite tool and a sniper attack type, you can capture this webpage and identify Position 87 as the session to use. Copy the URL, add “admin=87” (session #) to the end and gain access to the folder / file. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Use strong encryption with HTTPS protocol; secure cookie management; use strong session IDs that are long and difficult to guess; MFA. |

|  |  |
| --- | --- |
| **Vulnerability 11** | **Findings** |
| **Title** | Directory Traversal through welcome page |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | Directory traversal to access old disclaimers folder and view disclaimer\_1.txt file. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation; least privilege principle; use web application filter to filter requests containing malicious patterns. |

|  |  |
| --- | --- |
| **Vulnerability 12** | **Findings** |
| **Title** | OSINT framework; sensitive information |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Information |
| **Description** | OSINT framework, registrant name sshUser for Alice was discovered; Registrant email for employee [jlow@2U.com](mailto:jlow@2U.com) was discovered |
| **Images** |  |
| **Affected Hosts** | 34.102.136.180 as provided by TAs |
| **Remediation** | Remove and do not store sensitive data in public sites. Email is sometimes unavoidable but not user codes. |

|  |  |
| --- | --- |
| **Vulnerability 13** | **Findings** |
| **Title** | Open hosts, ports & their services |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | Scanned the IP and subnet 192.168.13.0/24 and found 5 hosts open, including information on Ports, Services and what is open and potentially vulnerable. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.0/24; open ports on 192.168.13.10; .11; .12; .13; .14 |
| **Remediation** | Disable unnecessary services; utilize firewalls to restrict access |

|  |  |
| --- | --- |
| **Vulnerability 14** | **Findings** |
| **Title** | Open port for host running Drupal service |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | Namp scan concludes Host IP 192.168.13.13 is running service Drupal; known vulnerabilities include SQL injection and XSS |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | Disable unnecessary services; utilize firewalls to restrict access |

|  |  |
| --- | --- |
| **Vulnerability 15** | **Findings** |
| **Title** | RCE vulnerability with Apache Struts |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | #1 - Nessus scan on 192.168.13.12: Apache struts: RCE vulnerability due to improper handling of Content-Type reader; can be exploited by a non-authenticated, remote attacker.  #2 - Nessus scan on 192.168.13.12: Apache struts: RCE vulnerability in Jakarta multipart due to improper handling of Content-Type header; unauthenticated remote attacker can exploit. Gained access to the host and able to cat into root directory. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Regularly apply updates and security patches on OS, applications and other dependencies; secure coding practices and avoid using functions that allow arbitrary command execution; apply principle of least privilege; |

|  |  |
| --- | --- |
| **Vulnerability 16** | **Findings** |
| **Title** | RCE Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Nmap scan reveals port 8009 open, version apache jserv; port 8080 open, version apache tomcat/coyote. Able to gain access using Metasploit and was able to cd into root directory. Known CVE-2020-1938. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | Restrict access using firewalls and allowlists of IPs; use strong authentication; regularly apply updates and security patches on OS, applications and other dependencies; implement security monitoring and IDS. |

|  |  |
| --- | --- |
| **Vulnerability 17** | **Findings** |
| **Title** | RCE Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Nmap scan reveals port 80 open, version apache httpd 2.4.7. . Able to gain access using Metasploit and gain access to /etc/sudoers directory and /etc/passwd directory. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | Restrict access using firewalls and allowlists of IPs; use strong authentication; assign / limit file and directory permissions; apply principle of least privilege; regularly apply updates and security patches on OS, applications and other dependencies. |

|  |  |
| --- | --- |
| **Vulnerability 18** | **Findings** |
| **Title** | RCE Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Nmap scan reveals port 80 open, version apache httpd 2.4.25. PHP RCE vulnerability with version of PHP running on remote server; affected by a remote code execution vulnerability due to insufficient validation of user input |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | Employ strong validation and authentication practices; regular updates and patches; implement security monitoring and IDS. |

|  |  |
| --- | --- |
| **Vulnerability 19** | **Findings** |
| **Title** | #1 - CVE-2019-14287 (sudo vulnerability)  #2 – Weak password |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Nmap scan reveals port 22 open, version OpenSSH 7.6p1 Ubuntu. Recon information from previous OSINT scan displayed a SSHUser name Alice. Gained access through weak password. Sudo access vulnerability allowed privilege escalation to root directory. Known exploits: CVE-2021-41617, CVE-2019-14287 |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Apply patches or upgrade sudo to a newer version; implement strong password policies; use MFA; educate employees about password policies. |

|  |  |
| --- | --- |
| **Vulnerability 20** | **Findings** |
| **Title** | OSINT framework; sensitive information |
| **Type (Web app / Linux OS / WIndows OS)** | Web app  Windows OS |
| **Risk Rating** | Critical |
| **Description** | Github search in company repository finds username and password hash. Password hash can be cracked to obtain user password. |
| **Images** |  |
| **Affected Hosts** | totalrekall in Github |
| **Remediation** | Remove and do not store sensitive data in public sites. |

|  |  |
| --- | --- |
| **Vulnerability 21** | **Findings** |
| **Title** | FTP vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Web app  Windows OS |
| **Risk Rating** | High |
| **Description** | Web vulnerability:  Nmap scan of subnet 172.22.117.0/24 shows port 21 ftp open on host 172.22.117.20. Username and password from previous exploit allows access through IP address on the URL.  Windows vulnerability:  FTP into host 172.22.117.20 through port 21, using username and password above to gain access to the machine which is Windows 10 machine. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.0/24, 172.22.117.20 |
| **Remediation** | Disable unnecessary services; utilize firewalls to restrict access; remove and do not store sensitive data in public sites. |

|  |  |
| --- | --- |
| **Vulnerability 22** | **Findings** |
| **Title** | SLMail vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Able to gain access through SLMail service, pop3 server (port 110), Windows 10 machine. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Update software for security patches; replace SLMail with a more secure alternative; block or limit unnecessary external or internal access; use IDS or IPS. |

|  |  |
| --- | --- |
| **Vulnerability 23** | **Findings** |
| **Title** | Task schedule to gain persistence |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Able to schedule a task to ensure persistence in the event access is somehow lost. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Implement Endpoint Detection & Response; regular monitoring to validate new or modified scheduled tasks; apply principle of least privilege to minimize attack surface. |

|  |  |
| --- | --- |
| **Vulnerability 24** | **Findings** |
| **Title** | Credential Access & Weak Authentication vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | LSA dump credentials from SAM ( security accounts manager ) and obtained a NTLM hash which was able to be cracked to obtain a password.  Able to move into C:\Users\Public\Documents to view files, directories, etc. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Strong hashing algorithm, including adding “salt” variable; enforce LSA protection; regular monitoring; enforce MFA policy. |

|  |  |
| --- | --- |
| **Vulnerability 25** | **Findings** |
| **Title** | Lateral movement into WinDC & Credential Access |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using credentials found in Windows10 machine, laterally move into WinDC. LSA dump credentials from cache to view credentials for Admin user with higher privilege; user name and password hash located and cracked. Gained access as NT Authority/System user and found all User accounts in C:\Windows\system32. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | Strong hashing algorithm, including adding “salt” variable; enforce LSA protection; enforce MFA policy; regular monitoring; role-based access control and limit admin users to restrict access to those who really need it. |

|  |  |
| --- | --- |
| **Vulnerability 26** | **Findings** |
| **Title** | Improper authentication and authorization vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | From list of users in previous vulnerability, we can view Administrator account and obtain password hash through DCsync. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | Protect DC by blocking unauthorized access and restricting network traffic relating to MS-DRSR; use privileged workstations; enforce MFA policy. |