| Cybersecurity |
| --- |
| Penetration Test Report |

Rekall Corporation

Penetration Test Report

**[MB OffSec], LLC**

# 

## 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)1

Vulnerability Findings [1](#_1ci93xb)3

# 

## Contact Information

| **Company Name** | MB OffSec, LLC |
| --- | --- |
| **Contact Name** | Matthew Bialas |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 5/1/24 | Matthew Bialas | Initial Draft |

# 

## 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.

* Rekall Corporation website utilizing input validation.
* Protection against basic SQL injection tactics.
* Separation of Administrator accounts and files from User accounts.
* Established usernames and passwords.

### 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.

* Cross-Site Scripting (XSS)
* Sensitive Data Exposure
* Local File Inclusion (LFI)
* SQL Injection
* Command Injection
* Brute Force Attack
* PHP Injection
* Session Management
* Directory Transversal
* Sensitive Data Exposure (Open-Source)
* Multiple Hosts and Open Ports
* Remote Code Execution (RCE)
* Privilege Escalation
* Weak Passwords
* Lateral Movement

## Executive Summary

Rekall Corporation (Rekall) engaged MB OffSec, LLC (MBOS) to conduct a thorough penetration test of its networks, systems, and internal/external applications to assess security and identify potential flaws.

The testing aimed to determine system-level weaknesses, exploit any discovered vulnerabilities, and access confidential information stored on the network. This assessment adhered to industry-accepted testing methodology and best practices.

The focus of the evaluation included the primary goal of identifying exploitable vulnerabilities and providing actionable recommendations for remediation. MB OffSec utilized a proven vulnerability testing methodology to assess all relevant components within scope regarding this goal, and other objectives, as requested by Rekall Corporation.

Key Objectives included:

* Find and exfiltrate any sensitive information within the domain.
* Escalate privileges to gain unauthorized access.
* Compromise multiple machines within the environment.

The assessment considered Rekall's actual business processes and potential threats, ensuring realistic results reflecting the organization's exposure levels to online threats.

Through its analysis, MB OffSec successfully identified critical vulnerabilities across Rekall's environment, highlighting areas requiring immediate attention and remediation. The findings and recommendations can be found below, beginning with the Summary Vulnerability Overview.

Overall, the penetration test report outlines identified vulnerabilities, their potential impact, and actionable recommendations for remediation to enhance Rekall's security posture and mitigate future risks to its networks and systems.

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| * Cross-Site Scripting (XSS) | **Critical** |
| * Sensitive Data Exposure | **High** |
| * Local File Inclusion (LFI) | **Critical** |
| * SQL Injection | **Critical** |
| * Command Injection | **Critical** |
| * Brute Force Attack | **Critical** |
| * PHP Injection | **High** |
| * Session Management | **Critical** |
| * Directory Transversal | **Medium** |
| * Sensitive Data Exposure (Open-Source) | **Medium** |
| * Multiple Hosts and Open Ports | **Critical** |
| * Remote Code Execution | **Critical** |
| * Apache Struts 2 Jakarta Multipart Parser RCE | **Critical** |
| * Apache Tomcat JSP Upload Bypass | **Critical** |
| * Apache mod\_cgi Bash Environment | **Critical** |
| * Drupal RESTful Web Services Unserialize | **Critical** |
| * Seattle Lab Mail 5.5 POP3 Buffer Overflow | **Critical** |
| * Privilege Escalation | **Critical** |
| * Weak Passwords | **Critical** |
| * Lateral Movement | **Critical** |

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

| **Scan Type** | **Total** |
| --- | --- |
| **Hosts** | 192.168.14.35 - totalrekall.xyz 192.168.13.1 - Linux Host Machine 192.168.13.10 - Linux OS  192.168.13.11 - Linux OS  192.168.13.12 - Linux OS  192.168.13.13 - Linux OS  192.168.13.14 - Linux OS  172.22.117.100 - Windows Host Machine  172.22.117.20 - Windows10 OS  172.22.117.10 - Server2019 - Domain Controller |
| **Ports** | 21 - FTP  22 - SSH  80 - HTTP  110 - POP3  139 - SMB  443 - HTTPS 8009 - AJP13  8080 - HTTP Proxy  8443 - HTTPS Proxy |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | **16** |
| **High** | **2** |
| **Medium** | **2** |
| **Low** | **0** |

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## Vulnerability Findings

| **Cross Site Scripting** | **Findings** |
| --- | --- |
| **Title** | **Flag 1-3: Cross Site Scripting (XSS)** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | MBOS successfully inserted alerts into multiple fields on the Rekall website using Cross-Site Scripting. The Memory page field included input validation settings, but these were routed around using script changes:  <SCRscriptIPT> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Input validation, encoding, and sanitization. |

| **Sensitive Data Exposure** | **Findings** |
| --- | --- |
| **Title** | **Flag4: Sensitive Data Exposure** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **High** |
| **Description** | Potential sensitive data appears in the HTTP response headers using a cURL request: curl -v http://192.168.14.35/About-Rekall.php |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Perform proper data encryption with strong, updated protocols. |

| **Local File Inclusion** | **Findings** |
| --- | --- |
| **Title** | **Flag 5-6: Local File Inclusion (LFI)** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | Upload of any .php file on the VR Planner “Choose your Adventure” page is accepted.  Input validation on the VR Planner “Choose your location” page checks for the presence of a .jpg file. To bypass this upload, MBOS named a script: script.jpg.php.  These vulnerabilities could result in malicious scripts being run on the database to modify or delete data. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Implement stronger input validation and sanitization practices. Ensure user input is thoroughly checked using a valid identifier to prevent unauthorized data manipulation. |

| **SQL Injection** | **Findings** |
| --- | --- |
| **Title** | **Flag 7: SQL Injection** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | A potential malicious SQL code was successfully input for backend database manipulation and access to a user account. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Use query parameters in the application code to separate SQL commands from user input. |

| **Sensitive Data Exposure** | **Findings** |
| --- | --- |
| **Title** | **Flag 8-9: Sensitive Data Exposure** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **High** |
| **Description** | The username and password were found in the HTML code, and viewable by highlighting the webpage.  Adding “robots.txt” to Rekall’s IP address reveals private areas of the site's contents, potentially exposing open additional exploit vulnerabilities. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Modify web page source code to remove or encrypt <input> tags.  Implement access controls and HTTP authentication at the web server level, restricting access to sensitive directories and files to authorized users only. |

| **Command Injection** | **Findings** |
| --- | --- |
| **Title** | **Flag 10-11: Command Injection** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | A Command Injection payload was utilized to reveal SIEM, server, firewall, Cloud, and load balancer information.   * www.welcometorecall.com && cat vendors.txt * www.welcometorecall.com | cat vendors.txt |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Implement input filtering mechanisms to block or sanitize potentially dangerous characters or commands from user-supplied input. Use regular expressions or predefined patterns to detect and reject malicious input. |

| **Brute Force Attack** | **Findings** |
| --- | --- |
| **Title** | **Flag 12: Brute Force Attack** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | A separate command injection was used to view the /etc/passwd file and admin credentials to successfully login to the Administrator account ‘melina’. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Implement input filtering to prevent access to directories and enable multi-factor authentication for user accounts to add an extra layer of security beyond passwords. |

| **PHP Injection** | **Findings** |
| --- | --- |
| **Title** | **Flag 13: PHP Injection** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **High** |
| **Description** | Using information found on robots.txt, a hidden webpage was identified and exploited using a payload to manipulate the URL. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Implement strict input validation and file handling to verify user input received by PHP scripts. Use whitelisting to only allow expected characters, and reject input containing potentially dangerous characters or patterns used in PHP code. |

| **Session Management** | **Findings** |
| --- | --- |
| **Title** | **Flag 14: Session Management** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | Utilizing Burp, a secret session ID was found, revealing access to sensitive Admin Legal Documents. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Define session expiration policies to automatically invalidate sessions after a period of inactivity to mitigate exposure to session hijacking attacks. Generate encrypted IDs to create non-guessable session tokens. |

| **Directory Transversal** | **Findings** |
| --- | --- |
| **Title** | **Flag 15: Directory Transversal** |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **High** |
| **Description** | Command injection on Rekall’s Welcome page input field reveals a Disclaimer directory. Directory Transversal was utilized to manipulate the URL and access old disclaimer files. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Sanitize user-controlled input to prevent malicious characters, including "../../". Use absolute paths when referencing files and directories within the web application to avoid reliance on user-supplied input for path construction. Remove outdated files unnecessary to business operations. |

**DAY 2**

| **Sensitive Data Exposure** | **Findings** |
| --- | --- |
| **Title** | **Flag 1-3: Sensitive Data Exposure (Open-Source)** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Medium** |
| **Description** | Potential sensitive data is exposed on [centralops.net](https://centralops.net/co/DomainDossier.aspx), revealed through ‘nslookup’, and listed through a certificate search on [crt.sh.](https://crt.sh/) |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 - totalrekall.xyz |
| **Remediation** | Determine and classify sensitive data with extra security controls. Data should then be filtered by sensitivity level and secured with the appropriate security controls to be viewable and modifiable by intended individuals only. |

| **Multiple Hosts/Open Ports** | **Findings** |
| --- | --- |
| **Title** | **Flag 4: Multiple Hosts and Open Ports** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | An ‘nmap’ scan revealed multiple hosts up and open ports within Rekall’s IP range 192.168.13.0/24. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.1 - Linux Host Machine 192.168.13.10-14 - Linux OS |
| **Remediation** | Review open ports on each host and assess the necessity for business operations. Close unnecessary open ports to reduce the attack surface and minimize the risk of exploitation. Implement firewall rules and access controls to restrict access and harden services to essential ports based on business requirements. |

| **Sensitive Data Exposure** | **Findings** |
| --- | --- |
| **Title** | **Flag 5: Sensitive Data Exposure** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **High** |
| **Description** | Another ‘nmap’ scan revealed the host 192.168.13.13 is running on the web CMS, Drupal, and potentially giving an outlet to further exploits. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 - Linux OS |
| **Remediation** | Apply application controls on all internet-facing policies to block applications with custom signatures. Configure a Denial of Service Policy and set the threshold low enough to block an NMAP scan. [fortinet.com](https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-NMAP-port-scanner/ta-p/196222) |

| **Apache Struts** | **Findings** |
| --- | --- |
| **Title** | **Flag 6: RCE - Apache Struts (See also Flag 10)** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | The Apache Struts 2 Jakarta Multipart Parser RCE vulnerability was found on host 192.168.13.12, which could allow the ability for malicious file upload and lead to Remote Code Execution. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 - Linux OS |
| **Remediation** | Apply the latest security patches or upgrades to Apache Struts. |

| **Apache Tomcat** | **Findings** |
| --- | --- |
| **Title** | **Flag 7: RCE - Apache Tomcat** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | The Apache Tomcat JSP Upload Bypass vulnerability was found on host 192.168.13.10, and could be exploited by attackers to upload a malicious JSP file and lead to Remote Code Execution. MBOS successfully executed a payload to open a shell session and gain root access. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 - Linux OS |
| **Remediation** | Apply the latest security patches or upgrades to Apache Tomcat. |

| **Shellshock** | **Findings** |
| --- | --- |
| **Title** | **Flag 8-9: RCE - Shellshock** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | The Apache mod\_cgi Bash Environment vulnerability was found on host 192.168.13.11, and could allow attackers to perform Remote Code Execution with crafted HTTP requests or other forms of input to a vulnerable system and gain unauthorized access through a root shell (Shellshock). MBOS utilized this exploit through a Meterpreter shell to access the </etc/sudoers> and <etc/passwd files> of this Rekall host. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 - Linux OS |
| **Remediation** | Apply the latest security patches and updates addressing the Apache mod\_cgi vulnerability. Update the Bash shell to a non-vulnerable version. |

| **Remote Code Execution** | **Findings** |
| --- | --- |
| **Title** | **Flag 10: RCE - Apache Struts (See also Flag 6)** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | The Apache Struts 2 Jakarta Multipart Parser RCE vulnerability was found on host 192.168.13.12, which could allow the ability for malicious file upload and lead to Remote Code Execution. MBOS was successfully able to obtain root access through a Meterpreter shell, and unzip/view sensitive files on this Rekall host. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 - Linux OS |
| **Remediation** | Apply the latest security patches or upgrades to Apache Struts. |

| **Drupal** | **Findings** |
| --- | --- |
| **Title** | **Flag 11: RCE - Drupal** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | The Drupal RESTful Web Services Unserialize vulnerability was found on host 192.168.13.13. In Drupal Core, some field types do not properly sanitize data from non-form sources and could lead to remote PHP code execution. [cvedetails.com](https://www.cvedetails.com/cve/CVE-2019-6340/). MBOS was able to exploit the vulnerability on this Rekall host through a Meterpreter shell and view server information. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 - Linux OS |
| **Remediation** | Apply the latest security patches to Drupal core and install any available security updates for contributed projects. [rapid7.com](https://www.rapid7.com/blog/post/2019/02/21/cve-2019-6340-drupal-core-remote-code-execution-what-you-need-to-know/) |

| **Privilege Escalation** | **Findings** |
| --- | --- |
| **Title** | **Flag 12: Privilege Escalation** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | With enumerated information from </etc/passwd>, password guessing was used to SSH into the user account ‘alice’, bypass sudo security policy restrictions, obtain root access, and view sensitive files. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 - Linux OS |
| **Remediation** | Apply the latest security patches or updates, update sudo configuration, and edit the sudoers file to adjust the affected user's privileges and restrict access to commands. |

**DAY 3**

| **Sensitive Data Exposure** | **Findings** |
| --- | --- |
| **Title** | **Flag 1-3: Sensitive Data Exposure (Open-Source)** |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Medium** |
| **Description** | Searching the totalrekall GitHub site repository reveals XAMPP user credentials for ‘trivera’. An nmap port scan of the Rekall subnet (172.22.117.0/24) then revealed two machines with open ports, one being HTTP (172.22.117.20).  Using the Windows10 IP address and ‘trivera’ credentials, MBOS was able to access sensitive files. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 - Windows10 OS |
| **Remediation** | Prioritize removal of sensitive data related to business operations from public facing web pages. |

| **SLMail** | **Findings** |
| --- | --- |
| **Title** | **Flag 4: RCE - SLMail** |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | The SLMail service was running on POP3 port 110 through the Windows10 machine and revealed the Seattle Lab Mail 5.5 POP3 Buffer Overflow vulnerability, which causes data to overflow into adjacent storage.  The vulnerability can cause a system crash or create an entry point for attackers to perform Remote Code Execution. MBOS utilized an exploit to open a Meterpreter shell and access sensitive files. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 - Windows10 OS |
| **Remediation** | Perform regular testing to detect and fix buffer overflows to ensure data written to a buffer is within acceptable boundaries. |

| **Privilege Escalation** | **Findings** |
| --- | --- |
| **Title** | **Flag 5: Privilege Escalation** |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | A Meterpreter shell was utilized to access scheduled tasks with SYSTEM user privileges to interact with tasks on the Windows10 machine. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 - Windows10 OS |
| **Remediation** | Conduct a thorough audit of all scheduled tasks configured on the system and enable task history tracking to maintain a record of task execution. |

| **Weak Passwords** | **Findings** |
| --- | --- |
| **Title** | **Flag 6-8: Weak Passwords** |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Maintaining SYSTEM privileges, MBOS utilized Kiwi, a Mimikatz extension that extracts passwords and hashes. Then with a Meterpreter shell into the Windows10 machine, attempts to crack Administrator passwords were successful. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 - Windows10 OS |
| **Remediation** | Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful. Require strong password complexity requiring passwords to be over 12 characters long, upper/lower case, & include a special character. Reset all user passwords. |

| **Lateral Movement** | **Findings** |
| --- | --- |
| **Title** | **Flag 8-9: Lateral Movement** |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | With acquired Administrator credentials, an SMB PsExec exploit was utilized to test password security and compromise the network. Lateral movement was then performed into the Server2019 Domain Controller to access sensitive files with another Meterpreter shell. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 - Server2019 - Domain Controller |
| **Remediation** | Implement network segmentation with strict access controls to divide the network into separate zones based on business functions, user roles, or sensitivity of data. Establish an IDS/IPS to identify and block suspicious activities. |

| **Weak Passwords** | **Findings** |
| --- | --- |
| **Title** | **Flag 10: Weak Passwords** |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Using Kiwi and DCSync, a credential dumping technique to obtain sensitive information from the Active Directory within the Domain Controller, the NTLM password hash of the user ‘Administrator’ was accessed. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 - Server2019 - Domain Controller |
| **Remediation** | Protect sensitive Domain Administrator credentials using strong encryption methods. Disable NTLM authentication protocols in favor of more secure alternatives such as Kerberos or NTLMv2. Implement logging and auditing capabilities in Active Directory to monitor changes to directory objects and unauthorized replication requests. |