Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

© 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

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

Contact Information

Company Name	7K seKurity
Contact Name	Kammrun Hebert
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	02/07/2023	Kammrun	Web Vulnerabilities
002	02/09/2023	Kammrun	Linux Servers
003	02/13/2023	Kammrun	Windows Servers
004	02/22/2023	Kammrun	Final Report Submitted

© 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.

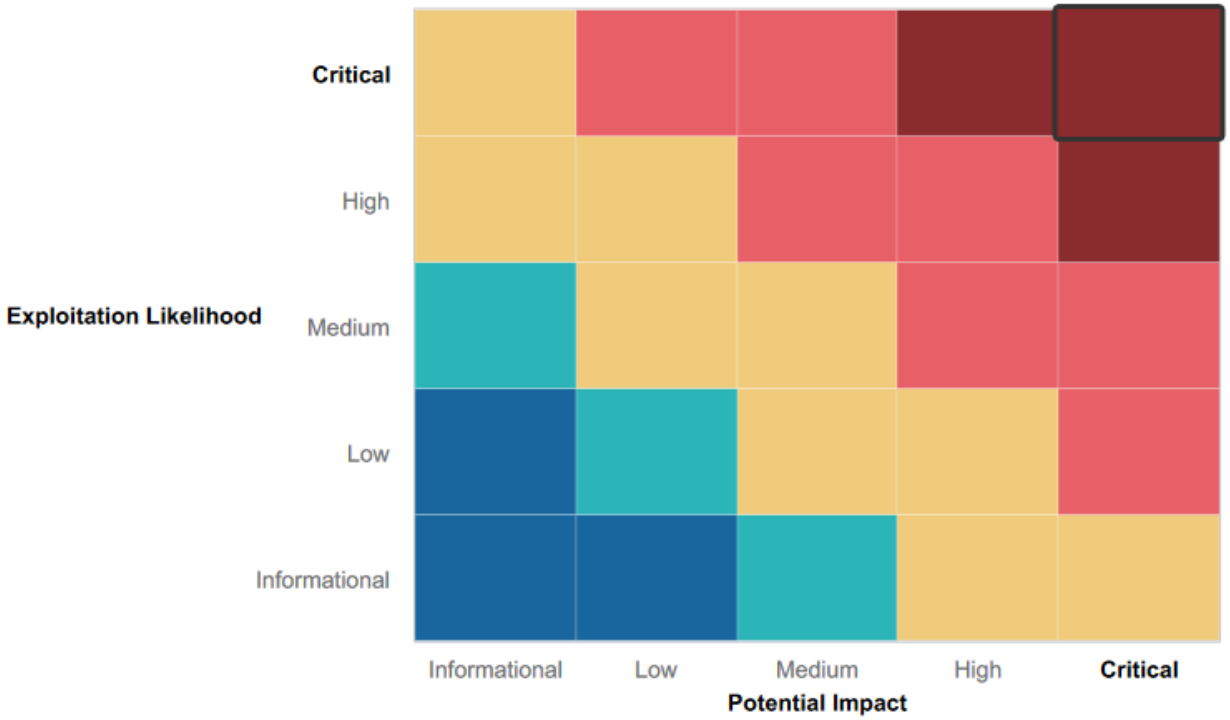
Executive Summary of Findings

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.

- Some web pages did require input validation as an attempt to prevent XXS and local file inclusion attacks
- Passwords were required to access to more sensitive data
- Not all ports were open on the Windows' servers
- Some flags were stored many directories down into the system

Summary of Weaknesses

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

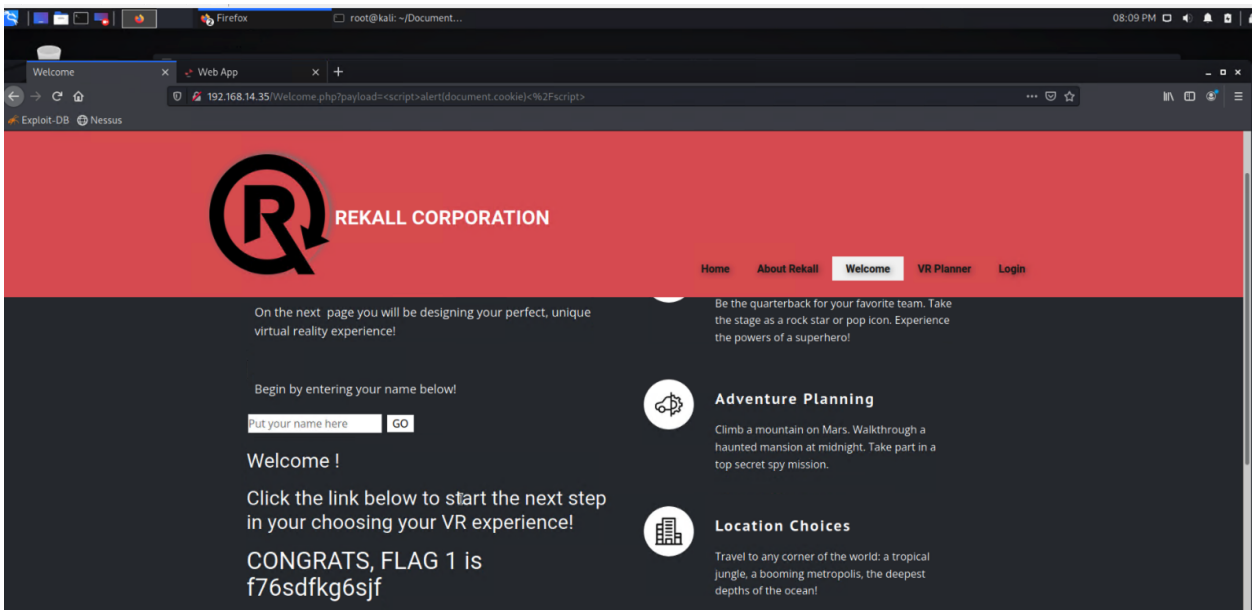
- Web pages vulnerable to XSS on several different webpages
- Sensitive data is easily found in HTTP source codes
- Login page is susceptible to SQL injections as well as brute force attacks
- Multiple web pages vulnerable to command injections as well as PHP injections
- Sessions are easily managed and manipulated to access legal data
- The vulnerability to command injections allows for easy traversal of system directories
- Too much sensitive information is publicly available
- Each host on the Linux servers was vulnerable to known exploits
- User's passwords on both servers are too easily cracked and/or guessed
- Open ports on the Windows' servers are susceptible to known exploits
- Administrators' passwords are too easily accessed and cracked

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

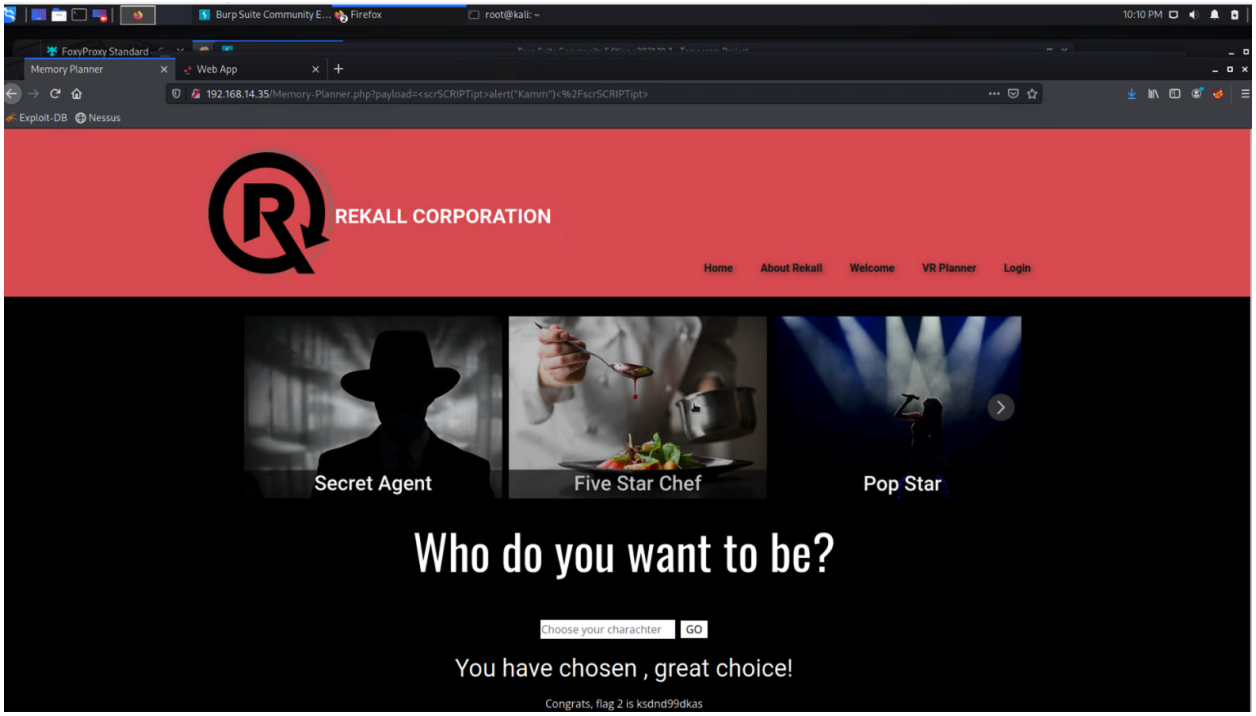
Executive Summary

Day 1: Web Application

We began our testing on the Weclome.php page of the website. Here, we were able to use a ***Cross site scripting (XSS) reflected*** attack on the only available field to access Flag1.

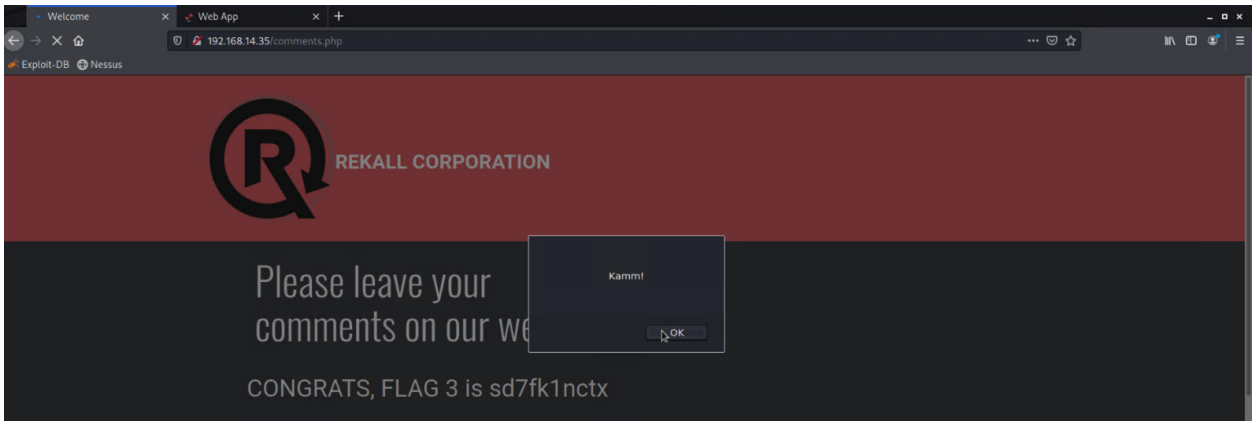


This led us to believe that more XSS vulnerabilities were present throughout the site. On the Memory-Planner.php page, we were able to bypass the input validation in the first field to perform an ***advanced XXS reflected*** attack which gave us Flag2.

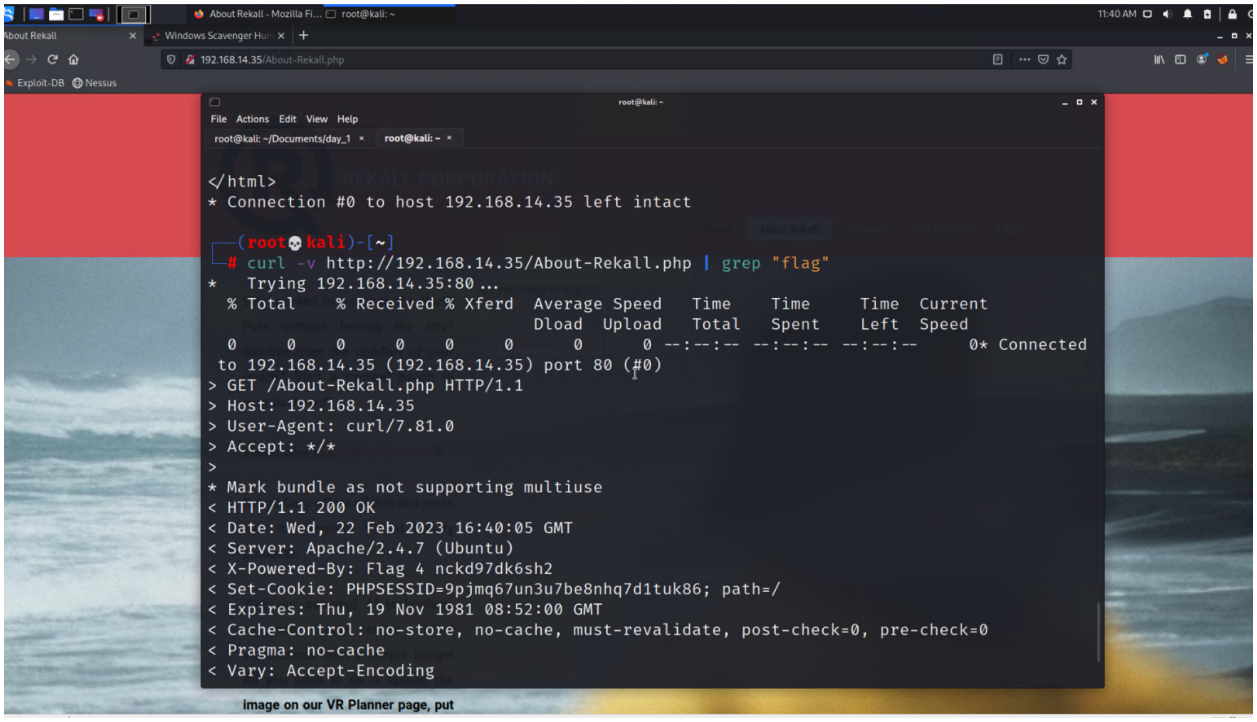


We continued to check other pages for this vulnerability and eventually found Flag3 on the comments.php page. This particular vulnerability could be considered more dangerous than the previous 2 because it is a ***stored XSS*** attack which causes it to remain on Rekall's servers.

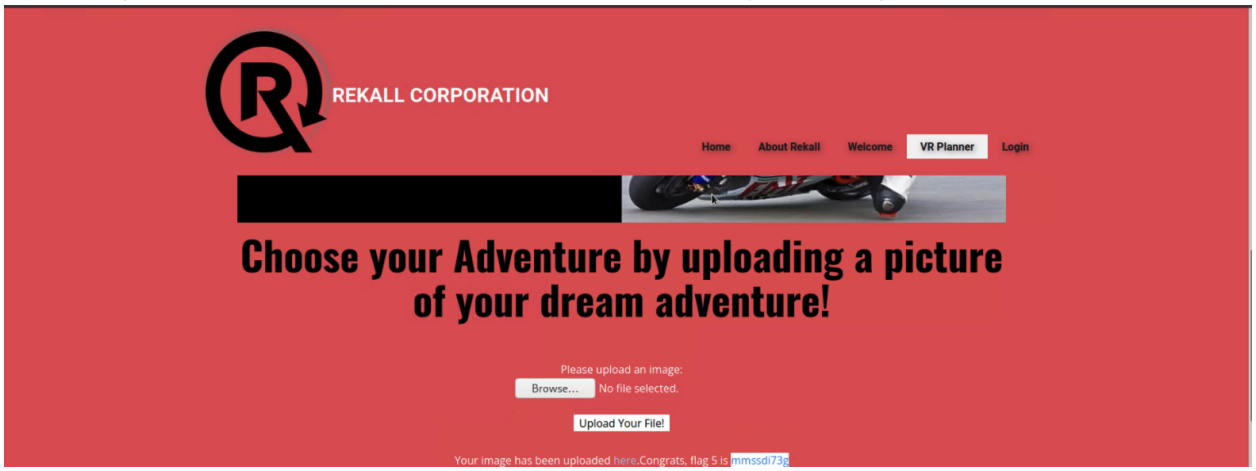
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



As we continued to search the contents of the site, we came across ***sensitive data exposure*** in the HTTP response headers of the About-Rekall.php page. We then used a curl command to find Flag4.

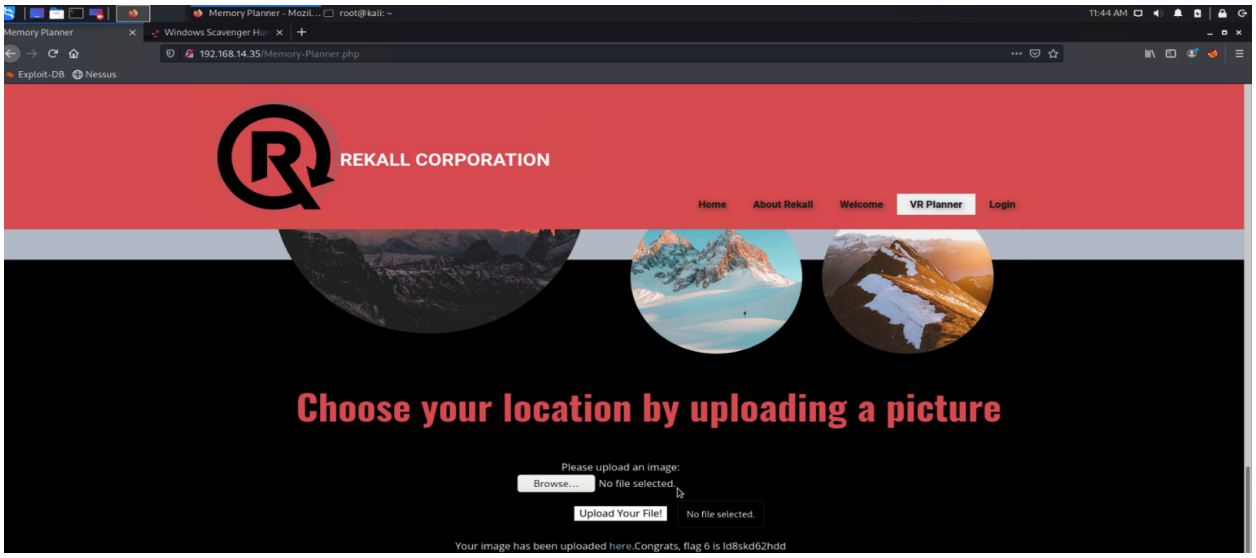


Upon further attempts to attack the Memory-Planner.php page, we were able to find Flag5 by performing a ***local file inclusion*** attack in the second field by uploading a PHP file.

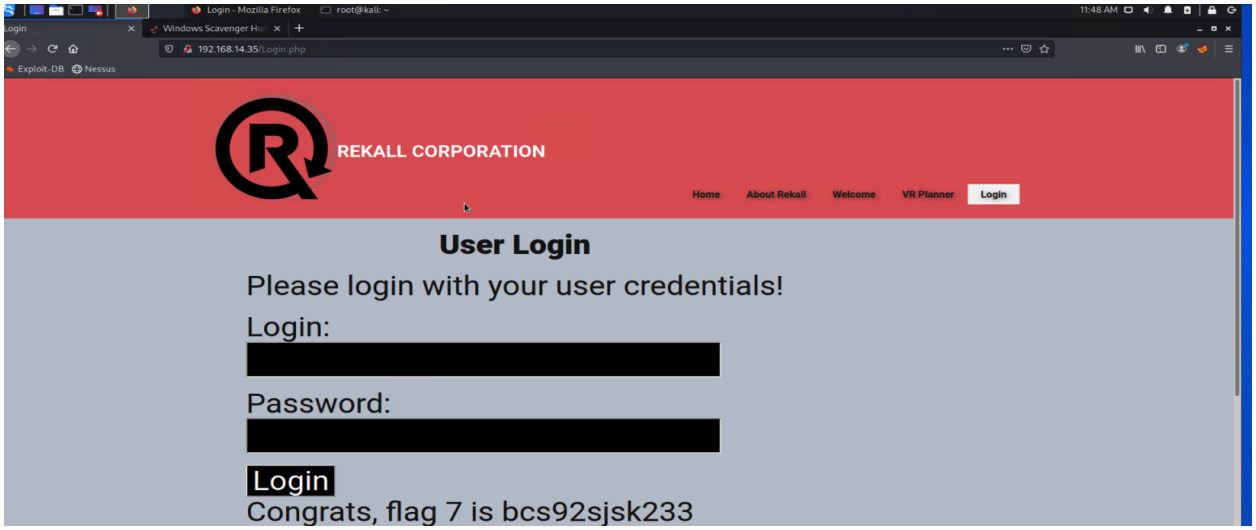


After multiple attempts to attack the Memory-Planner.php page, we were able to perform a more ***advanced local file inclusion*** attack in the third field to find Flag6.

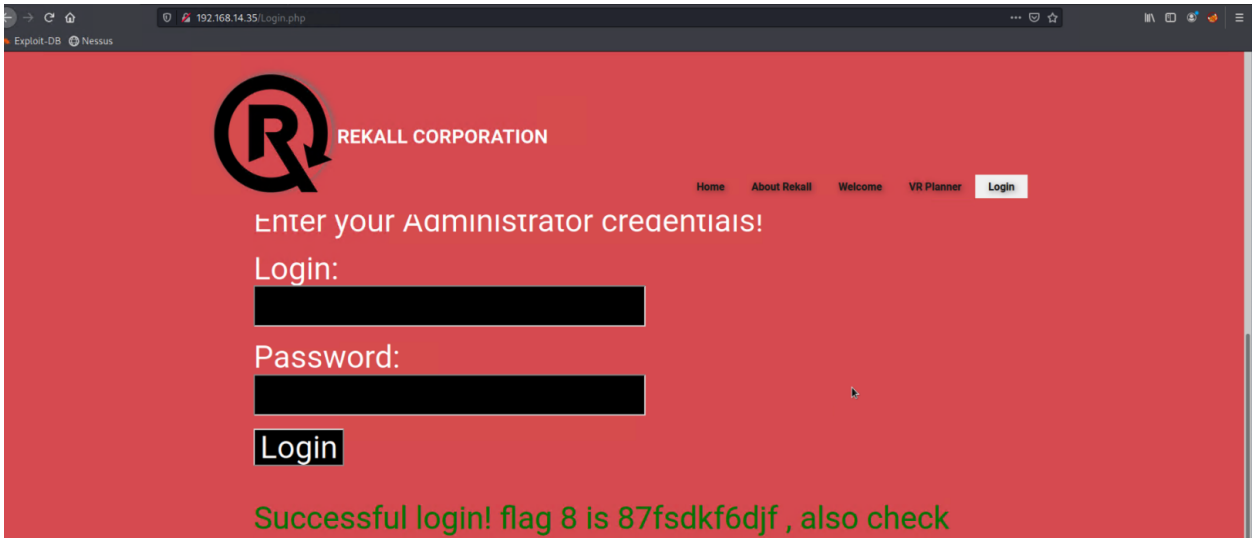
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



We were also able to find vulnerabilities on the Login.php page. We found Flag7 after performing a ***SQL injection*** on the first field.

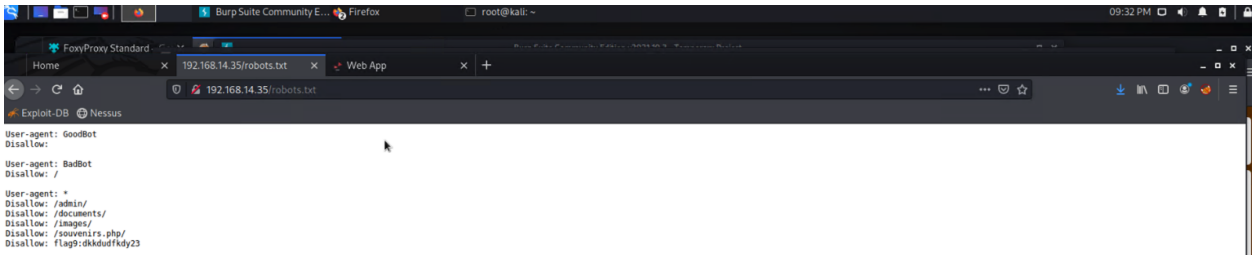


Then, we inspected the HTML source code of the same page where we found more ***sensitive data exposure***. We used the credentials we found to login and find Flag8.

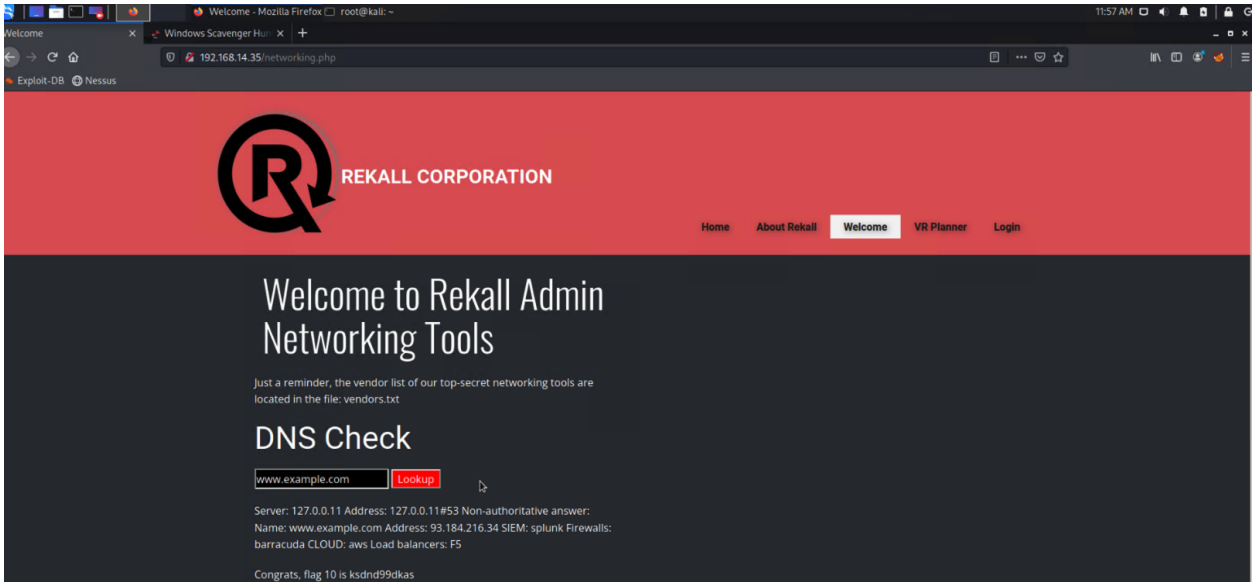


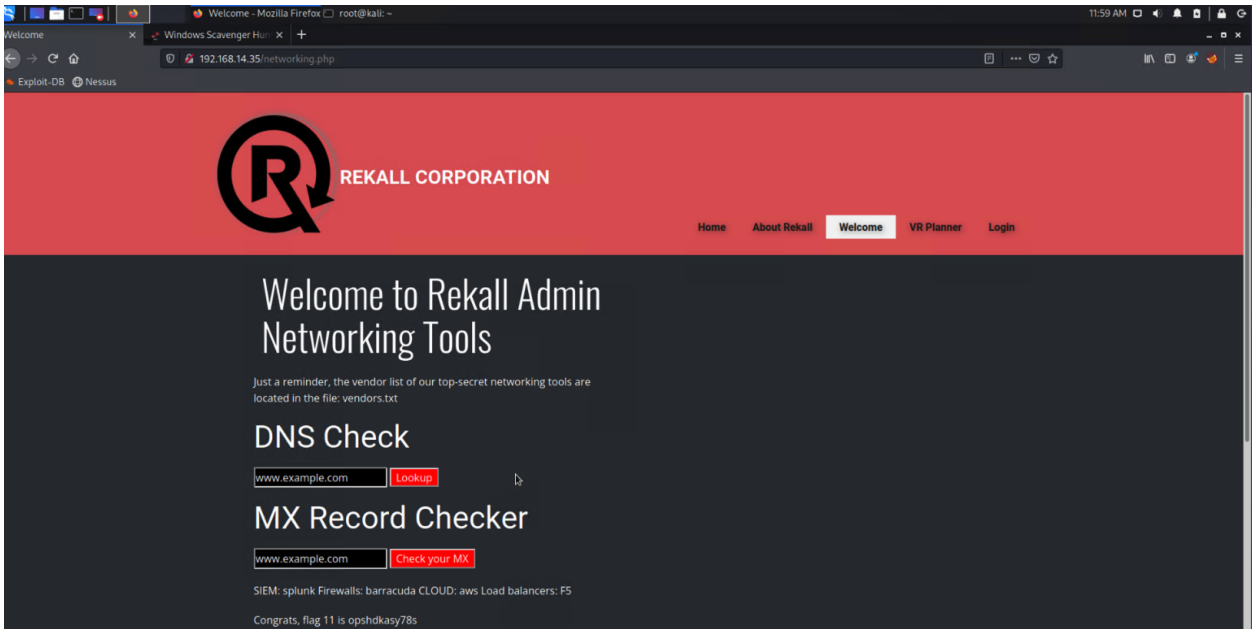
We then simply navigated to Rekall's robot.txt web page where we found more ***sensitive data exposure*** including Flag9.

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



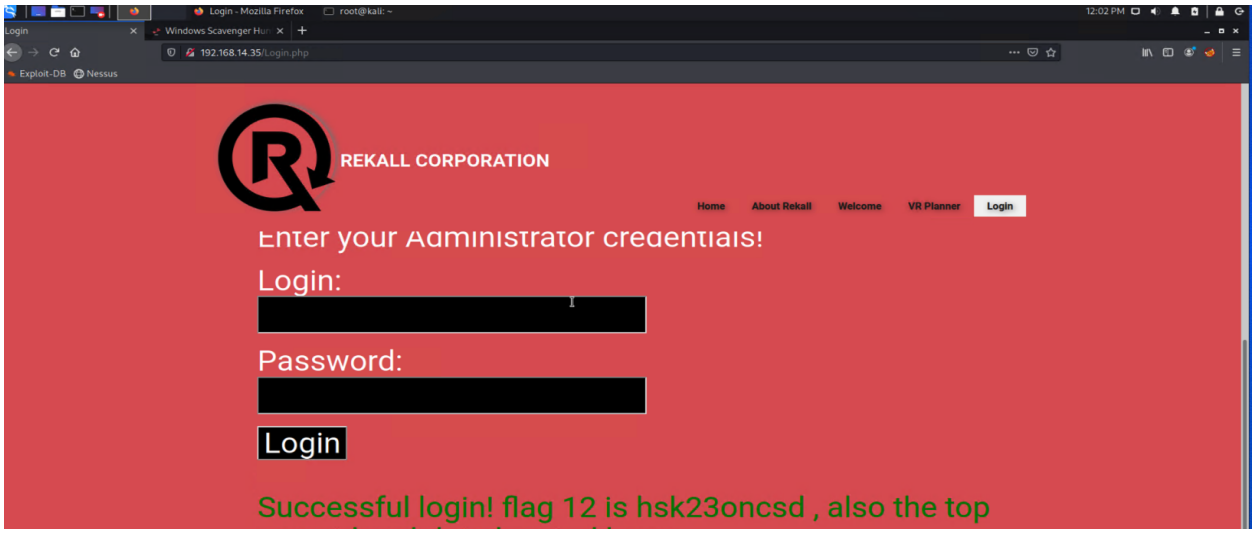
We then used information found on the networking.php page to perform a command injection in the first field and a more advanced command injection in the second field; giving us Flag10 and Flag 11.



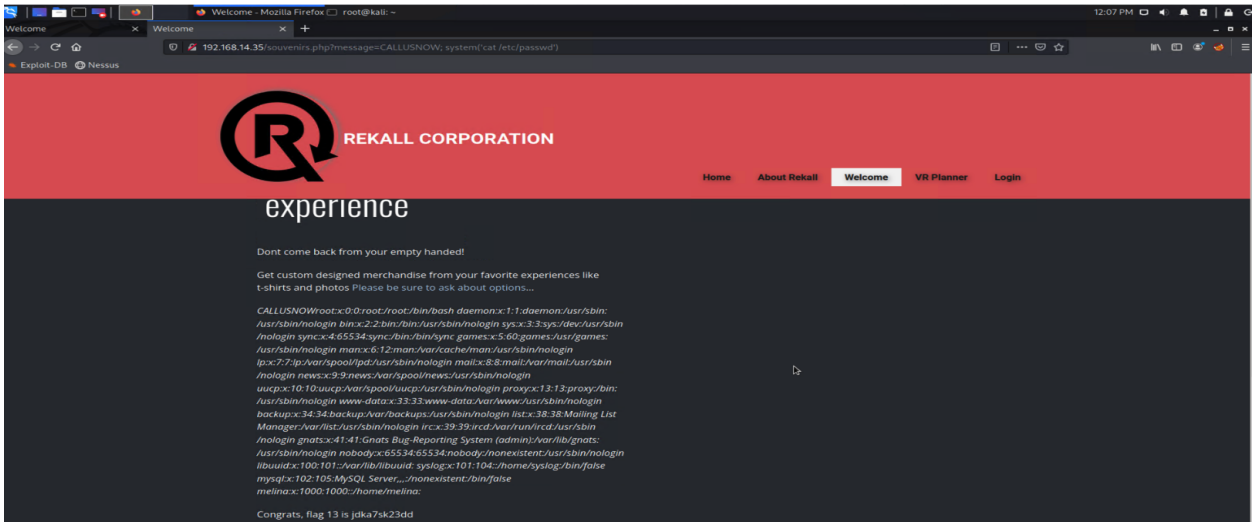


Upon further attempts to attack the Login.php page, we used the vulnerability from the previous 2 flags to perform ***brute force attack*** in the second field to find Flag12.

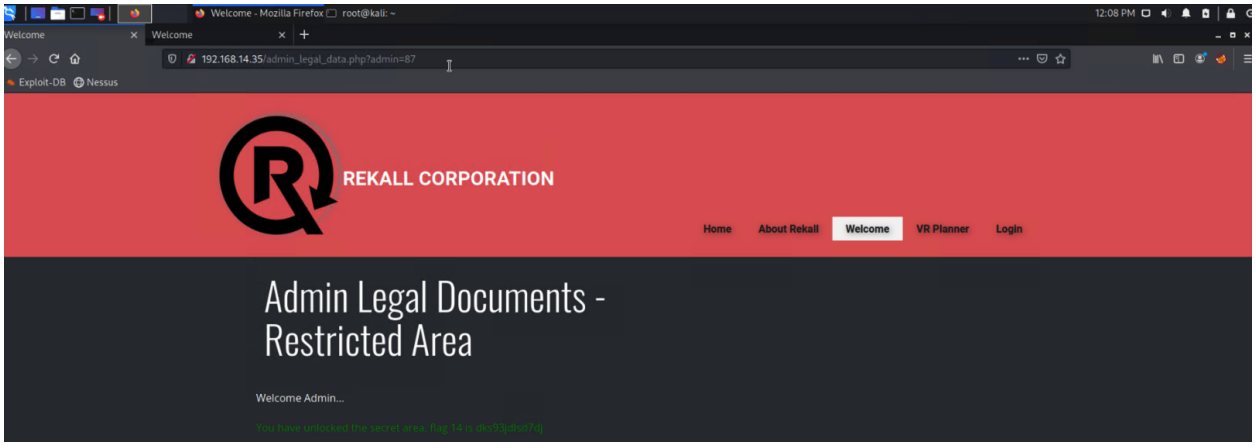
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



When we previously accessed the robots.txt file, we discovered a hidden webpage (souvenirs.php).On this webpage, we performed a ***PHP injection*** by changing the URL, where we found Flag13.

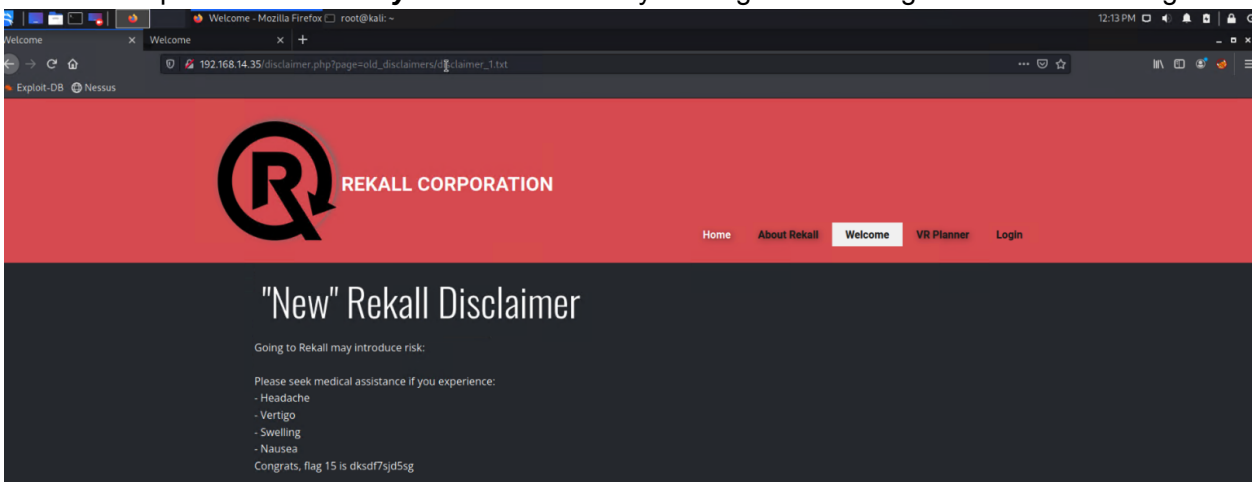


When we found Flag12, there was also a link to another page provided. After navigating to that page, we found that it was vulnerable to a ***session management*** attack. We used Burp Intruder to find the secret session ID that led us to Flag 14.



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

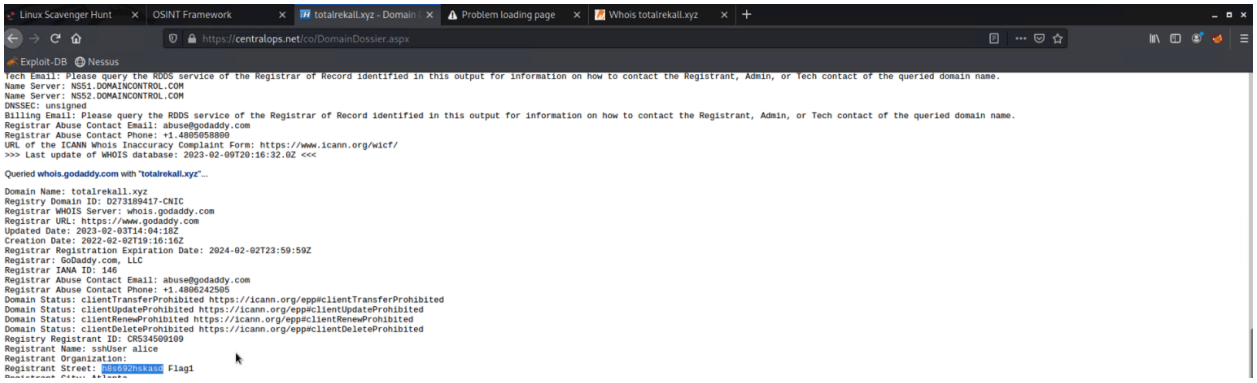
Our final vulnerability found on Rekall's we application was found on the Disclaimer.php page. We were able to perform a ***directory traversal*** attack by altering the URL to give us access to Flag15.



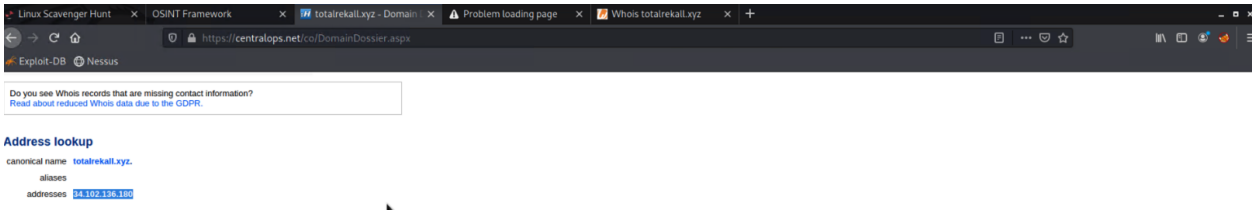
Day 2: Linux Servers

Reconnaisance

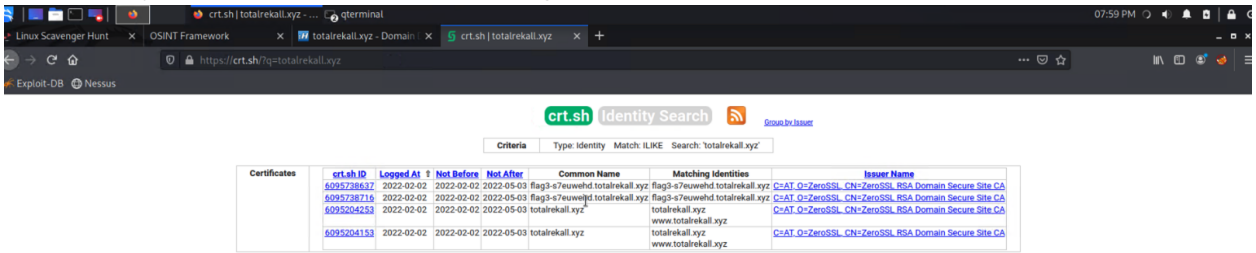
We began the second day of pen testing by performing ***OSINT*** reconnaissance on Rekall to find any ***open source data exposure***. We found Flag1 by viewing the WHOIS data for totalrekall.xyz.



Flag2 was found by performing a nslookup of totalrekall.xyz.



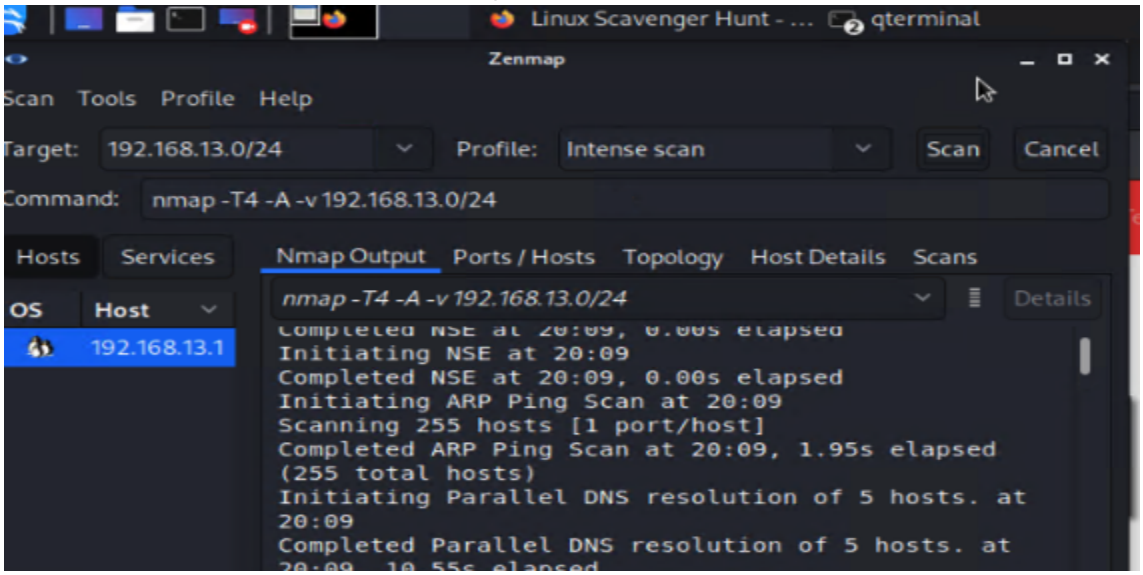
As we continued to use the OSNIT framework to gather information, we used crt.sh to search for totalrekall.xyz once more, and we found Flag3.



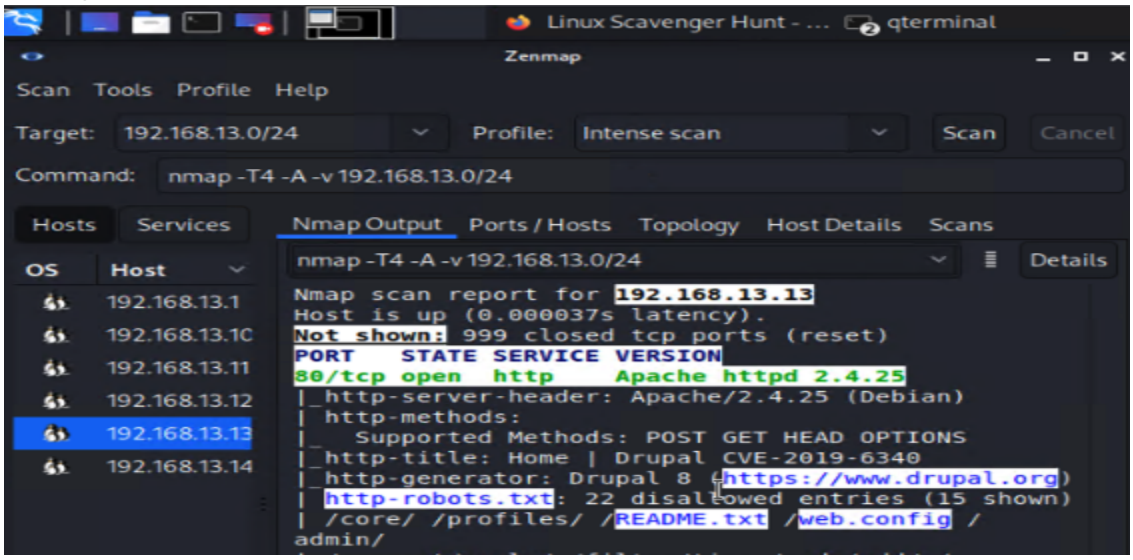
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Scanning

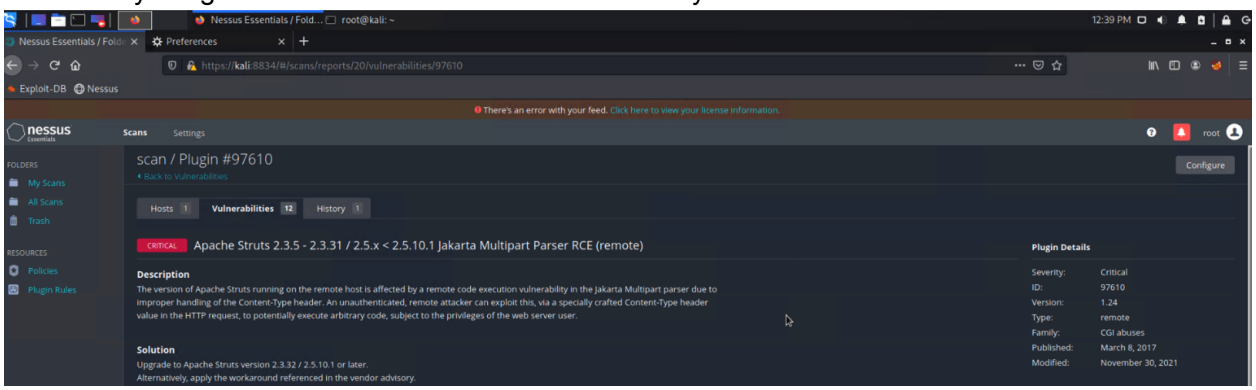
As we moved on from reconnaissance, we performed a Nmap scan of Rekall's network and determined that there were 5 hosts (Flag4) on the network.



Next, we performed a more aggressive Nmap scan to discover that host 192.168.13.13 (Flag5) was running Drupal.



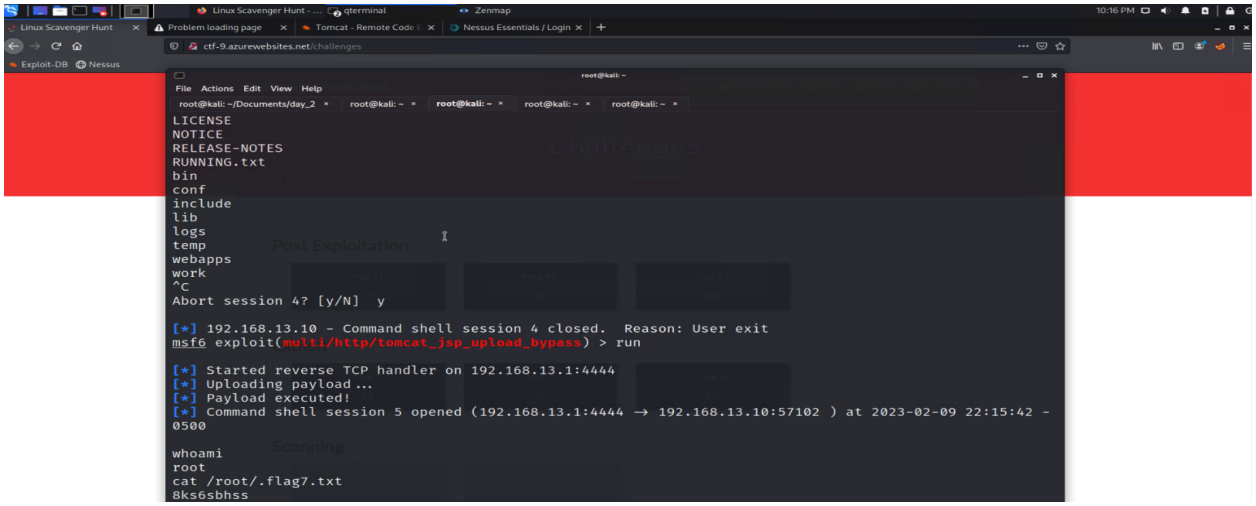
We then ran a Nessus scan on host 192.168.13.12 to find any possible vulnerabilities. Upon the completion of the scan, we found that the host could be susceptible to the ***Apache Struts*** vulnerability. Flag6 was the id number of this vulnerability.



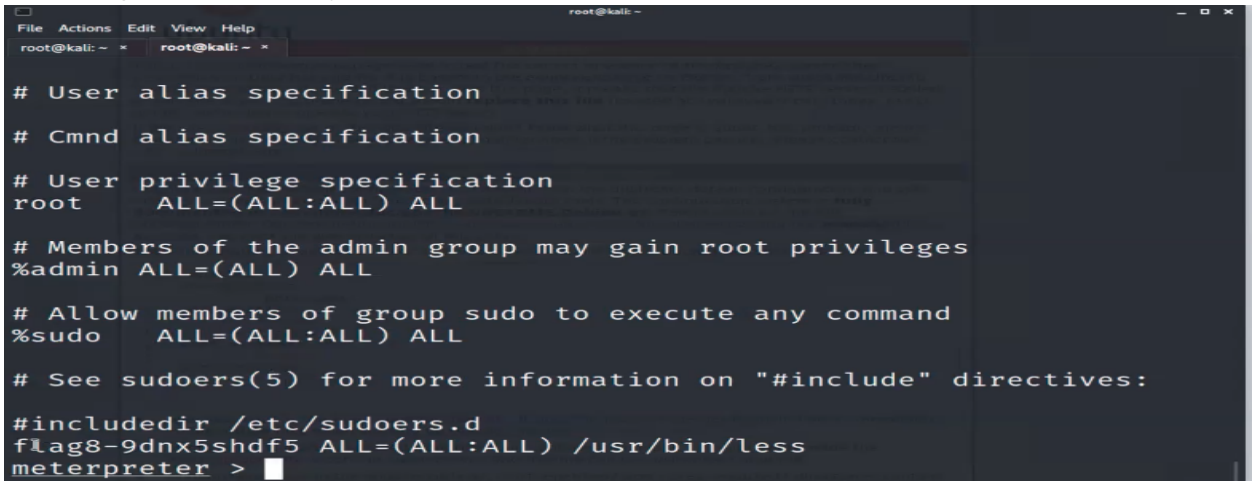
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Exploitation

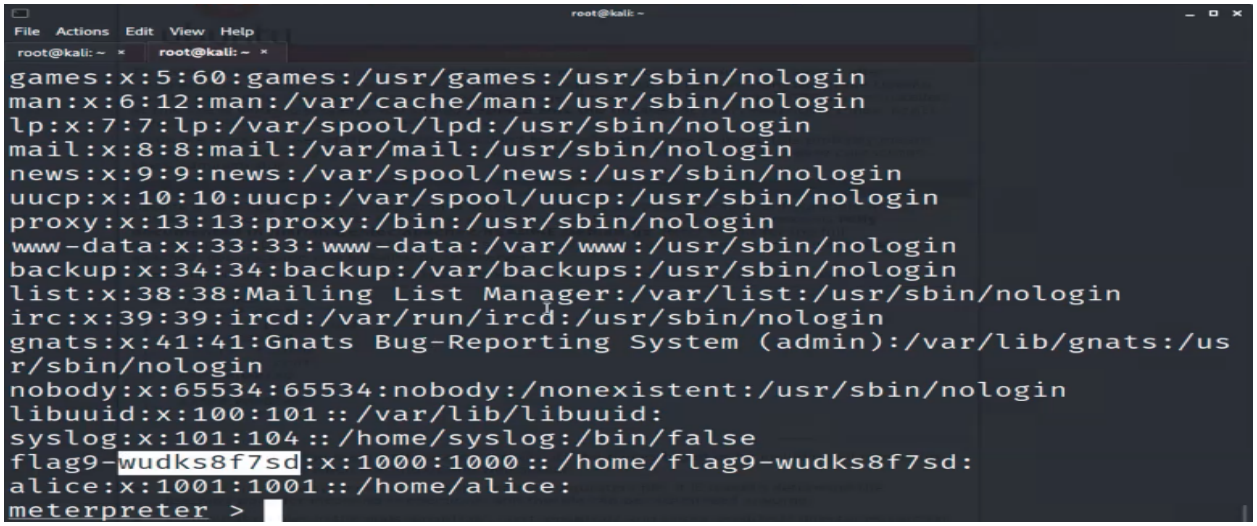
As we moved on to the exploit phase of the pen test, we used information found in our scans to aid us in our attempts. First, using MSFconsole, we exploited the ***Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617).*** This attack gave us access to the root directory of host 192.168.13.10 where we found Flag7.



We then moved on to host 192.168.13.11 which we discovered was vulnerable to ***Shellshock*** exploits. Again, we used MSFconsole to run this exploit against the target. Upon gaining access, we found Flag8 inside of the system's sudoers file.



We also found Flag9 inside the /etc/passwd file.

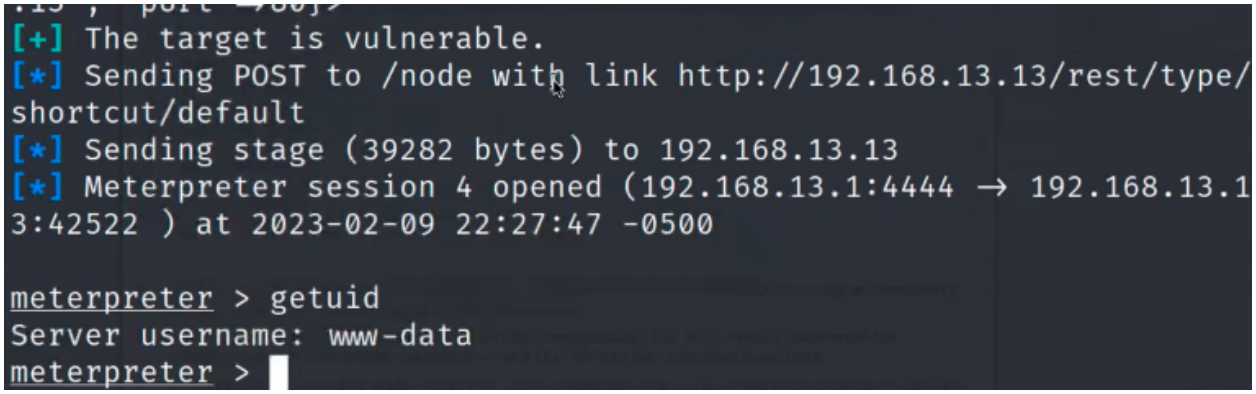


© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

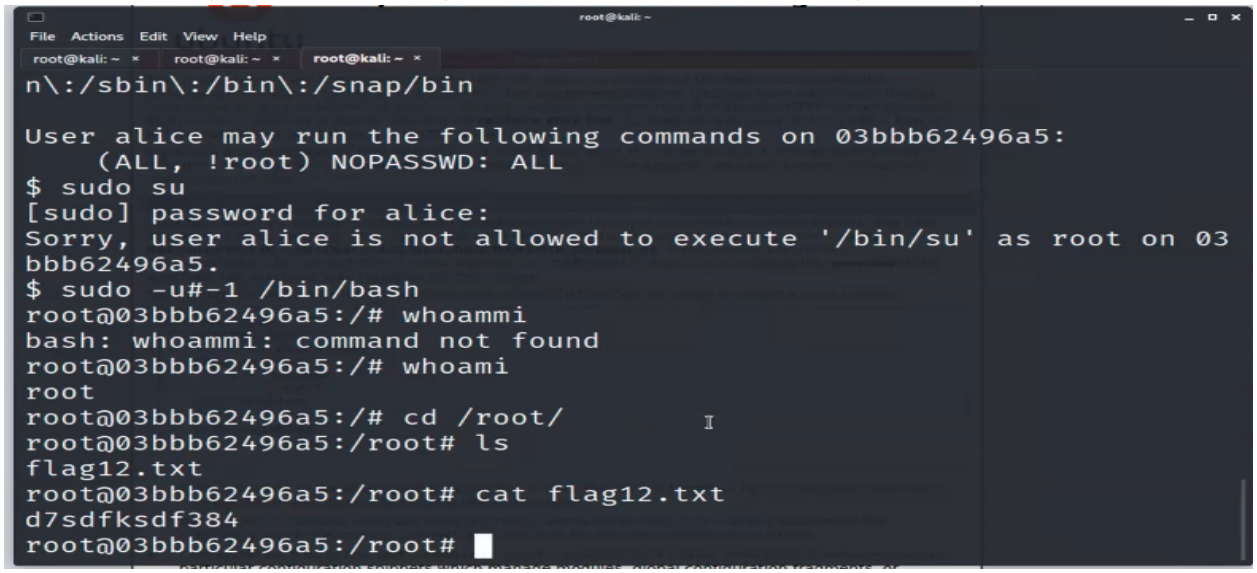
Post Exploitation

Referring back to our Nessus scan we performed, we moved on to host 192.168.13.12 to attack the ***Apache Struts*** vulnerability we discovered in the scan. Using MSFconsole, we performed an exploit to open a shell on the host machine. Then, we downloaded, and unzipped a file we found that contained Flag10.

Referring back to our aggressive Nmap scan we performed, we moved on to host 192.168.13.13 to attack the ***Drupal*** vulnerability we discovered. We were, once again, able to use MSFconsole to gain access to the host. We performed a command to get the user id which was Flag11.



Finally, we used information from our previous exploits to gain access to host 192.168.13.14 under the user: Alice. We then found a way to exploit vulnerability ***CVE-2019-14287***, which gave us root access into the system. After looking around a bit, we discovered Flag 12.

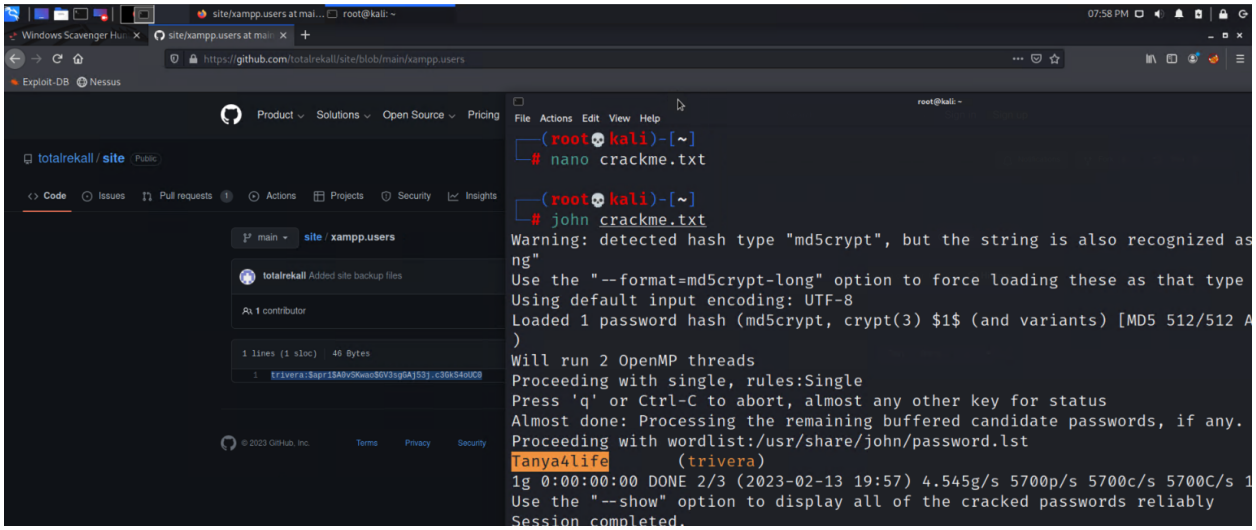


© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

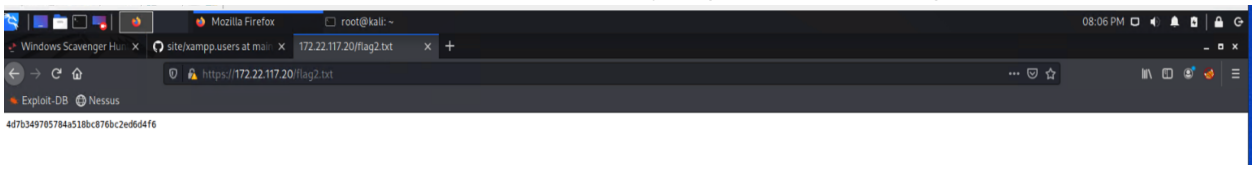
Day 3: Windows Servers

Reconnosaince/Scanning

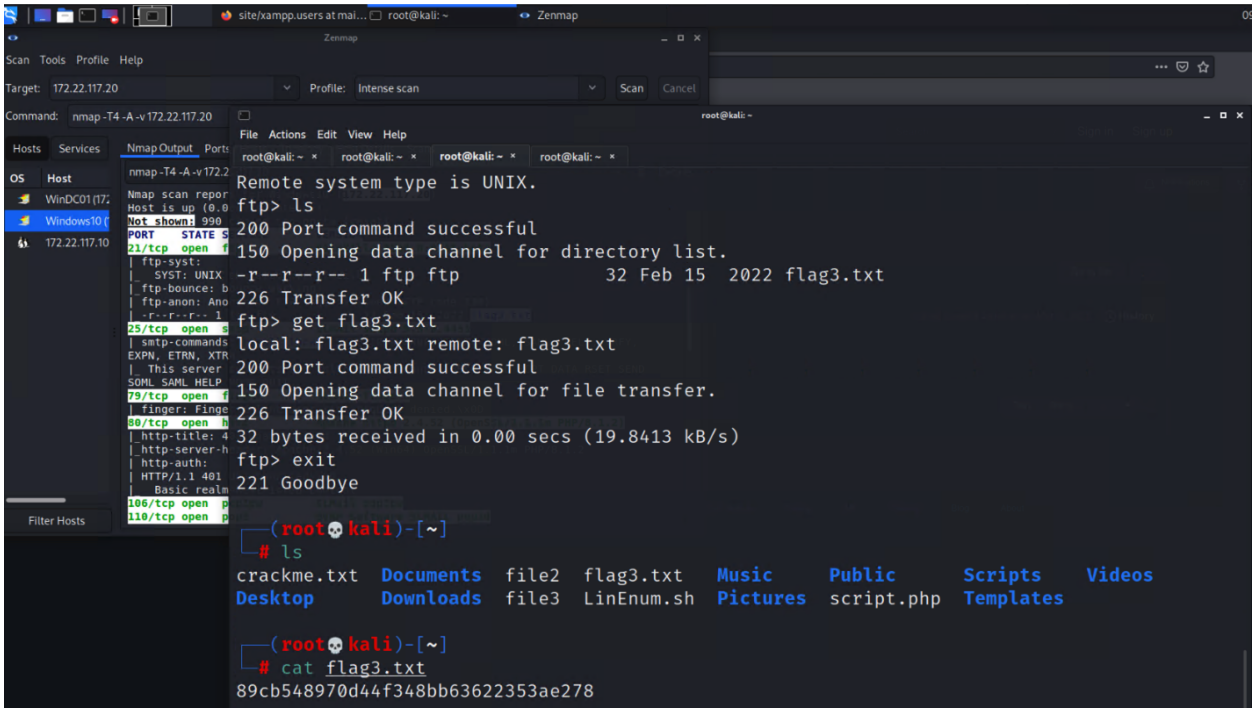
We began day 3 of our pen testing by performing more OSINT. While searching a GitHub repo, we found a username and password hash. With this hash, we cracked the user's password (Flag1).



Next, we performed a Nmap scan on the Window's subnet to check for any ***HTTP enumeration*** vulnerabilities. We discovered that host 172.22.117.20 had port 80 open. After navigating to that ip address, we input the credentials we found previously to gain access to Flag2.



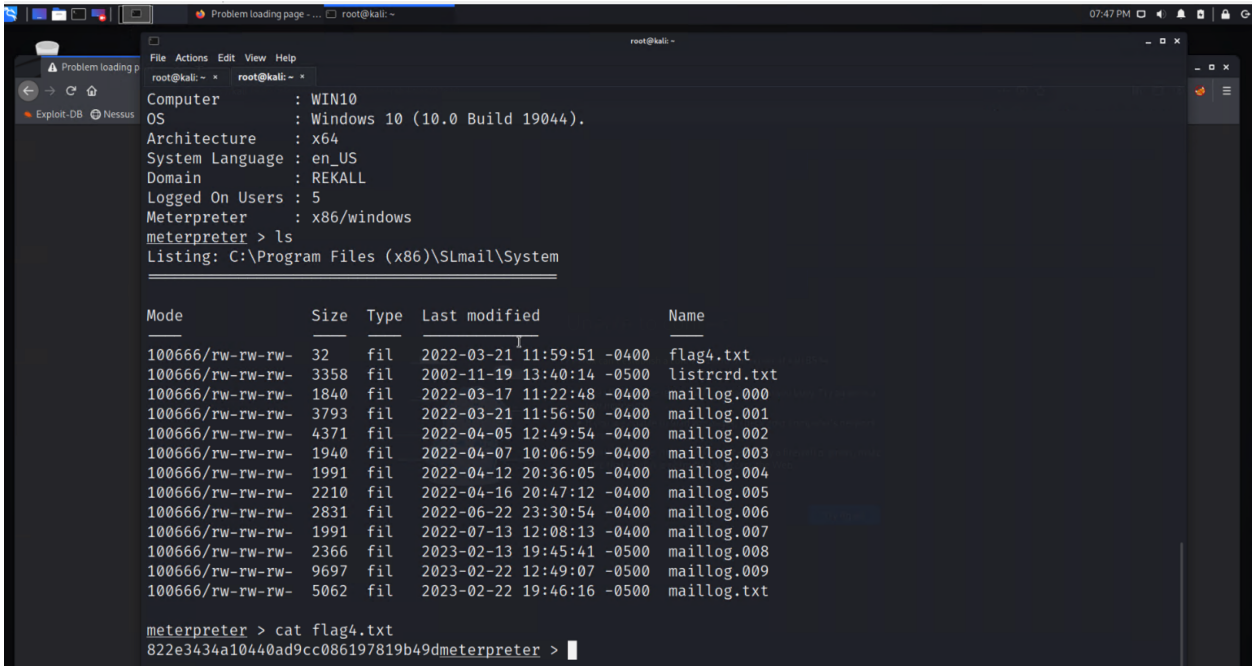
Upon reviewing our scan results , we found that the host was also susceptible to a known FTP vulnerability . We then gained ***FTP anonymous*** access to the host where we did some digging and found Flag3 inside a file.



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

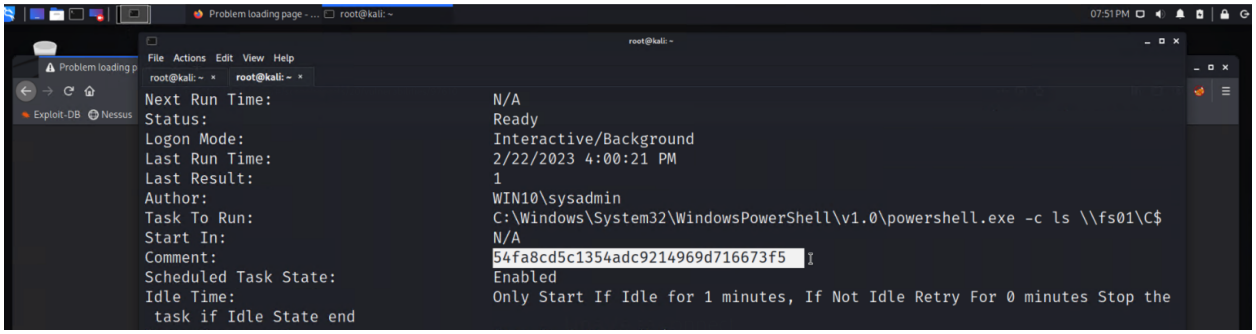
Exploitation

Our next step included us finding ways to exploit more of the open ports or services running on the system. We found that port 110 was running a version of ***SLMail*** with known vulnerabilities. Using MSFconsole, we used an exploit to gain access to the program files on host 172.22.117.20 where we found Flag4.

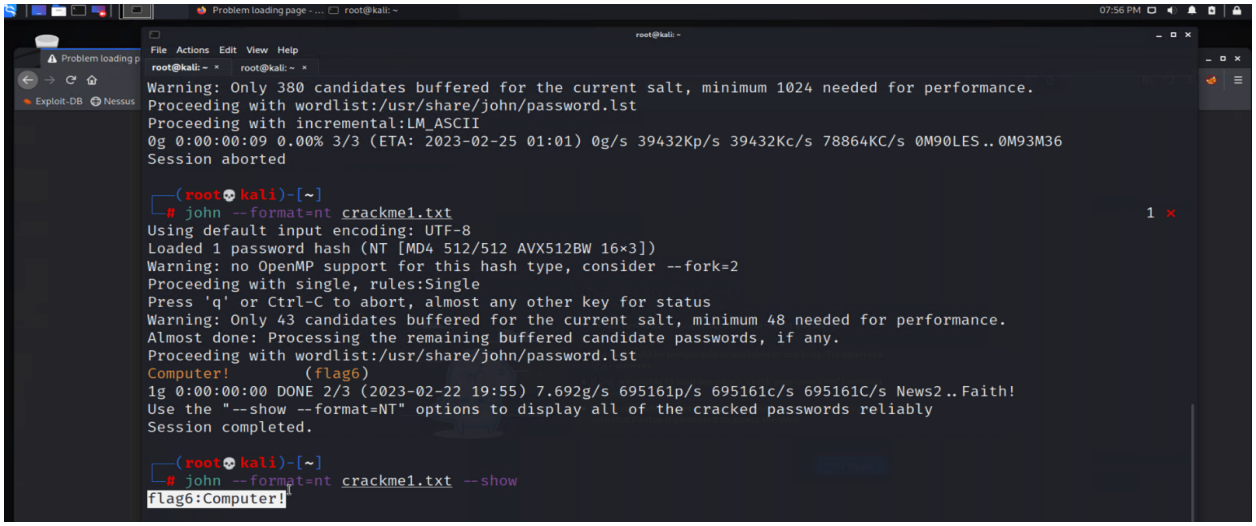


Post Exploitation

After gaining access to the host machine, we then began searching for more Flags. We found Flag5 by taking a look at the scheduled tasks on the system.

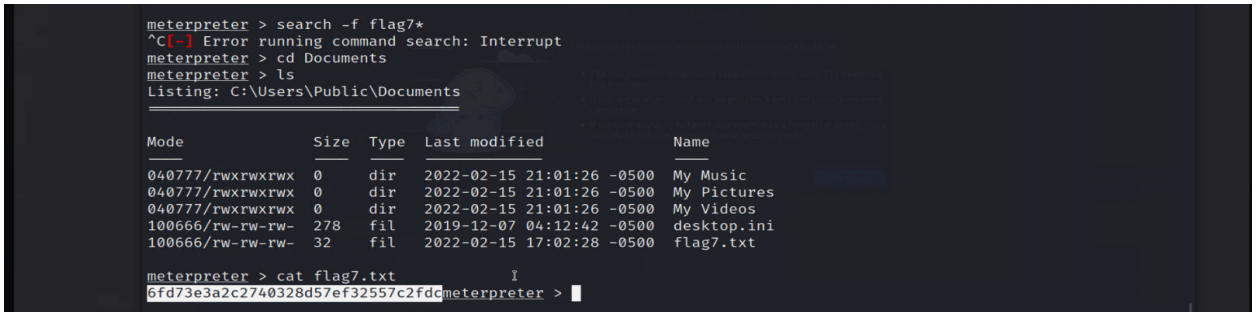


Next, we used the Kiwi extension in MSFconsole to dump user credentials in the system. Once finished, we cracked one of the password hashes to find Flag6.

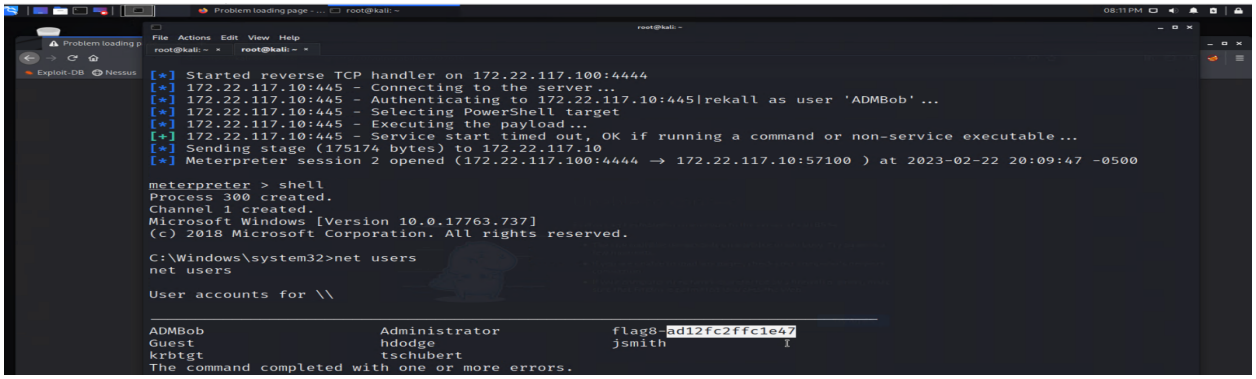


© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

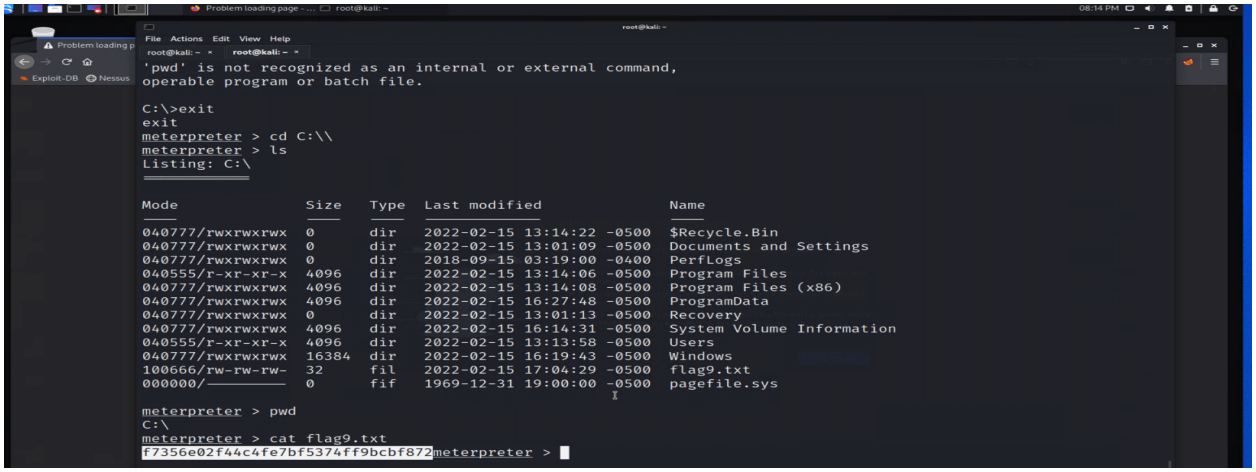
We continued to search the system until we found Flag7 in the /Users/Public/Documents directory.



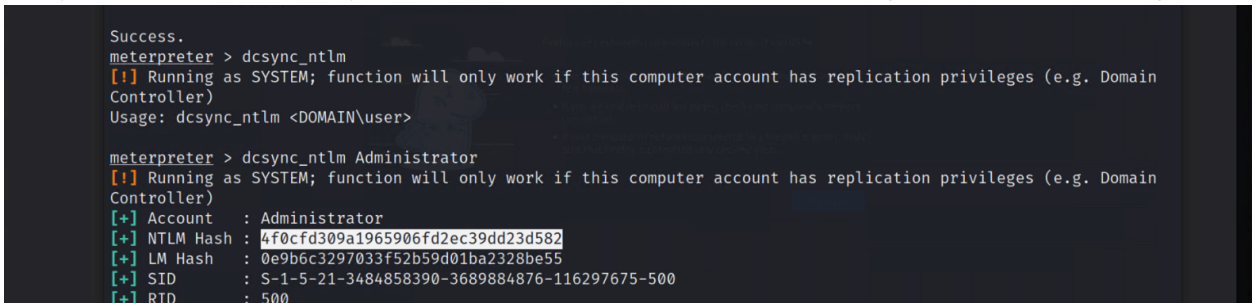
Next, we used the Kiwi extension to dump credentials cached on the Windows10 machine. We found an admin's stored username and password hash in the dump. After cracking that password hash, we used a ***PSExec*** exploit on MSFconsole to gain access to host 172.22.117.10 (Server2019). We then listed the users on that system where we found Flag8



Now that we had access to the Server2019 machine, we searched around until we found Flag9 in the root directory.



Lastly, we used Kiwi to DCSync the Administrator user on the server to get their pw hash (Flag10).



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

Summary Vulnerability Overview

Vulnerability	Severity
Cross site scripting (XSS) (reflected)	Medium
Cross site scripting (stored)	Critical
Sensitive data exposure on About-Rekall.php & robots.txt webpage	Low
Local file inclusion	High
SQL and PHP Injection	Critical
Sensitive data exposure on the Login.php webpage	Critical
Command injection on the networking.php webpage	High
Brute force attack	Critical
Session management	Critical
Directory Traversal	High
Open source exposed data (street address, ip, etc)	Informational
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock	Critical
Struts - CVE-2017-5638	Critical
Drupal - CVE-2019-6340	Critical
sudo CVE-2019-14287	Critical
Open source exposed data (user credentials)	High
port 21 FTP anonymous access	Critical
port 110 pop3 SLMail	Critical
PsExec	Critical
DCSync	Critical

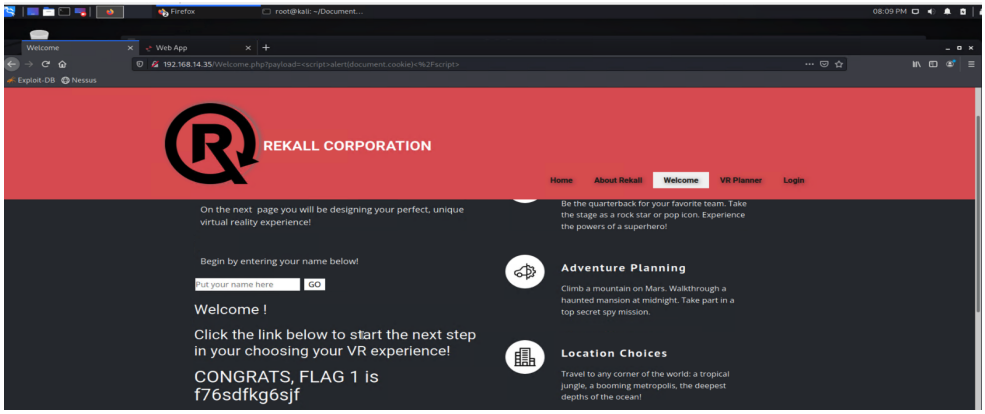
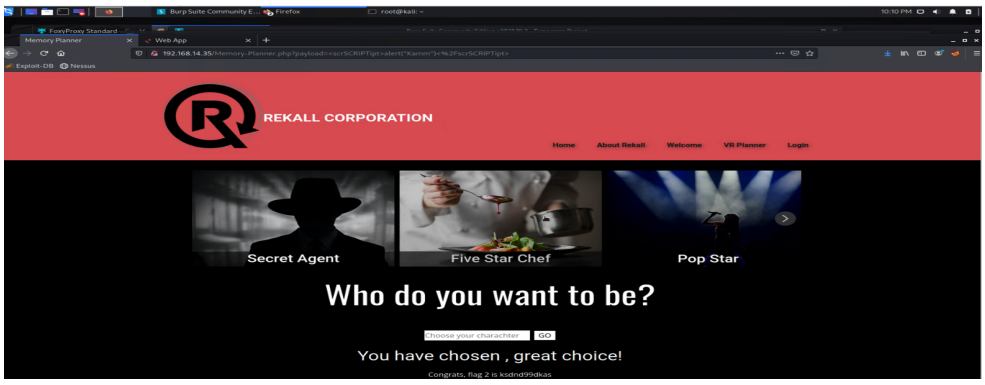
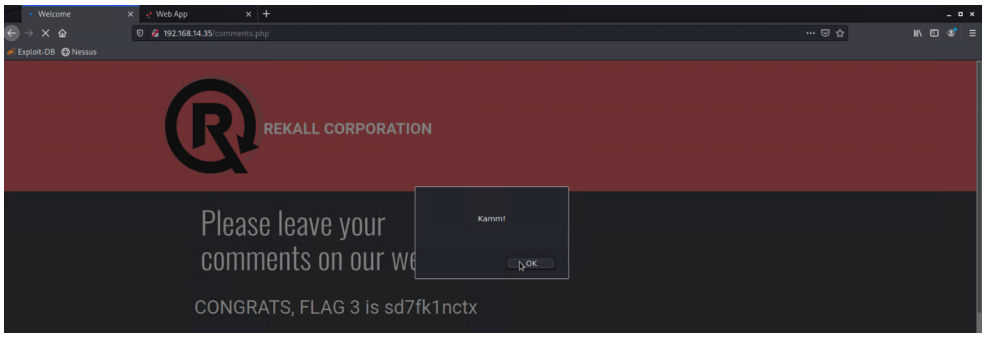
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	5 Linux / 2 Windows
Exploited Ports	1 Linux / 3 Windows

Exploitation Risk	Total
Critical	15
High	3
Medium	1
Low	1

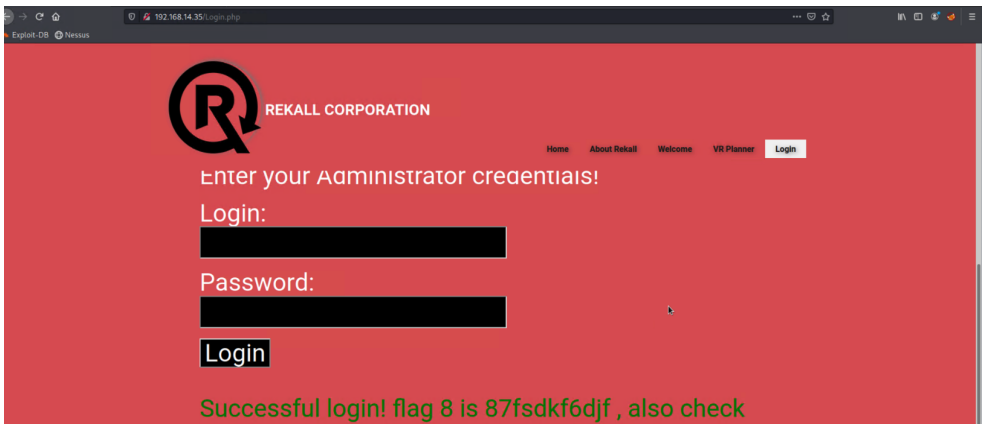
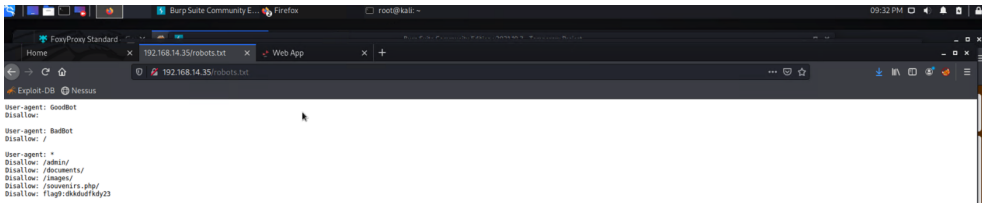
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability Findings

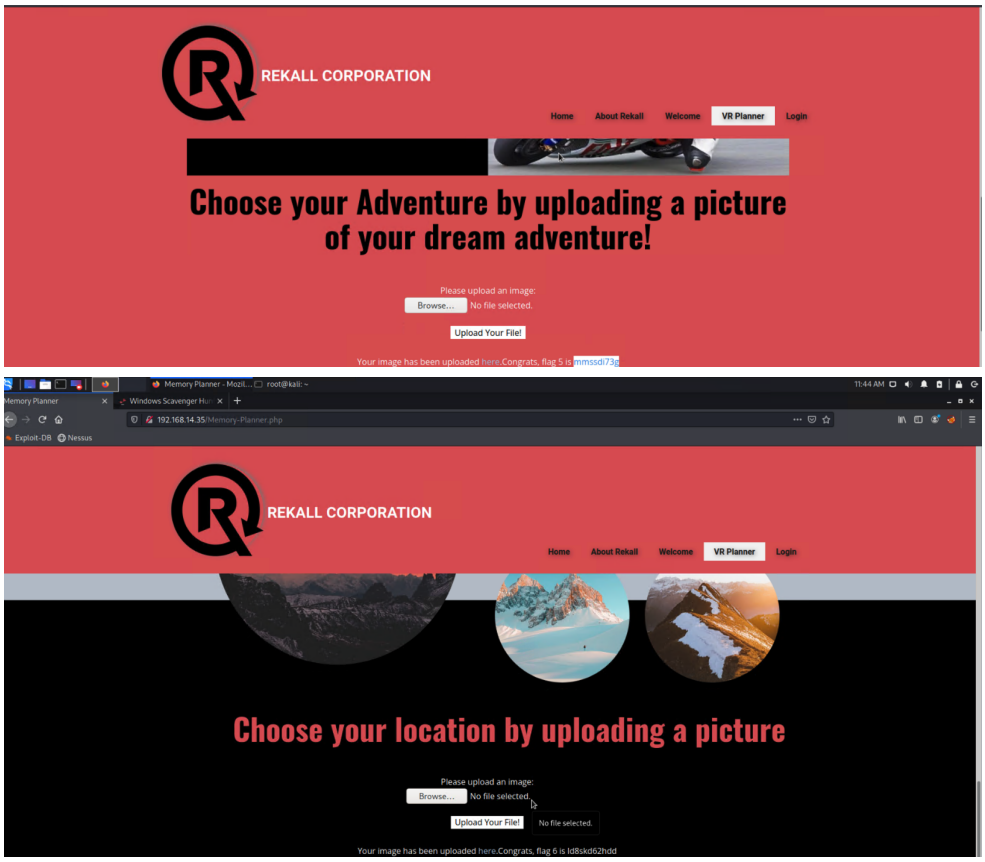
Vulnerability 1	Findings
Title	Cross Site Scripting (XSS) ; reflected and stored(flag3)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium, Critical (stored XSS)
Description	The Rekall web application had multiple web pages vulnerable to this exploit. Fields on the 'Welcome.php', 'Memory-Planner.php', and 'comments.php' pages were all susceptible to some form of XSS. Input validation was required in one field, but it was easily bypassed. Depending on the payload, if clicked, XXS can capture a user's private session cookies as well as load malware into the user's machine. Stored XSS is much more dangerous because it could impact all users who visit the infected page.
Images	  

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

Affected Hosts	192.168.14.35/Welcome.php; 192.168.14.35/Memory-Planner.php; 192.168.14.35/comments.php
Remediation	Use a HTTP response header that can prevent malicious scripts from running Enhance Rekall's server-side input validation (ex. instead of only removing values of <script>, remove different spelling variations of the word such as <Script> and <scRiPt>). OWASP also has information regarding preventing XSS on its website

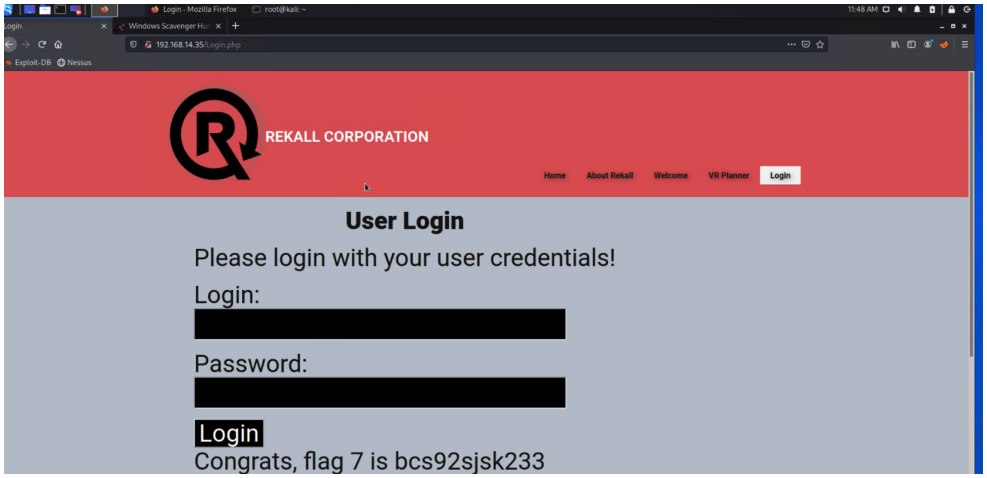
Vulnerability 2	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low, Critical
Description	By viewing the HTML source code, sensitive data such as employee usernames and passwords are encoded inside the webpage. These credentials can then be used to log into Rekall's servers by someone with unauthorized access. The robots.txt file is used by all websites , so may not pose a huge risk if important information is not able to be viewed there.
Images	 
Affected Hosts	192.168.14.35/About-Rekall.php; 192.168.14.35/Login.php; 192.168.14.35/robots.txt
Remediation	One way to mitigate this risk would be to allow logins to be handled by javascript as opposed to HTML. The server would need to create a unique value each time a page is loaded. Also,

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

Vulnerability 3	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	The ‘Memory-Planner.php’ webpage was extremely vulnerable to this attack. Without any server-side input validation, we were able to upload any PHP file in the second field to find Flag5. Furthermore, even with the restriction of .jpg files in field three, we were easily able to bypass this by saving the .jpg file as <file.jpg.php.> This is a serious vulnerability and can easily become a critical concern if the security is not enhanced on this page.
Images	
Affected Hosts	192.168.14.35/Memory-Planner.php
Remediation	It is good that Rekall attempted to mitigate this attack with some form of server-side input validation, but it was not enough. It would be more beneficial to increase the number of variations of file names/types that are not allowed to be uploaded.

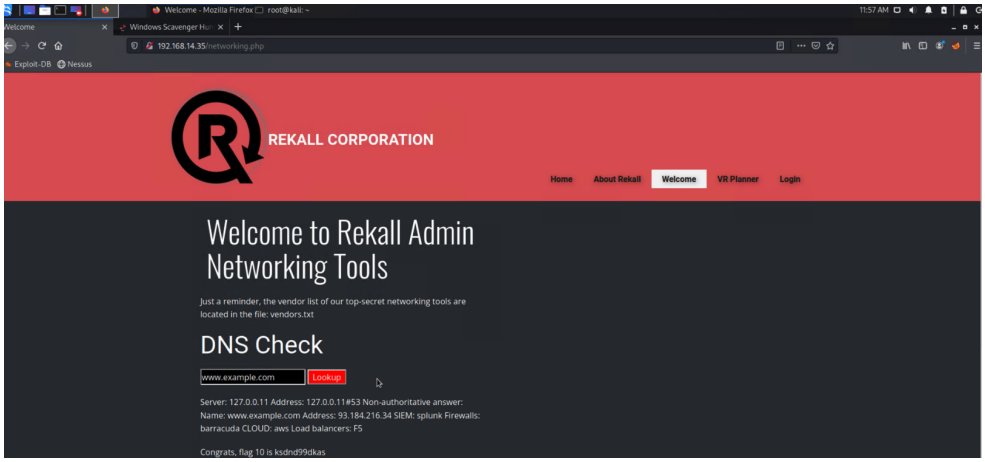
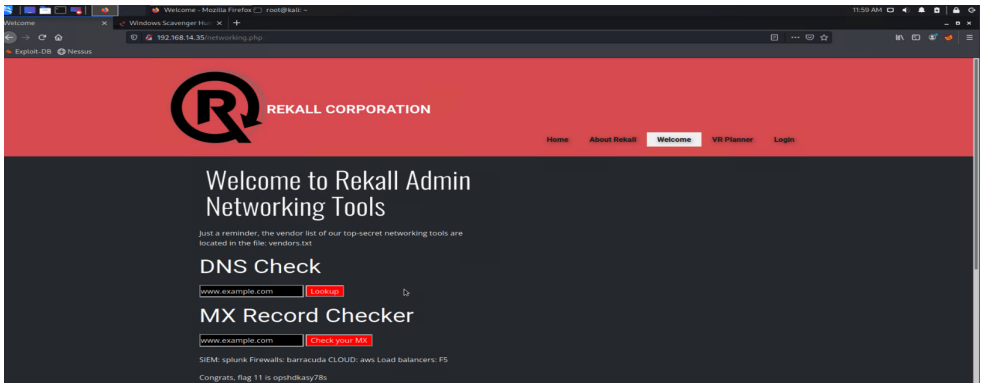
Vulnerability 4	Findings
Title	SQL Injection/PHP Injection

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

Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	We were able to use a simple, known SQL injection payload to exploit the Login.php page. Then, later we altered the URL on the souernirs.php page and imputed another payload. This can pose significant risks to a company depending on the sophistication of the payload. Several different payloads, when successfully injected, can cause private information like passwords to be exposed, or important information to be deleted from Rekall's servers.
Images	
Affected Hosts	192.168.14.35/Login.php; 192.168.14.35/souvenirs.php
Remediation	Once again, input validation has proven to be an effective way to mitigate this exploit. An example would be to only allow numerical single values as inputs from users. Another, even more secure strategy would be to restrict all input from the user, and instead use parameterized database queries.

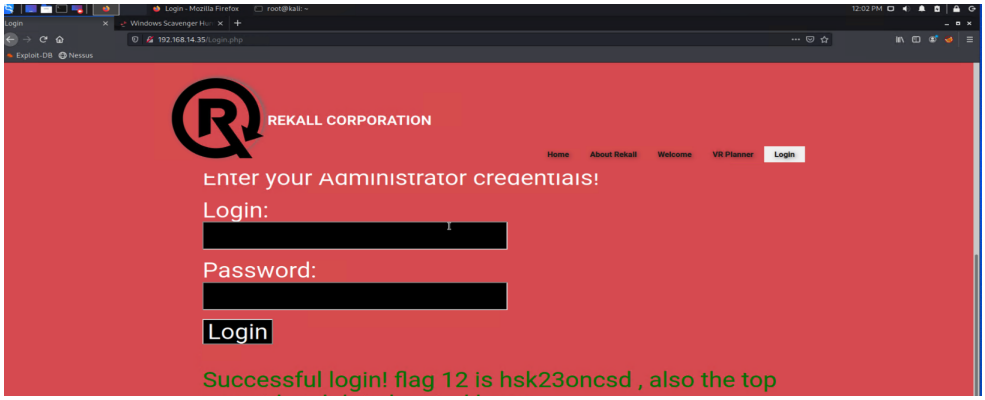
Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Once we found out that the 'networking.php' page was vulnerable to this attack, it was easy to input commands into both fields to access and view confidential files in Rekall's database. Depending on the contents of a file, this could potentially be disastrous for a company.

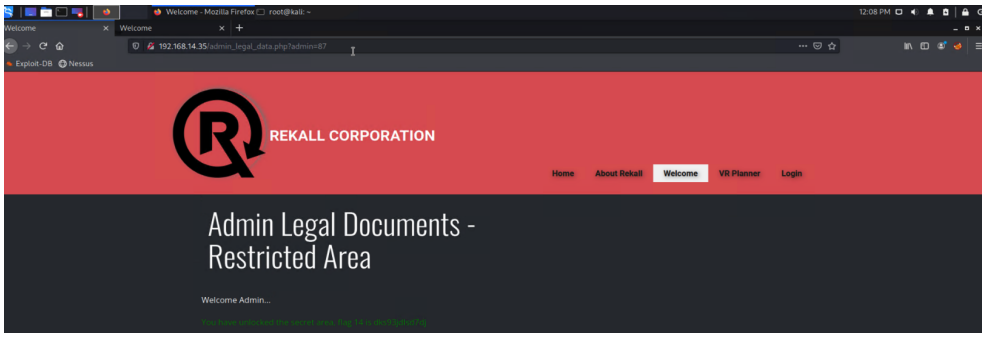
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Images	 
Affected Hosts	192.168.14.35/networking.php
Remediation	A way to completely avoid this risk would be to segregate confidential files from the web server and accessible directories. Another would be to establish permissions to restrict web server account accessibility.

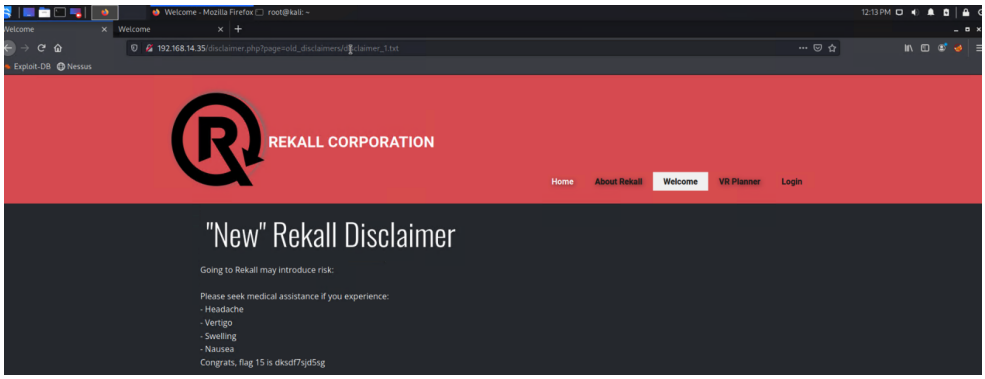
Vulnerability 6	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical

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

Description	By using the command injection vulnerability, we were able to access the /etc/passwd file and acquire a user's credentials. We then were able to use those credentials to access Flag12
Images	
Affected Hosts	192.168.14.35/Login.php
Remediation	This particular scenario could be prevented by remediating the previous vulnerability. However, requiring a complex password from employees could mitigate the effectiveness of a brute force attack. Also, locking an account after a failed number of login attempts is effective.

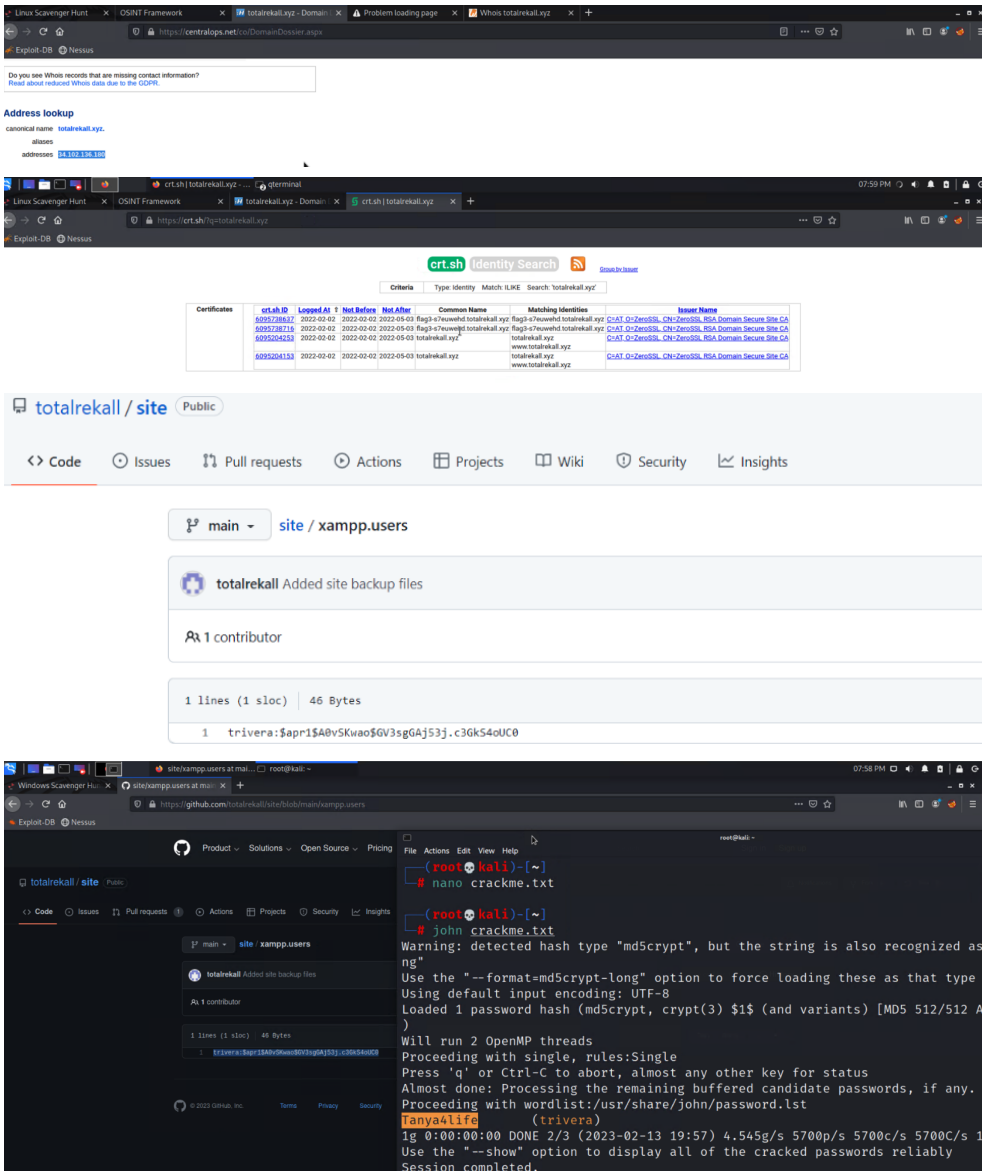
Vulnerability 7	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	As we exploited more and more areas of the website, we found links to other pages on the site that should not have been accessible by the public. One of those links led us to the 'admin_legal_data.php' page. Once on this page, we used the Intruder tool on Burp to find the secret session id (87) that gave us access to Flag14.
Images	
Affected Hosts	192.168.13.35
Remediation	One way to mitigate this vulnerability would be to have your web application generate session cookies that are difficult or complex.

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

Vulnerability 8	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	This vulnerability was made possible due to our previous command injection exploits we performed earlier. With access to Rekall's file system, we were able to easily navigate to any directory we wanted, and search the contents of that directory.
Images	
Affected Hosts	192.168.14.35/Disclaimer.php
Remediation	A way to completely avoid this risk would be to segregate confidential files from the web server and accessible directories. Another would be to establish permissions to restrict web server account accessibility.

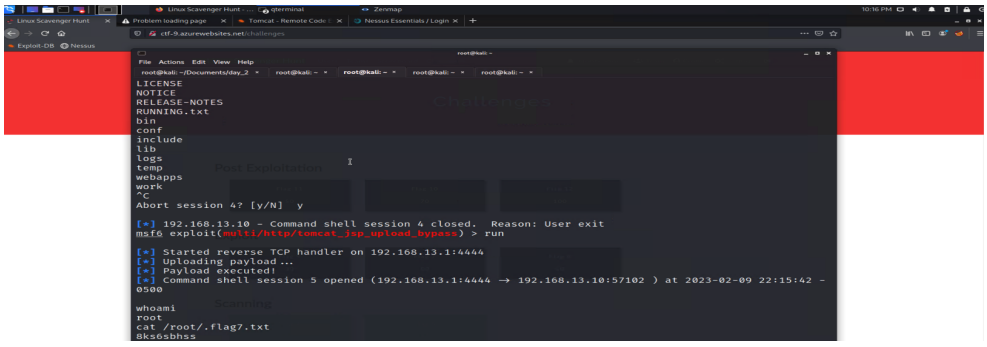
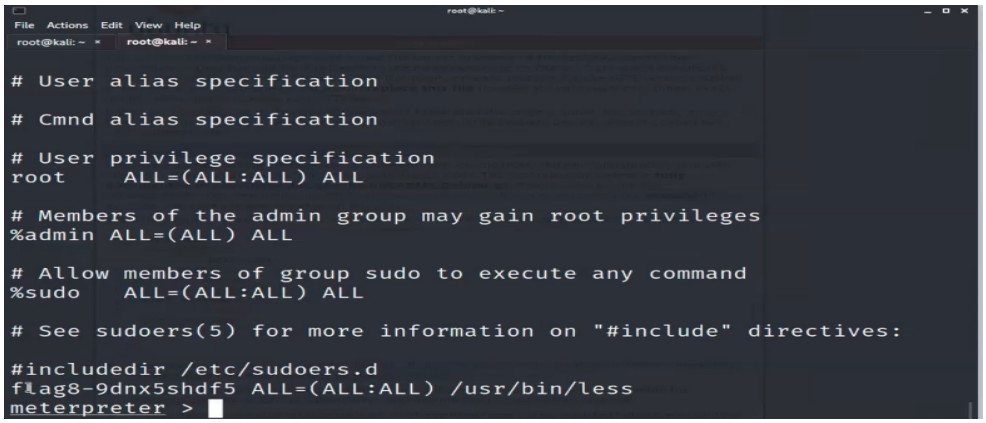
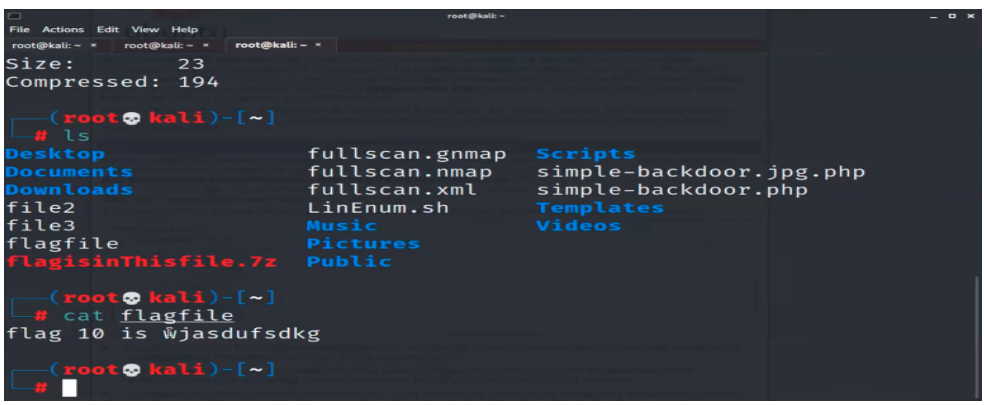
Vulnerability 9	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux & Windows
Risk Rating	Informational, High
Description	We used different parts of the OSINT framework to find out publicly available information about Rekall. Most of the information found does not pose an immediate threat to the company, but could potentially be used for one in the future. However, credentials for a user on the Windows10 machine was found online in a GitHub repo. The chances of finding these credentials without help may be low, but if they are found, they could pose a threat to Rekall's servers.

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

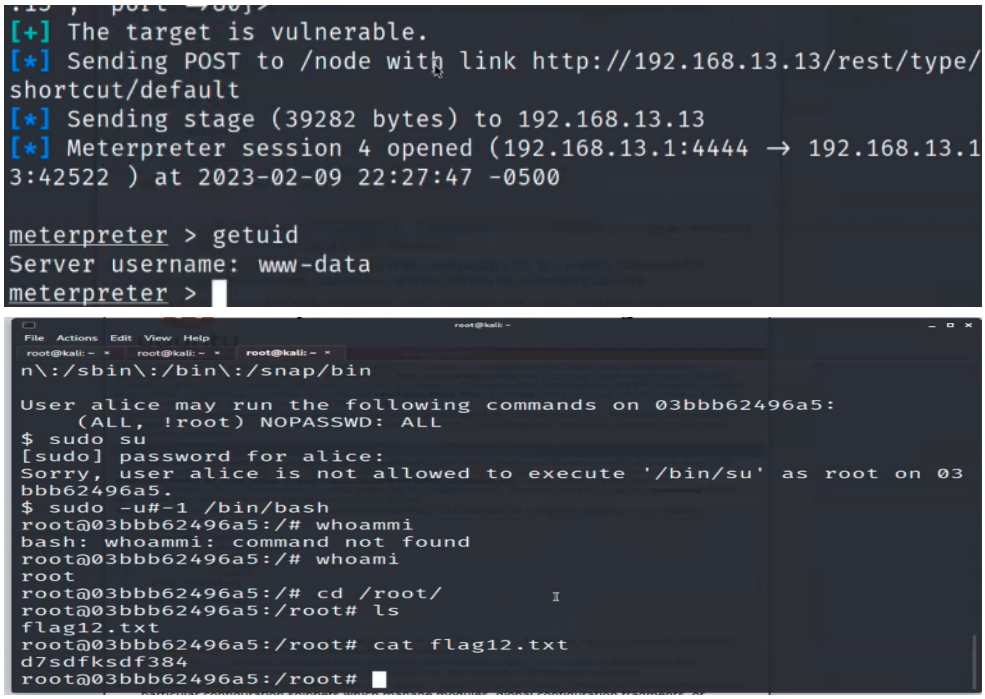
Images	
Affected Hosts	credentials were used to gain access to 172.22.117.20 (Windows)
Remediation	Since most of this information is required to be made available to the public, the only mitigation strategy

Vulnerability 10	Findings
Title	Metasploit Exploits: Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) ; Shellshock ; Struts - CVE-2017-5638 ; Drupal - CVE-2019-6340 ; sudo CVE-2019-14287

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

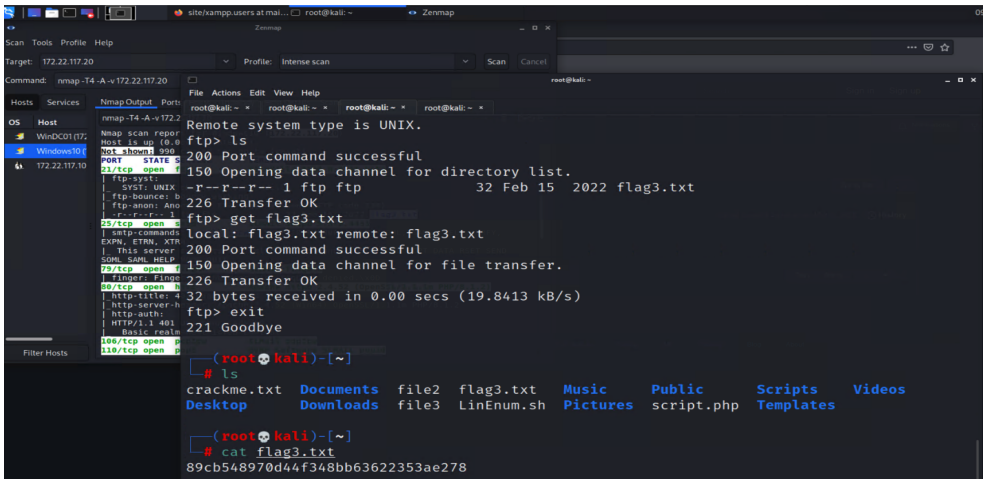
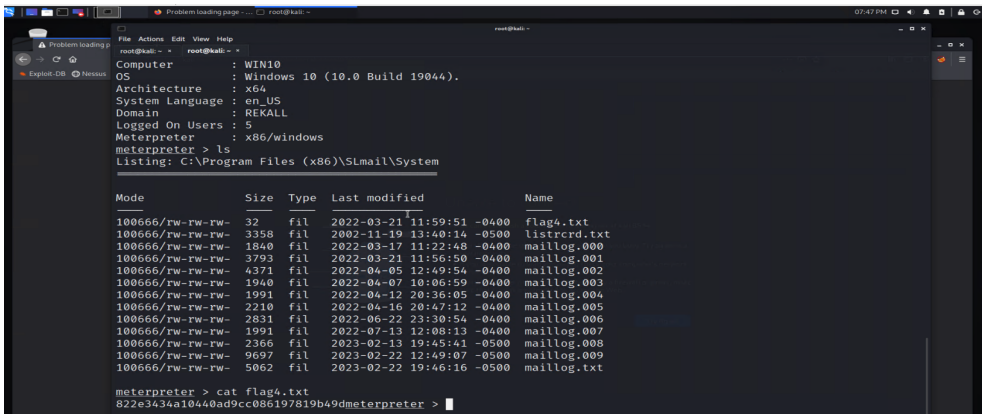
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	The CVE-2017-12617 vulnerability allowed us to use a shell to access the command line of host 192.168.13.10 where we then found Flag7. Next, we used the Shellshock exploit to open another shell on host 192.168.13.11. Here, we looked around until we found Flag8 in the sudoers file, and Flag9 in the /etc/passwd file. Then, we exploited the vulnerability CVE-2017-5638 by opening another shell on host 192.168.13.12. Once we gained access to the command line, we found a zipped file containing Flag10, which we then downloaded and unzipped to reveal the flag. Next, we opened a shell on host 192.168.13.13 by exploiting the CVE-2019-6340 vulnerability and obtaining the username. Lastly, we exploited vulnerability CVE-2019-14287 which allowed us to ssh into host 192.168.13.14 where we were then able to escalate our privileges to the root user. Once completed, we were able to view Flag12.
Images	  

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

	
Affected Hosts	192.168.13.10; 192.168.13.11; 192.168.13.12; 192.168.13.13; 192.168.13.14
Remediation	The good news is that each of these vulnerabilities and exploits are known, which therefore means there are strategies to mitigate and prevent these attacks. The first step would be to get a good understanding of why your system is vulnerable to these attacks; it could be open ports, or no security controls implemented. Depending on Rekall's budget, a SIEM could be put in place to help manage intrusions and potential security risks.

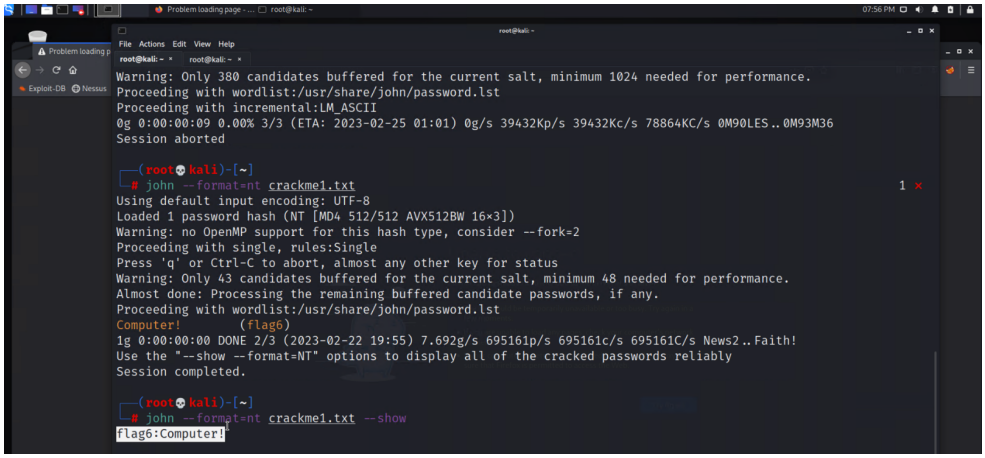
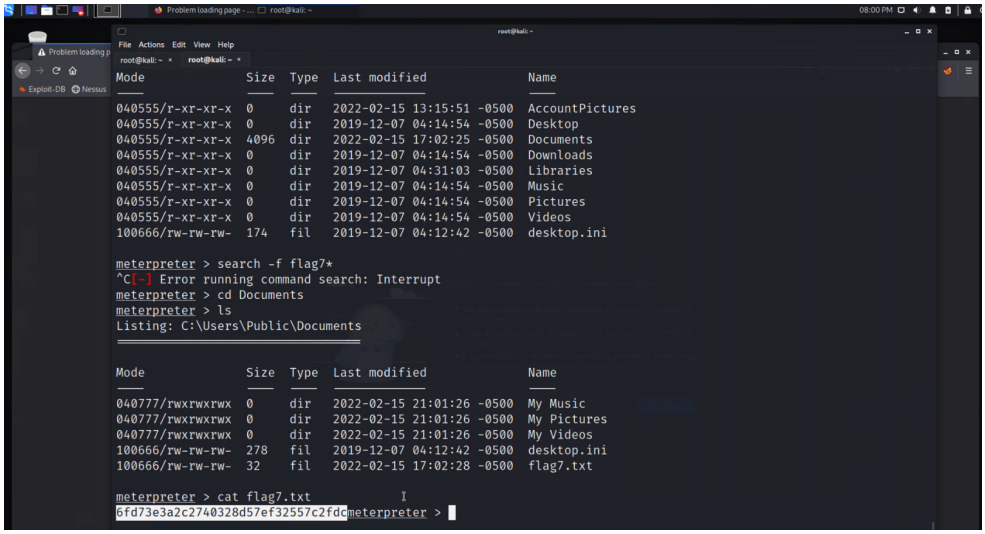
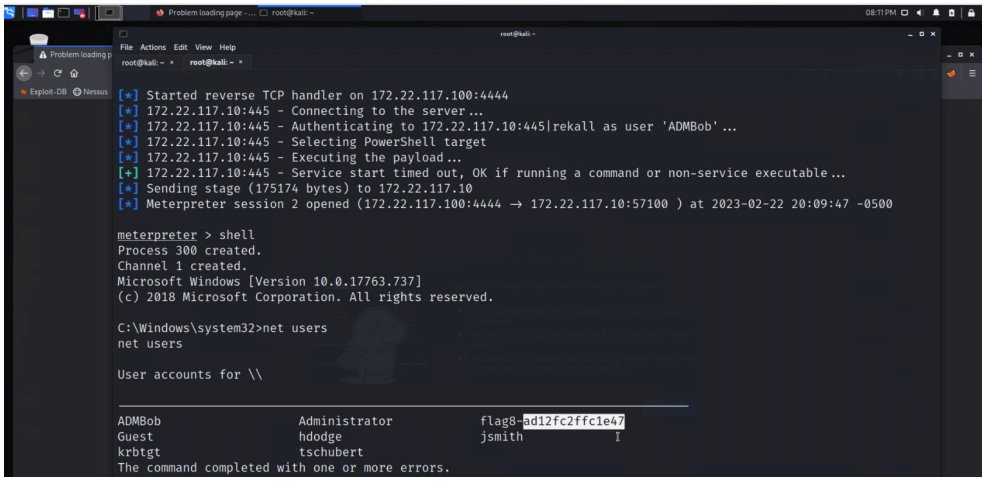
Vulnerability 11	Findings
Title	port 21 FTP anonymous access ; port 110 pop3 SLMail
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Upon reviewing the results of our Nmap scans, we discovered that port 21 was open and that FTP anonymous access was possible. We then immediately exploited this vulnerability to gain access to the server where we found Flag3. Next, we noticed that the SLMail service was running on SMTP port 25 and POP3 port 110. We then used MSFconsole to perform an exploit that gave us access to a Meterpreter shell on the system. Once inside, we were able to locate Flag4 inside the \SLmail\System directory

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

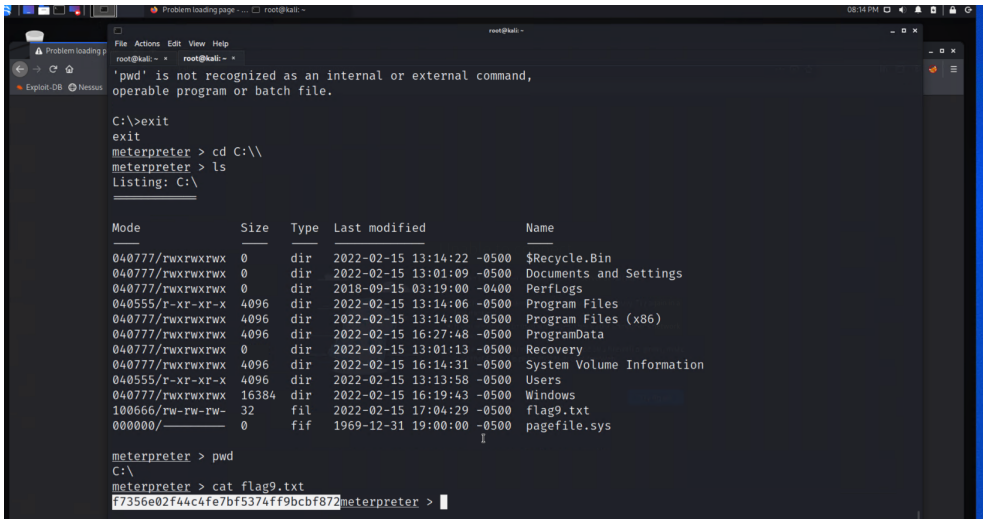
Images	 
Affected Hosts	172.22.117.20
Remediation	Close ports 21, 25, 110, and any other unnecessary ports. If any vulnerable ports are necessary, configure security controls that could detect and/or alert the IT team whenever a possible threat is imminent.

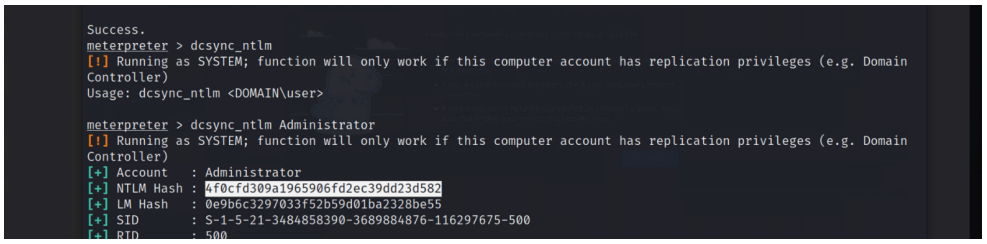
Vulnerability 12	Findings
Title	PsExec ; DCSync
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Once the SLMail vulnerability was exploited, we used the Metasploit extension kiwi to further infiltrate the system and move laterally throughout. We performed a credential dump which gave us the password hash for a user named Flag6. We then used a password cracker to find Flag6. Now that we had this user's credentials, we used them to search through the \Users\Public\Documents directory to find Flag7. Then, we continued to use kiwi to dump the cached credentials on the server. Once complete, we found an administrator's username and password hash. Once again, we cracked this password and discovered that these credentials gave us access to the

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

	Server2019 (172.22.117.10) machine. Next, we executed the PsExec exploit to obtain a shell on this server. Using the shell, we listed the users to find Flag8, and found Flag9 in the root directory. Lastly, we used kiwi to DCSync the Administrator user on the server to reveal their password hash (Flag10).
Images	  

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





Affected Hosts	172.22.117.20 ; 172.22.117.10
Remediation	A simple way to prevent a number of these exploits would be to require users, and especially administrators to have more complex passwords. Also, just as some of the Linux exploits are known, both of these Windows exploits are also known. This can be a good thing if the security team at Rekall takes the time to explore the exploits themselves on the open web. There are a number of different sites and repos that detail the exploits as well as ways to combat against them. Lastly, as mentioned previously, a proper SIEM could greatly assist with addressing a number of the security concerns facing Rekall.

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