

Raven Security

Vulnerability Assessment And Penetration Testing Report

Business Confidential

Date: June 7th, 2021

Project: Raven Security

# Table of Contents

[Table of Contents 2](#_Toc9866461)

[Confidentiality Statement 3](#_Toc9866462)

[Disclaimer 3](#_Toc9866463)

[Contact Information 3](#_Toc9866464)

[Assessment Overview 4](#_Toc9866465)

[Assessment Components 4](#_Toc9866466)

[External Penetration Test 4](#_Toc9866467)

[Finding Severity Ratings 5](#_Toc9866468)

[Scope 6](#_Toc9866469)

[Scope Exclusions 6](#_Toc9866470)

[Client Allowances 6](#_Toc9866471)

[Executive Summary 7](#_Toc9866472)

[Attack Summary 7](#_Toc9866473)

[Security Strengths 8](#_Toc9866474)

[SIEM alerts of vulnerability scans 8](#_Toc9866475)

[Security Weaknesses 8](#_Toc9866476)

[Missing Multi-Factor Authentication 8](#_Toc9866477)

[Weak Password Policy 8](#_Toc9866478)

[Unrestricted Logon Attempts 8](#_Toc9866479)

[Vulnerabilities by Impact 9](#_Toc9866480)

[External Penetration Test Findings 10](#_Toc9866481)

[Insufficient Lockout Policy – Outlook Web App (Critical) 10](#_Toc9866482)

[Additional Reports and Scans (Informational) 13](#_Toc9866483)

# Confidentiality Statement

This document is the exclusive property of Raven Security and Cyber Walkers Security . This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Raven Security and Cyber Walkers Security.

Cyber Walkers Security may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Cyber Walkers Security prioritized the assessment to identify the weakest security controls an attacker would exploit. Cyber Walkers Security recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

|  |  |
| --- | --- |
|  |  |

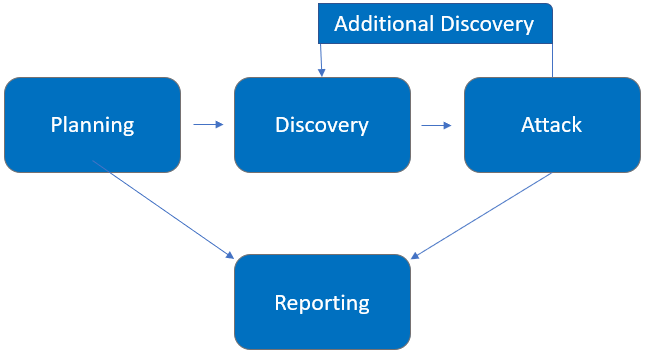
|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| **Raven Security** | | |
| Steven | User | Email: [steven@raven.com](mailto:john.smith@demo.com) |
| Michael | User | Email: [michael@raven.com](mailto:jim.smith@demo.com) |
| Raven | User | N/A |
| **Cyber Walkers Security Security** | | |
| Abhishek Joshi | Penetration Tester | Office:+918788295760  Email: [cyberwalker123@gmail.com](mailto:hadams@tcm-sec.com) |

# Assessment Overview

From June 7th, 2021 to June 7th, 2019, Raven Security engaged Cyber Walkers Security to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

## External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Cyber Walkers Security engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| External Penetration Test | 192.168.0.0/24,  192.168.1.0/24 |

* Full scope information provided in “**Raven Security Full Findings.xslx”**

## Scope Exclusions

Per client request, Cyber Walkers Security did not perform any Denial of Service attacks during testing.Raven Security is a vulnerable machine i have to gather all the flags

## Client Allowances

Raven Security did not provide any allowances to assist the testing.

## Target:

Raven Security is a vulnerable machine i have to gather all the flags and find the Weakness and Security Loopholes. Raven Security is a target we are performing a vulnerability assessment and penetration testing on their machine.

# Executive Summary

Cyber Walkers Security evaluated Raven Security’s external security posture through an external network penetration test from June 7th, 2021 to June 7th, 2019. By leveraging a series of attacks, Cyber Walkers Security found critical level vulnerabilities that allowed full internal network access to the Raven Security headquarter office. It is highly recommended that Raven Security address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Vulnerabilities Found:

|  |  |
| --- | --- |
| Step | Vulnerabilities |
| 1 | Open Port Vulnerability |
| 2 | User Credential Disclosure |
| 3 | Source Code Disclosure |
| 4 | MYSQL Database Access Credential Leaks |
| 5 | Privilege escalation |

# Security Strengths

## SIEM alerts of vulnerability scans

During the assessment, the Raven Security security team alerted Cyber Walkers Security engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the Cyber Walkers Security engineer’s attacker IP address within minutes of scanning and was capable of blacklisting Cyber Walkers Security from further scanning actions.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

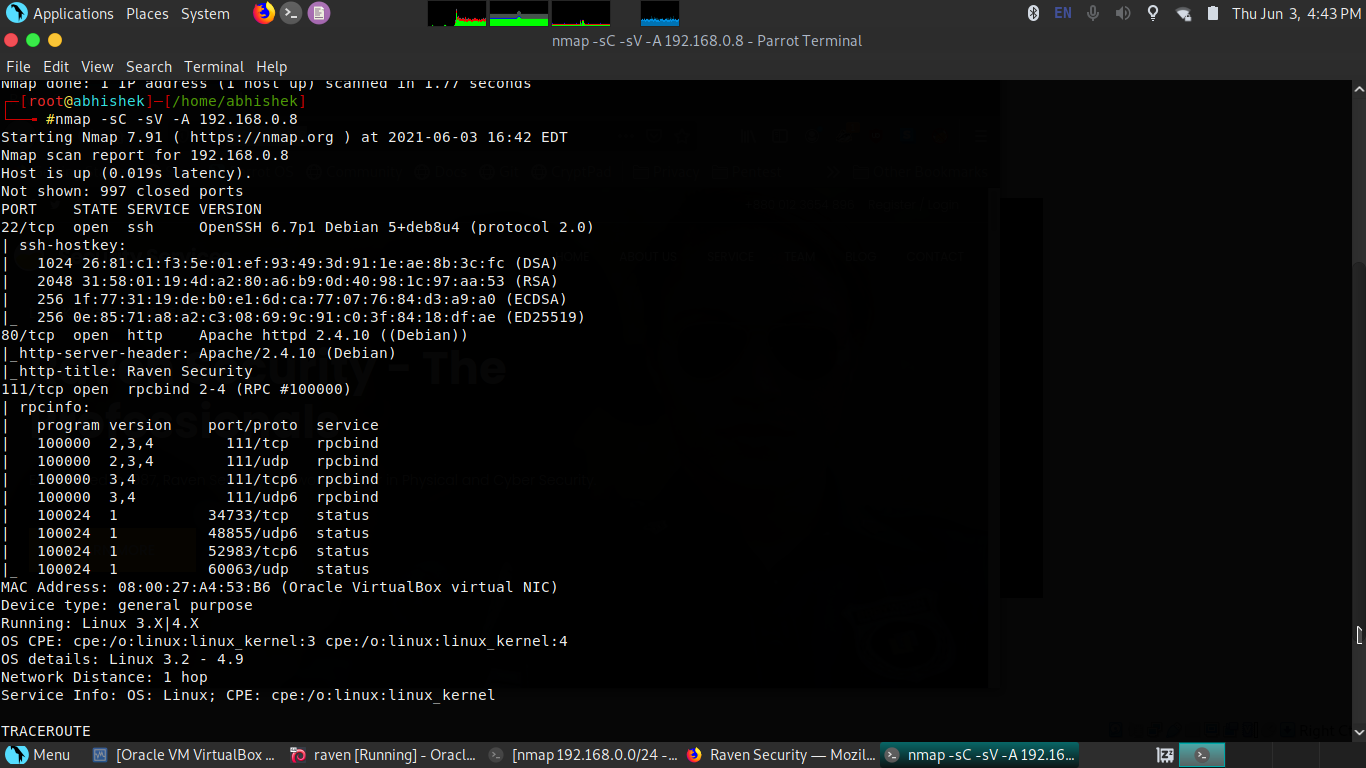
## Penetration Test Findings

Open Port Vulnerability (Critical)

|  |  |
| --- | --- |
| Description: | Commonly Hacked Ports  Common ports, such as SSH port 21 FTP port 22 be vulnerable to hackers. In your security tests, be sure to check these commonly hacked TCP and UDP ports:  TCP port 21 — FTP (File Transfer Protocol)  TCP port 22 — SSH (Secure Shell)  TCP port 23 — Telnet  TCP port 25 — SMTP (Simple Mail Transfer Protocol)  CP and UDP port 53 — DNS (Domain Name System)  TCP port 110 — POP3 (Post Office Protocol version 3)  TCP and UDP port 135 — Windows RPC  TCP and UDP ports 137–139 — Windows NetBIOS over TCP/IP  TCP port 1433 and UDP port 1434 — Microsoft SQL Server  hacker can take a advantages and exploit to gain a access on your system and servers  Raven Security allow SSH port for communicate with weak user and password implementation attacker can gain access using password cracking algorithm. |
| Impact: | Critical |
| System: | 192.168.0.10 |
| References: | <https://lifars.com/2020/10/are-open-ports-a-security-risk/>  <https://www.acunetix.com/blog/articles/danger-open-ports-trojan-trojan/#:~:text=Open%20ports%20are%20used%20by,vulnerability%20that%20can%20be%20exploited.> |

**Exploitation Proof of Concept**

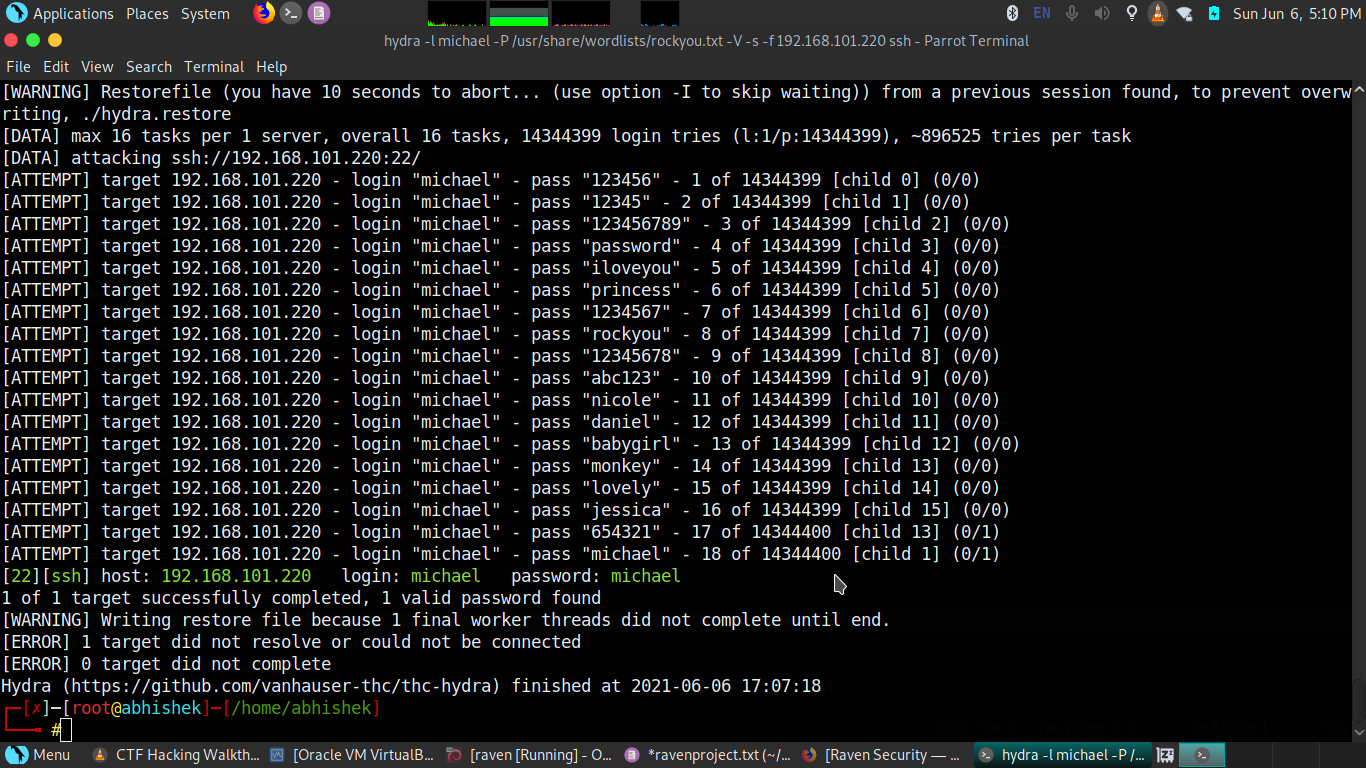
Cyber Walkers Security gather sensitive open ports which is open port vulnerability attacker can use the sensitive port for exploitation and gain a access in this scenario “Raven Security” allow to communicate SSH port and there is no strong Password Protection (**Note:** A full list of compromised accounts can be found in “**Raven Security Full Findings.xslx”**.).



on this figure i scan the sensitive ports on “Raven Security” there are SSH,HTTP, And RPCBIND Ports was open

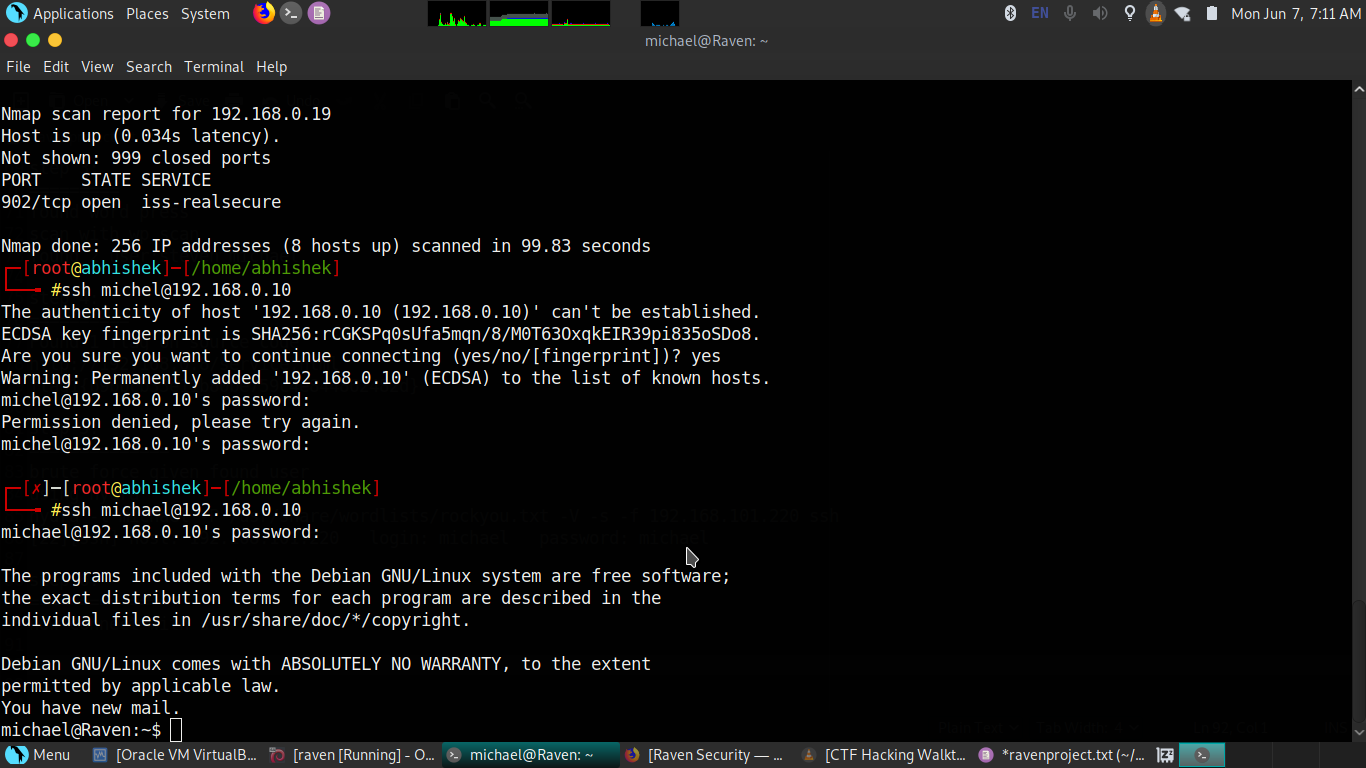
Using SSH port attacker gain the access with the help of password cracking algorithm FTP port also responsible for the gaining access on a system there are total “65535 PORTS” in a Network

Password Cracking Attack On SSH:



I got the “user” and “password” which is very weak i got the username because there is user credential leaks vulnerability attacker can also gain username and pass using information gathering and create a dictionary for password cracking attack

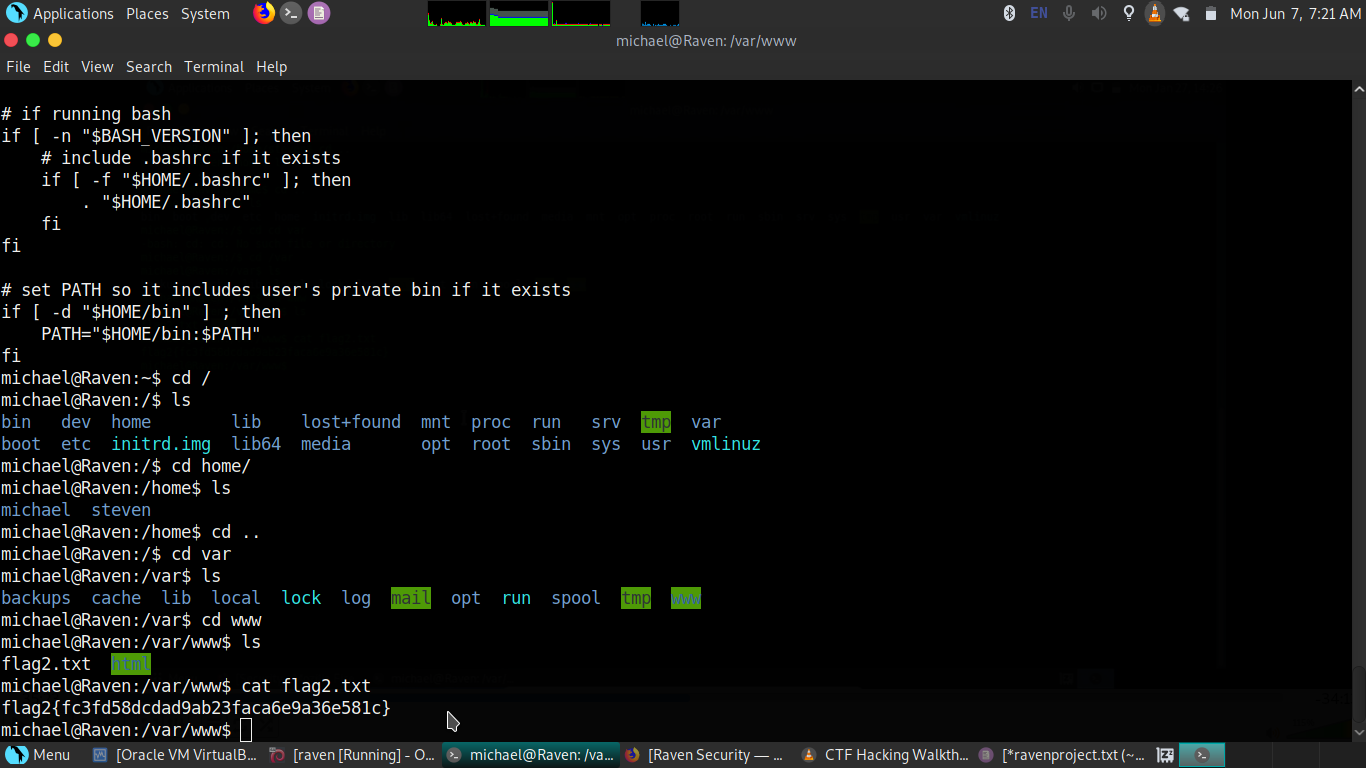
Gain The Access:

****

Found the flag “FLAG2.txt”

Path:michael@Raven:/var/www$

Flag 2: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}



**Remediation**

|  |  |
| --- | --- |
| Who: | Raven Security |
| Vector: | Remote |
| Action: | Cyber Walkers Security recommends that Raven Security:  Sensitive Port Should be closed if you want to use that port for your services and availability you have to make a firewall filter on these port and if any SSH,FTP,MYSQL port was open put a strong user and password implementation username will be unique and password should be more than 14 characters . |

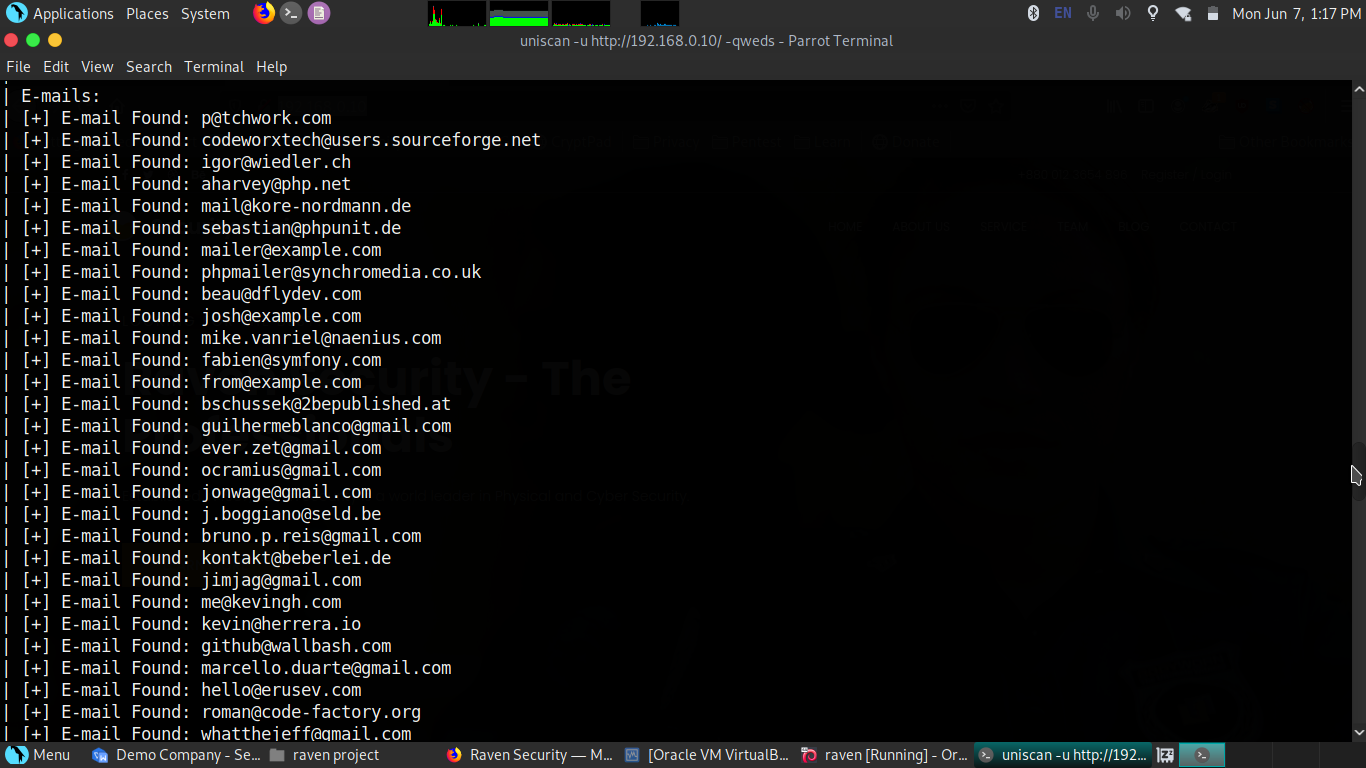
User Credential Disclose (Medium)

|  |  |
| --- | --- |
| Description: | Hacker can find user credentials for personal use or exploitation user they can use for brute forcing,selling on dark web,sending phishing mails and malwares ..etc. User personal credentials is very important to hide from an attackers |
| Impact: | Medium |
| System: | 192.168.0.10 |
| References: | <https://www.acunetix.com/vulnerabilities/web/possible-username-or-password-disclosure/> |

**Exploitation Proof of Concept**

Cyber Walkers Security gather sensitive user information using automation scan. Attacker can gaining the access of system using SSH port with the help of password cracking algorithm using the credentials (**Note:** A full list of compromised accounts can be found in “**Raven Security Full Findings.xslx”**.).

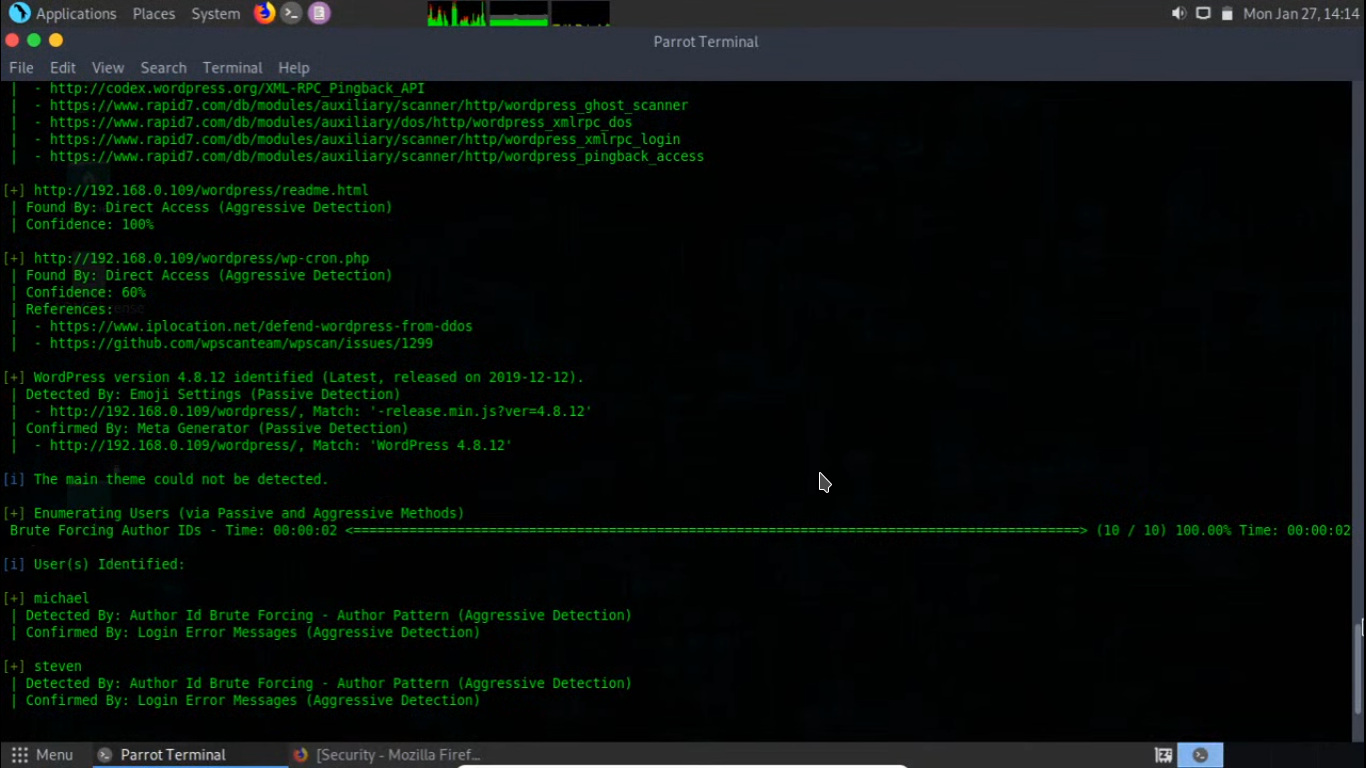
Uniscan Report:



“Raven Security” also have wordpress

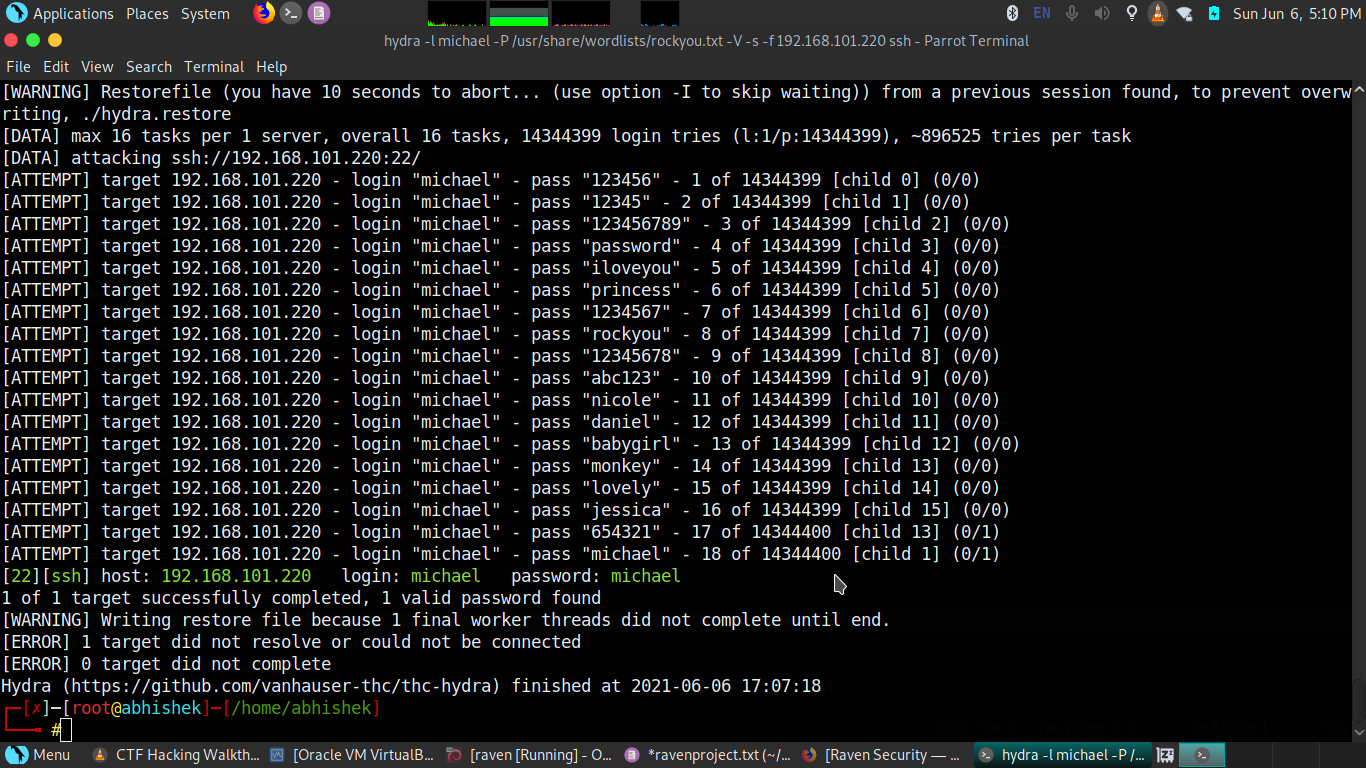
path:http://192.168.0.10/wordpress/

Wp-Scan Report:



you can see two user i found “Steven” and “Michael” using this two user i gain the access of the system using SSH port

Hydra Report:



**Remediation**

|  |  |
| --- | --- |
| Who: | Raven Security |
| Vector: | Local |
| Action: | Cyber Walkers Security recommends that Raven Security:  secure wordpress hide user credentials and dont disclose in source code and publicly on website or dont provide any pdf who contain all the credentials |

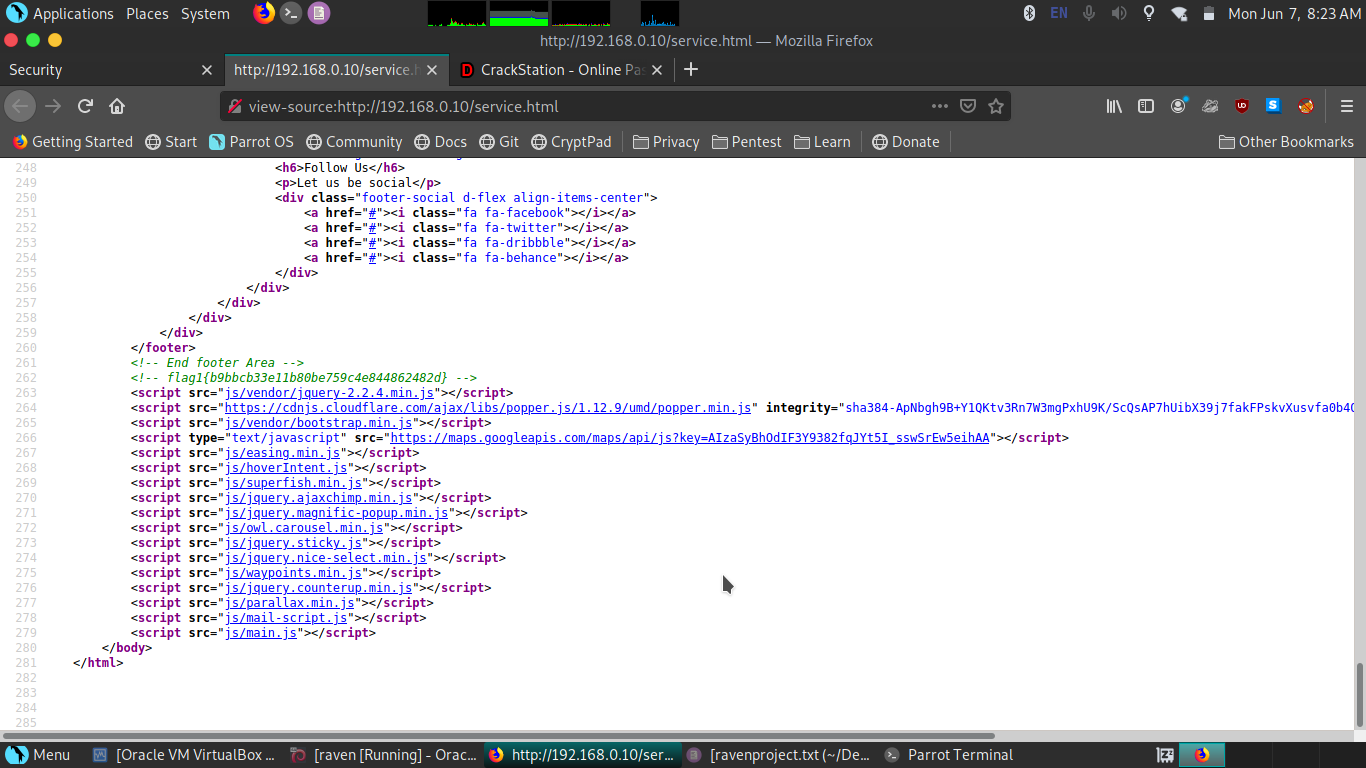
Source Code Disclosure (Medium)

|  |  |
| --- | --- |
| Description: | Information disclosure on a source code attacker can know about your website technologies they can easily plan for exploitation some times on source code attacker find username and passwords or credit card and debit card credentials in this scenario i found the “FLAG1” disclose on source code |
| Impact: | Medium |
| System: | 192.168.0.10 |
| References: | <https://portswigger.net/kb/issues/006000b0_source-code-disclosure> |

**Exploitation Proof of Concept**

Cyber Walkers Security gather source code disclosure on “Raven Security” attacker can know about website technologies and sometimes its store user credential and debit or credit card informtaion (**Note:** A full list of compromised accounts can be found in “**Raven Security Full Findings.xslx”**.).

Source Code Flag Info:



Found Flag 1 :flag1{b9bbcb33e11b80be759c4e844862482d}

path:http://192.168.0.8/service.html

**Remediation**

|  |  |
| --- | --- |
| Who: | Raven Security |
| Vector: | Informational |
| Action: | Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. Review the cause of the code disclosure and prevent it from happening. |

MySQL Database Access (Critical)

|  |  |
| --- | --- |
| Description: | Attacker can exploit on you database there is many types of attacks to gain access on database sql injection on website,gain access through MSQL port,first gain system access the gain access of your database.In this scenario “Raven Security” Leaks the MYSQL “user” and “password” with the help of this attacker can access MYSQL database server and retrive the data . |
| Impact: | Critical |
| System: | 192.168.0.10 |
| References: | <https://dev.mysql.com/doc/mysql-security-excerpt/8.0/en/password-management.html>  <https://www.oreilly.com/library/view/mysql-reference-manual/0596002653/ch04s02.html> |

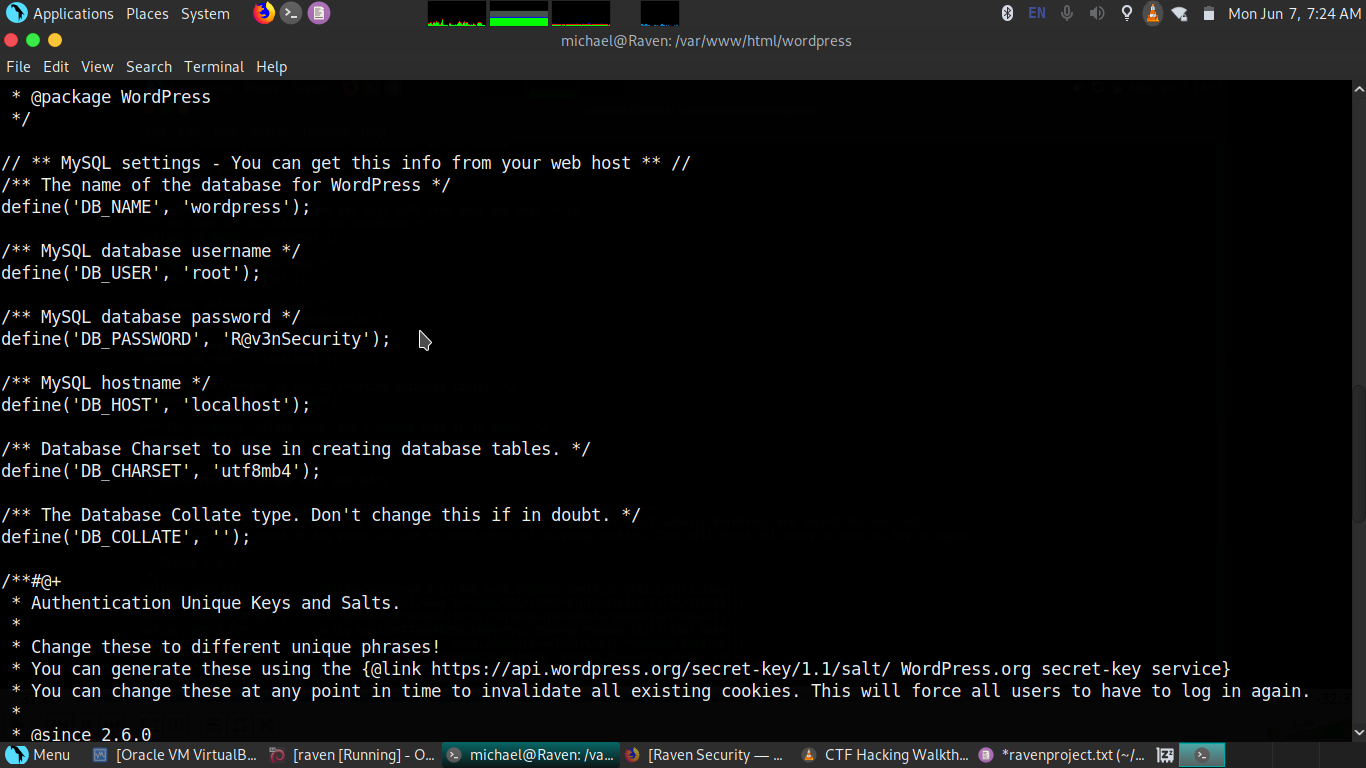
**Exploitation Proof of Concept**

Cyber Walkers Security gather MYSQL “user” and “password” with the help of this credential user can access the database and retrieve the data “Raven Security” leak “user” and “password” of MYSQL after gaining the system access in “Raven Security” there is no MYSQL port are open but after use of SSH gain the access and then gain the MYSQL access and find the “FLAG” (**Note:** A full list of compromised accounts can be found in “**Raven Security Full Findings.xslx”**.).

MYSQL credential leaks:

Path:michael@Raven:/var/www/html/wordpress$

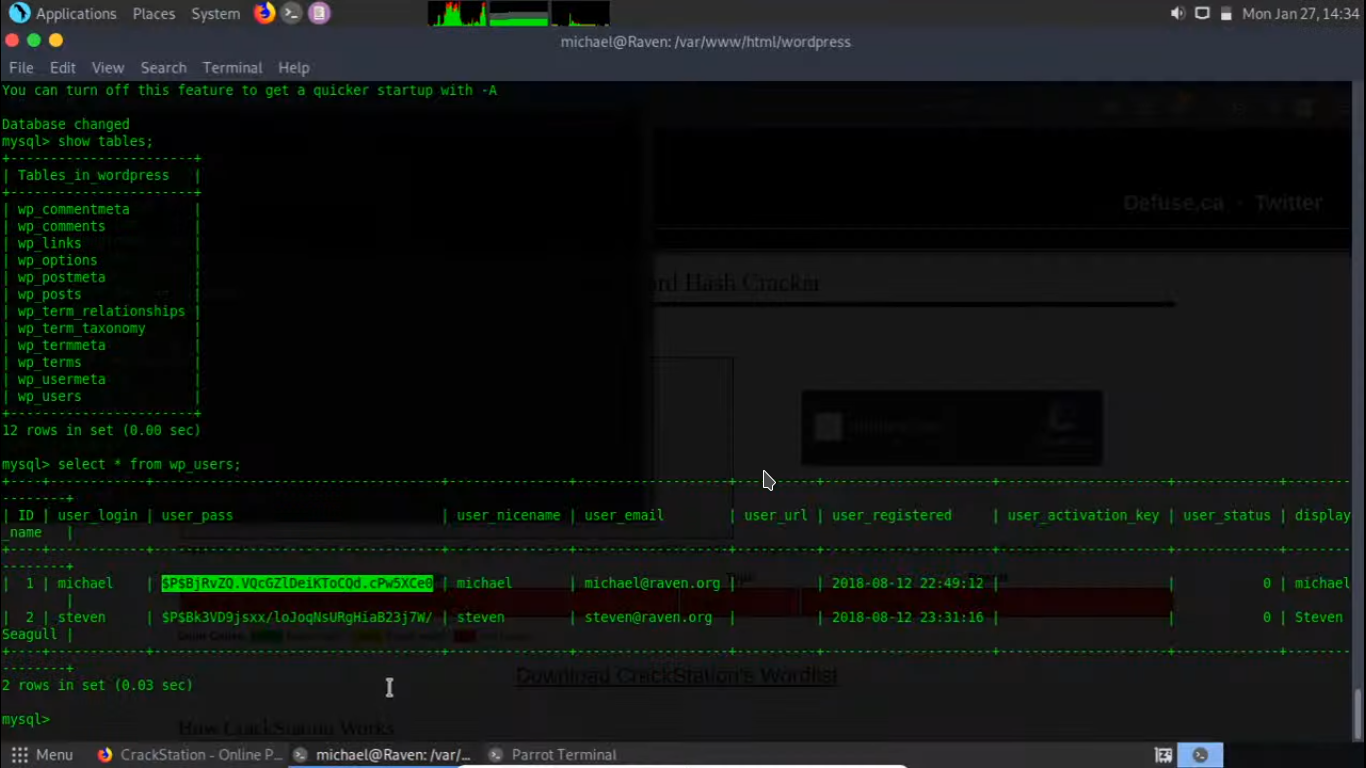
“wp-config.php” file contains these database credentials



Find:Steven root password on database

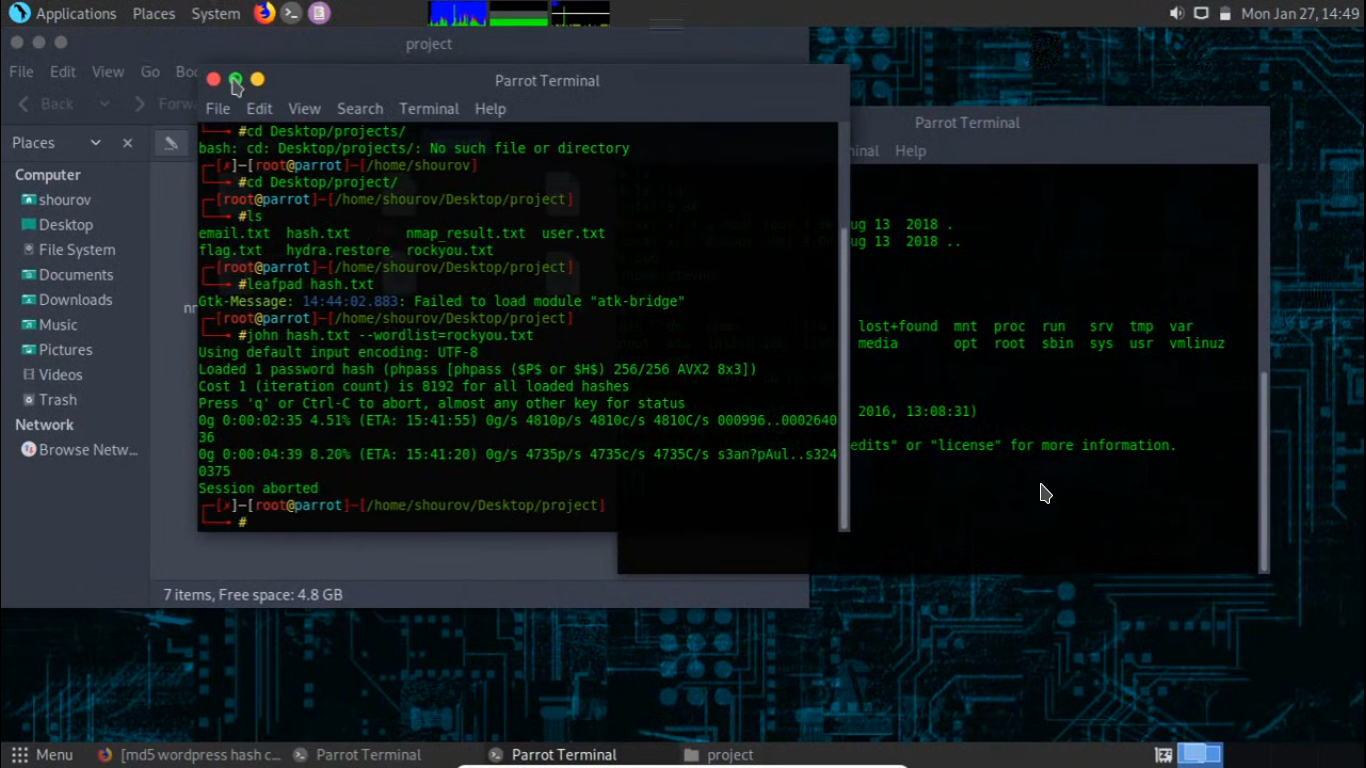
we find the hashes on the database after cracking the hashes find the Steven root password

hashes report:



after find the hashes crack and find the Steven root password

password result:



password is :

#john ravenhash.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8

Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])

Cost 1 (iteration count) is 8192 for all loaded hashes

Will run 4 OpenMP threads

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

pink84 (?)

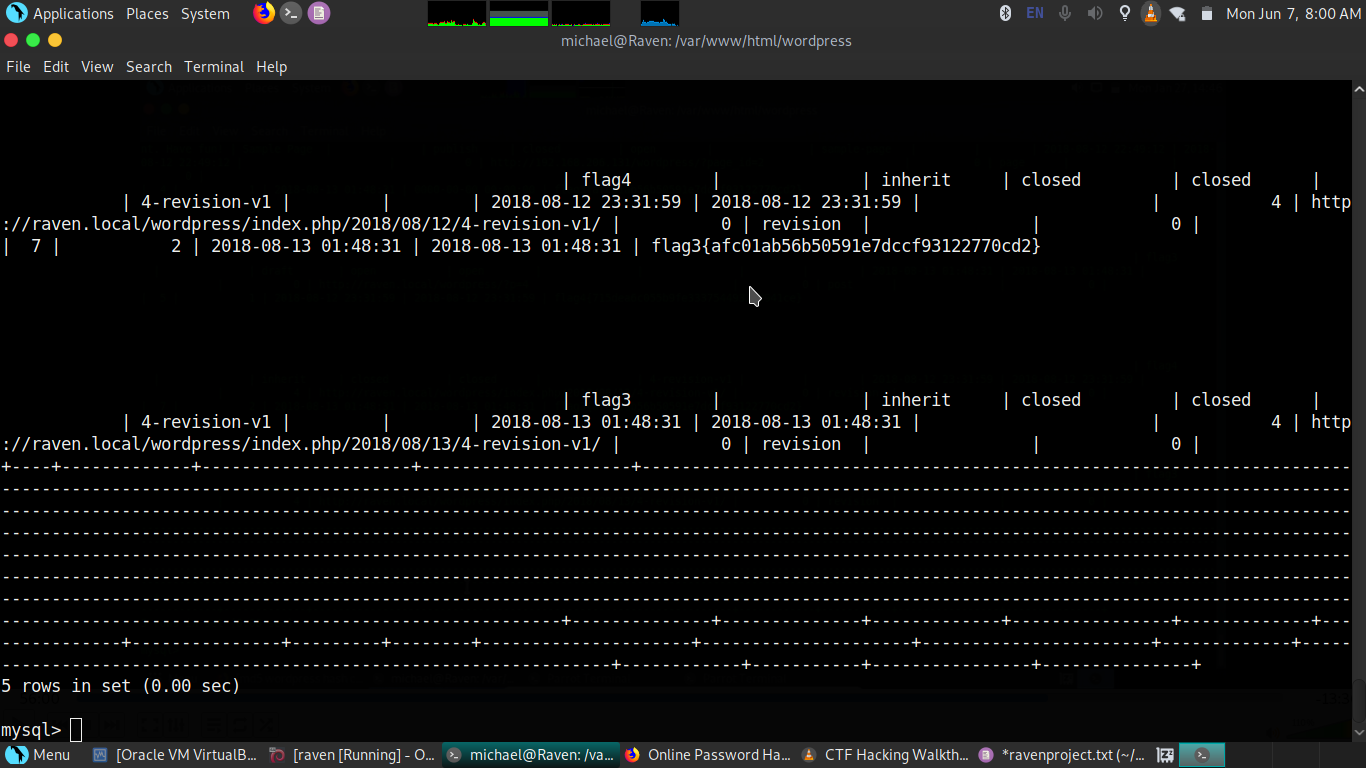
1g 0:00:00:02 DONE (2021-06-07 07:55) 0.4310g/s 19862p/s 19862c/s 19862C/s tamika1..james03

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

Session completed

key found :pink8

Found Flag3 on database:



Flag3:flag3{afc01ab56b50591e7dccf93122770cd2}

**Remediation**

|  |  |
| --- | --- |
| Who: | Raven Security |
| Vector: | Remote |
| Action: | Close,filter or put strong “user” and “password protection” on MYSQL server  hide your “user” and “passwords” leaks on any files rather than its text file or any configuration file you have to hide from attacker to secure your database and your database version should up-to date put a firewall if any web server are running put a WAF(web application firewall). |

Privilage Escalation (Critical)

|  |  |
| --- | --- |
| Description: | Privilege escalation happens when a malicious user exploits a bug, design flaw, or configuration error in an application or operating system to gain elevated access to resources that should normally be unavailable to that user. The attacker can then use the newly gained privileges to steal confidential data, run administrative commands or deploy malware – and potentially do serious damage to your operating system, server applications, organization, and reputation. In this blog post, we will look at typical privilege escalation scenarios and learn how you can protect user accounts in your systems and applications to maintain a good security posture.Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. Review the cause of the code disclosure and prevent it from happening. |
| Impact: | Critical |
| System: | 192.168.0.10 |
| References: | <https://www.netsparker.com/blog/web-security/privilege-escalation/>  <https://portswigger.net/web-security/access-control> |

Cyber Walkers Security gather access using SSH i found 2 credentials “steven” and “michael” final flag found in “Steven” user after getting privilege escalation we found the “Steven” root password on MYSQL database and gain the access as a root user (**Note:** A full list of compromised accounts can be found in “**Raven Security Full Findings.xslx”**.).

Running python spwan script for getting a root

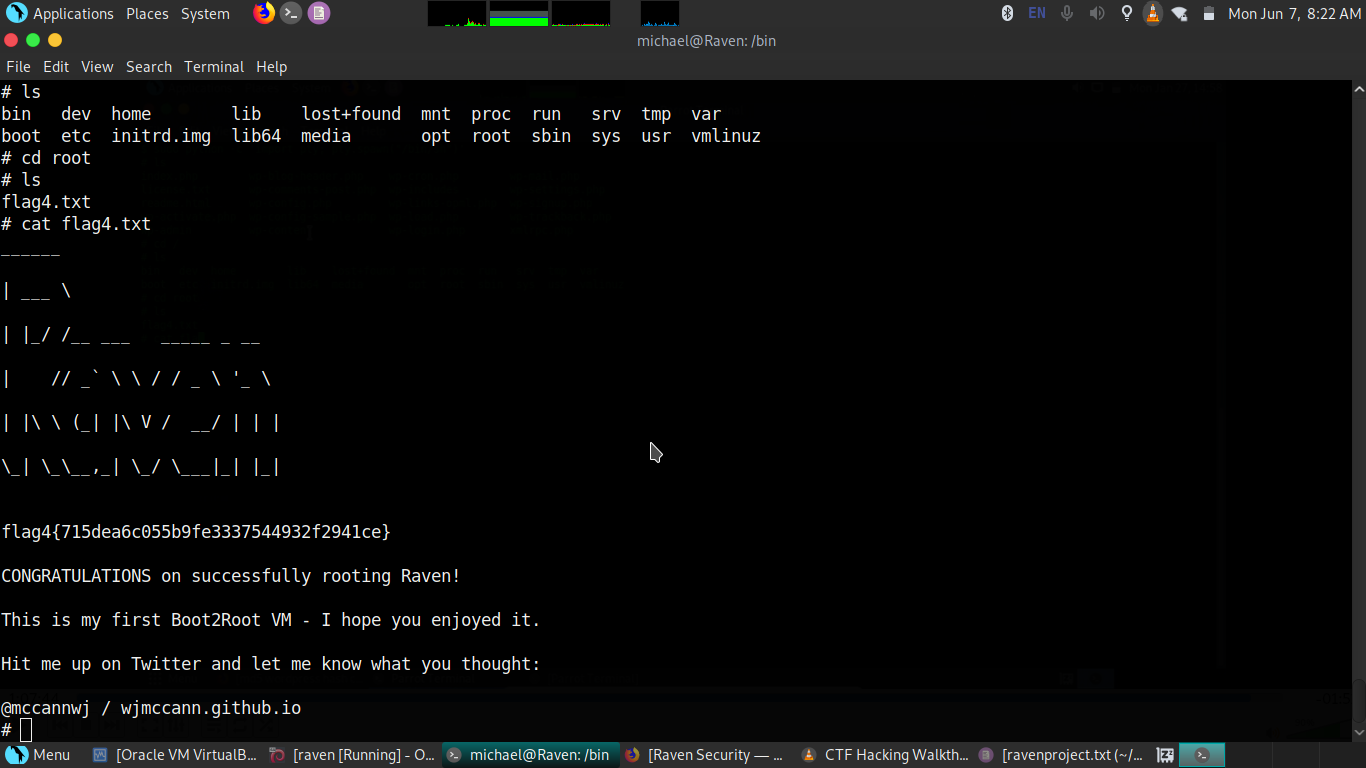
Script:$ sudo python -c 'import pty; pty.spawn("/bin/sh")'

After putting a password we found via cracking a hash

Password found:pink84

Found a final “FLAG4”

path:# cd /root



Tools:

1. Nikto
2. uniscan
3. hydra
4. john the ripper
5. hash-identifier
6. ssh connection



Last Page