OPEN ACCESS

Manuscript ID:
ASH-2023-11026219

Volume: 11

Issue: 2

Month: October

Year: 2023

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 10.07.2023

Accepted: 20.09.2023

Published: 01.10.2023

Citation:
Harivignesh, KS. “Possibility of Gaining Full Access to the Server Through Vulnerability of the Website.” *Shanlax International Journal of Arts, Science and Humanities*, vol. 11, no. 2, 2023, pp. 112–14.

DOI:
https://doi.org/10.34293/sijash.v11i2.6219

Possibility of Gaining Full Access to the Server Through Vulnerability of the Website

K.S. Harivignesh[1]
Independent Researcher

Abstract
We have got the ip address of the server and we have found the open ports and host discovery. Found that port 80 is open and has a website which is vulnerable to sql injection (add admin user) by the outdated CMS version of the website. We have added as admin user and got the reverse shell in the server through the website. We have explored the database and put the backdoor to listen the server. After testing this we have cleared the logs.

Keywords: Penetration Testing, Linux Server, Vulnerability, Gaining Full Access.

Introduction

Every systems has different vulnerability as a penetration tester or security tester need to test the systems in possible different ways to get the security vulnerabilities here we perform a method of gaining full access to the server through website and we can deface the website using these methods.

Tools Used

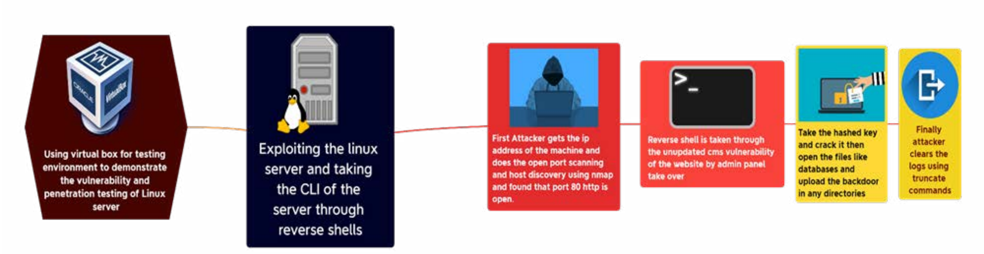
- Nmap – port scanning and host discovery.
- Robots.txt – check the directory for disallowed files to be shown in client side.
- Searchsploit – Getting exploits for the particular vulnerability.
- Hash cat – Cracking the hashed password.
- Python –m http.server – Creating and rising or up the server to transfer the files data’s.
- Wget – For downloading the files or data’s from which the server is up.
- Virtual box – Installing test Linux server and kali Linux.
- Net cat - listener for reverse connection from target Linux machine.
- Hashid – Used to identify the hash algorithm or hash mode type.
- Xmindmap – To create mind map for working model.

Operating System

- Kali Linux – Source machine (our operating system for testing the target).
- Linux Ubuntu 3.13.0-43-generic – Target Linux machine for penetration testing.

[1] This penetration testing project is conducted in the virtual machine for testing purpose. Don’t use it on real time systems and it’s only for educational purpose only.

Working Model


Using virtual box for testing environment to demonstrate the vulnerability and penetration testing of Linux server
Exploiting the linux server and taking the CLI of the server through reverse shells
First Attacker gets the ip address of the machine and does the open port scanning and host discovery using nmap and found that port 80 http is open.
Reverse shell is taken through the unupdated cms vulnerability of the website by admin panel take over
Take the hashed key and crack it then open the files like databases and upload the backdoor in any directories
Finally attacker clears the logs using truncate commands

Procedure

1. We have got the ip address of the Linux server and made port scanning and host discovery using nmap.We have found that the http 80 port is open and http service is running on the apache webserver on the target Linux machine.
2. To check the version and other details we have explored the robots.txt and explored the changelog.txt to see the version number of the website and got CMS Drupal 7.30 version (was fixed in 7.32).
3. Checked for the vulnerability of the website version we have found that the website is vulnerable to "drupalgeddon sql injection (add admin user)" and it means we can add a admin of the website. We can also do Website defacement.
4. We use kali Linux as the operating system for information gathering and penetration testing. Using searchsploit we performed the exploit by using the python.
5. After adding the admin username and password we have logged in inside the website as admin and found that the php filter options is enabled so that we can upload any php script to reflect and get as our result. We tried to do reverse shells.
6. We have found the php reverse shell scripts and uploaded as the content mean while we set the listener net cat using "nc –nlvp 1234" to listen and capture the reverse connection from the target Linux server.
7. We have got the reverse shell of the server and now to get the privilege we use python shell spawning means that will take us to low privilege into the system as normal user. We have got the user privilege but we need to get root user privilege to get access to the etc directory in which it has password containing files.
8. So we find the Linux kernel version of the Linux machine using "uname –a" command in Linux and its Linux Ubuntu 3.13.0-43 generic.
9. Now we have found the exploit of Linux Ubuntu 3.1.3-0-43 kernel version is vulnerable and exploit is 'overlayfs' Local Privilege Escalation - 34292.c.We up the server using python –m http.server in our kali Linux machine and download the exploit using Wget tool in "tmp" directory in target machine. It is c program script and it is executed using "gcc 34292.c –o Linuxexploitand./Linuxexploit is used to become root user.Now we can access the etc and get the shadow file to get the hashed password.
10. We use Hashid tool to get what type hashing algorithm is used to hash the password and we found that is "sha 512 crypt".Now we use this in hashcat tool to get the password so we make a separate wordlist and give possible passwords and use hashcat tool like "hashcat –m1800 –a 3 <hashedpasswordfile><wordlist>.
11. It found the password of the root user so that we can login to the Linux server and we found that /var/www/html – web root of apache webserver contains all webpages and database files in default/sites/ directory we have saw a config. php file which has configuration of databases. We open and viewed the database username and password and we opened the databases and explored the databases of normal login usernames and passwords. Now as the possibility an attacker can put backdoor as any files and listen the server. As we are doing penetration testing we found the vulnerability and exploited it in testing environment and we found the possibility of gaining full access to the server through vulnerability of the website.

Conclusion

- Website should not expose the version of the server and cms as publically.
- Website and server should be properly updated whenever technology is upgrading.
- Should not use weak passwords.
- Robots.txt files should not expose the disallow and allowed pages.
- Website should have ssl certificate enable to make secured communication.
- Server should be updated regularly.
- Possibility of gaining full access to the server through vulnerability of the website is done in testing environment using virtual box and it's only for educational purpose. Do not use it for illegal purpose.

References

Aqua Security. *Reverse Shell: How it Works, Examples and Prevention Tips*, https://www.aquasec.com/cloud-native-academy/cloud-attacks/reverse-shell-attack

CVE Details. *Vulnerability Details : CVE-2010-2075*, https://www.cvedetails.com/cve/CVE-2010-2075/

CVE Details. *Vulnerability Details : CVE-2015-1328*, https://www.cvedetails.com/cve/CVE-2015-1328/

Github. *PHP Reverse Shell*, https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Muller, Tobias. *Internet of Vulnerable Things,* https://raw.githubusercontent.com/otsmr/internet-of-vulnerable-things/main/Internet_of_Vulnerable_Things.pdf

Murari, Gopichand. *Exploiting the Vulnerabilities on Metasploit 3(Ubuntu) Machine using Meta Sploit Framework and Methodologies*. Concordia University of Edmonton, 2020.

Author Details

K.S. Harivignesh, *Independent Researcher,* ***Email ID****: hariresearchfoundation@gmail.com*