HIDE AND SEEK

CTF challenge

[Publish Date]

European Cyber Security Challenge 2019
Bucharest, Romania

1. Initial Write-Up

Description:

Know Your Brand PLC is about to launch a new live server. The devops team is very confident about their work's quality, yet you as an ethical hacker have an alternate opinion. You made a bet that you can recover the proof.txt from the root directory. Prove them you are right.

2. Challenge specifications

- Category: Linux/Network/Exploiting/Reversing/
- Difficulty: Hard
- Expected time to solve: 4 hours to solve (aprx)

3. Technical specifications

Challenge Technical Specification, data to set up and access to the environment.

- IP address: network assigned
- Ubuntu 16.04
- challenges / MklOp4lkA112c
- exploit ssh, mySQL, pyhton, remote code execution, php reverse shell
- proof.txt
- Minimum setup requirements 2GB, 2 cores

4. Questions and answers

1. *CTF Specific questions:*

Q/A that can be directly introduced in a CFT format. This year upload of files can be included, also REGEXPs.

2. *Non-Flag specific:*

Open Questions: Answers that may need a minimum development. (No suitable for CTF but useful for training and for a better understanding of the challenge) Multiple choice answer

Question:

What is the hash of proof.txt?

Answer: 4a9e28defab690fca3955bf1f5a744e1

Question:

Which function is the key to progress?

Answer:

OTP_passwd function

Question:

What is the hidden directory's name?

Answer:

secret_page_of_webcalendar_AAX

Question:

What is the name of vulnerability for Webcalendar 1.2.3?

Answer:

remote code execution

5. Attack Scenario

As security team member of the organisation you made a bet with the devops team that you will be able penetrate their freshly developed services, before they will put it in live environment. The devops team is very confident about their work quality, yet you as experienced ethical hacker have an alternate opinion.

6. Installation instructions

Setup for the organizers

The attached 'challenge_7' VM needs to be imported into the virtualization environment, the VM's will gain IP address from the network, they have no pre-set IPs. Players need to be able to connect to the defined subnet

Setup for the players

After installing and starting VirtualBox they can access the VM from their network (bridge, NAT, NAT network, host only). The VMs have no pre-set IPs.

7. Tools needed

- General Linux tools
- General web scripting/coding knowledge
- Exploit
- Code injection scripting
- Reverse shell
- General python knowledge

8. Walkthrough (writeup)

Description:

1. Webserver is running on port 1. Port number 1 is restricted and disabled in most browser. It is necessary to reconfigure the browser in order to connect to port number 1.
2. There are 3 directories: auth, html and test
3. In the /test directory two PHP files can be found. They belong to the /auth directory.

4. Analysing source code (especially OTP_passwd function) one can write a small script in order to retrieve secret information from the server (see: CH7_retrieve.py).
5. The hidden directory is: secret_page_of_webcalendar_AAX
6. There is a secret.txt in the following url: html/secret/secret.txt . This file is just for confusion, and not necessary to compromise this server.
7. Webcalendar 1.2.3 can be found on the following url: **http://192.168.0.110:1/**html/secret_page_of_webcalendar_AAX/login.php
8. Webcalendar 1.2.3 is vulnerable to remote code execution vulnerability. Exploit can be found on exploit-db: https://www.exploit-db.com/exploits/18775/
9. Create interactive reverse shell: python -c 'import pty; pty.spawn("/bin/bash")'
10. Ubuntu 12.04/14.04/14.10/15.04 is vulnerable to overlayfs Local Root Shell.
11. Download and compile the following exploit to gain root access: https://www.exploit-db.com/exploits/37292