SECURE SERVICES

CTF challenge

[Publish Date]

European Cyber Security Challenge 2019

Bucharest, Romania

1. Initial Write-Up

News is full of security breaches and unpatched systems exposed to known vulnerabilities every day. You as security researcher experience on a daily base the evidence of this and came across in interesting server, which seems to use an unpatched operating system.

2. Challenge specifications

- Category: Linux/Network/Exploiting/Reversing/ ShellShock
- 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 15.04
- challenges / TTzui45lp376hd3
- exploit ssh, mySQL, pyhton, remote code execution, php reverse shell, shellshock
- proof.txt
- Minimum setup requirements 2GB, 2 cores

4. Questions and answers

Question:

What is the hash of proof.txt?

Answer: b2f29e0607e1455db56324f0a8d77e54

Question:

What is the directory to be found at robots.txt?

Answer:

secure-cgi-directory

Question:

What is the name of the exploit to use?

Answer:

Shellshock

Question:

What is the vulnerability to use to gain root access?

Answer:

Overlayfs Local Root Shell

5. Attack Scenario

Example:

You as security researcher experience on a daily base the evidence of this and came across in interesting server, that seems to use an unpatched operating system.

6. Installation instructions

Setup for the organizers

The attached 'challenge_8' 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

Tools needed for the solution of the challenge

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

8. Artefacts Provided

Name	Format	Comment	Checksum (SHA256)
Challenge_8.zip	Compressed zip		d5158a97c21c8db361e01bca36af93ab586c9b3cc44c0cf565fe089323782d3a
CH8_shellshock.py	Python script		6a764249762a50c6c6c983fdc57c07fa96ad1199c0bc28638e2329af8ea0c8c6

9. Walkthrough (writeup)

Description:

1. Webserver is running on port 80 and port 32451.
2. Robots.txt can be found on port 32451.
3. /secure-cgi-directory can be found on robots.txt
4. There is a test.cgi file in the secure-cgi-directory.
5. test.cgi is vulnerable to ShellShock.
6. Create a reverse shell using the Shellshock exploit. See the following custom python code (CH4_shellshock.py exploit)
7. All outgoing ports are disabled by uwf firewall. Only tcp/53 port is allowed for outgoing connection.
8. Ubuntu 12.04/14.04/14.10/15.04 is vulnerable to overlayfs Local Root Shell.
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
12. Be aware that Exploit can not be compiled under www-data.
13. There is a user called: john and the password is john
14. Switch to john user within the reverse shell terminal. Change user and compile the overlayfs exploit.