Homework #4: Pentesting

Assignment Details

This homework is due by Friday, Feburary 26th at 01:00 PM ET (before class). Remember there are no late submissions for the homework so please complete it by then.

For this assignment, be sure to document your process, don't just give the answers! Write as if you were explaining to yourself before you figured it out.

Please add the following header to your assignment:

> **Name:** {Firstname Lastname}
>
> **UID:** {Your UID}
>
> **Honor Pledge:** *I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.*

Assignment Goal: Apply the techniques and terminologies covered in Lecture #4 to emulate basic penetration testing.

Assignment Questions

Consider the following scenarios

1. **(15 points each)** You have a limited shell with the following binaries running with the SETUID bit set:

   - `/usr/bin/vim`
   - `/usr/bin/find`

   How might you be able to abuse the fact the SETUID bit is set to escalate your privilege?

2. On a server you don't yet control you have the ability for the server to repeat your input back to you. However, the input is "sanitized" (as seen below).
    - **(10 points)** Can you make the program echo "I have spaces now!"?
    - **(20 points)** Can you reverse shell yourself? (Use the IP address `127.0.0.1` or `localhost`)

```
#!/usr/bin/python3

from os import system

def injectme(user_input: str):
    sanitized = user_input.lower().replace(" ", "-") # what does this do?
    system("/bin/bash -c  \"echo "+sanitized+"\"")

if __name__ == "__main__":
    while True:
        injectme(input("String to echo: "))
```

Feel free to use this code to test your command injection skills

3. You are a Red Teamer who just ran an nmap scan on a target, the output of which is below.

    Using the information from this scan:

    - **(10 points)** Can you find a critical vulnerability for the software version running on the service? (Give the CVE ID)
    - **(10 points)** Are you able to find a working exploit for this CVE?

```
$ nmap -p 80 -sV [TARGET]
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-19 11:45 +05
Nmap scan report for [TARGET]
Host is up (3.37s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.17

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds
```

Scoring

This homework will be graded out of 100 points. The three questions make up 80 total points, and the remaining 20 points are based on the thoroughness of the writeup (Not just giving the answers to each section).