University *of* Massachusetts Amherst

CS491G CTF Report

S-Computer Networking Lab CTF Report

Author:
Christopher Dahl

Department:
Computer Science

Cursus:
Graduate

April 25, 2023

1 Description

This CTF consist of trhee servers. Let's call then server 1, server 2 and server 3.
The entry server (server 1) has two users: `ctfuser` and `admin`. There is a file called `flag.txt` in the admin users home directory which belongs to admin so the initial access user `ctfuser` can not access it. Server 2 has an HTTP Server running although at port 3, so the fact that it is a webserver at all has to be figured out by other means first. Once the web server is accessed there is a hint in the `/robots.txt` file: The `/webconsole` directory is referred in the robots.txt file. Once the /webconsole directory is accessed you find an interactive shell inside the browser and can access a file called `secret` inside the root directory of the server. This secret is a base64 encoded private rsa key. Once decoded this private key can be used to access the `admin` users of server 1 and 3. An additional challenge being that the admin user from server 1 can only be accessed from server 3 so you have to jump from server 1 to 3 and back to 1. So now the flag.txt file can be accessed, although this is not actually a text file but actually a binary executable which includes a number guessing game. Only when given the right number as parameter it will output the flag.

2 Key Challenges

The key challenges of this CTF include:

- Find the web server: This is a simple nmap scan.
- Figure out that the web server is a web server: A simple nmap scan reveals the open port 3. Then you can connect to port 3 with netcat, send a newline and the server will output an HTTP error message.
- Connect to the web server with a browser: The webconsole is nearly impossible to use over command line tools like netcat, curl etc. And because the web server is not accessible from the users network it is necessary to forward the port to a local port on ssh.
- Download the private key: The webconsole does not allow copy and paste operations from the browser window. You can technically use cat to view the private key and try to copy paste it from the webpages source in the browsers dev tools and strip a bunch of html tags from it. But the easiest way is to use cp to copy the private key to location exposed by the webserver. Than you can just use the browser to download the file.
- Decode the Base64 file
- Jump through server 3.
- Figure out that the flag.txt file is an executable. Should be apparent when trying to inspect it with cat. The file command is not on installed on the server but if needed the file can be downloaded with scp and inspected on your local machine.
- Make the flag.txt file executable: Just use `chmod +x`
- Win the number guessing game: This is easy as the program tells you if the number is too high or low, so it can be solved in logarithmic time.

3 Instructions to solve CTF

- Connect to the ssh server (add the commands for the jump server)

```
ssh ctfuser@localhost
```

- Find out the network:

```
ip a
```

- Scan the network

```
nmap 192.168.0.0/24
```

- Discover that the service running on container 2 port 3 is a web server:

```
nc 192.168.0.3 3
```

- Exit SSH and create a tunnel to this service through the access container:

```
ssh -L 8080:192.168.0.3:3 -p 222 ctfuser@localhost
```

- Connect a web browser to this port 8080 and check the `robots.txt` file.
- Go to the `/webconsole` path on the webserver.
- Discover the id_rsa file in the public directory:

```
cp /secret /var/www/html
```

- Decode the base64 secret to a private rsa key:

```
base64 --decode secret > id_rsa
```

- Download the key from `http://localhost:8080/id_rsa`
- Using this key connect to container 1 again with admin user by jumping over container 4:

```
ssh -J ctfuser@localhost,ctfuser@192.168.0.4 admin@192.168.0.2 -i id_rsa
```

- Make the `flag.txt` file executable:

```
chmod +x flag.txt
```

- Win the guessing game:

```
./flag.txt 50
```