CyberSploit1

Nmap

```
nmap -sC -sV -p- 192.168.222.92 -oA cybersploit1-nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 22:34 CDT
Nmap scan report for 192.168.222.92
Host is up (0.074s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 01:1b:c8:fe:18:71:28:60:84:6a:9f:30:35:11:66:3d (DSA)
|   2048 d9:53:14:a3:7f:99:51:40:3f:49:ef:ef:7f:8b:35:de (RSA)
|_  256 ef:43:5b:d0:c0:eb:ee:3e:76:61:5c:6d:ce:15:fe:7e (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Hello Pentester!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.66 seconds
```

Web page source shows username.

Drib shows a base64 string on the robots.txt page.

Decoding it gives us a youtube link.

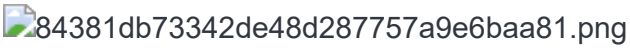
```
cybersploit{youtube.com/c/cybersploit}
```

Using this link with the username we found ealier, we can ssh onto the box.

After running linpeas we see that the box is running a vulnerable kernel verision.

Searching around, we find a kernel exploit we can try.
https://www.exploit-db.com/exploits/37292

We move over the exploit code and compile it on the machine.



Once we run the compiled exploit, we are now elivated to root.