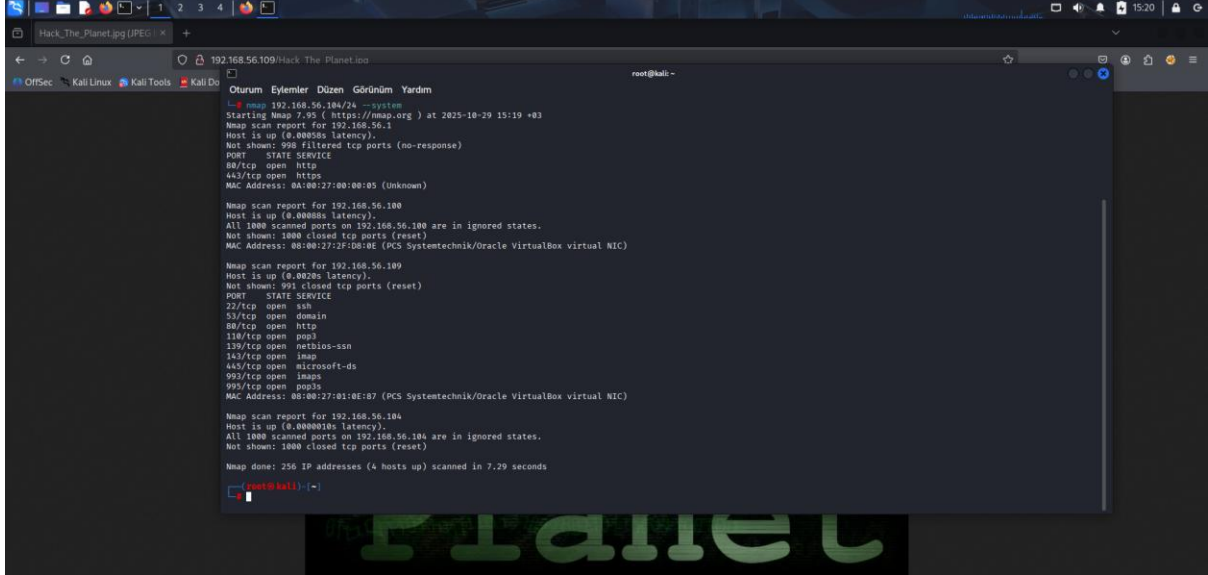


HACKFEST 2016:QUAQOR

Öncelikle bi nmap taraması ile açık portları ve ip adresini buluyorum hemen.



```
Oturum Eylemler Düzen Görünüm Yardım
root@kali:~# nmap 192.168.56.104/24 -sS -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 15:19 +03
Nmap scan report for 192.168.56.1
Host is up (0.0000s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:00:00:05 (Unknown)

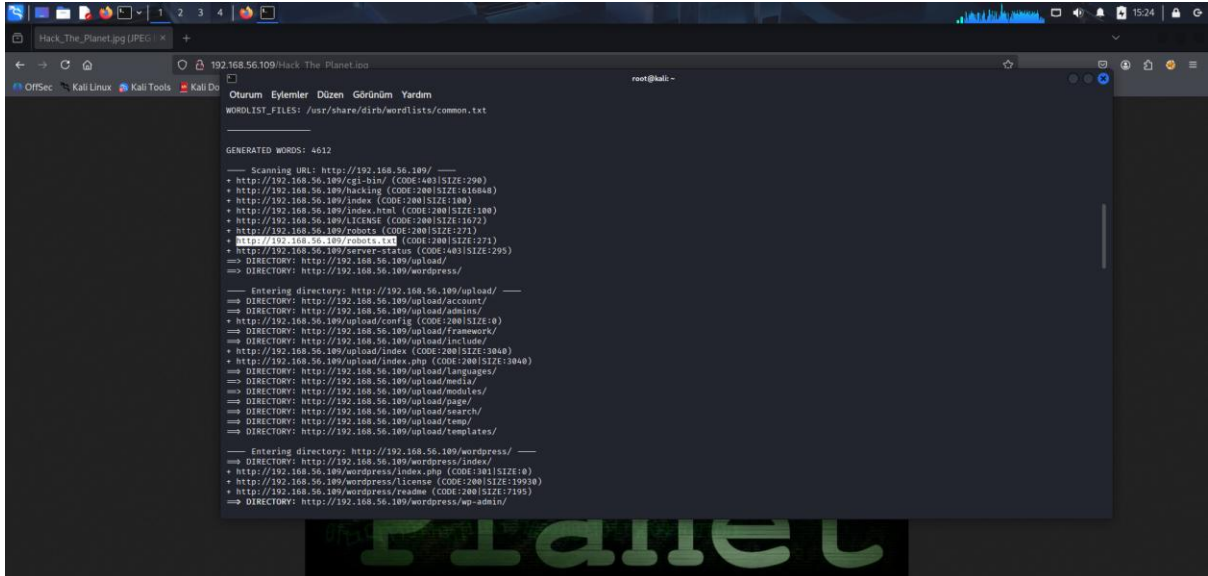
Nmap scan report for 192.168.56.100
Host is up (0.0000s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:00:00:05 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.109
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  microsoft-ds
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 08:00:27:01:0E:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.104
Host is up (0.0000016s latency).
All 1000 scanned ports on 192.168.56.104 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.29 seconds
```

Açık portları ve ip adresini buluyorum ve taramayı genişletmek amacıyla dirb de kullanıyorum. Burada robots.txt dosyası var tarayıcıdan robots.txt ye gidiyorum.



```
Oturum Eylemler Düzen Görünüm Yardım
root@kali:~# dirb http://192.168.56.109/ -w /usr/share/dirb/wordlists/common.txt

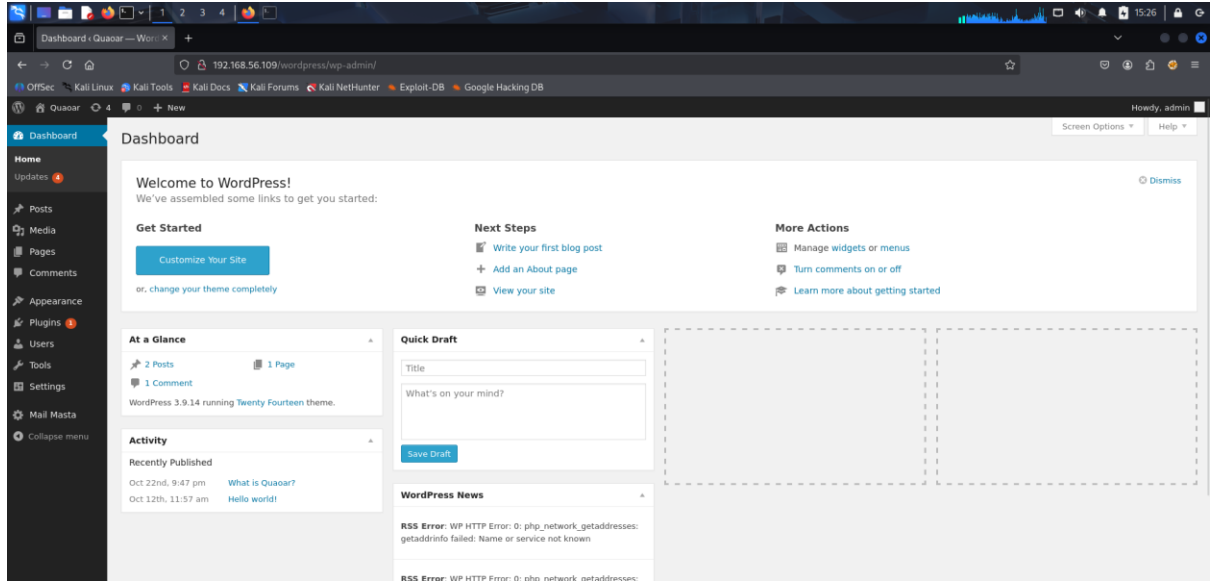
GENERATED WORDS: 4612

-- Scanning URL: http://192.168.56.109/ --
+ http://192.168.56.109/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.56.109/hacking (CODE:200|SIZE:16048)
+ http://192.168.56.109/index (CODE:200|SIZE:100)
+ http://192.168.56.109/index.html (CODE:200|SIZE:100)
+ http://192.168.56.109/LICENSE (CODE:200|SIZE:1672)
+ http://192.168.56.109/robots (CODE:200|SIZE:271)
+ http://192.168.56.109/robots.txt (CODE:200|SIZE:271)
+ http://192.168.56.109/robots.txt (CODE:403|SIZE:295)
=> DIRECTORY: http://192.168.56.109/upload/
=> DIRECTORY: http://192.168.56.109/wordpress/

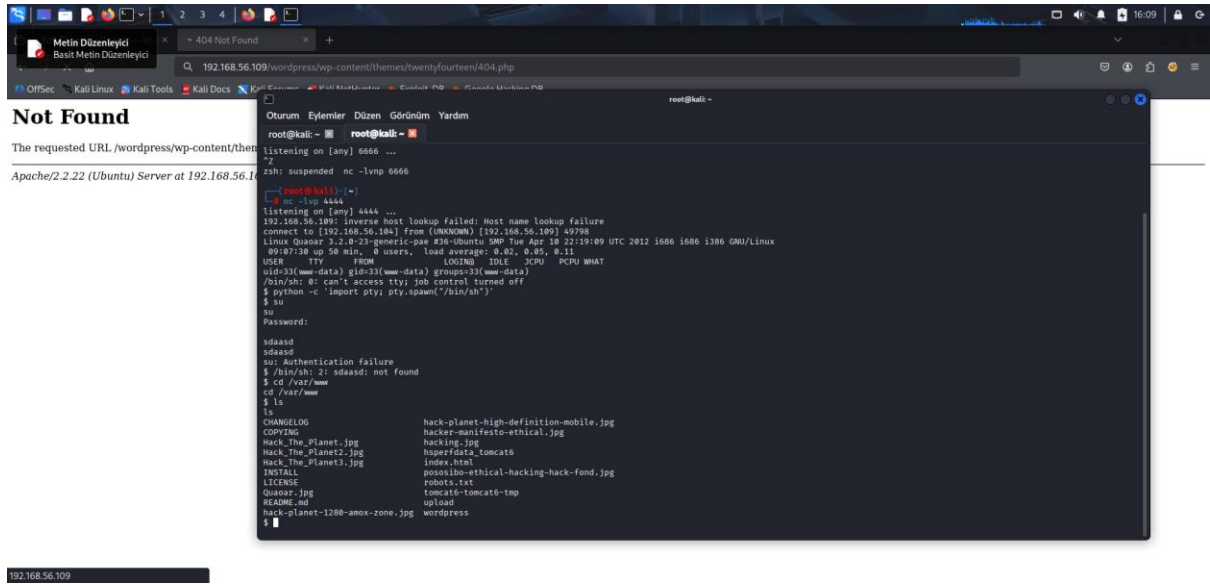
-- Entering directory: http://192.168.56.109/upload/ --
=> DIRECTORY: http://192.168.56.109/upload/account/
=> DIRECTORY: http://192.168.56.109/upload/admins/
=> http://192.168.56.109/upload/config (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.56.109/upload/framework/
=> DIRECTORY: http://192.168.56.109/upload/include/
+ http://192.168.56.109/upload/index (CODE:200|SIZE:2000)
+ http://192.168.56.109/upload/index.php (CODE:200|SIZE:1040)
=> DIRECTORY: http://192.168.56.109/upload/languages/
=> DIRECTORY: http://192.168.56.109/upload/media/
=> DIRECTORY: http://192.168.56.109/upload/modules/
=> DIRECTORY: http://192.168.56.109/upload/page/
=> DIRECTORY: http://192.168.56.109/upload/patches/
=> DIRECTORY: http://192.168.56.109/upload/temp/
=> DIRECTORY: http://192.168.56.109/upload/templates/

-- Entering directory: http://192.168.56.109/wordpress/ --
=> DIRECTORY: http://192.168.56.109/wordpress/index/
+ http://192.168.56.109/wordpress/index.php (CODE:301|SIZE:0)
+ http://192.168.56.109/wordpress/license (CODE:200|SIZE:19930)
+ http://192.168.56.109/wordpress/readme (CODE:200|SIZE:795)
=> DIRECTORY: http://192.168.56.109/wordpress/wp-admin/
```

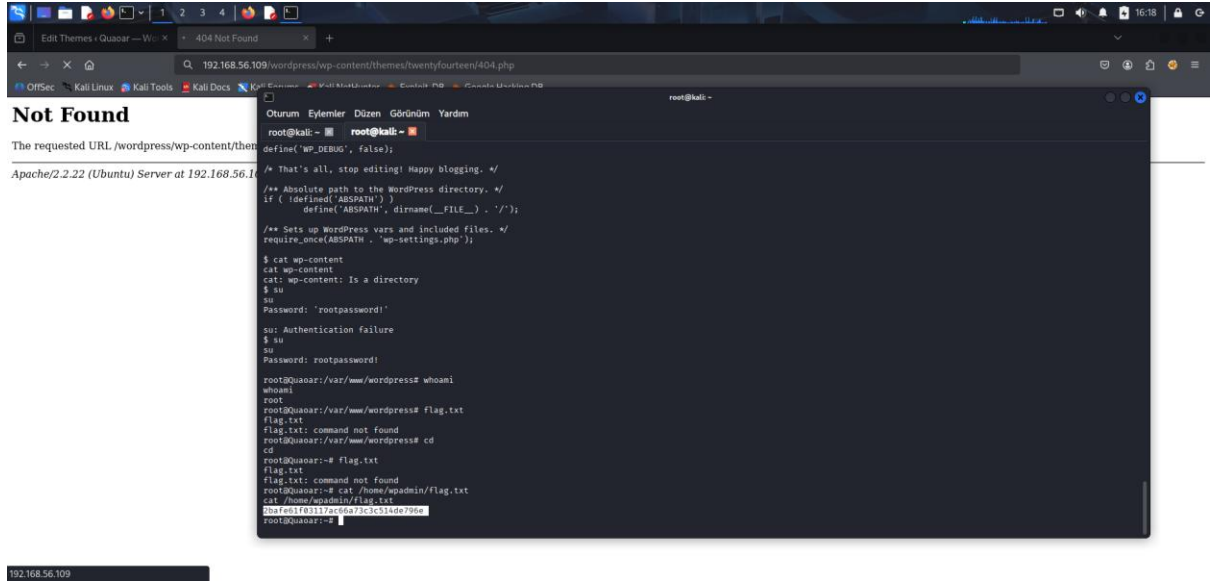
Burada da /wordpress/ yazıyor hemen oraya gidiyorum.



Şimdi apperance kısmından editöre geliyorum ve buraya bir php kodu yerleştirmem gerekiyor reverse shell php nin kodunu buraya yapııştırıyorum ve dinleyici açıyorum. Sonrasında dinleme başlıyor dinleme başlayınca python ile shelli import etmek gerekiyor ve bunu yapıyorum.



Artık root olmaya çalışacağım ama benden bir şifre istiyor ls ile tarama yapıyorum. Burada biraz tökezliyorum sonrasında wordpress dizinini tarıyorum ve karşıma çıkan yerleri tarıyorum config dosyasının içinde şifreyi buluyorum ve root oluyorum sonra da flag txt yi çalıştırıyorum.



ÖZET

Genel olarak diğer ctflerden farklı biraz daha kolay olmasıydı sadece root olmak için wordpress dizinini açıp taramak biraz düşündürücüydü. Yine de gayet eğlenceli güzel bir ctf olduğunu düşünüyorum.