专注APT攻击与防御
https://micropoor.blogspot.com/

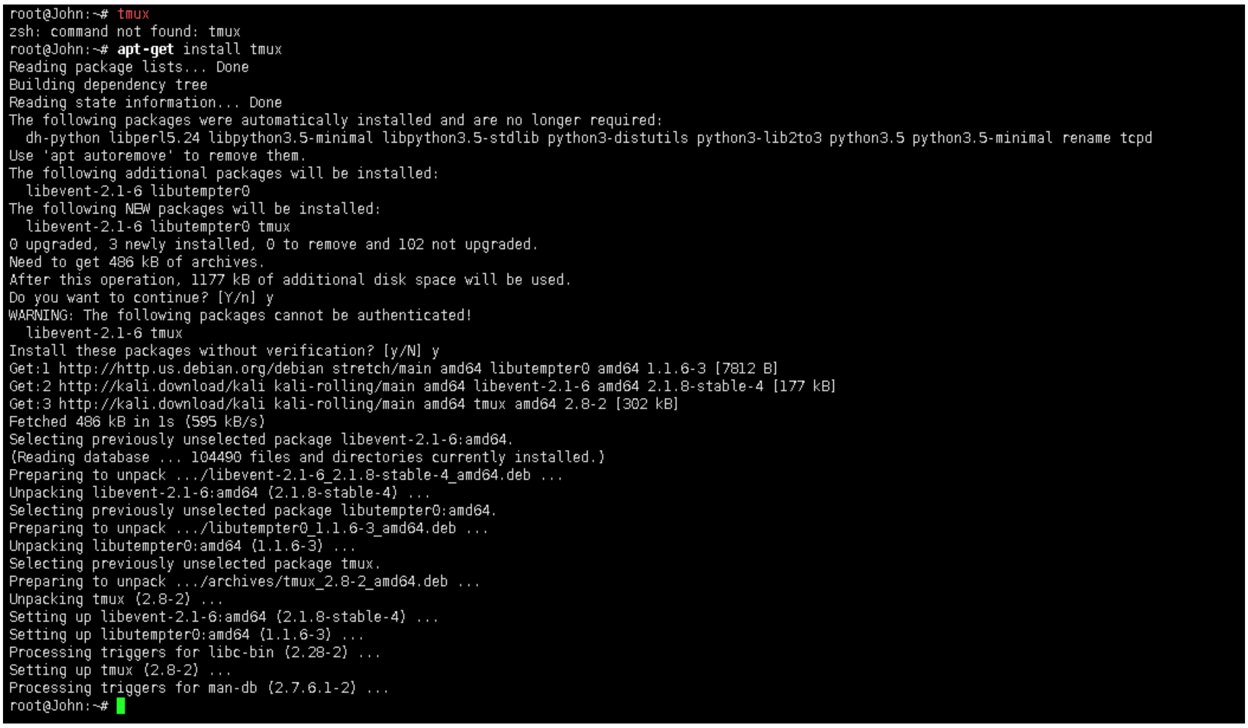
在写第五季的时候，vps掉线了，ssh重新登录后，无法切到MSF session下，想到部分同学如果在vps上操作也会遇到这个问题，故本季解决该问题。

- tmux是什么？

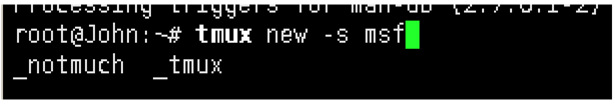
Tmux是一个优秀的终端复用软件，类似GNU Screen，但来自于OpenBSD，采用BSD授权。使用它最直观的好处就是，通过一个终端登录远程主机并运行tmux后，在其中可以开启多个控制台而无需再“浪费”多余的终端来连接这台远程主机。是BSD实现的Screen替代品，相对于Screen，它更加先进：支持屏幕切分，而且具备丰富的命令行参数，使其可以灵活、动态的进行各种布局和操作。

- Tmux的使用场景

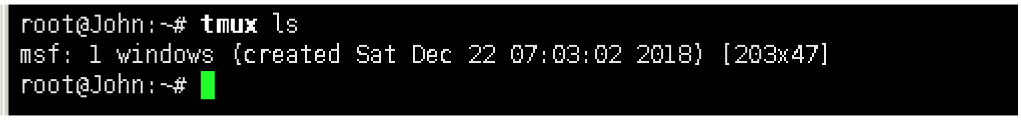
1. 可以某个程序在执行时一直是输出状态，需要结合nohup、&来放在后台执行，并且ctrl+c结束。这时可以打开一个Tmux窗口，在该窗口里执行这个程序，用来保证该程序一直在执行中，只要Tmux这个窗口不关闭
2. 公司需要备份数据库时，数据量巨大，备份两三天弄不完，这时不小心关闭了终端窗口或误操作就前功尽弃了，使用Tmux会话运行命令或任务，就不用担心这些问题。
3. 下班后，你需要断开ssh或关闭电脑，将运行的命令或任务放置后台运行。
4. 关闭终端,再次打开时原终端里面的任务进程依然不会中断
5. 在渗透过程中，意外因网络等原因ssh掉线，tmux可以恢复session会话



```
root@John:~# tmux
zsh: command not found: tmux
root@John:~# apt-get install tmux
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dh-python libperl5.24 libpython3.5-minimal libpython3.5-stdlib python3-distutils python3-lib2to3 python3.5 python3.5-minimal rename tcpd
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libevent-2.1-6 libutempter0
The following NEW packages will be installed:
  libevent-2.1-6 libutempter0 tmux
0 upgraded, 3 newly installed, 0 to remove and 102 not upgraded.
Need to get 486 kB of archives.
After this operation, 1177 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
WARNING: The following packages cannot be authenticated!
  libevent-2.1-6 tmux
Install these packages without verification? [y/N] y
Get:1 http://http.us.debian.org/debian stretch/main amd64 libutempter0 amd64 1.1.6-3 [7812 B]
Get:2 http://kali.download/kali kali-rolling/main amd64 libevent-2.1-6 amd64 2.1.8-stable-4 [177 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 tmux amd64 2.8-2 [302 kB]
Fetched 486 kB in 1s (595 kB/s)
Selecting previously unselected package libevent-2.1-6:amd64.
(Reading database ... 104490 files and directories currently installed.)
Preparing to unpack .../libevent-2.1-6_2.1.8-stable-4_amd64.deb ...
Unpacking libevent-2.1-6:amd64 (2.1.8-stable-4) ...
Selecting previously unselected package libutempter0:amd64.
Preparing to unpack .../libutempter0_1.1.6-3_amd64.deb ...
Unpacking libutempter0:amd64 (1.1.6-3) ...
Selecting previously unselected package tmux.
Preparing to unpack .../archives/tmux_2.8-2_amd64.deb ...
Unpacking tmux (2.8-2) ...
Setting up libevent-2.1-6:amd64 (2.1.8-stable-4) ...
Setting up libutempter0:amd64 (1.1.6-3) ...
Processing triggers for libc-bin (2.28-2) ...
Setting up tmux (2.8-2) ...
Processing triggers for man-db (2.7.6.1-2) ...
root@John:~# 
```



```
Processing triggers for man-db (2.7.6.1-2)
root@John:~# tmux new -s msf
_notmuch  _tmux
```

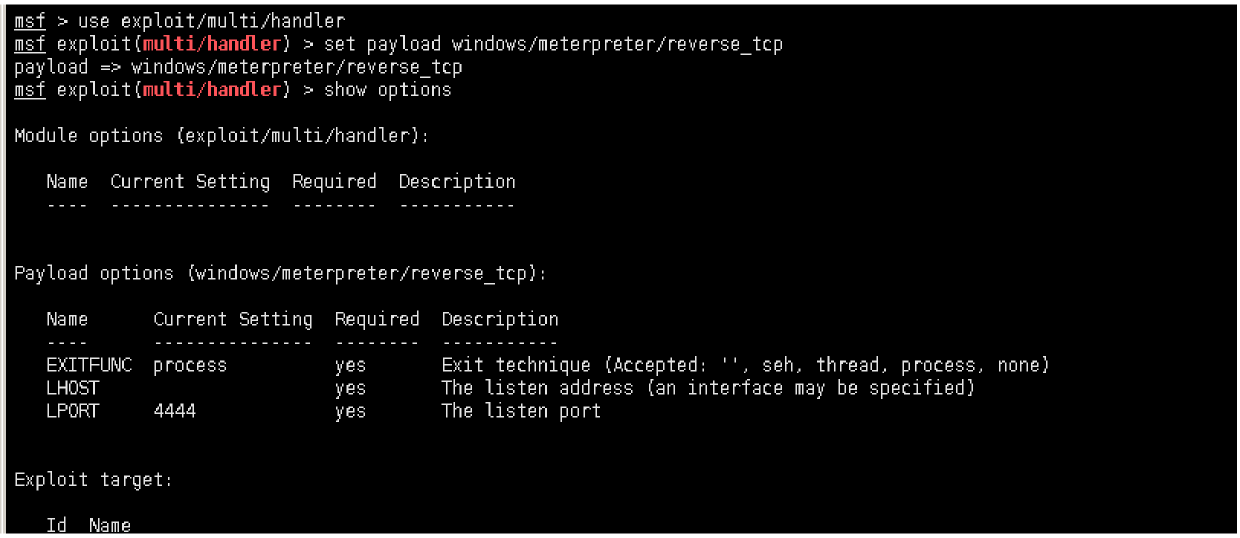


```
root@John:~# tmux ls
msf: 1 windows (created Sat Dec 22 07:03:02 2018) [203x47]
root@John:~# 
```

tmux 常用操作命令：

- tmux new -s session1 新建会话
- ctrl+b d 退出会话，回到shell的终端环境 //tmux detach-client
- tmux ls 终端环境查看会话列表
- ctrl+b s 会话环境查看会话列表
- tmux a -t session1 从终端环境进入会话
- tmux kill-session -t session1 销毁会话
- tmux rename -t old_session_name new_session_name 重命名会话
- ctrl + b $ 重命名会话 (在会话环境中)

还原会话



```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
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                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

- Micropoor