入侵检测

- 本地检测方法
- 云平台的检测方法

查看系统日志

查看安全相关日志

- ssh远程登录失败日志

```
[root@instructor ~]# grep -i Failed /var/log/secure
May 20 12:15:35 instructor sshd[12070]: Failed password for root from 192.168.1.12 port 50720 ssh2
May 20 12:15:48 instructor sshd[12086]: Failed password for root from 192.168.1.144 port 52765 ssh2
```

- ssh远程登录成功日志

```
[root@instructor ~]# grep -i Accepted /var/log/secure
Oct 24 12:18:06 chao sshd[7086]: Accepted password for root from 172.16.130.91 port 41415 ssh2
Oct 24 12:18:06 chao sshd[7084]: Accepted password for root from 172.16.130.81 port 42986 ssh2
```

- 统计登录成功或登录失败的ip,并进行去重降序排列

```
grep -i Accepted /var/log/secure |awk '{print $(NF-3)}' |grep '^[0-9]' |sort |uniq -c |sort -rn
```

```
grep -i Failed /var/log/secure |awk '{print $(NF-3)}' |egrep '^[0-9]' |sort |uniq -c |sort -rn
```

- 查看历史用户登录信息 last
  - 查看最后5条登录信息

```
[root@localhost ~]# last -a -5
root     pts/2        Mon Feb 25 06:21   still logged in    192.168.2.1
root     pts/1        Mon Feb 25 01:10   still logged in    :0
root     :0           Mon Feb 25 01:09   still logged in    :0
root     pts/0        Sun Feb 24 23:39   still logged in    192.168.2.1
reboot   system boot  Sun Feb 24 23:36 - 06:21  (06:45)     3.10.0-862.el7.x86_64
```

  - 查看指定时间之前登录信息

```
[root@localhost ~]# last -a -t 20190210123030
#2019-02-10 12:30:30之前
```

  - 查看登录系统的用户相关信息

```
[root@localhost ~]# last -a -f /var/log/btmp
```

- 查看记录每个用户最后的登入信息

```
[root@localhost ~]# lastlog
用户名           端口     来自             最后登陆时间
root             pts/2    192.168.2.1      一 2月 25 06:21:27 +0800 2019
bin                                        **从未登录过**
daemon                                     **从未登录过**
adm                                        **从未登录过**
lp                                         **从未登录过**
sync                                       **从未登录过**
shutdown                                   **从未登录过**
halt                                       **从未登录过**
mail                                       **从未登录过**
operator                                   **从未登录过**
games                                      **从未登录过**
ftp                                        **从未登录过**
nobody                                     **从未登录过**
systemd-network                            **从未登录过**
dbus                                       **从未登录过**
polkitd                                    **从未登录过**
libstoragemgmt                             **从未登录过**
```

```
rpc                                             **从未登录过**
colord                                          **从未登录过**
gluster                                         **从未登录过**
saslauth                                        **从未登录过**
amandabackup                                    **从未登录过**
abrt                                            **从未登录过**
setroubleshoot                                  **从未登录过**
rtkit                                           **从未登录过**
pulse                                           **从未登录过**
rpcuser                                         **从未登录过**
nfsnobody                                       **从未登录过**
unbound                                         **从未登录过**
chrony                                          **从未登录过**
qemu                                            **从未登录过**
radvd                                           **从未登录过**
tss                                             **从未登录过**
usbmuxd                                         **从未登录过**
geoclue                                         **从未登录过**
ntp                                             **从未登录过**
sssd                                            **从未登录过**
gdm              :0                             日 2月 24 23:36:56 +0800 2019
gnome-initial-setup :0                             一 2月 11 22:03:38 +0800 2019
sshd                                            **从未登录过**
avahi                                           **从未登录过**
postfix                                         **从未登录过**
tcpdump                                         **从未登录过**
tom              :0                             一 2月 11 22:06:38 +0800 2019

```

- 统计当前在线状态

```
[root@localhost ~]# w
 06:27:49 up  3:18,  4 users,  load average: 0.00, 0.04, 0.13
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    192.168.2.1      23:39    5:09m  1.11s  1.11s -bash
root     :0       :0               01:09   ?xdm?   3:10   0.34s /usr/libexec/gn
root     pts/1    :0               01:10    5:14m  0.13s  0.13s bash
root     pts/2    192.168.2.1      06:21    5.00s  0.13s  0.02s w
```

- 查看系统主日志

```
[root@localhost ~]# less /var/log/messages
```

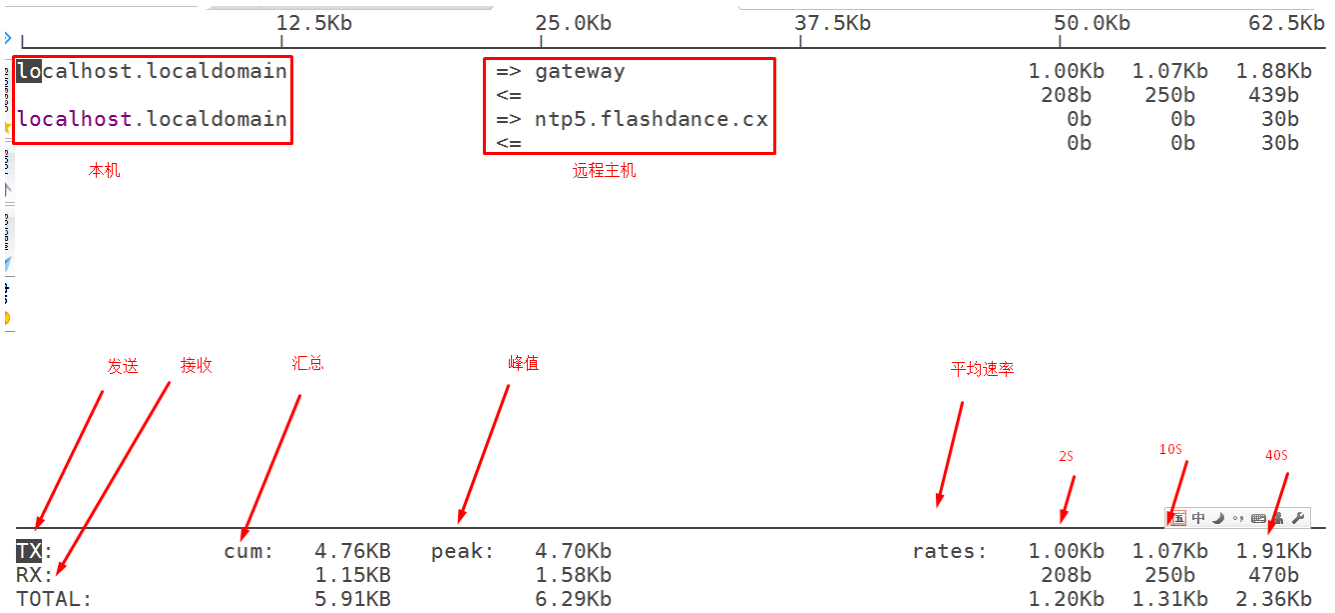
- 查看计划任务

```
[root@localhost ~]# less /var/log/cron
[root@localhost ~]# cat /var/spool/cron/*
[root@localhost ~]# less /etc/crontab
[root@localhost ~]# ls /etc/cron.*
```

查看异常流量

- iftop 动态查看网卡接口流量

```
[root@localhost ~]# yum -y install epel-release
[root@localhost ~]# yum -y install iftop
[root@localhost ~]# iftop -i ens33
```



- 流量监控

Cacti,Zabbix,Ganglia,Prometheus+grafana等

- 数据包抓取

wireshark,tcpdump,sniffer

- tcpdump
  - 基本用法

```
# tcpdump -i eth0 -nnv
# tcpdump -i eth0 -nnv -c 100
# tcpdump -i eth0 -nnv -w /file1.tcpdump
# tcpdump  -nnv -r /file1.tcpdump
```

  - 条件：port,host,net

```
# tcpdump -i eth0 -nnv not port 80
# tcpdump -i eth0 -nnv port 22
# tcpdump -i eth0 -nnv port 80
# tcpdump -i eth0 -nnv net 192.168.0.0/24
# tcpdump -i eth0 -nnv host 192.168.0.15
# tcpdump -i eth0 -nnv dst port 22
# tcpdump -i eth0 -nnv src port 22
```

  - 协议作为条件

```
# tcpdump -i eth0 -nnv arp
# tcpdump -i eth0 -nnv icmp
# tcpdump -i eth0 -nnv udp  #udp协议
# tcpdump -i eth0 -nnv tcp  #tcp协议，三次握手及四次断开
# tcpdump -i eth0 -nnv ip   #ip协议
# tcpdump -i eth0 -nnv vrrp #keepalived使用协议
```

  - 多条件：与关系(and) 或关系(or) 非关系(not)

```
# tcpdump -i eth0 -nnv not net 192.168.0.0/24
# tcpdump -i eth0 -nnv not port 80
# tcpdump -i eth0 -nnv host 192.168.0.15 and port 22
# tcpdump -i eth0 -nnv host 192.168.0.15 and host 192.168.0.33
# tcpdump -i eth0 -nnv host 192.168.0.15 or host 192.168.0.33
# tcpdump -i eth0 -nnv  \( host 192.168.0.15 and port 22 \)   or  \( host
192.168.0.33 and port 80 \)

# tcpdump -i eth0 -nnv host 192.168.0.110 and  port 22 or port 80
# tcpdump -i eth0 -nnv host 192.168.0.110 and \( port 22 or port 80\)

# tcpdump -i eth0 -nnv host 192.168.0.110 and port 80
# tcpdump -i eth0 -nnv host 192.168.0.110 and ! port 80
```

- 条件为TCP仅有SYN标记的

```
# man tcpdump
# tcpdump -i eth0 -nnv tcp[13]==2

                |C|E|U|A|P|R|S|F|
                |---------------- |
                |0 0 0 0 0 0 1 0 |
                |---------------- |
                |7 6 5 4 3 2 1 0|
# tcpdump -i eth0 -nnv tcp[13]==2 and port 22 -w ssh-conn.tcpdump

条件是：TCP仅有SYN/ACK标记的
# tcpdump -i eth0 -nnv tcp[13]==18

                |C|E|U|A|P|R|S|F|
                |---------------- |
                |0 0 0 1 0 0 1 0 |
                |---------------- |
                |7 6 5 4 3 2 1 0|

# tcpdump -i eth0 -nnv tcp[13]==17
```

检查可疑进程

- 基本工具 ps pstree top netstat ss
  - ps

系统进程一般还有“[]”

```
ps -aux | less
```

- pstree

显示每个程序的完全指令，包含路径、参数或是常驻服务标识、列出树状图时特别标注现在执行的程序

```
pstree -a
pstree -h
```

- top

按cpu、内存排序

```
top -d 1
按P以CPU使用排序
按M以内存使用排序
```

- netstat

查看网络连接情况

```
netstat -anputl
```

- ss

查看某个协议或端口的监听状态

```
ss -an | grep tcp

ss -an | grep 22
```

- 根据文件或端口查找进程
  - 根据某文件查看正在被某些进程使用

```
lsof /usr/sbin/vsftpd
fuser /usr/local/nginx/sbin/nginx
```

- 根据某个端口查看对应进程

```
lsof -i TCP:22
fuser -v 22/tcp
```

扩展：

- Kernel Audit 内核审计

文件完整性检查

- 检验RPM包完整性

没有显示说明包没有被修改

```
rpm -V bash
rpm -V kernel
rpm -V vsftpd
rpm -Vf /etc/ssh/sshd_config
```

- md5sum/sha1sum检测
  - 获取当前的/etc 目录md5值

```
find /etc -type f -exec md5sum {} \; >/tmp/`date +%F%H%M`-md5.txt
```

  - 修改文件、删除文件、添加文件

  - 重新获取/etc目录的md5值

```
find /etc -type f -exec md5sum {} \; >/tmp/`date +%F%H%M`-md5.txt
```

- 对比以上md5值获取操作过的文件

```
diff /tmp/1-md5.txt /tmp/2-md5.txt
```

扩展：

- HIDS:AIDE 高级入侵检测环境