应急响应

linux应急响应

具备的前置知识

通用知识：操作系统、WEB、数据库、网络设备

安全知识：流行攻击手法、新的攻击技术

Rootkit检查：

rkhunter、chkrootkit

系统命令：

ps、pmap、top、kill

ls、strings、strace、rpm

lsof、netstat

chkconfig、crontab(启动)

webshell检查：

webshell.py、find、grep、findstr

网络工具攻击：

tcpdump、wireshark、Colasoft Capsa(科来)

日志分析工具：

Logview、LogParse、EmEditor

wtmp—who -u /var/log/wtmp(记录用户登录成功和持续时间，二进制文件)

btmp—last -f /var/log/btmp（登陆失败日志）

lastlog—lastlog -f /var/log/lastlog（每个用户最后登录时间）

日志分析工具：

Logview、LogParse、EmEditor

/etc/init.d　服务启动脚本目录

Kill　-STOP pid　挂起pid对应的进程

日志文件

/var/log/secure：记录登录系统存取数据的文件；
例如:pop3，ssh，telnet，ftp等都会记录在此.

/var/log/cron：用来记录crontab这个服务的内容；

```
46371 Dec  8 06:16:32 localhost sshd[29316]: Disconnected from 192.168.200.58 port 7219 [preauth]
46372 Dec  8 06:16:32 localhost unix_chkpwd[29336]: password check failed for user (root)
46373 Dec  8 06:16:32 localhost sshd[29334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.200.58  user=root
46374 Dec  8 06:16:32 localhost sshd[29334]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
46375 Dec  8 06:16:33 localhost sshd[29275]: Failed password for root from 192.168.200.63 port 34718 ssh2
46376 Dec  8 06:16:33 localhost unix_chkpwd[29337]: password check failed for user (root)
46377 Dec  8 06:16:33 localhost sshd[29275]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
46378 Dec  8 06:16:33 localhost sshd[29301]: Failed password for root from 192.168.200.63 port 34720 ssh2
46379 Dec  8 06:16:33 localhost unix_chkpwd[29338]: password check failed for user (root)
46380 Dec  8 06:16:33 localhost sshd[29301]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
46381 Dec  8 06:16:33 localhost sshd[29320]: Failed password for root from 192.168.200.63 port 34730 ssh2
46382 Dec  8 06:16:33 localhost sshd[29320]: Accepted password for root from 192.168.200.63 port 34730 ssh2
46383 Dec  8 06:16:33 localhost sshd[29303]: Failed password for root from 192.168.200.63 port 34722 ssh2
46384 Dec  8 06:16:33 localhost sshd[29303]: Connection closed by 192.168.200.63 port 34722 [preauth]
46385 Dec  8 06:16:33 localhost sshd[29303]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.200.63  user=root
46386 Dec  8 06:16:33 localhost sshd[29305]: Failed password for root from 192.168.200.63 port 34724 ssh2
46387 Dec  8 06:16:33 localhost sshd[29305]: Connection closed by 192.168.200.63 port 34724 [preauth]
46388 Dec  8 06:16:33 localhost sshd[29305]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.200.63  user=root
46389 Dec  8 06:16:33 localhost sshd[29308]: Failed password for root from 192.168.200.63 port 34726 ssh2
46390 Dec  8 06:16:33 localhost sshd[29323]: Failed password for root from 192.168.200.63 port 34732 ssh2
46391 Dec  8 06:16:33 localhost sshd[29308]: Connection closed by 192.168.200.63 port 34726 [preauth]
46392 Dec  8 06:16:33 localhost sshd[29323]: Connection closed by 192.168.200.63 port 34732 [preauth]
46393 Dec  8 06:16:33 localhost sshd[29308]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.200.63  user=root
46394 Dec  8 06:16:34 localhost sshd[29310]: Failed password for root from 192.168.200.63 port 34728 ssh2
```

谢谢观赏