SANGFOR 深信服科技

深信服产业教育中心 SANGFOR EDUCATION CENTER

linux应急响应

深信服产业教育中心
SANGFOR EDUCATION CENTER

教学目标

- 理解Linux应急响应的思路
- 掌握Linux应急响应的常用命令

目录

识别现象

- **通过系统运行状态、安全设备告警，主机异常现象来发现可疑现象**
- **通常的可疑现象有**
  - 资源占用
  - 异常登录
  - 异常文件
  - 异常连接
  - 异常进程

进程排查

- **进程检查**
- **Linux因为其默认的进程权限分离，每个进程有不同的权限，所以从进程用户名上能给我们很多信息**
  - 比如从mysql用户启动了一些非mysql的进程

```
mysql 63763 45.3 0.0 12284 9616 ? R 01:18 470:54 ./db_temp/dazui.4
mysql 63765 0.0 0.0 12284 9616 ? S 01:18 0:01 ./db_temp/dazui.4
mysql 63766 0.0 0.0 12284 9616 ? S 01:18 0:37 ./db_temp/dazui.4
mysql 64100 45.2 0.0 12284 9616 ? R 01:20 469:07 ./db_temp/dazui.4
mysql 64101 0.0 0.0 12284 9616 ? S 01:20 0:01 ./db_temp/dazui.4
```

  - 类似还有webshell执行反弹连接，会显示apache的用户权限

进程排查

深信服产业教育中心
SANGFOR EDUCATION CENTER

查看资源占用

top

```
top - 10:26:51 up  1:27,  2 users,  load average: 0.00, 0.01, 0.05
Tasks: 206 total,   1 running, 205 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1865308 total,    79976 free,   903596 used,   881736 buff/cache
KiB Swap:  2097148 total,  2096628 free,      520 used.   713172 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
  630 root      20   0  320124   6520   5056 S   0.3  0.3   0:05.45 vmtoolsd
 2380 sangfor   20   0  402504  18940  14980 S   0.3  1.0   0:06.25 vmtoolsd
    1 root      20   0  128236   6296   3576 S   0.0  0.3   0:01.94 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.15 ksoftirqd/0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S   0.0  0.0   0:00.24 kworker/u256:0
    7 root      rt   0       0      0      0 S   0.0  0.0   0:00.02 migration/0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S   0.0  0.0   0:00.43 rcu_sched
   10 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 lru-add-drain
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.03 watchdog/0
```

进程排查

- **查看所有进程**
  - ps -ef
- **根据进程PID查看进程详细信息**
  - lsof -p PID

```
[root@localhost ~]# lsof -p 2657
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND  PID USER   FD   TYPE             DEVICE SIZE/OFF    NODE NAME
sshd    2657 root  cwd    DIR                8,3      224      64 /
sshd    2657 root  rtd    DIR                8,3      224      64 /
sshd    2657 root  txt    REG                8,3   853040 2433842 /usr/sbin/sshd
sshd    2657 root  mem    REG                8,3    37240  831101 /usr/lib64/libnss_sss.so.2
sshd    2657 root  mem    REG                8,3    15480  415406 /usr/lib64/security/pam_lastlog.so
sshd    2657 root  mem    REG                8,3    15632  415388 /usr/lib64/libpam_misc.so.0.82.0
sshd    2657 root  mem    REG                8,3   309280  845272 /usr/lib64/security/pam_systemd.so
sshd    2657 root  mem    REG                8,3    19600  415407 /usr/lib64/security/pam_limits.so
sshd    2657 root  mem    REG                8,3    11152  415405 /usr/lib64/security/pam_keyinit.so
sshd    2657 root  mem    REG                8,3    40784  415414 /usr/lib64/security/pam_namespace.so
sshd    2657 root  mem    REG                8,3    11200  415410 /usr/lib64/security/pam_loginuid.so
```

- **查看启动时间**
  - ps -p PID -o lstart

```
[root@localhost ~]# ps -p 706 -o lstart
                  STARTED
Wed Apr 14 08:59:20 2021
```

进程排查

- 对于一些异常的文件，初步判断，可以用strings显示里面的可读字符串，并进行grep

```
[root@localhost ~]# strings /usr/sbin/sshd  |more
/lib64/ld-linux-x86-64.so.2
libfipscheck.so.1
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
_fini
FIPSCHECK_verify
```

- 查看进程可执行文件
  - ls -la /proc/PID/exe
- 查看进程树，使用pstree

文件排查

- 查找指定时间的文件
- 查找根目录下，修改时间小于1天的文件
  - find / -mtime -1

mtime 也可以对应为 mmin指修改分钟，m意为modify

相应也可改为ctime ,atime,分别意为create，access

- 也可结合文件名进一步查找
  - find /var/www/html/ -mtime -1 -name *.php

```
[root@localhost ~]# find /var/www/html/ -mtime -100 -name *.php
/var/www/html/11.php
/var/www/html/123.php
```

  - find /etc/ /usr/bin/ /usr/sbin/ /bin/ /usr/local/bin/ /var/spool/cron/ -type f -mtime -3 | xargs ls -al

文件排查

- 入侵者通常会替换系统的内置命令达到隐藏的目的
- 查看系统命令是否存在异常，如大小、修改时间、创建时间等
- ls -altS /usr/sbin | head -30

```
[root@localhost ~]# ls -alS /usr/sbin  | head -30
total 69364
-rwxr-xr-x.  1 root root     3016944 Feb 22 17:24 zabbix_server_mysql
-rwxr-xr-x.  1 root root     2776016 Apr 13  2018 NetworkManager
-r-xr-xr-x.  1 root root     2174664 Apr 11  2018 lvm
-rwxr-xr-x.  1 root root     2027776 Apr 11  2018 wpa_supplicant
-rwxr-xr-x.  1 root root     1856480 Apr 11  2018 eapol_test
-rwxr-xr-x.  1 root root     1330336 Oct 21  2017 grub2-install
-rwxr-xr-x.  1 root root     1241656 Apr 11  2018 ModemManager
-rwxr-xr-x.  1 root root     1239096 Apr 11  2018 pdata_tools
-rwxr-xr-x.  1 root root     1070352 Oct 21  2017 grub2-sparc64-setup
-rwxr-xr-x.  1 root root     1070184 Oct 21  2017 grub2-bios-setup
-rwxr-xr-x.  1 root root     1066144 Oct 21  2017 grub2-probe
-rwxr-xr-x.  1 root root     1049080 Oct 21  2017 grub2-macbless
-rwxr-xr-x.  1 root root      975200 Apr 10  2018 ldconfig
-rwxr-xr-x.  1 root root      942304 Apr 11  2018 tcpdump
-rwxr-xr-x.  1 root root      908472 Apr 11  2018 lshw
-rwx------.  1 root root      881168 Apr 10  2018 build-locale-archive
-rwxr-xr-x.  1 root root      853040 Apr 11  2018 sshd
-rwxr-xr-x.  1 root root      843608 Apr 11  2018 iscsid
-rwxr-xr-x.  1 root root      817616 Apr 11  2018 iscsiadm
-rwx------.  1 root root      790576 Apr 10  2018 glibc_post_upgrade.x86_
-rwxr-xr-x.  1 root root      761840 Apr 10  2018 sln
-rwxr-xr-x.  1 root root      729744 Apr 13  2018 ntpd
-rwxr-xr-x.  1 root root      719296 Apr 11  2018 smartctl
```

网络排查

- **查看当前已建立的TCP连接**
  - netstat -antulp | grep ESTABLISHED
- **查看反弹连接**
  - netstat -antulp | grep bash
- **查看本机开放的端口**
  - netstat -antulp
- **查看某一端口的具体应用**
  - lsof -i:22

```
[root@localhost ~]# lsof -i:22
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd      706 root    3u  IPv4  23565      0t0  TCP *:ssh (LISTEN)
sshd      706 root    4u  IPv6  23567      0t0  TCP *:ssh (LISTEN)
sshd     2657 root    3u  IPv4  38546      0t0  TCP localhost.localdomain:ssh->192.168.164.1:51924 (ESTABLISHED)
[root@localhost ~]#
```

用户排查

- **查看uid或gid为0的用户**
  - grep :0 /etc/passwd

```
[root@localhost ~]# grep :0  /etc/passwd
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
operator:x:11:0:operator:/root:/sbin/nologin
[root@localhost ~]#
```

- **查看passwd文件的最后修改记录**
  - stat /etc/passwd

用户排查

- 统计所有用户的shell相关信息
  - cat /etc/passwd | awk -F: '{print $7}' | sort | uniq -c

```
[root@localhost ~]# cat /etc/passwd | awk -F: '{print $7}' | sort | uniq -c
      2 /bin/bash
      1 /bin/false
      1 /bin/sync
      1 /sbin/halt
     43 /sbin/nologin
      1 /sbin/shutdown
```

- 重点检查有登录权限的用户
  - cat /etc/passwd | grep bash

用户排查

- 查看用户登录时间 last 或 lastlog

```
[root@localhost ~]# last
root     pts/0          192.168.164.1    Wed Apr 14 09:00   still logged in
sangfor  :0             :0               Wed Apr 14 09:00   still logged in
reboot   system boot  3.10.0-862.el7.x Wed Apr 14 08:59 - 14:39  (05:40)
root     pts/1          192.168.164.1    Mon Mar 29 16:22 - crash (15+16:36)
sangfor  pts/0          :0               Mon Mar 29 16:22 - 19:10  (02:48)
sangfor  :0             :0               Mon Mar 29 16:22 - 19:10  (02:48)
reboot   system boot  3.10.0-862.el7.x Mon Mar 29 16:15 - 14:39 (15+22:24)
root     pts/0          192.168.164.1    Wed Mar 24 15:04 - down   (02:16)
reboot   system boot  3.10.0-862.el7.x Wed Mar 24 14:25 - 17:20  (02:55)
```

```
[root@localhost ~]# w
 14:39:14 up  5:40,  2 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
sangfor  :0       :0               09:00   ?xdm?   1:33   0.22s /usr/libexec/gnome-session-binary --session gnome-clas
root     pts/0    192.168.164.1    09:00    2.00s  0.38s  0.02s w
[root@localhost ~]#
```

用户排查

- 查看允许sudo的用户
  - more /etc/sudoers | egrep -v "^#|^$"

```
[root@localhost ~]# more /etc/sudoers | egrep -v "^#|^$"
Defaults   !visiblepw
Defaults    always_set_home
Defaults    match_group_by_gid
Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"
Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin
root    ALL=(ALL)       ALL
%wheel  ALL=(ALL)       ALL
[root@localhost ~]#
```

- 继续检查wheel组包含的用户
  - grep wheel /etc/group

```
[root@localhost ~]# grep wheel /etc/group
wheel:x:10:sangfor
```

历史命令

- linux因为其命令行的特殊性，可以通过history命令来查看用户之前的操作
- history记录位于用户home目录下的.bash_history文件中。
- 可以直接cat ~/ .bash_history 查看历史记录

持久化查询

- **Linux的持久化方式不如windows复杂，通常有以下四种方式**
  - 定时任务
  - 开机服务
  - 开机启动
  - 驱动加载

定时任务排查


```
[root@localhost ~]# crontab -l
no crontab for root
[root@localhost ~]#
```

- crontab -l
- 定时任务还应检查以下文件和文件夹
  - /var/spool/cron/*
  - /etc/crontab
  - /etc/cron.d/*
  - /etc/cron.daily/*
  - /etc/cron.hourly/*
  - /etc/cron.monthly/*
  - /etc/cron.weekly/
  - /etc/anacrontab
  - /var/spool/anacron/*

开机启动项排查

深信服产业教育中心
SANGFOR EDUCATION CENTER

- Linux开机有多种运行级别，不同级别下加载的启动文件也不相同

启动级别	含义
0	关机
1	单用户模式，用于系统修复。可以理解为windows的安全模式
2	不完全的命令行，不含NFS
3	完全的命令行（通常使用）
4	系统保留
5	图形模式
6	重启

- 查看当前启动级别，当前为5，即图形式模式
  - runlevel

```
[root@localhost ~]#
[root@localhost ~]# runlevel
N 5
```

开机启动项排查

- 不同启动级别会加载不同启动文件
- 检查下述文件或文件夹
  - /etc/rc.d/*
  - /etc/rc.local
  - /etc/rc[0-6].d
  - /etc/inittab

开机服务检查

- chkconfig --list
- 0-6依然是系统启动级别

```
[root@localhost ~]# chkconfig --list

Note: This output shows SysV services only and does not include native
      systemd services. SysV configuration data might be overridden by native
      systemd configuration.

      If you want to list systemd services use 'systemctl list-unit-files'.
      To see services enabled on particular target use
      'systemctl list-dependencies [target]'.

netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:off   3:off   4:off   5:off   6:off
[root@localhost ~]#
```

linux日志分析

- **Linux使用rsyslog管理日志**
- **通常关注的日志有**
  - /var/log/messages：内核及公共消息日志
  - /var/log/cron：计划任务日志
  - /var/log/dmesg：系统引导日志
  - /var/log/maillog：邮件系统日志
  - /var/log/lastlog：用户登录日志
  - /var/log/boot.log：记录系统在引导过程中发生的时间
  - /var/log/secure：用户验证相关的安全性事件
  - /var/log/wtmp：当前登录用户详细信息
  - /var/log/btmp：记录失败的的记录
  - /var/run/utmp：用户登录、注销及系统开、关等事件；

linux日志分析

- **Linux因为有强大的文本处理工具，如sed、awk等，所以从日志中提取信息相对容易，但前提是熟悉sed，awk，正则表达式等应用，下面列出一些常用举例**
- **定位有多少IP在爆破主机的root帐号：**
  - grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more
- **定位有哪些IP在爆破：**
  - grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c

linux日志分析

- **爆破用户名字典是什么?**
  - grep "Failed password" /var/log/secure|perl -e 'while($_=<>){ /for(.*?) from/; print "$1\n";}'|uniq -c|sort -nr

- **登录成功的IP有哪些:**
  - grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

- **登录成功的日期、用户名、IP:**
  - grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

linux工具使用

- **常用的Linux应急响应工具有**
  - chkrootkit，用于检查rootkit隐藏
  - 官网http://www.chkrootkit.org/

chkrootkit是用于在本地检查rootkit迹象的工具。它包含：

- **chkrootkit**：用于检查系统二进制文件中rootkit修改的shell脚本。
- **ifpromisc.c**：检查接口是否处于混杂模式。
- **chklastlog.c**：检查是否删除了lastlog。
- **chkwtmp.c**：检查wtmp删除。
- **check_wtmpx.c**：检查是否删除了wtmpx。（仅Solaris）
- **chkproc.c**：检查LKM木马的迹象。
- **chkdirs.c**：检查LKM木马的迹象。
- **strings.c**：快速而肮脏的字符串替换。
- **chkutmp.c**：检查utmp删除。

  - rkhunter（Rootkit Hunter）是基于Unix的工具，可扫描rootkit，后门程序和可能的本地 漏洞。
  - webshell检测工具，深信服EDR检测
  - https://edr.sangfor.com.cn/#/introduction/wehshell

总结

- 结合linux应急响应的常见维度，进行linux应急响应分析

SANGFOR
深信服科技

深信服产业教育中心
SANGFOR EDUCATION CENTER

THANK YOU

深 信 服 产 业 教 育 中 心