黑客教你11個步驟完美排查，服務器是否已經被入侵

Caesar 手機電腦雙黑客 昨天

世界那麼大，謝謝你來看我！！關注我你就是個網絡、電腦、手機小達人

> **文章來源：LemonSec**

隨著開源產品的越來越盛行，作為一個Linux運維工程師，能夠清晰地鑑別異常機器是否已經被入侵了顯得至關重要，個人結合自己的工作經歷，整理了幾種常見的機器被黑情況供參考。

背景信息：以下情況是在CentOS 6.9的系統中查看的，其它Linux發行版類似

1.入侵者可能會刪除機器的日誌信息，可以查看日誌信息是否還存在或者是否被清空，相關命令示例：

```
[root@hlmcen69n3 ~]# ll -h /var/log/*
-rw-------. 1 root root 2.6K Jul  7 18:31 /var/log/anaconda.ifcfg.log
-rw-------. 1 root root  23K Jul  7 18:31 /var/log/anaconda.log
-rw-------. 1 root root  26K Jul  7 18:31 /var/log/anaconda.program.log
-rw-------. 1 root root  63K Jul  7 18:31 /var/log/anaconda.storage.log
```

```
[root@hlmcen69n3 ~]# du -sh /var/log/*
8.0K /var/log/anaconda
4.0K /var/log/anaconda.ifcfg.log
24K  /var/log/anaconda.log
28K  /var/log/anaconda.program.log
64K  /var/log/anaconda.storage.log
```

2.入侵者可能創建一個新的存放用戶名及密碼文件，可以查看/etc/passwd及/etc/shadow文件，相關命令示例：

```
[root@hlmcen69n3 ~]# ll /etc/pass*

-rw-r--r--. 1 root root 1373 Sep 15 11:36 /etc/passwd

-rw-r--r--. 1 root root 1373 Sep 15 11:36 /etc/passwd-



[root@hlmcen69n3 ~]# ll /etc/sha*

----------. 1 root root 816 Sep 15 11:36 /etc/shadow

----------. 1 root root 718 Sep 15 11:36 /etc/shadow-
```

3.入侵者可能修改用戶名及密碼文件，可以查看/etc/passwd及/etc/shadow文件內容進行鑑別，相關命令示例：

```
[root@hlmcen69n3 ~]# more /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
```

```
[root@hlmcen69n3 ~]# more /etc/shadow
root:*LOCK*:14600::::::
bin:*:17246:0:99999:7:::
daemon:*:17246:0:99999:7:::
```

4.查看機器最近成功登陸的事件和最後一次不成功的登陸事件，對應日誌“/var/log/lastlog”，相關命令示例：

```
[root@hlmcen69n3 ~]# lastlog
Username         Port     From             Latest
root                                       **Never logged in**
bin                                        **Never logged in**
daemon                                     **Never logged in**
```

5.查看機器當前登錄的全部用戶，對應日誌文件“/var/run/utmp”，相關命令示例：

```
[root@hlmcen69n3 ~]# who
stone    pts/0        2017-09-20 16:17 (X.X.X.X)
test01   pts/2        2017-09-20 16:47 (X.X.X.X)
```

6.查看機器創建以來登陸過的用戶，對應日誌文件“/var/log/wtmp”，相關命令示例：

```
[root@hlmcen69n3 ~]# last

test01   pts/1        X.X.X.X   Wed Sep 20 16:50   still logged in

test01   pts/2        X.X.X.X   Wed Sep 20 16:47 - 16:49  (00:02)
```

```
stone    pts/1        X.X.X.X   Wed Sep 20 16:46 - 16:47  (00:01)

stone    pts/0        X.X.X.X   Wed Sep 20 16:17   still logged in
```

7.查看机器所有用户的连接时间（小时），对应日志文件“/var/log/wtmp”，相关命令示例：

```
[root@hlmcen69n3 ~]# ac -dp
        stone                                  11.98
Sep 15      total       11.98
        stone                                  67.06
Sep 18      total       67.06
        stone                                   1.27
        test01                                  0.24
Today       total         1.50
```

8.如果发现机器产生了异常流量，可以使用命令“tcpdump”抓取网络包查看流量情况或者使用工具”iperf”查看流量情况

9.可以查看/var/log/secure日志文件，尝试发现入侵者的信息，相关命令示例：

```
[root@hlmcen69n3 ~]# cat /var/log/secure | grep -i "accepted password"

Sep 20 12:47:20 hlmcen69n3 sshd[37193]: Accepted password for stone from X.X.X.X po

Sep 20 16:17:47 hlmcen69n3 sshd[38206]: Accepted password for stone from X.X.X.X po

Sep 20 16:46:00 hlmcen69n3 sshd[38511]: Accepted password for stone from X.X.X.X po

Sep 20 16:47:16 hlmcen69n3 sshd[38605]: Accepted password for test01 from X.X.X.X p
```

```
Sep 20 16:50:04 hlmcen69n3 sshd[38652]: Accepted password for test01 from X.X.X.X p
```

10.查询异常进程所对应的执行脚本文件

1>top命令查看异常进程对应的PID

```
top - 17:05:36 up 4 days, 19:23,  2 users,  load average: 0.00, 0.00, 0.00
Tasks: 126 total,   1 running, 125 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.2%us,  0.2%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   3530640k total,   426356k used,  3104284k free,   121752k buffers
Swap:        0k total,        0k used,        0k free,   108564k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 1850 root      20   0  360m  16m 4452 S  0.3  0.5  46:55.54 python
    1 root      20   0 21392 1560 1240 S  0.0  0.0   0:03.76 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
```

2>在虚拟文件系统目录查找该进程的可执行文件

```
[root@hlmcen69n3 ~]# ll /proc/1850/ | grep -i exe
lrwxrwxrwx. 1 root root 0 Sep 15 12:31 exe -> /usr/bin/python


[root@hlmcen69n3 ~]# ll /usr/bin/python
-rwxr-xr-x. 2 root root 9032 Aug 18  2016 /usr/bin/python
```

11.如果确认机器已经被入侵，重要文件已经被删除，可以尝试找回被删除的文件

Note:

参考Link：http://www.cnblogs.com/ggjucheng/archive/2012/01/08/2316599.html

1>当进程打开了某个文件时，只要该进程保持打开该文件，即使将其删除，它依然存在于磁盘中。这意味着，进程并不知道文件已经被删除，它仍然可以向打开该文件时提供给它的文件描述符进行读取和写入。除了该进程之外，这个文件是不可见的，因为已经删除了其相应的目录索引节点。

2>在/proc 目录下，其中包含了反映内核和进程树的各种文件。/proc目录挂载的是在内存中所映射的一块区域，所以这些文件和目录并不存在于磁盘中，因此当我们对这些文件进行读取和写入时，实际上是在从内存中获取相关信息。大多数与 lsof 相关的信息都存储于以进程的 PID 命名的目录中，即 /proc/1234 中包含的是 PID 为 1234 的进程的信息。每个进程目录中存在着各种文件，它们可以使得应用程序简单地了解进程的内存空间、文件描述符列表、指向磁盘上的文件的符号链接和其他系统信息。lsof 程序使用该信息和其他关于内核内部状态的信息来产生其输出。所以lsof可以显示进程的文件描述符和相关的文件名等信息。也就是我们通过访问进程的文件描述符可以找到该文件的相关信息。

3>当系统中的某个文件被意外地删除了，只要这个时候系统中还有进程正在访问该文件，那么我们就可以通过lsof从/proc目录下恢复该文件的内容。

假设入侵者将/var/log/secure文件删除掉了，尝试将/var/log/secure文件恢复的方法可以参考如下：

a.查看/var/log/secure文件，发现已经没有该文件

```
[root@hlmcen69n3 ~]# ll /var/log/secure

ls: cannot access /var/log/secure: No such file or directory
```

b.使用lsof命令查看当前是否有进程打开/var/log/secure，

```
[root@hlmcen69n3 ~]# lsof | grep /var/log/secure
rsyslogd   1264      root    4w      REG
8,1  3173904     263917 /var/log/secure (deleted)
```

c.从上面的信息可以看到 PID 1264（rsyslogd）打开文件的文件描述符为4。同时还可以看到/var/log/ secure已经标记为被删除了。因此我们可以在/proc/1264/fd/4（fd下的每个以数字命名的文件表示进程对应的文件描述符）中查看相应的信息，如下：

```
[root@hlmcen69n3 ~]# tail /proc/1264/fd/4
Sep 20 16:47:21 hlmcen69n3 sshd[38511]: pam_unix(sshd:session): session closed for
Sep 20 16:47:21 hlmcen69n3 su: pam_unix(su-l:session): session closed for user root
Sep 20 16:49:30 hlmcen69n3 sshd[38605]: pam_unix(sshd:session): session closed for
Sep 20 16:50:04 hlmcen69n3 sshd[38652]: reverse mapping checking getaddrinfo for 19
Sep 20 16:50:04 hlmcen69n3 sshd[38652]: Accepted password for test01 from 106.120.7
Sep 20 16:50:05 hlmcen69n3 sshd[38652]: pam_unix(sshd:session): session opened for
```

```
Sep 20 17:18:51 hlmcen69n3 unix_chkpwd[38793]: password check failed for user (root
Sep 20 17:18:51 hlmcen69n3 sshd[38789]: pam_unix(sshd:auth): authentication failure
Sep 20 17:18:52 hlmcen69n3 sshd[38789]: Failed password for root from 51.15.81.90 p
Sep 20 17:18:52 hlmcen69n3 sshd[38790]: Connection closed by 51.15.81.90
```

d.从上面的信息可以看出，查看/proc/1264/fd/4就可以得到所要恢复的数据。如果可以通过文件描述符查看相应的数据，那么就可以使用I/O重定向将其重定向到文件中，如:

```
[root@hlmcen69n3 ~]# cat /proc/1264/fd/4 > /var/log/secure
```

e.再次查看/var/log/secure，发现该文件已经存在。对于许多应用程序，尤其是日志文件和数据库，这种恢复删除文件的方法非常有用。

来自：铭的随记
链接：cnblogs.com/stonehe/p/7562374.html

```
[root@hlmcen69n3 ~]# ll /var/log/secure
-rw-r--r--. 1 root root 3173904 Sep 20 17:24 /var/log/secure


[root@hlmcen69n3 ~]# head /var/log/secure
Sep 17 03:28:15 hlmcen69n3 sshd[13288]: reverse mapping checking getaddrinfo for 13
Sep 17 03:28:15 hlmcen69n3 unix_chkpwd[13290]: password check failed for user (root
Sep 17 03:28:15 hlmcen69n3 sshd[13288]: pam_unix(sshd:auth): authentication failure
Sep 17 03:28:17 hlmcen69n3 sshd[13288]: Failed password for root from 51.15.64.137
Sep 17 03:28:18 hlmcen69n3 sshd[13289]: Received disconnect from 51.15.64.137: 11:
Sep 17 03:28:22 hlmcen69n3 sshd[13291]: reverse mapping checking getaddrinfo for 13
Sep 17 03:28:22 hlmcen69n3 unix_chkpwd[13293]: password check failed for user (root
Sep 17 03:28:22 hlmcen69n3 sshd[13291]: pam_unix(sshd:auth): authentication failure
```

```
Sep 17 03:28:24 hlmcen69n3 sshd[13291]: Failed password for root from 51.15.64.137
Sep 17 03:28:25 hlmcen69n3 sshd[13292]: Received disconnect from 51.15.64.137: 11:
```

喜欢的小伙伴记得三连击！！！

声明：本人分享该教程是希望大家，通过这个教程了解信息安全并提高警惕！本教程仅限于教学使用，不得用于其他用途触犯法律，本人一概不负责，请知悉！如有侵权请告知删除。

免责声明：本文旨在传递更多市场信息，不构成任何投资建议和其他非法用途。文章仅代表作者观点，不代表手机电脑双黑客立场。以上文章之对于正确的用途，仅适用于学习