EECS 3482 Lab 5

Jonathan Baldwin

Chapter 1

Introduction to Linux Operating Systems Auditing

```
$ systemctl start auditd.service
$ cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
```

... many lines cut ...

```
type=USER_START msg=audit(1554077993.984:259): pid=3841 uid=0 auid=0 ses=7
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_open
 ↪  grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_sys
 ↪  acct="root" exe="/usr/sbin/sshd" hostname=gateway addr=10.0.2.2 terminal=ssh res=success'
type=CRYPTO_KEY_USER msg=audit(1554077993.990:260): pid=3845 uid=0 auid=0 ses=7
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=destroy kind=server
 ↪  fp=SHA256:f0:52:51:d8:eb:cf:25:aa:6f:2a:d3:36:32:5a:9b:77:aa:5d:0e:d1:3a:2d:f1:3c:a7:31:52:ea:24:41:ca
 ↪  direction=? spid=3845 suid=0  exe="/usr/sbin/sshd" hostname=localhost.localdomain addr=?
 ↪  terminal=pts/1 res=success'
```

```
type=CRYPTO_KEY_USER msg=audit(1554077993.990:261): pid=3845 uid=0 auid=0 ses=7
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=destroy kind=server
 ↪  fp=SHA256:d3:4a:e8:14:9c:55:93:5f:1f:1d:9d:f4:6e:d0:d9:ce:ad:61:76:5e:a0:05:da:97:c5:a4:49:df:62:41:e4
 ↪  direction=? spid=3845 suid=0  exe="/usr/sbin/sshd" hostname=localhost.localdomain addr=?
 ↪  terminal=pts/1 res=success'
type=CRYPTO_KEY_USER msg=audit(1554077993.990:262): pid=3845 uid=0 auid=0 ses=7
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=destroy kind=server
 ↪  fp=SHA256:f2:31:49:2b:89:50:6f:d6:2d:7b:e3:dd:6b:a6:a9:fb:7e:89:a6:ff:9f:12:7a:93:57:85:4b:d1:21:99:51
 ↪  direction=? spid=3845 suid=0  exe="/usr/sbin/sshd" hostname=localhost.localdomain addr=?
 ↪  terminal=pts/1 res=success'
type=USER_LOGIN msg=audit(1554077993.996:263): pid=3845 uid=0 auid=0 ses=7
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=login id=0
 ↪  exe="/usr/sbin/sshd" hostname=gateway addr=10.0.2.2 terminal=/dev/pts/1 res=success'
type=USER_START msg=audit(1554077993.998:264): pid=3845 uid=0 auid=0 ses=7
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=login id=0
 ↪  exe="/usr/sbin/sshd" hostname=gateway addr=10.0.2.2 terminal=/dev/pts/1 res=success'
type=CRED_REFR msg=audit(1554077994.001:265): pid=3845 uid=0 auid=0 ses=7
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
 ↪  grantors=pam_unix acct="root" exe="/usr/sbin/sshd" hostname=gateway addr=10.0.2.2
 ↪  terminal=ssh res=success'

$ auditctl
usage: auditctl [options]
    -a <l,a>            Append rule to end of <l>ist with <a>ction
    -A <l,a>            Add rule at beginning of <l>ist with <a>ction
    -b <backlog>        Set max number of outstanding audit buffers
                        allowed Default=64
    -c                  Continue through errors in rules
    -C f=f              Compare collected fields if available:
                        Field name, operator(=,!=), field name
    -d <l,a>            Delete rule from <l>ist with <a>ction
                        l=task,exit,user,exclude
                        a=never,always
    -D                  Delete all rules and watches
    -e [0..2]           Set enabled flag
    -f [0..2]           Set failure flag
                        0=silent 1=printk 2=panic
    -F f=v              Build rule: field name, operator(=,!=,<,>,<=,
                        >=,&,&=) value
    -h                  Help
    -i                  Ignore errors when reading rules from file
    -k <key>            Set filter key on audit rule
    -l                  List rules
    -m text             Send a user-space message
    -p [r|w|x|a]        Set permissions filter on watch
                        r=read, w=write, x=execute, a=attribute
    -q <mount,subtree>  make subtree part of mount point's dir watches
    -r <rate>           Set limit in messages/sec (0=none)
    -R <file>           read rules from file
    -s                  Report status
    -S syscall          Build rule: syscall name or number
    -t                  Trim directory watches
    -v                  Version
    -w <path>           Insert watch at <path>
    -W <path>           Remove watch at <path>
    --loginuid-immutable  Make loginuids unchangeable once set
```

```
    --reset-lost         Reset the lost record counter
$ auditctl -l
No rules
$ auditctl -a exit,always -F path=/etc/passwd -F perm=wa
$ auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Error sending add rule data request (Rule exists)
$ ausearch -f /etc/passwd
<no matches>
$ adduser xyz
$ ausearch -f /etc/passwd
----
time->Sun Mar 31 20:20:06 2019
type=PROCTITLE msg=audit(1554078006.323:268): proctitle=616464757365720078797A
type=PATH msg=audit(1554078006.323:268): item=0 name="/etc/passwd" inode=17609528 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554078006.323:268):  cwd="/root"
type=SYSCALL msg=audit(1554078006.323:268): arch=c000003e syscall=2 success=yes exit=5
 ↪  a0=55cd87f0cce0 a1=20902 a2=0 a3=8 items=1 ppid=3867 pid=3884 auid=0 uid=0 gid=0 euid=0
 ↪  suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=7 comm="adduser" exe="/usr/sbin/useradd"
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Sun Mar 31 20:20:06 2019
type=CONFIG_CHANGE msg=audit(1554078006.332:271): auid=0 ses=7 op=updated_rules
 ↪  path="/etc/passwd" key=(null) list=4 res=1
----
time->Sun Mar 31 20:20:06 2019
type=PROCTITLE msg=audit(1554078006.332:272): proctitle=616464757365720078797A
type=PATH msg=audit(1554078006.332:272): item=4 name="/etc/passwd" inode=17609550 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=3 name="/etc/passwd" inode=17609528 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=2 name="/etc/passwd+" inode=17609550 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=1 name="/etc/" inode=16777281 dev=fd:00
 ↪  mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=PARENT
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=0 name="/etc/" inode=16777281 dev=fd:00
 ↪  mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=PARENT
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554078006.332:272):  cwd="/root"
type=SYSCALL msg=audit(1554078006.332:272): arch=c000003e syscall=82 success=yes exit=0
 ↪  a0=7ffe48fc1200 a1=55cd87f0cce0 a2=7ffe48fc1170 a3=55cd8809ebf0 items=5 ppid=3867 pid=3884
 ↪  auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=7
 ↪  comm="adduser" exe="/usr/sbin/useradd"
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
$ grep -o 'syscall=\([0-9]*\)'
$ cut -d= -f2
$ xargs -l ausyscall
$ ausearch -f /etc/passwd
open
rename
$ dir /etc/passwd -l
```

```
-rw-r--r--. 1 root root 835 Mar 31 20:20 /etc/passwd
$ chmod 640 /etc/passwd
$ dir /etc/passwd -l
-rw-r-----. 1 root root 835 Mar 31 20:20 /etc/passwd
$ ausearch -f /etc/passwd
----
time->Sun Mar 31 20:20:06 2019
type=PROCTITLE msg=audit(1554078006.323:268): proctitle=616464757365720078797A
type=PATH msg=audit(1554078006.323:268): item=0 name="/etc/passwd" inode=17609528 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554078006.323:268):  cwd="/root"
type=SYSCALL msg=audit(1554078006.323:268): arch=c000003e syscall=2 success=yes exit=5
 ↪  a0=55cd87f0cce0 a1=20902 a2=0 a3=8 items=1 ppid=3867 pid=3884 auid=0 uid=0 gid=0 euid=0
 ↪  suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=7 comm="adduser" exe="/usr/sbin/useradd"
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Sun Mar 31 20:20:06 2019
type=CONFIG_CHANGE msg=audit(1554078006.332:271): auid=0 ses=7 op=updated_rules
 ↪  path="/etc/passwd" key=(null) list=4 res=1
----
time->Sun Mar 31 20:20:06 2019
type=PROCTITLE msg=audit(1554078006.332:272): proctitle=616464757365720078797A
type=PATH msg=audit(1554078006.332:272): item=4 name="/etc/passwd" inode=17609550 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=3 name="/etc/passwd" inode=17609528 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=2 name="/etc/passwd+" inode=17609550 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=1 name="/etc/" inode=16777281 dev=fd:00
 ↪  mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=PARENT
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554078006.332:272): item=0 name="/etc/" inode=16777281 dev=fd:00
 ↪  mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=PARENT
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554078006.332:272):  cwd="/root"
type=SYSCALL msg=audit(1554078006.332:272): arch=c000003e syscall=82 success=yes exit=0
 ↪  a0=7ffe48fc1200 a1=55cd87f0cce0 a2=7ffe48fc1170 a3=55cd8809ebf0 items=5 ppid=3867 pid=3884
 ↪  auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=7
 ↪  comm="adduser" exe="/usr/sbin/useradd"
 ↪  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Sun Mar 31 20:20:06 2019
type=PROCTITLE msg=audit(1554078006.365:274):
 ↪  proctitle=63686D6F6400363430002F6574632F706173737764
type=PATH msg=audit(1554078006.365:274): item=0 name="/etc/passwd" inode=17609550 dev=fd:00
 ↪  mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL
 ↪  cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554078006.365:274):  cwd="/root"
type=SYSCALL msg=audit(1554078006.365:274): arch=c000003e syscall=268 success=yes exit=0
 ↪  a0=ffffffffffffff9c a1=1d880f0 a2=1a0 a3=7fffaa3be3e0 items=1 ppid=3867 pid=3897 auid=0
 ↪  uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=7 comm="chmod"
 ↪  exe="/usr/bin/chmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
```

```
$ grep -o 'comm=[^ ]*'
$ cut '-d"' -f2
$ ausearch -f /etc/passwd
adduser
adduser
chmod
$ ausearch -f /etc/passwd
$ aureport -f -i

File Report
===============================================
# date time file syscall success exe auid event
===============================================
1. 31/03/19 20:20:06 /etc/passwd open yes /usr/sbin/useradd root 268
2. 31/03/19 20:20:06 /etc/passwd ? yes ? root 271
3. 31/03/19 20:20:06 /etc/passwd rename yes /usr/sbin/useradd root 272
4. 31/03/19 20:20:06 /etc/passwd fchmodat yes /usr/bin/chmod root 274
$ ausearch -m LOGIN --start today -i
----
type=LOGIN msg=audit(31/03/19 20:07:08.116:87) : pid=2737 uid=root
 ↪  subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=tty1
 ↪  old-ses=4294967295 ses=1 res=yes
----
type=LOGIN msg=audit(31/03/19 20:07:26.460:103) : pid=12969 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=2 res=yes
----
type=LOGIN msg=audit(31/03/19 20:12:13.332:86) : pid=2725 uid=root
 ↪  subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=tty1
 ↪  old-ses=4294967295 ses=1 res=yes
----
type=LOGIN msg=audit(31/03/19 20:12:50.881:122) : pid=3750 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=2 res=yes
----
type=LOGIN msg=audit(31/03/19 20:17:09.394:143) : pid=3775 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=3 res=yes
----
type=LOGIN msg=audit(31/03/19 20:18:10.341:171) : pid=3795 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=4 res=yes
----
type=LOGIN msg=audit(31/03/19 20:18:43.497:200) : pid=3805 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=5 res=yes
----
type=LOGIN msg=audit(31/03/19 20:19:29.808:228) : pid=3831 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=6 res=yes
----
type=LOGIN msg=audit(31/03/19 20:19:53.847:257) : pid=3841 uid=root
 ↪  subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none)
 ↪  old-ses=4294967295 ses=7 res=yes
```

Chapter 2

Introduction to Snort IDSs Rules

1. Direction of Traffic (<–>, ->, <-)
   - The `->` symbol is used to indicate traffic from internal network to external network.
   - The `<>` symbol is used to indicate bidirectional traffic between internal and external networks.
   - The `<>` symbol is used to indicate traffic from external to internal networks.
2. Setup of Network Addresses (HOME_NET, EXTERNAL_NET, and ipvar)
   - Declare all hosts in the internal network: `ipvar HOME_NET 192.168.1.0/24`
   - Declare all hosts in the external network: `ipvar EXTERNAL_NET !HOME_NET`
   - Declare the variable net100 for the 192.168.1.0, class C subnet and the and the 10.1.1.0, class A subnet: `ipvar net100 [192.168.1.0/24, 10.1.1.0/8]`
   - Declare clientA as IP list that has two IPs:192.168.0.1 and 10.0.1.1: `ipvar clientA [192.168.0.1,10.0.1.1]`
3. Declare internal servers
   - Declare all of the web servers of your network: (HTTP_SERVERS, HOME_NET): `ipvar HTTP_SERVERS HOME_NET`
   - Declare all E-mail servers of your network: `ipvar SMTP_SERVERS [192.168.1.32,192.168.1.33]`
   - Declare all of DNS servers of your network: `ipvar DNS_SERVERS 192.168.1.1`
   - Declare all of secure shell servers of your network: `ipvar SSH_SERVERS HOME_NET`
   - Declare all of file servers of your network: `ipvar FTP_SERVERS HOME_NET`
   - Declare all IP telephony servers of your network: `ipvar SIP_SERVERS 192.168.1.64`
4. Declaring Ports
   - Specify list port numbers that web servers are run on: `portvar HTTP_PORTS [80,443,8080]`
   - Specify list of all ports that of type SHELLCODE except the http port: `portvar SHELLCODE !HTTP_PORTS`
   - Specify List of ports you want to look for SSH connection on: `portvar SSH_PORTS [22,2222]`
   - Specify the ports variable: `well_known` with the rang of port number 0 through 1024: `portvar well_known [0:1024]`
5. Simple Rules (Notice that content rules are case sensitive unless you use the "nocase" option)
   - Write a rule that alerts for any tcp traffic from any external network to any internal network (use action as alert, source IP as any, source port number as any, destination IP as any, destination port as HTTP port number, and the payload is has a HEAD, PUT, POST, or Delete but not !GET: `alert tcp any any -> any 80 (content: !"GET";)`
   - Write a rule that alerts with the message "Backdoor signature was detected – Subseven Trojan", where traffic is directed from the external network to external network, the signature value/payload is "|0d0a5b52504c5d30303 and the reference number for the vulnerability is arachnids,485: `alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "Backdoor signature was detected - Subseven Trojan";content: "|0d0a5b52504c5d3030320d0a|"; reference: arachnids,485)`
   - Use the "bidirectional operator" and the "log" action command to record both sides of telnet sessions directed to from any network and port (except to from 192.168.0.1/24) to 192.168.1.0/24 subnet at port 23: `log tcp !192.168.1.0/24 any <> 192.168.1.0/24 23 (msg:"TELNET")`