Website Monitoring with Auditd

Setting up Auditd for custom file monitoring

Type of Systems: Linux based web server
Complete Goal: Monitor website files for changes

Relevant Info:

- Temporary watches and rules can be added using the `auditctl` command, with the same arguments and syntax as in the audit.rules file
- Auditd also monitors some system information and events by default, even when there are no rules listed.
- In the file watch command `-p` specifies which types of file usage to monitor:
    - `r` is read
    - `w` is write
    - `x` is execute
    - `a` is attribute changes

Steps:

1. Acquire command line access to the server (with sudo), whether direct or through ssh.
2. Install/update Auditd:
    a. For Debian based distros:
        i. `sudo apt-get update` to update the package lists
        ii. `sudo apt-get install auditd` to install `auditd`
    b. For RHEL based distros:
        i. `sudo yum install audit audit-libs` to install auditd
3. Configure Auditd to start at boot and then start it with
    a. `sudo systemctl enable auditd`
    b. `sudo systemctl start auditd`
4. Check default rules:
    a. `sudo auditd -l` to list all current rules
    b. If the rule “-a never, task” is listed, it needs to be removed as it will override our rules: delete it with `sudo auditctl -d never, task`
    c. The list should now say ‘No Rules’
5. Adding custom file watching rules:
    a. All permanent rules need to be added to `/etc/audit/audit.rules`. To do this:

   i. Locate the website's html file directory. They are often in `/var/www/html`, so that's what we'll use here.
   ii. Enter the rules file with `sudo nano /etc/audit/audit.rules`
   iii. Add a custom directory watch at the bottom of the file by adding a line: `-w /var/www/html -p wa -k mysite` (mysite is simply the key to find these logs in the log files, so it can be whatever you want)
   iv. Write out and quit with Ctrl O and Ctrl X
   v. Restart auditd with `sudo systemctl restart auditd`
6. Testing out the watch:
   a. Check that your rules are loaded with `auditctl -l` (it should show the rules)
   b. Add a file to the html directory, or change an existing file(remember that the site might be live)
   c. Check the auditd report by either limiting to the key, or limiting the report to files:
      i. `sudo aureport -f` limits the report to file logs only
      ii. `sudo ausearch -k mysite` searches for the given key

Appendix:

Example Rules (they go in /etc/audit/audit.rules)
See https://gist.github.com/Neo23x0/9fe88c0c5979e017a389b90fd19ddfee for more

Watch your binaries
-w /bin -p wa -k binaries
-w /usr/bin -p wa -k binaries
-w /usr/local/bin -p wa -k binaries

Watch etc files for modification
-w /etc -p wa -k etc_files

Watch shadow for reading
-w /etc/shadow -p r -k shadow

Watch for changing password
-w /usr/bin/passwd -p x -k passwd_modification

Watch for use of the curl command

-w /usr/bin/curl -p x -k curl_used

Use With Filebeat

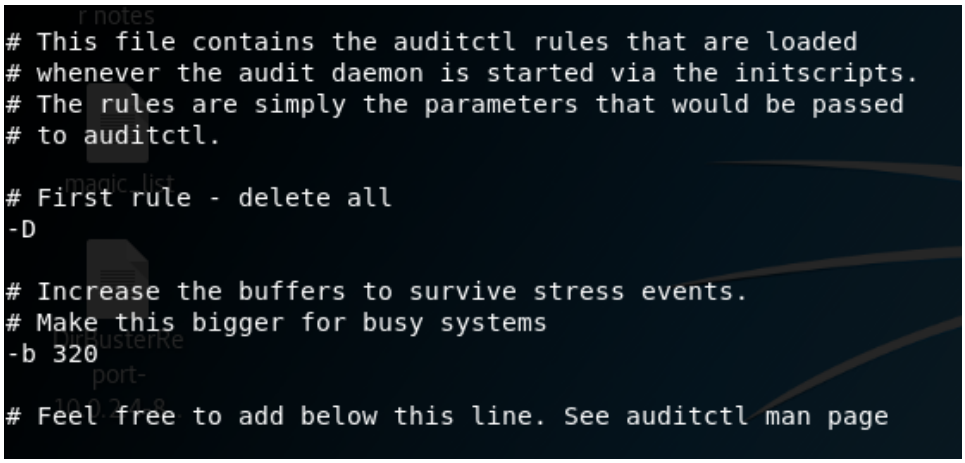
Filebeat has a module that will ingest auditd logs, populate them with elasticsearch fields, and update them to your elasticsearch database. The module is called “auditd”. With a default filebeat install, you can enable the module by moving the file “/etc/filebeat/modules.d/auditd.yml.disabled” to “/etc/filebeat/modules.d/auditd.yml”.

Sources

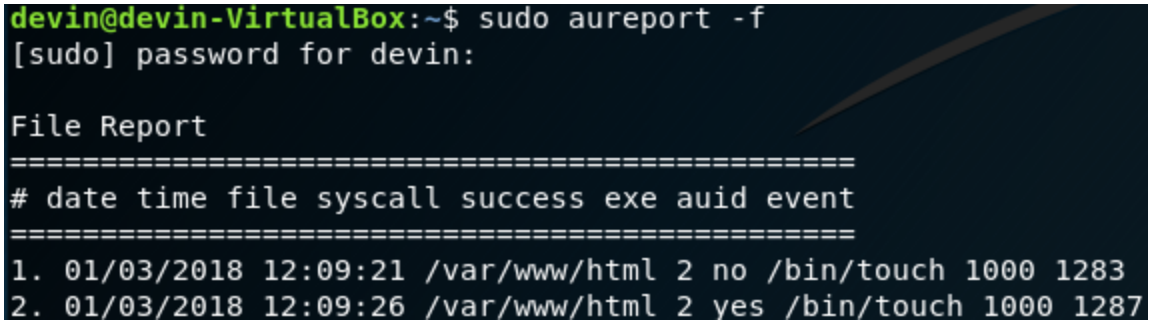
- Digital Ocean CentOS Audit Guide
- Linux System Monitoring with Audit

Screenshots

Default audit.rules file:



Sample aureport output:



Sample of ausearch output:

```
devin@devin-VirtualBox:~$ sudo ausearch -k mysite
[sudo] password for devin:
----
time->Tue Jan  2 15:26:38 2018
type=CONFIG_CHANGE msg=audit(1514924798.160:842): auid=1000 ses=33 op=add_rule key="mysite" list=4 res=1
----
time->Wed Jan  3 11:46:09 2018
type=CONFIG_CHANGE msg=audit(1514997969.945:1217): auid=4294967295 ses=4294967295 op=remove_rule key="mysite"
 list=4 res=1
----
time->Wed Jan  3 12:09:21 2018
type=PROCTITLE msg=audit(1514999361.779:1283): proctitle=746F75636800666F6F
type=PATH msg=audit(1514999361.779:1283): item=0 name="/var/www/html" inode=180615 dev=08:01 mode=040755 ouid
=0 ogid=0 rdev=00:00 nametype=PARENT
type=CWD msg=audit(1514999361.779:1283): cwd="/var/www/html"
type=SYSCALL msg=audit(1514999361.779:1283): arch=c000003e syscall=2 success=no exit=-13 a0=7fff894da81c a1=9
41 a2=1b6 a3=69d items=1 ppid=6404 pid=10706 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=
1000 sgid=1000 fsgid=1000 tty=pts8 ses=33 comm="touch" exe="/bin/touch" key="mysite"
----
time->Wed Jan  3 12:09:26 2018
type=PROCTITLE msg=audit(1514999366.715:1287): proctitle=746F75636800666F6F
type=PATH msg=audit(1514999366.715:1287): item=1 name="foo" inode=133187 dev=08:01 mode=0100644 ouid=0 ogid=0
 rdev=00:00 nametype=CREATE
type=PATH msg=audit(1514999366.715:1287): item=0 name="/var/www/html" inode=180615 dev=08:01 mode=040755 ouid
=0 ogid=0 rdev=00:00 nametype=PARENT
type=CWD msg=audit(1514999366.715:1287): cwd="/var/www/html"
type=SYSCALL msg=audit(1514999366.715:1287): arch=c000003e syscall=2 success=yes exit=3 a0=7ffcda577946 a1=94
1 a2=1b6 a3=69d items=2 ppid=10707 pid=10708 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts8 ses=33 comm="touch" exe="/bin/touch" key="mysite"
```