Linux Security

Auditd

- Extended logging based on auditd rules

```
auditctl            # configure rules
auditsearch         # search for events
auditreport         # create report

/etc/audit/rules.d/audit.rules
/etc/audit/auditd.conf

auditctl -w path_to_file -p permissions -k key_name
# or in rules file:
-w path_to_file -p permissions -k key_name

sudo ausearch -i -k user-modify
```

```
# basic audit system parameters
-D
-b 8192
-f 1
-e 1

# some file and directory watches with keys
-w /var/log/audit/ -k LOG_audit
-w /etc/audit/auditd.conf -k CFG_audit_conf -p rxwa
-w /etc/audit/audit.rules -k CFG_audit_rules -p rxwa

-w /etc/passwd -k CFG_passwd -p rwxa
-w /etc/sysconfig/ -k CFG_sysconfig
# an example system call rule
-a entry,always -S umask
```