

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

Sysmon for linux

- Linux port of sysmon
- Uses eBPF instead of kernel hooks
 - extended Berkley Packet Filter
- Creates events instead of log entries (?)

```
sudo ./sysmon -accepteula
sudo ./sysmon -i

systemctl status sysmon
```

all_in_one.xml

```
all-in-one.xml
<Sysmon schemaversion="4.70">
  <EventFiltering>
    <!-- Event ID 1 == ProcessCreate. Log all newly created
processes -->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="" exclude=""/>
    </RuleGroup>
    <!-- Event ID 3 == NetworkConnect Detected. Log all network
connections -->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="" exclude=""/>
    </RuleGroup>
    <!-- Event ID 5 == ProcessTerminate. Log all processes
terminated -->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="" exclude=""/>
    </RuleGroup>
    <!-- Event ID 9 == RawAccessRead. Log all raw access read -->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="" exclude=""/>
    </RuleGroup>
    <!-- Event ID 10 == ProcessAccess. Log all open process
operations -->
    <RuleGroup name="" groupRelation="or">
      <ProcessAccess onmatch="" exclude=""/>
    </RuleGroup>
    <!-- Event ID 11 == FileCreate. Log every file creation -->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="" exclude=""/>
    </RuleGroup>
    <!--Event ID 23 == FileDelete. Log all files being deleted -->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="" exclude=""/>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

```
sudo ./sysmon -c all-in-one.xml
```

```
sudo tail -f /var/log/syslog | sudo /opt/sysmon/sysmonLogView
```