SAMHAIN

What is Samhain?

- The Samhain host-based intrusion detection system (HIDS) provides **file integrity checking** and **log file monitoring/analysis**, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes.
- Samhain been designed to monitor multiple hosts with potentially different operating systems, providing **centralized logging and maintenance**, although it can also be used as standalone application on a single host.
- Samhain is an open-source multiplatform application for POSIX systems (Unix, Linux, Cygwin/Windows).

Centralized Management

- Samhain can be used standalone on a single host, but its particular strength is centralized monitoring and management. The complete management of a samhain system can be done from one central location. To this end, several components are required. A full samhain client/server system is built of the following components:
  - The samhain file/host integrity checker
  - The yule log server
  - A relational database
  - The Beltane web-based console
  - The deployment system

Host Integrity Monitoring

- Samhain is extensible by modules that can be compiled in at the users' discretion. The following list shows which modules are currently available.
  - Logfile monitoring/analysis
  - Windows registry check
  - Kernel integrity
  - SUID/SGID files
  - Open ports
  - Process check
  - Mount check
  - Login/logoff events

Log Facilities

- The verbosity and on/off status of each log facility can be configured individually.
  - Central log server. Messages are sent via encrypted TCP connections. Clients need to authenticate to the server.
  - Syslog.
  - Console (if daemon) / stderr.
  - Log file. To prevent unauthorized modifications of existing log records, the log file entries are signed.
  - E-mail (built-in mailer). E-mail reports are signed to prevent tampering. It is possible to configure different filters for different recipients.
  - Database (currently MySQL, PostgreSQL, and Oracle are supported; support for unixODBC is
  - untested).
  - Execute external program - this can be used to implement arbitrary additional logging facilities, or to perform active response to events.

Running Samhain

Configure:

```
sh$ ./configure
```

Compile:

```
sh$ make
```

Install:

```
sh$ make install
```

Customize:

```
sh$ vi /etc/samhainrc
```

Initialize the baseline database:

```
sh$ samhain -t init
```

Start the samhain daemon:

```
sh$ samhain -t check -D
```

```
samhain has been configured as follows:
    System binaries: /usr/local/sbin
 Configuration file: /etc/samhainrc
      Manual pages: /usr/local/man
    Data directory: /var/lib/samhain
     Database file: /var/lib/samhain/samhain_file
          PID file: /run/samhain.pid
          Log file: /var/log/samhain_log
          Base key: 725456810,698389996
```

```
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<d:   6, -:   0, l:   0, |:   0, s:   0,
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/linux_x86-64>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/linux_x86-64/remote>
INFO   :  [2019-10-01T23:06:26-0400] msg=<d:   2, -:   3, l:   0, |:   0, s:   0,
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/linux_x86-64/local>
INFO   :  [2019-10-01T23:06:26-0400] msg=<d:   2, -:  20, l:   0, |:   0, s:   0,
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/linux_x86-64/dos>
INFO   :  [2019-10-01T23:06:26-0400] msg=<d:   2, -:   7, l:   0, |:   0, s:   0,
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<d:   5, -:   0, l:   0, |:   0, s:   0,
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/php>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/php/remote>
INFO   :  [2019-10-01T23:06:26-0400] msg=<d:   2, -: 199, l:   0, |:   0, s:   0,
 c:   0, b:   0>
INFO   :  [2019-10-01T23:06:26-0400] msg=<Checking      [ReadOnly]>, path=</usr/
share/exploitdb/exploits/php/webapps>
```