KIT
Karlsruher Institut für Technologie

Samhain

Ursula Epting

egi CSIRT

STEINBUCH CENTRE FOR COMPUTING - SCC

Samhain

Samhain – (similar e.g. Tripwire, …)

- File integrity / host-based intrusion detection system
- Info at http://www.la-samhna.de/samhain/
- Server/Client – standalone
- Beltane - web console

Samhain

- New installed system
- Install Samhain
- Configure Samhain
- Initialize Database
- Get noticed about modifications on file system

Samhain Installation – Standalone Example (1)

-
  ```
  # ./configure
  --with-gpg=/usr/bin/gpg
  --with-checksum="/usr/bin/gpg:
  C2B10A7D 417103C1
  BCAADEB6  3ADFB3FD
  352B6A78 D0804809"
  --with-fp="91F6 8331 C03C
  9E31 C267  4D07 AB87 80D5
  8AFE ED81"
  --enable-static
  --enable-install-name=phantasy
  --enable-micro-stealth=414
  --enable-login-watch
  --enable-suidcheck &&make
  ```
- make install; make boot

- with gpg support,
- checksum of gpg-binary => no modification of gpg possible
- Fingerprint of Admin gpg-Key => Key can not be modified, signs configuration file and database
- Use static binary not linked to shared libraries
- Use name 'phantasy' instead of 'samhain'

Samhain Installation – Standalone Example (2)

-
  ```
  # ./configure
  --with-gpg=/usr/bin/gpg
  --with-checksum="/usr/bin/gpg:
  C2B10A7D 417103C1
  BCAADEB6  3ADFB3FD
  352B6A78 D0804809"
  --with-fp="91F6 8331 C03C
  9E31 C267  4D07 AB87 80D5
  8AFE ED81"
  --enable-static
  --enable-install-name=phantasy
  --enable-micro-stealth=129
  --enable-login-watch
  --enable-suidcheck &&make
  ```
- make install; make boot

- replace all strings 'samhain' in the binary with 129 - no strings|grep samhain possible – black hat won't find samhain easily
- Monitor all login/logout events
- Monitor suid/guid files
- Install and start at boot

Samhain – File-Signature

- A 192-bit cryptographic checksum computed using the TIGER hash algorithm (alternatively SHA-1 or MD5 can be used)
- Inode, type, owner and group, access permissions
- On Linux only: flags of the ext2 file system (see man chattr)
- Timestamps (ctime, mtime, atime ~ change/modify/access)
- File size, number of hard links
- Minor and major device number
- Name of linked file (for symbolic links)

Samhain – Policies

- ReadOnly – All changes reported except access time
- Attributes - Only modifications of ownership, access permissions, and device number will be checked
- IgnoreAll - No modifications will be reported
- IgnoreNone - All modifications, including access time, but excluding ctime, will be reported
- Logfiles - Modifications of timestamps, file size, and signature will be ignored
- GrowingLogFiles - Modifications of timestamps, and signature will be ignored. Modification of the file size will only be ignored if the file size has increased.

Samhain - Log levels

Level	Significance
None	Not logged.
Debug	Debugging-level messages.
Info	Informational messages.
Notice	Normal conditions.
Warn	Warning conditions.
Mark	Timestamps.
Err	Error conditions.
Crit	Critical conditions.
Alert	Program startup/normal exit, or fatal error, causing abnormal program termination.

Samhain – assign severity to policy violations

```
[EventSeverity]
 #
 # these are policies
 #
SeverityReadOnly=crit
SeverityLogFiles=crit
SeverityGrowingLogs=warn
SeverityIgnoreNone=crit
SeverityIgnoreAll=info
```

Example report

```
-----BEGIN MESSAGE-----
[2010-08-26T01:18:46+0200] host-kit.gridka.de
CRIT   :  [2010-08-26T01:00:20+0200] msg=<POLICY
[ReadOnly] --------T->, path=</etc/shadow>, ctime_old=<[2010-
08-25T20:03:04]>, ctime_new=<[2010-08-25T22:03:06]>,
mtime_old=<[2010-08-25T20:03:04]>, mtime_new=<[2010-08-
25T22:03:06]>,
CRIT   :  [2010-08-26T00:53:20+0200] msg=<Login>,
name=<freddy>, tty=<pts/10>, host=<hostname.ou.edu>,
ip=<129.15.30.146>, time=<[2010-08-26T00:53:20+0200]>,
status=<1>
-----BEGIN SIGNATURE-----
088FE65E173C4859124B5617BE2B7FE1019C7EAD20FC253
5000008 1282723041::host-kit.gridka.de
-----END MESSAGE-----
```

End

- Questions?

Link

- http://www.la-samhna.de/samhain/