Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

Studiengang Kommunikationsinformatik
Prof. Dr.–Ing. Damian Weber

Systemmanagement und Sicherheit

8. Übung

Aufgabe 1 (syslog)

Verifizieren Sie, dass der `syslogd` auf dem Ihnen zugeordneten `play`–Rechner aktiv ist.

Verifizieren Sie, dass der `syslogd` beim Bootvorgang gestartet werden darf (`/etc/rc.conf` oder `/etc/default/rc.conf`).

Kontrollieren Sie die Abhängigkeiten bzgl. der Startreihenfolge innerhalb des Startskripts von `syslogd`. Benutzen Sie hierbei das `grep`–Kommando um Skripts zu finden, die vor oder nach `syslogd` gestartet werden.

Verifizieren Sie mit Hilfe des `ps`–Kommandos, dass der `syslogd` keine Meldung über das Netzwerk empfangen darf.

Entnehmen Sie die für netzwerkweite Systemmeldungen notwendige Option der Manualpage und erlauben Sie dem gesamten `play`–Rechnernetz Nachrichten an Ihren `syslogd` zu senden. Hierfür muss die Variable `syslogd_flags` innerhalb `/etc/rc.conf` neu gesetzt und `syslogd` neu gestartet werden.

Schreiben Sie ein C–Programm *syslogger*, das drei Kommandozeilenparameter erhält:

- eine Facility (`auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, mark, news, ntp, security, syslog, user, uucp, local0, ..., local7`)
- eine Priority (`emerg, alert, err, warning, notice, info, debug`) und
- einen Meldungstext.

Das Programm *syslogger* soll den angegebenen Text mit der gegebenen Facility und Priority an den `syslogd` senden und die Option setzen, dass die `PID` des Prozesses ebenfalls in der Logdatei erscheint.

Beispiel:

```
$ ./syslogger kern warning "Warnung innerhalb Kernel"
```

sollte zu einer Meldung wie

```
Jun  30 12:10:49 play5 syslogger[1655]: Warnung innerhalb Kernel
```

führen. Erweitern Sie die `/etc/syslog.conf`–Datei, damit Sie die Korrektheit Ihres Programms anhand von Facility und Priority testen können. Dies kann zum Beispiel dadurch geschehen, dass Sie für eine bestimmte Facility alle Prioritäten und für eine bestimmte Priority einige Facilities trennen (d.h. in verschiedene Logdateien umleiten).

Verifizieren Sie, dass `syslogd` keine Meldungen schreibt, wenn die angegebene Zieldatei nicht existiert.

Erzeugen Sie eine neue Datei `/var/log/local1` und weisen Sie den syslog–Daemon an, diese Datei für `local1`–Messages zu verwenden.

Bitten Sie ein anderes Team, seine `/etc/syslog.conf` Datei so einzurichten, daß Ihr `syslogd` Nachrichten des fremden Systems empfängt.

Aufgabe 2 (Security Event Auditing)

Befolgen Sie die Schritte im Abschnitt *Security Event Auditing* des FreeBSD-Handbuchs, um auf dem `play`–Rechner das Audit–Subsystem einzuschalten.

Hinweise:

- dies ist nur in der englischsprachigen Anleitung beschrieben
- hierfür muss der Kernel neu compiliert werden.