htw saar

Studiengang Kommunikationsinformatik
Prof. Dr.–Ing. Damian Weber
Dipl.-Inf. Marion Bohr
Sarah Theobald, M.Sc.

Systemmanagement und Sicherheit

8. Übung

Aufgabe 1 (syslog)

Diese Aufgabe soll in der experimentellen `play`–Umgebung bearbeitet werden.
Der System–Logging Daemon wird Teil einer der nächsten Vorlesungen sein. Lesen Sie

`http://www.freebsd.org/doc/en/books/handbook/configtuning-syslog.html`

Schreiben Sie mit dem logger Shell–Utility eine Meldung in `/var/log/messages`. Siehe Manualpage `logger(1)`.
Verifizieren Sie, dass der System Logging Daemon `syslogd` aktiv ist.
Verifizieren Sie, dass der `syslogd` beim Bootvorgang gestartet werden darf (siehe `/etc/rc.conf` oder `/etc/defaults/rc.conf`).
Kontrollieren Sie die Abhängigkeiten bzgl. der Startreihenfolge innerhalb des Startskripts `/etc/rc.d/syslogd` 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 (Parameter mit denen syslogd gestartet wurde?)..
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 play05 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 (dig)

Diese Aufgabe kann auf dem normalen Useraccount im ISL bearbeitet werden.

Finden Sie mit Hilfe des Kommandozeilen–Tools `dig` heraus

a) wie die Nameserver heißen, die die Domain `bundestag.de` verwalten

b) wie die Mailserver der Domain `bundestag.de` heißen

c) welchen Namen der Rechner mit der IP `77.87.229.26` hat

Webrecherche: Finden Sie heraus, an welchem Standort die Firma angesiedelt ist, die den Nameservice für `bundestag.de` betreibt.

Verifizieren Sie mittels `http://www.iplocation.net/` den Serverstandort des DNS-Servers für die Domain `bundestag.de`.