Betriebssystem UNIX - Systemadministration und Sicherheit
2.Praktikum (13.11.2013)

Im Praktikumspool sind auf den Rechner die Betriebssysteme SuSE 11.4, Debian, Ubuntu, OpenBSD bzw. Solaris installiert. Es sollen Init-Scripte erstellt werden, die beim Wechsel in den Systemstatus 3 und 5 abgearbeitet werden. Beachten Sie, dass bei SuSE die Init-Scripte parallel gestartet werden (startpar, insserv, .depend.start,...). Fügen Sie Ihre Scripte in diesen Startmechanismus ein.

1. Schreiben Sie ein Init-Script, das Datum und Uhrzeit in ein File /var/log/datum schreibt (anhängen).
2. Schreiben Sie ein Script für eines der folgenden Probleme:

   a) Die lokalen Dateisysteme (aller Partitionen) sollen auf Veränderungen hinsichtlich der installierten Programme mit s-Bit und root-Eigentümer untersucht werden. Die erkannten Veränderungen sollen in der Protokoll-Datei „/var/log/changes-yyyymmdd-hhmmss“ aufgelistet werden. Dabei ist „yyyymmdd-hhmmss“ durch eine Datums- und Uhrzeitangaben zu ersetzen, die dem Startzeitpunkt des Scripts entspricht.

   b) Nach dem kompletten Hochfahren des Systems (letzter Dienst) soll geprüft werden, welche Ports geöffnet sind. Relevant sind hier „TCP Listen“ und „UDP“. Erstellen Sie eine sortierte Liste, in der identische Einträge nur genau einmal erscheinen und vergleichen Sie diese mit dem Resultat vom letzten Mal. Im Falle von Änderungen soll ein File /var/log/netstat-yyyymmdd-hhmmss mit den Änderungen erzeugt werden.

   Das Kommando „netstat“ gibt Auskunft über offene Ports. Informieren Sie sich in den Man-Pages über das konkrete Aufrufformat. Weitere nützliche Kommandos sind bspw. „grep“, „grep –v“, „awk –F; ‘/foo/{print $4}‘, „sort –n“, „uniq“.

b.w.

c) Welche Prozesse laufen nach dem kompletten Hochfahren? Sortieren Sie diese nach dem Namen und bestimmen Sie die Anzahl der Prozesse. Vergleichen Sie die Ergebnisse mit dem letzten Resultat. Eventuelle Änderungen sollen in ein File /var/log/prozesse-yyyymmdd-nnmmss gespeichert werden.

3. Wahlweise, nur für SuSE 12.x. Erweitern Sie den Startmechanismus Ihrer Scripte (1, 2a, 2b) so, dass das Script nicht beendet wird und eine Überwachung jeweils nach 15 Minuten wiederholt wird (Zyklus im Script, sleep). Realisieren Sie dabei, dass das Script nach einem Absturz automatisch sofort wieder gestartet wird und der Test sofort wieder neu ausgeführt wird (systemd, systemctl, /etc/systemd/system/????.service).
4. In Anwesenheitsliste eintragen.