10.9 Praktische Aufgaben

10.9.1 Tripwire

1. Laden Sie sich das RPM Paket für Red Hat 7.x von `http://www.tripwire.org/` herunter und installieren Sie es, nachdem Sie überprüft haben, das das Programm `siggen` auf Ihrem Rechner existiert.
2. Ändern Sie das mitgelieferte Policyfile so ab, daß
   - die Verzeichnisse von Tripwire definiert sind,
   - Sie auf Ihrem Rechner nur `/etc` überwachen
   - die Wertigkeiten der zu überwachenden Files und Verzeichnisse festgelegt sind,
   - die Tripwire-Binaries überwacht werden,
   - die Tripwire-Konfigurationsfiles überwacht werden

   und generieren Sie das von Tripwire einzulesende Policyfile.
3. Initialisieren Sie die Datenbank mit dem derzeitig gültigen Stand.
4. Ändern Sie eines der in `/etc/` beheimateten Konfigurationsfiles ab, fügen Sie ein Testfile innerhalb eines Unterverzeichnisses von `/etc` hinzu. Starten Sie nun einen Integritätscheck. Was sehen Sie?
5. Der so erzeugte Stand soll anhand des erzeugten Berichtes als Ist-Stand in die Integritätsdatenbank aufgenommen werden.
6. Machen Sie die vorher gemachten Änderungen rückgängig und ändern Sie die Datenbank anhand eines interaktiven Integritätschecks.

10.9.2 Snort

1. Installieren Sie Snort über YaST2.
2. Lassen Sie die Defaultkonfiguration unverändert und starten Sie Snort über das Startskript.
3. Lassen Sie von Ihrem Partnerrechner einen Nmap auf Ihre Maschine laufen. Was sehen Sie in den Logfiles?
4. Lassen Sie einen Nessusscan auf Ihre Maschine laufen. Was sehen Sie in den Logfiles?