MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München

Prof. Dr. D. Kranzlmüller
Dr. N. gentschen Felde

Praktikum IT-Sicherheit
Übungsblatt 09

22. **Tripwire/Samhain**

(a) Installieren Sie Tripwire (siehe auch `http://sourceforge.net/projects/tripwire/`) bzw. seinen Nachfolger Samhain, nachdem Sie überprüft haben, dass das Programm „*siggen*“ (auch erhältlich unter `http://sourceforge.net/projects/siggen/`) auf Ihrem Rechner existiert.

(b) Ändern Sie das mitgelieferte Policyfile so ab, dass...

- die Verzeichnisse von Tripwire/Samhain definiert sind,
- Sie auf Ihrem Rechner nur das Verzeichnis `/etc` überwachen,
- die Wertigkeiten der zu überwachenden Files und Verzeichnisse festgelegt sind,
- die Tripwire- bzw. Samhain-Binaries überwacht werden und
- die Tripwire- bzw. Samhain-Konfigurationsfiles überwacht werden

und generieren Sie das von Tripwire/Samhain einzulesende Policyfile.

(c) Initialisieren Sie die Datenbank mit dem nun gültigen Stand.

(d) 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?

(e) Der so erzeugte Stand soll anhand des erzeugten Berichtes als Ist-Stand in die Integritätsdatenbank aufgenommen werden.

(f) Machen Sie die vorher gemachten Änderungen rückgängig und ändern Sie die Datenbank anhand eines interaktiven Integritätschecks.

23. **Snort**

(a) Installieren Sie Snort auf allen Ihnen zur Verfügung stehenden Rechnern im Praktikumsnetz.

(b) Erstellen Sie eine Snort-Testregel, die jedes eingehende ICMP-Paket protokolliert. Provozieren Sie einen Eintrag in Ihren Log-Dateien, der durch die gerade erstellte Regel verursacht wird und deaktivieren Sie die Testregel wieder.

(c) Fügen Sie in der Standardkonfiguration einen Eintrag hinzu, so dass Portscans ihres Rechners als Ziel protokolliert werden und starten Sie Snort über das Startskript. Tragen Sie zusätzlich Snort als zu startenden Dienst für die Runlevel 2, 3 und 5 ein.

(d) Lassen Sie von Ihrem Partnerrechner einen Portscan auf Ihre Maschine laufen. Was sehen Sie in den Logfiles?

(e) Lassen Sie einen Nessusscan auf Ihre Maschine laufen. Was sehen Sie in den Logfiles?