MNM

TEAM _______ Munich Network Management Team

Ludwig-Maximilians-Universität München und Technische Universität München Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit Übungsblatt 10

23. Tripwire

- (a) Laden Sie sich ein Installations-Paket für Tripwire von http:// sourceforge.net/projects/tripwire/ herunter und installieren Sie es, nachdem Sie überprüft haben, dass das Programm "siggen" (erhältlich unter http://sourceforge.net/projects/siggen/) auf Ihrem Rechner existiert.
- (b) Ändern Sie das mitgelieferte Policyfile so ab, das
 - 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.

- (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.

24. **Snort**

- (a) Installieren Sie Snort über YaST.
- (b) Lassen Sie die Defaultkonfiguration unverändert und starten Sie Snort über das Startskript.
- (c) Lassen Sie von Ihrem Partnerrechner einen Nmap auf Ihre Maschine laufen. Was sehen Sie in den Logfiles?
- (d) Lassen Sie einen Nessusscan auf Ihre Maschine laufen. Was sehen Sie in den Logfiles?