Aufgabe IDS/ IPS mit Snort

Grundlagen

Nachfolgender Abschnitt beschreibt die Grundlagen zu Snort (Quelle: wikipedia.org)

Snort ist ein freies Network Intrusion Detection System (NIDS) und ein Network Intrusion Prevention System (NIPS). Es kann zum Protokollieren von IP-Paketen genauso wie zur Analyse von Datenverkehr in IP-Netzwerken in Echtzeit eingesetzt werden. Die Software wird überwiegend als Intrusion-Prevention-Lösung eingesetzt, um Angriffe unmittelbar ereignisgesteuert automatisch zu blockieren. Snort wurde von Martin Roesch programmiert und wird jetzt von dessen Firma Sourcefire weiterentwickelt. Diese wurde im Oktober 2013 von Cisco übernommen. Im Jahr 2009 wurde Snort in die „Open Source Hall of Fame" von InfoWorld als eine der besten Vertreter freier Open Source Software („greatest open source software of all time")[1] aufgenommen. Das Maskottchen von Snort ist ein Ferkel mit grosser, schnaubender (englisch snort) Nase.

Theorie-Aufgaben zu Snort bzw. HIDS- und NIDS-Lösungen

Was versteht man in der Netzwerktechnik unter dem Begriff "Promiscuous Mode"?

.....

.....

.....

.....

.....

.....

Was sind "False Positives"? Machen Sie ein Beispiel. Warum ist eine hohe Anzahl von "False Positives" kritisch?

.....

.....

.....

.....

.....

.....

Was sind "False Negatives"? Machen Sie auch hier ein Beispiel. Auf was deutet ein "False Negative" hin?

.....

.....

.....

.....

.....

.....

Worin besteht der eigentliche Unterschied zwischen einer IDS- und IPS-Lösung?

.....

.....

.....

.....

.....

.....

Worin besteht der Unterschied zwischen einer NIDS- und HIPS-Lösung?

.....

.....

.....

.....

.....

.....

Snort Praxis

Sie benötigen die beiden virtuellen Maschinen **Kali** und **m182-rev2**. Wenn Sie die beiden Maschinen nicht mehr haben, laden Sie sich diese aus dem Classroom herunter. Das root-Passwort haben Sie sich bereits in der ersten Modulwoche mittels Bruteforce-Angriff besorgt😉. Melden Sie sich mit dem Benutzer root an.

Ablauf SNORT-Workshop

Snort ist in der Grundinstallation bereits vorhanden. Im Verzeichnis **/etc/snort** finden Sie alle benötigten Dateien bzw. Konfigurationsdateien, welche Sie für diesen Workshop benötigen.

Bilden Sie Dreiergruppen innerhalb der Klasse. Erstellen Sie in der Datei **/etc/snort/rules/local.rules** die folgenden Regeln, sodass Ihr System am Schluss folgende Szenarien zu erkennen kann. Jedes Gruppenmitglied realisiert die Regeln auf der eigenen Instanz. Die erarbeiteten Theoriegrundlagen sowie die Ergebnisse aus dem Praxisteil über IDS, IPS, NIDS, HIPS usw. sind prüfungsrelevant.

- ICMP-Anfragen
- Verbindungsversuche über Telnet und SSH
- Verbindungsversuche über FTP

Um die Funktion Ihrer Regeln zu testen geben Sie den nachfolgenden Befehl ein:

snort -T -c /etc/snort/snort.conf

Am Ende der Ausgabe sollten Sie ein "Successfully" sehen.

Starten Sie nun Snort mit dem folgenden Befehl. Ausgaben werden damit direkt auf der Kommandozeile ausgegeben.

snort -v -c /etc/snort/snort.conf -A console

Hilfsmittel

Internet

Sozialform

Gruppenarbeit

Zeit

60 Minuten