Praktikum Netzwerksicherheit

Versuch 5: Bedrohungen im Netzwerk und Intrusion Detection Systems (IDS)

Immer wieder kommt es zu Einbrüchen an am Internet angeschlossenen Rechnern. Auch Viren und Würmer sind mittlerweile schon regelmäßiges Thema der Berichterstattung in den Medien. Dies zeigt, wie akut und vielfältig die Bedrohungen sind, denen ein am Internet angeschlossenes IT System ausgesetzt ist. In diesem Versuch sollen daher einige typische Bedrohungen analysiert werden. Die Ausführung der Angriffe ist dabei als Vortragsversuch gestaltet, die Aufgabe der Studenten ist es, den Angriff mit Hilfe eines Netzwerksniffers (wireshark) *mitzuschneiden*, dazu werden alle Rechner in ein Ethernet Segment aufgenommen. Danach sollen Sie die mitgeschnittenen Pakete analysieren und die Vorgehensweise des Angreifers analysieren.

Im 2. Teil des Versuches werden die Möglichkeiten der netzwerkbasierten Intrusion Detection ausgetestet. Dabei kommt das Open Source IDS *Snort* zum Einsatz. Die vorher gezeigten Angriffe gelten nun als Basis für das IDS. Diese Angriffe wurden von Ihnen mit einem Netzwerksniffer aufgezeichnet und analysiert. Nun soll ein IDS eingerichtet werden, dass solche Angriffsversuche automatisch erkennen kann. Ein netzwerkbasiertes IDS besteht im Wesentlichen aus einem Sniffer und einem Analysator, wobei der Analysator den Netzwerkverkehr auf *Angriffssignaturen*, d.h. bestimmte eindeutige Sequenzen, die auf den jeweiligen Angriff hindeuten, prüft.

Vorwissen und Infos zur Vorbereitung:

- Netzwerktechnik und TCP/IP
- IDS Snort — www.snort.org
- Write your own snort rules — http://oreilly.com/pub/h/1393
- Snort rule writing for the IT professional — Part1 & Part 2

Praktische Durchführung
1. Teils: Live-Hacking

Der Betreuer wird einen Angriff vorführen. Um welche Angriffe es sich handelt, wird erst am Übungstag entschieden.

Aufgabe

Beobachten Sie die Angriffe, versuchen Sie Ihren Packetsniffer richtig einzustellen, so dass Sie nur den gewünschten Traffic zwischen Angreifer und Opfer sehen. Nachdem die Aktion ausgeführt wurde, haben Sie Zeit im Internet zu recherchieren, um welchen Angriff es sich handelt. Versuchen Sie anhand der aufgezeichneten Pakete herauszufinden, was passiert ist.

Praktische Durchführung
2. Teils: Konfiguration des IDS

Allgemeines

Als Intrusion-Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion-Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.

Wir wollen zur Überwachung einen sog. netzbasierten Sensor aufsetzen: Netzbasierte Sensoren (Netzsensoren) überwachen den Netzverkehr eines Rechners oder eines ganzen Teilnetzes auf verdächtige Ereignisse. Zum Betrieb jedes Netzsensors wird typischerweise ein separater Rechner eingesetzt, so dass andere Applikationen nicht gestört werden können. Teilweise liefern Hersteller Netzsensoren nur noch in Kombination mit der zugehörigen Hardware/Software-Plattform, als so genanntes *Appliance*.

Snort

Die Konfigurationsdateien und Angriffssignaturen befinden sich im Verzeichnis `/etc/snort/`. Die zentrale Konfigurationsdatei heißt `/etc/snort/snort.conf`, die Angriffssignaturen befinden sich in den Dateien mit der Endung *.rules im Ordner* `/etc/snort/rules/`, sie werden von der zentralen Konfigurationsdatei eingebunden.

Die Snort Angriffssignaturen bestehen aus mehreren Teilen:

- Angabe von Quelle und Ziel:
  Hier werden Quell- und Zieladresse, sowie Quell- und Zielport, sowie das Protokoll angegeben.
- Angabe von Paketeigenschaften und Inhalten:
  Hier werden z. B. Bytesequenzen aus den Paketen oder TCP Flags angegeben.
- Aktionsteil:
  Hier wird angegeben, was bei Erkennen der spezifizierten Angriffssignatur unternommen werden soll.

Betrachten sie eine beliebige Regel aus der Datei *web-iis.rules* und schlagen Sie die verwendeten Optionen im Handbuch nach. Machen Sie sich klar, wann diese Angriffssignaturspezifikation erfüllt ist.

Aufgabe

Installieren Sie Snort auf der Kommandozeile (als root) mit `apt-get install snort` *(HOME_NET=141.62.66.0/24).*

Falls Snort nicht richtig gestartet wird, finden Sie Hinweise in `/var/log/syslog` oder starten Sie Snort direkt (als root) mit `snort -c /etc/snort/snort.conf`. Folgende zwei Einstellungen sind für diese Umgebung wichtig:

- In `/etc/default/snort` muss der Kommandoparameter '`-k none`' hinzugefügt werden.
- Um lesbare Meldungen der Angriffe zu bekommen, muss '`output alert_fast: alert.log`' in die Konfigurationsdatei `/etc/snort/snort.conf` eingefügt werden.

Wenn Snort richtig läuft, landen erkannten Angriffe in `/var/log/snort/alert.log`

Versuchen Sie nun eigene Snort Regeln zu schreiben. Diese können Sie in die Datei `/etc/snort/rules/local.rules` eintragen. Starten Sie Snort nach dem Eintragen oder Ändern von Regeln jeweils neu!

Tipp: Wird *local.rules* überhaupt eingebunden?

- Schreiben Sie eine Regel, die auf TCP SYN Pakete auf Port 111 anspricht!
- Versuchen Sie eine Regel zu schreiben, die anspricht, wenn ein Paket die Bytesequenz *istestlabor* enthält! (Zum Testen können Sie diesen String als ftp login probieren.)

Nachbereitung und Protokoll

Neben einer einführenden Beschreibung zum Thema sollte das Protokoll folgende Punkte beinhalten:

Teil 1 - Hacking:

- Zeigen Sie anhand der aufgezeichneten Pakete, um welche Angriffe es sich handelt und was genau passiert ist.

Teil 2 - IDS:

- Auszüge aus der Konfigurationsdateien von Snort, vor allem die von Ihnen vorgenommenen Änderungen.
- Kommentierte Auszüge aus den Snort Logfiles