LU02h - LB2 - Fokusthema: DoS / DDoS

1. Einleitung

BruteForce-Attacken beschränken sich häufig auf einzelne Dateien, sind aber auch im Interenet nicht so selten wie man meint. Und es gibt viele Varianten, weshalb wir uns auf die nachdfolgenden Angriffsvarianten beschränken

2. Angriffsvarianten

Angreifer sind beschränken sich heute nicht mehr auf das simple Ausprobieren von Varianten. Stattdessen werden bei BF-Attacken die nachfolgenden Methoden angewendet

2.1 Full: Simple and Plain

Durch ausprobieren von allen Möglichkeiten aus einem Zeichensatz wie die Arabischen Zahlen, das Alphabet und die Sonderzeichen natürlich.

2.2 Dictionaries

Häufig verwendeten Passwörter werden bei dieser Technik in einem Wörterbuch gespeichert. Der Angriff erfolgt dann mit diesem Wörtern aus dem Wörterbuch

2.3 Distributed Brute-Force

Verteilt die Arbeit auf viele Maschinen/Server (Botnet oder Cluster) fuer hoehere Geschwindigkeit. Man kann das sehr gut simulieren indem man den jeweiligen Scripten einen bestimmten Zahlenbereich gibt.

2.4 Rainbow-Tables / Precomputed Attacks

Nutzt vorgerechnete Hash→Passwort Tabellen fuer schnellen Lookup — funktioniert nur ohne Salt oder mit gleichen Salts.

3. Gegenmassnahmen gegen Brute Force

Unanhängig ob bei lokalen oder zentralen Systemen, gibt es die nachfolgenden Gegenmassnahmen gegen

3.1 Einfache Massnahmen

- Lineare Latenzzeit/Linear Delay: Nach jedem Versuch wird eine bestimmte Zeit (0.5 - 2 Sekunden) gewartet
- Zunehmende Latenzzeit/Progressiv Delay: Beim ersten Fehlversuch muss 10 Sekunden gewartet werden, danach 1 Minute, ….

3.2 Mittel-Komplexe Massnahmen

- Anzahl Versuche beschränken und anschliessend User sperren
- Captcha oder ähnliches einbauen

3.3 Komplexe Massnahmen

- Logging: Fehlerversuche werden gelogged und ggfs. Alarm ausgelöst.

4. Bewertung

Nachfolgend finden Notenstufen bzw. die Anforderungen, um diese Noten zu erreichen.

Note 4.0 - 4.5

Software/Programmierung

- Es ist eine vulnerabler (node.js oder python) Server vorhanden, dass überwunden werden muss
- Es können Angriffe mittels der unter 2.1 und 2.2 beschrieben Art durchgeführt werden
- Es gibt eine *secure-Version* der Software, bei der erfolge Angriff mittels eine der unter 3.1 genannten Massnahmen verunmöglicht wurde.

Formale Aspekte

- Die Best-Practice-Coding-Standard wurden eingehalten
- Es wird colaborativ gearbeitet inkl. einer Ausfallsicherheit und Versionierung

Abgrenzung

- Es braucht kein Frontend, sprich der Angriff und die Verteidigung können im gleichen Script sein.
- Sprich der Fokus liegt auf dem Server

Note 4.5 - 5.2

Software/Programmierung

- Es ist eine vulnerabler (node.js oder python) Server vorhanden, dass überwunden werden muss
- Es können Angriffe mittels der unter 2.1, 2.2 und 2.3 beschrieben Art durchgeführt werden

- Es gibt eine *secure-Version* der Software, bei der erfolge Angriff mittels eine der unter 3.1 und 3.2 genannten Massnahmen verunmöglicht wurde.

Formale Aspekte

- Die Best-Practice-Coding-Standard wurden eingehalten
- Es wird colaborativ gearbeitet inkl. einer Ausfallsicherheit und Versionierung

Abgrenzung

- Es braucht kein Frontend, sprich der Code kann entweder über Commandline oder als separates Angriffsscriptdurchgeführt werden.
- Bei dieser Version gibt es den Server und ein Script, dass den Agriff durchführt

Note 5.3 - 6.0

Software/Programmierung

- Es ist eine vulnerabler (node.js oder python) Server vorhanden, dass überwunden werden muss
- Es können Angriffe mittels der unter 2.1, 2.2, 2.3 und 2.4beschrieben Art durchgeführt werden
- Es gibt eine *secure-Version* der Software, bei der erfolge Angriff mittels eine der unter 3.1, 3.2 und 3.3 genannten Massnahmen verunmöglicht wurde.

Formale Aspekte

- Die Best-Practice-Coding-Standard wurden eingehalten
- Es wird colaborativ gearbeitet inkl. einer Ausfallsicherheit und Versionierung

Abgrenzung

- Es braucht kein Frontend, sprich der Code kann entweder über Commandline oder als separates Angriffsscriptdurchgeführt werden.
- Bei dieser Version gibt es den Server und ein Script, dass den Agriff durchführt

---