Merkblatt Brute Force Attacks

Grundlagen

Bei einer Brute-Force-Attacke handelt es sich um den Versuch Passwörter zu entwenden, Systeme zu übernehmen oder Zugriff auf vertrauliche Daten durch automatisiertes, wahlloses Ausprobieren zu erhalten.
Diese Angriffsmethode nutzt «rohe Gewalt» also brute Force, indem sie wahllos verschiedene Zeichenketten automatisiert ausprobiert.
Logischerweise ist die Erfolgssausicht höher je mehr Kombinationen ausgetestet werden.
Grundsätzlich lässt sich jedes Geheimnis durch Ausprobieren lösen.
Jedoch braucht man umso mehr Zeit desto komplexer das Geheimnis ist.

Voraussetzungen

Voraussetzungen für eine Brute-Force-Attacke sind in der Regel leistungsstarke Computersysteme sowie automatisierte Tools, die in Kombination ein performantes Abarbeiten möglichst vieler Lösungsansätze erlaubt.

Arten von Brute-Force-Attacken

Traditioneller Brute-Force-Angriff

Wenn keine Informationen zu Kennwörtern oder Accountnamen verfügbar sind und die Angreifer lediglich alle möglichen Kombinationen von Login-Daten testen, spricht man von herkömmlichem Brute Force. Umso stärker die dabei eingesetzte Hardware ist, desto schneller werden die gesuchten Kennwörter gefunden.

Dictionary-Angriff

Bei Dictionary-Angriffen werden wie der Name schon andeutet, vorhandene Wortlisten mit geläufigen Nutzernamen und Passwörtern eingesetzt, um digitale Zugänge zu knacken.

Rainbow-Table-Angriff

Haben Angreifer Zugriff auf die im System hinterlegten Passwörter, sind diese in der Regel nicht im Klartext, sondern lediglich als Hashwert gespeichert. Auf den sogenannten Rainbow Tables sind die Hashwerte der gängigsten Passwörter enthalten. Per automatisiertem Abgleich dieser Daten lassen sich die zutreffenden Kennwörter ermitteln.

Credential Stuffing

Beim sogenannten Credential Stuffing sind bereits die vollständigen Zugangsdaten bekannt, nicht jedoch der Dienst oder die Plattform, auf welcher sie zutreffen. Die Angreifer machen sich bei dieser Brute-Force-Methode die Bequemlichkeit auf Anwenderseite zu nutze. Da trotz regelmäßiger Warnungen immer noch viele Anwender ein und dieselbe E-Mail-Passwort-Kombination für mehrere Dienste nutzen, ist es für Cyberkriminelle ein Leichtes zahlreiche Konten zu kapern, sobald diese Informationen einmal bekannt sind. Meist stammen die erbeuteten Login Informationen aus Datenpannen von Internetdiensten. Im Darknet werden ganze Listen mit diesen Datensätzen gehandelt. Um möglichst schnell und unerkannt vorzugehen, setzen Angreifer auf Botnetze, die getarnt und mit unterschiedlichen IP-Adressen unzählige parallele Anmeldeversuche starten.

Credential Cracking

Im Gegensatz zum Credential Stuffing sind bei Angriffen mittels Credential Cracking noch nicht die gesamten Zugangsdaten bekannt. Beispielsweise besitzen die Angreifer einen Nutzernamen für ein

bestimmtes Konto. Das dazugehörige Passwort fehlt allerdings. Um nun das korrekte Kennwort zu bestimmen, können Angreifer entweder Passwortlisten mit den gängigsten Kennwörtern sukzessive abarbeiten oder den Schlüssel komplett nach dem Zufallsprinzip errechnen. Auch hierfür werden in der Regel Botnetze eingesetzt, um die Angriffe zu verschleiern und zu beschleunigen.

Schutzmassnahmen

Es gibt mehrere Methoden, um sich vor Brute Force Attacken zu schützen. Eine Kombination dieser Methoden ist vermutlich das sicherste Schutzkonzept. Unten sind jetzt mehrere Massnahmen aufgelistet, welche vor Brute Force Attacken schützen:

- Komplizierte Passwörter:
  Man soll Passwörter benutzen die aus möglichst vielen Zeichen und aus möglichst vielen verschiedenen Zeichentypen bestehen diese sind viel schwerer zu knacken.
- Absicherung des Kennwortmechanismus:
  Es wird nachdem ein falsches Passwort eingegeben wurde die Eingabe eines Kennworts für ein bestimmtes Zeitintervall gesperrt. Dieses Intervall kann dann nach jeder weiteren Falscheingabe erhöht werden. Das Verlangsamt den Prozess massiv. Apple zum Beispiel ist dabei sogar noch einen Schritt weitergegangen. Da wird das komplette Nutzerkonto nach einer gewissen Anzahl an fehlgeschlagenen Log-in Versuchen gesperrt.
- Mehr-Wege-Authentifizierung:
  Die Mehr-Wege-Authentifizierung, also meistens die Zwei-Faktor-Authentifizierung wird von vielen Anbietern optional angeboten. Diese verkompliziert den Anmeldevorgang etwas, da neben dem Passwort noch eine weitere Komponente benötigt wird. Dabei kann es sich um die Beantwortung einer Geheimfrage, die Eingabe einer PIN oder ein sogenanntes Captcha handeln.

Beispiel Angriff und Schutzmassnahme

Angriff

Zur Demo habe ich das Tool Hydra benutzt.
Im Kali Linux System ist Hydra normalerweise vorinstalliert. Ich habe es jedoch auf einer Ubuntu VM selbst installieren müssen. Mittels des Befehles:
«sudo apt-get install hydra-gtk»
Hydra ist ein Tool das geeignet ist um Brute Force Attacken auszuführen. Es ist dafür ausgelegt, um so schnell wie möglich alle möglichen Kombinationen eines Passworts oder Usernamens abzufragen.
Danach habe ich diesen Befehl in der Konsole ausgeführt, um die Webapplikation anzugreifen:

hydra 192.168.43.111 http-form-post "/BruteForceAttack/login.php:user=^USER^&password=^PASSWORD^:false" -l admin -x 4:4:1 -o hydra-results.txt

Die verschiedenen Argumente bedeuten das:
«Hydra»=Tool
«192.168.43.111» = IP der Webapplikation
«http-form-post» = Protokoll
«/BruteForceAttack/login.php» = Pfad zum Login Formular
«:user» = Name des Benutzer Parameters wie er beim Login Formular heisst
«=^USER^» = Parameter für den User welcher eingesetzt werden soll
«password» = Name des Password Parameters wie er beim Login Formular heisst.
«=^PASSWORD^» = Parameter für das Passwort welches eingesetzt werden soll

«-l admin» = Für den ersten Parameter wird admin mitgegeben.
«-x 4:4:1» = Für den zweiten Parameter werden alle Kombinationen abgefragt die mindestens 4 bis maximal 4 Zeichen haben und nur aus Zahlen bestehen. Also die Erste «4» steht für minimale Anzahl Zeichen die zweite «4» für maximale Anzahl Zeichen und die «1» für nur Zahlen. Für nur Kleinbuchstaben wäre der Parameter, der mitgegeben werden muss, «a». Und für nur Grossbuchstaben «A».
«-o hydra-results.txt» = In dieses Text File werden alle Kombinationen reingeschrieben die ausprobiert wurden.

Also sieht der Befehl in Pseudo-Code etwa so aus:
IP Protokoll Pfad(LoginFormular):Parameter=^USER^&Parameter=^PASSWORD^:Fehlermeldung -l Username(bekannt) -x MinAnzahlStellen:MaxAnzahlStellen:Zeichentypen -o TextFile Resultat

Danach werden alle möglichen Kombinationen von Hydra ausgetestet. Wenn es eine Kombination gefunden hat, die funktioniert, wird diese in der Konsole ausgegeben.

Schutz

Der beste Schutz gegen diese Attacken sind kompliziertere Passwörter zu benutzen. Das kann man zum Beispiel als Programmierer ganz einfach so machen das man eine mindestlänge bei der Eingabe festlegt. In HTML sieht das etwa so aus:

```
<input type="password"  minlength="7" maxlength="10">
```

Dann kann der User bei der Registrierung nur Passwörter erstellen, die eine Mindestlänge von 7 haben.
Dass kann man auch noch weiterziehen zum Beispiel das es mindestens einen Grossbuchstaben und eine Zahl beinhalten muss.