LU02f - LB2 - Fokus: BruteForce

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. Attacken

2.1 Einfache ausführbare Angriffe

- **Mono-Alphabet:** Das Passwort ist bis zu 10 Zeichen lang und besteht aus einem Mono-Zeichensatz, sprich entweder 0..9, oder a..z, oder A..Z, etc.

2.2 Mittelschwer ausführbare Angriffe

- **Dictionaries:** Anstatt alle Versuche auszuprobieren, wird mit aus bestehenden Daten wie Email, Geburtstag, etc Permustationen des möglichen Passwortes ausprobiert.
- **Poly-Alphabet:** Das Passwort ist bis zu 10 Zeichen lang und besteht aus einem *Poly-Zeichensatz*, sprich einer Kombinatio aus 0..9, a..z, A..Z, Sonderzeichen.

2.3 Komplexe Angriffe

- **Rainbow-Tables:** Die Attacke geschieht mit vorbereiteten Look-Up Dateien (Hash-Plain)
- **Paralellilisert:** Es wird mit mehreren Instanzen angegriffen, wobei jede Instanz einen bestimmten Wertebereich übernimmt.

3. Gegenmassnahmen gegen Brute Force

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

3.1 Leichte Gegenmassnahmen

- **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

- **Counter-Limit:** Anzahl Versuche beschränken und anschliessend User sperren
- **UserInteraktion:** Captcha oder ähnliches einbauen

3.3 Komplexe Massnahmen

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

4. Bewertung

4.1 Angriff

Noten	Beschreibung	Hinweis
4.1.1	+0.75	Angriff gemäss einer Variante von 2.1
4.1.2	+0.75	Angriff gemäss je einer Variante und 2.2
4.1.3	+1.00	Angriff gemäss je einer Variante 2.3
4.1.4	+0.50	Angriff ist jeweils in separaten Files untergebracht

4.2 Verteidigung

Noten	Beschreibung	Hinweis
4.2.1	+0.75	Verteidigung gemäss einer Variante von 3.1
4.2.2	+0.75	Verteidigung gemäss je einer Variante und 3.2
4.2.3	+1.00	Verteidigung gemäss je einer Variante 3.3
4.2.4	+1.00	Angriff und Verteidigung sind in separaten Files untergebracht

4.3 Bonus

Noten	Beschreibung	Hinweis
4.3.1	+0.25	Die Thementeams werden in Konkurenz zueinander treten. Sofern ein wesentzlicher Teambeitrag vorhanden ist, erhält jedes Gewinnerteam jeweils einen Bonus von 0.25 Notenpunkten.
4.3.2	+0.50	Für die 2. und 3. Angriffe oder Verteidigungen wird die Hälfte der vollen Punktezahl der jeweiligen Massnahme vergeben

4.4 Malus

Noten	Beschreibung	Hinweis	
4.4.1	-1.00	Die Best-Practice-Coding-Standard wurden nicht eingehalten	Python
4.4.2	-0.50	Es wird nicht kollaborativ und Ausfallsicher (inkl. Versionierung) gearbeitet	
4.4.3	-2.00	Es können Fragen zum Lösungcode nicht korrekt oder gar nicht beantwortet werden.	
4.4.4	-1.50	Pro angefangenem Tag Verspätung	
4.4.5	-0.50	Pro Downloadversuch: Link funktioniert nicht (abgelaufen, Berechtigungen fehlen, etc.)	

Noten	Beschreibung	Hinweis	
4.4.6	-0.50	Schriftsprache: Die Lernenden verwenden nicht die offiziellen Schriftsprache.	
4.4.7	-0.10	Verspäteter Anfang des Teams: pro Minute Verspätung	
4.4.8	-1.00	Team oder Teammitglieder erscheinen nicht zum Gespräch (Ausnahme: Höhere Gewalt). Abzug erhalten nur betroffenen Personen	
4.4.9	-1.00	Team ist nicht vorbereitet beim Fachgespräch	

4.5 Hinweise

- Es braucht kein Frontend, sprich der Code kann entweder über Commandline oder als separates Angriffsscriptdurchgeführt werden.
- Jedes Teammate kann alle Fragen zum Fousthema beantworten, sprich der Wissentransfer im Tandem wird durch das Tandem sichergestellt.
- Bei Ungleicher Performance im Tandem wird individuell benotet.
