Angriffsvektoren & Filterblasen

Krihjin

25.03.2019

Eine kurze (;)) Übersicht

1. Der technische Weg - Angriffsmöglichkeiten
   1.1 Welche Angriffsarten gibt es?
   1.2 Was ist Brute Force?
   1.3 Keylogger
2. Der "soziale" Weg - Social Engineering
   2.1 Soziale Medien - Ein Traum für Social Engineering
3. Filterblasen
   3.1 Fallbeispiel
   3.2 Auslöser
   3.3 Wie kann ich sowas verhindern?
4. Fazit?

1. Der technische Weg - Angriffsmöglichkeiten

1.1 Welche Angriffsarten gibt es?

- Passwort erraten (hat bestimmt jeder mal gemacht)
- Brute Force Attacke
- Keylogger
- Malware wird z.B. sehr gerne über Links verteilt, kann aber auch auf Datenträgern vorhanden sein!
- Es gibt aber noch einige mehr!

1.2 Was ist Brute Force?

- ist eine beliebte Angriffsform, um Passwörter herauszufinden oder Daten zu entschlüsseln
- beschreibt ein automatisiertes Vorgehen, bei dem wahllos Buchstaben, Zahlen und Sonderzeichen ausprobiert werden
- bei der Abwehr eines solchen Angriffs ist entscheident, wie lang der Schlüssel ist (Verschlüsselung) und die Komplexität des Passwortes

Zum Vergleich : Bei einem 32-Bit-Schlüssel wären es 4 Milliarden Möglichkeiten, die die heutigen Personal Computer in Minuten durchpobiert hätten.
Bei einem 128-Bit-Schlüssel würde ein solcher Angriff mehrere tausend Jahre dauern!

Maximale Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0-9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a-z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A-Z;a-z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A-Z;a-z;0-9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

Abbildung: Rechenzeit bei einer Brute Force Attacke

Quelle:
https://de.wikipedia.org/wiki/Passwort

So ein Angriff kann aber unter Umständen sehr viel Zeit in Anspruch nehmen, bzw. lange geplant sein!

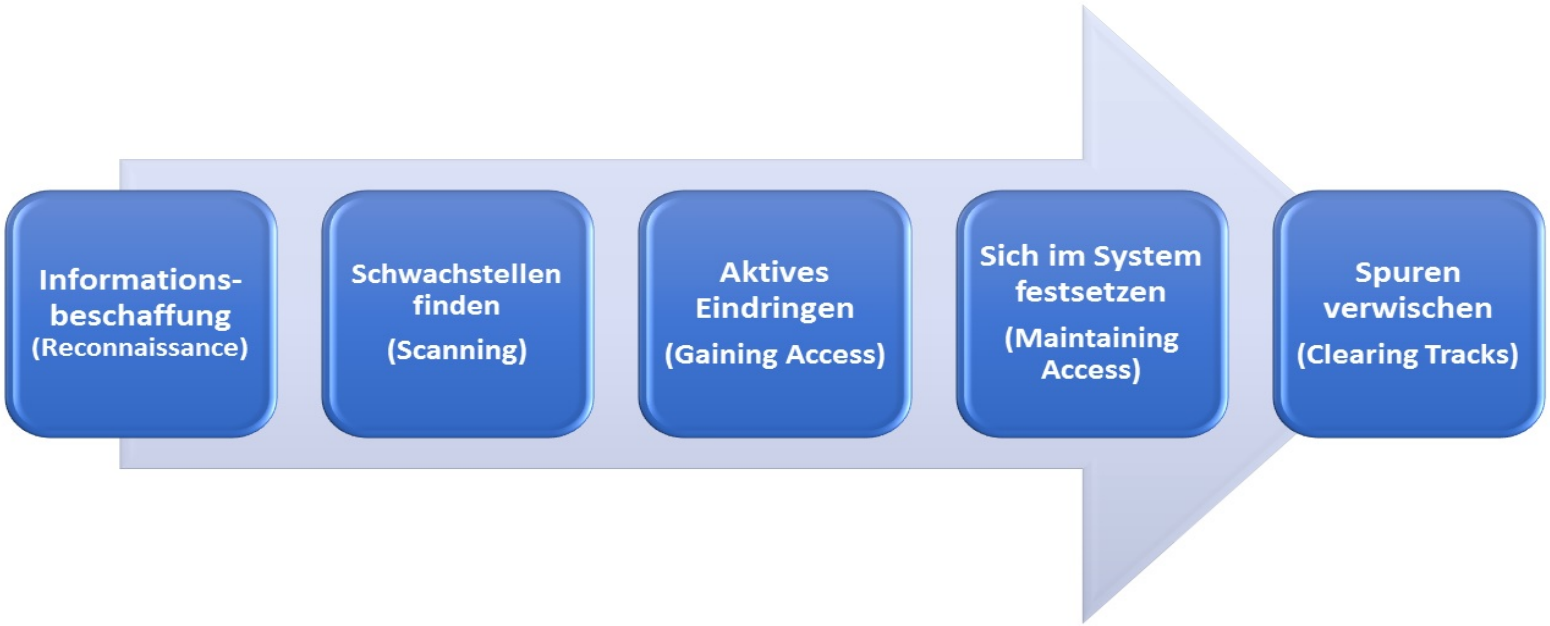

Abbildung: Anatomie eines Angriffs

Bild zur Verfügung gestellt von : Herr Amberg, Quelle : www.udemy.com, Material vom Kurs Ëthical Hacking"

1.3 Keylogger!

Eine weitere Gefahr sind Keylogger, die alle Tastenanschläge mitschneiden, die getätigt werden. Ausgebaute Keylogger schneiden sogar die Mausbewegungen mit oder machen Screenshots / Aufnahmen vom Bildschirm, oder dir!

2. Social Engineering - Der "soziale" Weg

- Bedeutet, mit Hilfe sozialer Interaktion persönliche Informationen herauszufinden oder sogar einen Angriff einzuleiten
- verdeutlicht, wieso es nicht gut ist, persönliche Informationen jedem preis zu geben
- dient in der Regel als Vorbereitung des eigentlichen Angriffs
- ist ggf. schwierig zu durchschauen, je nachdem wie gut der "Angreifer" ist

2.1 Soziale Medien - Ein Traum für Social Engineering

- stellt einen unfassbaren Pool an persönlichen Informationen dar:
- "Realer" Name, Alter, Geschlecht, Name des Haustiers, Geburtsdatum uvm.

3. Filterblasen

- = Informationsblasen
- entstehen, wenn z.B. Websites durch Algorithmen vorrauszusagen wollen, welche Informationen der Nutzer auffinden möchte
- sind auch in sozialen Medien wie Facebook, Instagram, Twitter u.Ä. vorhanden
- hängen nicht zwangsläufig mit Fakenwes zusammen, können diese aber begünstigen
- Filterblasen können deine Meinungen **beeinflussen** - und das unbewusst!

3.1 Fallbeispiel ;)

Stell dir vor, Freunde von dir Liken einen bestimmten Post auf Facebook oder kommentieren diesen. Je nachdem wie du dich vorher verhalten hast (viele Beiträge deiner Freunde angeklickt, geliked oder selbst kommentiert), wird dir der Algorithmus nun diese neuen Beiträge anzeigen. Dabei lässt zunehmend andere Meinungen zu dem selben Thema außen vor.
Das Ergebnis : eine Filter-/Informationsblase!

3.2 Auslöser

- Liken / Kommentieren eines Beitrags
- Teilen eines Beitrags
- Besuchen von Websites

3.3 Wie kann ich so etwas verhindern?

- Nutze möglichst viele verschiedene Quellen, nicht nur eine.
- Hinterfrage Nachrichten - gleiche diese bei verschiedenen Berichterstattern ab.
- Eine weitere gute Frage ist : Muss ich das jetzt wirklich kommentieren / liken?

4. Welches Fazit zieht ihr darauß?

Ein paar Tipps:

- verwendet keinen Datenträger, wenn ihr nicht genau wisst, was drauf ist!
- Links, denen ihr nicht vollkommen vetraut, solltet ihr nicht aufrufen!
- sparsam mit persönlichen Informationen umgehen ;)