Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Universität der Bundeswehr München
Institut für Softwaretechnologie

Konzeption und Implementierung eines Szenarios zum Angriff auf Identitäten für die Cyber Range

Form der Arbeit / Form of this work:	Bachelorarbeit / Masterarbeit
Themenschwerpunkte / Main focus:	IT-Sicherheit, Identitätsmanagement
Voraussetzungen / Prerequisites:	Grundkenntnisse IT-Sicherheit
Lehrstuhl für / Professorship for:	Prof. Dr. Wolfgang Hommel
Betreuung / Supervisor:	Daniela Pöhn

Hintergrund und Motivation / Background Information and Motivation

Authentifizierungsmethoden können aus drei Kategorien ausgewählt werden: Wissen (z.B. Passwort oder PIN), Besitz (z.B. Hardwaretoken oder Smartphone) und Biometrie (z.B. Fingerabdruck oder Iris). Häufig wird jedoch auf Passwörter aufgebaut. Private Endnutzer haben je nach Statistik 80 bis 150 Online-Accounts, die zumindest in der Theorie ein Passwort benötigen[1]. Wenn Nutzer das Passwort für all ihre Dienste verwenden, können sie es in der Regel gut merken, die Auswirkung von einem Security Incident sind jedoch größer. Einfache Passwörter, wie *123456*, *test1*, *qwerty* und *iloveyou* (vgl. *rockyou.txt* und andere Wordlists), können zudem leicht gecrackt werden. Ein weiteres Problem sind Default-Passwörter. Ein Angreifer kann in einem sogenannten Password Spraying Angriff eine Liste von Benutzernamen und Standardpasswörtern bei einer oder mehreren Anwendungen ausprobieren. Ein gutes Passwort ist einmalig, leicht zu merken und robust[2].

Es zeigt sich, dass diese Regel nur bedingt beachtet wird. Immer wieder werden Credential-bezogene Security Incidents, wie Credential Stuffing (vgl. z.B. The North Face[3]), publik. Durch Datenlecks, Bruteforcing und Phishing gelangen immer wieder Listen an Nutzerna-

[1] `https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic`, aufgerufen am May 5, 2022

[2] vgl. BSI, `https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html;jsessionid=571F1F52CD812D01E490D234927F80FD.internet461`, aufgerufen am May 5, 2022

[3] `https://threatpost.com/credential-stuffing-attack-north-face/161190/`, aufgerufen am May 5, 2022

men und Passwörtern ins Internet[4]. Credential stuffing ist ein Angriff, der automatisiert diese gestohlene Nutzernamen und Passwörter für andere Dienste ausprobiert. Dies hat den Hintergrund, dass noch immer Nutzer dasselbe Passwort oder ein bestimmtes Passwortmuster für mehrere Dienste einsetzen. Je sensibler ein Zugang ist, wie beispielsweise beim Online-Banking, umso wichtiger ist jedoch eine starke Authentifizierung. Die bisher beschriebenen Angriffe zählen zu den Account Take Over Angriffen.

Angreifer versuchen jedoch nicht nur ein einzelnes Benutzerkonto, sondern direkt das Identitätsmanagementsystem im Hintergrund, wie OpenLDAP (Lightweight Directory Access Protocol) und Active Directory (AD), anzugreifen. Dies kann beispielsweise durch Konfigurationsfehler und Implementierungsfehler möglich werden. Ein Beispiel mit sehr großer Auswirkung ist Zerologon (CVE-2020-1472)[5]. Über diese Verwundbarkeit können Angreifer die Kontrolle über einen Domain Controller, und somit alle damit verwalteten Geräten, übernehmen. Dies hat insbesondere im Rahmen von föderiertem Identitätsmanagement weitreichendere Auswirkungen.

Um verschiedene Angriffe und Gegenmaßnahmen testen zu können, bietet es sich an, Real-World-Szenarien für Trainingsumgebungen wie die Cyber Range ICE&T zu entwickeln. Hier können sowohl Angriff als auch Gegenmaßnahmen gezielt trainiert und reale Probleme nachgestellt werden.

Ziel der Arbeit / Goal of this Thesis

Das Ziel der Arbeit ist es in einem ersten Schritt einen Überblick über Angriffe auf Identitäten, sowohl auf einzelne Konten als auch Identitätsmanagementsysteme, zu schaffen. Zusätzlich soll der Aufbau von Cyber Range Trainingszenarien betrachtet werden. Basierend auf Szenarien werden Anforderungen an das Konzept gestellt. Die Anforderungen dienen zusätzlich verwandte praktische und wissenschaftliche Arbeiten zu evaluieren.

Diese ersten Schritte dienen als Grundlage für ein generisches Konzept von verschiedenen Trainingsszenarien mit Fokus Angriff auf Identitäten (insbesondere Identitätsmanagementsysteme). Exemplarisch sollen ein bis zwei Szenarien (Red oder Blue Team) umgesetzt, dokumentiert und evaluiert werden.

Damit ergeben sich folgende Arbeitsschritte:

- Einleitung, Motivation und Einordnung der Arbeit.
- Grundlagen: Angriffe auf Identitäten und Identitätsmanagementsysteme, Aufbau von Cyber Range Trainingsszenarien.

[4] vgl. HaveIbeenPwned, `https://haveibeenpwned`, und HPI Identity Leak Checker, `https://sec.hpi.de/ilc/search`, aufgerufen am May 5, 2022

[5] `https://www.secura.com/uploads/whitepapers/Zerologon.pdf`, aufgerufen am May 5, 2022

- Anforderungsanalyse basierend auf Szenarien. Hier kann bereits auf Red und Blue Team sowie den organisatorischen/konzeptionellen Ablauf eingegangen werden.
- Evaluation von praktischen und wissenschaftlichen Arbeiten in diesem Bereich basierend auf den aufgestellten Szenarien.
- Konzeption einer generischen Trainingsmöglichkeit für Identitätsmanagement (Red oder Blue Team).
- Praktische Umsetzung von einem oder zwei Szenarien über virtuelle Maschinen sowie deren Dokumentation.
- Evaluation des Konzepts und der praktischen Umsetzung.
- Fazit und Ausblick auf weiterführende Arbeiten

Kontakt / Contact

Bei Problemen oder Fragen, nehmen Sie bitte Kontakt auf mit / If you have any problems or questions, please contact:

Name / Name: Dr. Daniela Pöhn
Adresse / Address: Cascada Gebäude, Carl-Wery-Str. 18-22, Raum 2718
Tel. / Phone: 7356
E-Mail / Email: daniela.poehn@unibw.de