Projektdokumentation zur Studienarbeit „Ausarbeitung eines Active Directory Security Kurses“

Studienprojekt

im Studiengang
Wirtschaftsinformatik

vorgelegt von

Friedemann Zurhorst
Matr.-Nr.: 760280

am 15. Februar 2022
an der Hochschule Esslingen

Erstprüfer/in:	Prof. Dr. Rer. Nat. Tobias Heer
Zweitprüfer/in:	Prof. Dr. Dominik Schoop

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

Identity- und Accessmanagementsysteme sind der Grundpfeiler eines jeden Unternehmens. Durch die Bereitstellung eines solchen Systems, und der damit einhergehenden Verwaltung von digitalen Identitäten, ist es überhaupt erst möglich ein sicheres Arbeitsumfeld zu schaffen.

Ohne die Möglichkeit, jedem Benutzer einen Account bzw. eine digitale Identität zuzuweisen, wäre es nicht möglich einen granularen Zugriff auf Ressourcen zu ermöglichen geschweige denn zu steuern. Durch diese Berechtigungen können Zugriffe auf Informationen, Systeme, Applikationen, aber auch Prozesse und vieles mehr gesteuert werden. Es ist nicht gewollt, dass jeder Mitarbeiter auf jede Komponente des Unternehmens Zugriff hat, da dies nicht nur zu erhöhtem Verwaltungsaufwand führt, sondern auch enorme Sicherheitsrisiken mit sich bringt. Man stelle sich vor, jeder Mitarbeiter könnte auf die Mitarbeiterstammdaten zugreifen und diese gegebenenfalls sogar verändern, oder ein verärgerter Mitarbeiter könnte Firmengeheimnisse einsehen und kopieren. Doch die Sicherheitsbedenken umfassen nicht nur Bedrohungen von innen, sondern auch von außen. Ein Hacker hätte sofortigen Vollzugriff auf alle Ressourcen, was katastrophale Folgen für das Unternehmen hätte. Sowohl finanzieller- als auch Ansehensverlust sind denkbar, je nach Ausmaß eines Angriffs.

Als Gegenmaßnahme müssen strikte Berechtigungs- und Zugriffskontrollen geplant und etabliert werden, damit jeder Mitarbeiter nach dem „principle of least privilege“ nur auf diese Ressourcen Zugriff bekommt, die er für seine tagtägliche Arbeit benötigt.

Sobald ein Angreifer ein Zielnetzwerk infiltriert, und die nähere Umgebung ausgekundschaftet (Reconnaissance) hat, ist das nächste Ziel die Rechteausweitung (Privilege Escalation). Ein Angreifer kann nicht genau steuern, an welcher Stelle er in das Unternehmensnetzwerk eindringt, und hat somit nicht direkten Zugriff auf die gesuchten Ressourcen. Demnach muss er sich die benötigten Accounts beziehungsweise Berechtigungen erst durch mehrere Schritte aneignen, um schlussendlich zum gewünschten Ziel zu kommen.

Wie man sieht, spielt das Identity- und Accessmanagementsystem eine zentrale Rolle in der heutigen IT-Systemlandschaft, und ist aus dem alltäglichen Gebrauch nicht wegzudenken, auch wenn ein Großteil der Anwender nicht konkret damit in Kontakt kommt.

2 Motivation

Mit fortschreitender Digitalisierung der Unternehmen, werden diese auch öfters Ziele von Hackerangriffen beziehungsweise Datendiebstahls. Dementsprechend ist die Absicherung solcher Identity- und Accessmanagementsystemen ein zentraler Bestandteil der IT-Sicherheitsstrategie der Unternehmen. Auch mit dem Paradigmenwechsel zu Zero-Trust-Modellen, ist eine sichere Identitätslösung notwendig, um die Sicherheit zu gewährleisten. Doch diese Thematik wird nur selten bis gar nicht an den Universitäten, geschweige denn in den Ausbildungen behandelt. Aufgrund meines breiten Vorwissens im System- und Netzwerkadministrationsbereich mit Schwerpunkt Windows Systemen, als auch spezieller Tätigkeit im Active Directory Security Bereich, bot sich mir die Gelegenheit dieses Wissen im Studienprojekt in Form eines Kurses zu strukturieren und in Zukunft potenziell weiterzugeben.

Auch wenn die aktuellen Kursinhalte lediglich die Grundlagen vermitteln sollen, reicht es dennoch, um die Grundidee des Identity- und Accessmanagements und dessen Sicherheit rüberzubringen. Prinzipiell bietet die Thematik aber noch einen viel umfassenderen Ausbau des Kurses.

3 Kursbeschreibung

Dieser Kurs soll eine Einsicht in die Funktionsweise des Microsoft Active Directory, und den dazugehörigen gängigen Angriffen geben.

3.1 Zielgruppe

Dieser Kurs richtet sich an Studierende mit Interesse an IT-Security und speziell Identity- und Accessmanagementsystemen (hier Active Directory).

Voraussetzungen:

- Netzwerkkenntnisse
- Grundlegende Programmierkenntnisse

3.2 Lernziele

Die Studierenden erwerben Kenntnisse über das Active Directory und den eingesetzten Kommunikationsprotokollen (Kerberos, LDAP und NTLM). Die Studierenden kennen die Funktionsweise von Berechtigungsstrukturen.

Sie sind in der Lage Daten aus dem Active Directory auszulesen, Berechtigungsstrukturen zu verstehen und zu evaluieren und Kerberos Transaktionen nachzuvollziehen. Weiterhin erwerben sie die Fähigkeit zur Ausnutzung der gängigen Sicherheitslücken im Active Directory sowie die Manipulation von Kerberos Transaktionen.

3.2.1 Fachliche Kompetenzen

Die Studierenden:

- Kennen die Funktionsweise von gängigen Authentifizierungsprotokollen
- Können gängige Schwachstellen im Active Directory identifizieren
- Können gängige Tools im Active Directory Security Umfeld bedienen

3.2.2 Methodische Kompetenz

Die Studierenden sind in der Lage:

- Die Sicherheit einer Active Directory Installation einzuschätzen

3.3 Empfohlene Literatur

- W. Boswell: Inside Windows Server 2003

4 Kursaufbau

Der Kurs gliedert sich im Wesentlichen in drei Teile. Zuerst kommen die Grundlagen, die näher erläutern was das Active Directory ist und wie es funktioniert, anschließend die Authentifizierungsmechanismen und zum Schluss die Zugriffskontrolle.

Diese Themen decken somit die grundlegenden Funktionen ab, die das Active Directory bereitstellt (Autorisierung und Authentisierung), mit dem Zusatz der Einleitung und Motivation.

4.1 Einführung und Grundlagen

Wie bereits beschrieben, haben reguläre Mitarbeiter selten bis gar keinen Kontakt mit dieser Art von Systemen, weswegen es wichtig ist, überhaupt erst ein Bewusstsein dafür zu schaffen.

Angefangen damit, was ein Identity- und Accessmanagement System überhaupt macht, und wofür man es braucht. Anschließend erfolgt die Überleitung zum Active Directory und dessen Ökosystem, mit anschließender Überleitung warum die Sicherheit eines solchen Systems eine hohe Priorität hat

4.2 Architektur

Es ist essenziell zu verstehen, wie ein System funktioniert, bevor man sich über weiterführende Themen wie Sicherheit Gedanken macht. Dementsprechend folgt ein Exkurs in die Architektur des Active Directories. Es folgen Themen, die die Datenbank, das Zugriffsprotokoll LDAP, die Administration, und Gruppen-(Richtlinien) beschreiben.

4.3 Authentifizierung

Eine weitere Kernkomponente des Active Directories sind die Authentifizierungsmechanismen, die eine zentrale Rolle bei der Benutzung als auch bei offensiven Aktionen spielen. Es werden die Funktionsweisen von NTLMv1 und v2, als auch Kerberos näher erläutert, wobei der Fokus auf Kerberos liegt, da es sich hierbei um die modernere und meistgenutzte Authentifizierungskomponente handelt. Anschließend erfolgt noch ein kurzer Exkurs zu den Service Principal Names, die eine zentrale Rolle bei der Authentifizierung bei Diensten (z.B. SQL, IIS, o.ä.) mittels Kerberos spielen.

4.3.1 Authentifizierung – Offensive Methoden

Aufbauend auf der Funktionsweise von Kerberos, folgen nun die Erläuterung der offensiven Tools und Vorgängen. Es wird auf die einzelnen Möglichkeiten zum Missbrauch von Tickets und NTLM Hashes eingegangen, als auch die Benutzung und Funktionsweise von Mimikatz, dem „Swiss Army Knife of Windows Credentials“. Des Weiteren wird auch das Red-/Blue-Team Tool „BloodHound“ vorgestellt, welches sich als veritables Tool im Active Directory Bereich entwickelt hat. Es bietet eine umfassende Übersicht über die Berechtigungs- und Zugriffsstrukturen im Active Directory, und wird deshalb sowohl bei Red- als auch bei Blue-Team Engagements sehr häufig benutzt, um Sicherheitslücken zu identifizieren.

4.4 Zugriffskontrolle

Zuletzt erfolgt die Einführung in die letzte Komponente des Active Directories, der Zugriffskontrolle. Es wird erklärt, wie die Zugriffskontrolle mittels Access Control Lists realisiert werden, wie ein Securitydescriptor aufgebaut ist, der Unterschied zwischen DACL und SACL wird näher beleuchtet, und anschließend die Access Control Entries betrachtet.

Außerdem erfolgt noch eine Übersicht, wie Windows die Access Control Entries evaluiert und interpretiert. Weiterhin wird auch die Vererbung und Delegation näher erklärt, da es sich hierbei um wichtige Mechanismen der Zugriffskontrolle handeln, die auch für das weitere Verständnis wichtig sind.

4.4.1 Zugriffskontrolle – Offensive Methoden

Es folgen wieder die Erklärungen, wie entsprechende Access Control Entries eine Rechteausweitung ermöglichen. Dafür werden sowohl die eingebauten Tools wie PowerShell, als auch darauf aufbauende Module wie PowerView benutzt. Außerdem inkludiert ist auch eine Ausführung über die Angriffsmethoden DCSync und DCShadow, welche zwar nicht strikt auf Zugriffsberechtigungen beschränken, sondern auch Kerberos bzw. Replikationsmechanismen zurückgreifen. Dennoch sind die Grundlagen für diese beiden Angriffe besondere Berechtigungen, die dieses Vorgehen erst ermöglichen.

5 Labor

Begleitend zum Kurs wird auch ein praktischer Aufgabenteil bereitgestellt, um die erlernten Vorgehensweisen und Tools auch anzuwenden und somit die Kenntnisse zu vertiefen.

Hierfür werden zwei virtuelle Maschinen bereitgestellt, die zum einen ein Windows Active Directory und zum anderen einen Windows Client bereitstellen. Das Active Directory wird mit Daten gefüllt, um eine Struktur nachzubilden, die in etwa einem kleinen Unternehmen entspricht. Weiterhin werden dann absichtlich schädliche Berechtigungen vergeben, die eine Rechteausweitung zulassen. Außerdem werden auch Aufgaben in Verbindung mit Mimikatz bereitgestellt, beispielsweise Credential-/Token Theft oder Angriffe wie DCSync/DCShadow. Aufgrund des Umfangs des Labors, wird dieser Teil aktuell noch erarbeitet.

5.1 Topologie

Die Topologie des Labors ist einfach gehalten, um unnötige Komplexität zu vermeiden. Dies würde zu einem erheblichen Mehraufwand führen, um das Labor zu entwerfen und später auch automatisiert zu installieren und bereitzustellen.

In Abbildung 1 ist die Topologie des Netzwerks schematisch dargestellt. Zu sehen ist der Active Directory Server, der Tool beziehungsweise Clientcomputer als auch der Jumphost. Letzterer ist mit mehreren Netzwerkkarten ausgestattet, sodass er sowohl von außen erreichbar ist als auch eine Verbindung zum abgeschotteten Active Directory Netzwerk herstellen kann. Zu keinem Zeitpunkt soll ungewollter Datenverkehr aus dem abgeschotteten Netzwerk nach außen, in das Produktionsnetzwerk dringen. Der Jumphost fungiert als DMZ und reicht lediglich RDP nach außen weiter, um eine Verbindung in das interne Netzwerk zu ermöglichen.

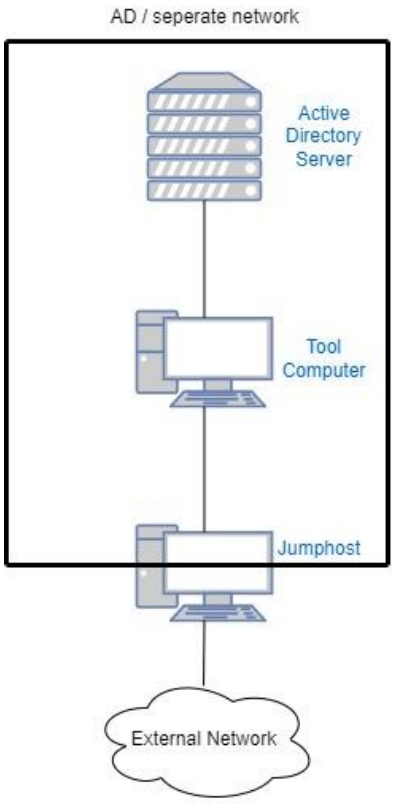

Abbildung 1: Netzwerktopologie der Laborumgebung

5.2 Aufgaben und Angriffsszenarien

5.2.1 Privilege Escalation

Ziel dieser Aufgaben ist es, durch falsch beziehungsweise schädliche Berechtigungen, Zugriff auf andere Accounts zu erhalten. Darunter fallen Access Control Entries wie:

- MemberOf
- GenericAll
- WriteOwner
- GetChanges / GetChangesAll (ermöglicht DCSync/DCShadow)

Diese erlauben entweder die Modifikation der Zugriffsberechtigung eines Objekts oder wie im letzten Fall sich als Domain Controller auszugeben, und somit den Datenbankinhalt auszulesen oder sogar zu verändern. Sobald die Zugriffsberechtigungen modifizierbar sind, bieten sich vielerlei Möglichkeiten das Objekt dahingehend zu manipulieren, um Zugriff darauf zu erhalten. Beispielsweise können Passwörter zurückgesetzt, Gruppenmitgliedschaften (und damit Zugriffsberechtigungen auf Ressourcen) geändert, Service Principal Names hinzugefügt, oder andere Einstellungen geändert werden.

Die Möglichkeiten sind je nach Art des Objekts verschieden. Gruppenrichtlinienobjekte bieten dann zum Beispiel lediglich die Möglichkeit, Kontrolle über einen oder mehrere Computer zu erlangen für den diese Gruppenrichtlinie gilt. Für Benutzer bieten sich oben genannte Möglichkeiten

5.2.2 Kerberos

Auch zum Authentifizierungsmechanismus gibt es verschieden Aufgaben die zu lösen sind, wobei die Möglichkeiten aufgrund des Laboraufbaus begrenzt ist. Dies stellt jedoch kein größeres Problem dar, da die skizzierten Szenarien als Vermittlung der Funktionsweise ausreichen.

Teil des Labors werden sowohl Pass-the-Hash als auch Golden Ticket Angriffe sein. Hier gilt es, den Hash eines angemeldeten Benutzers aus dem Arbeitsspeicher auszulesen und mittels Mimikatz ein valides Ticket-granting-Ticket vom Domain Controller ausstellen zu lassen. Durch diese Vorgehensweise ist es möglich, die Identität eines Benutzers zu „stehlen“, sich als diesen auszugeben und auf dessen Ressourcen zuzugreifen beziehungsweise weiterführende Angriffe einzuleiten.

Die als „Golden Ticket“ bekannte Angriffsmöglichkeit, bietet einem Angreifer einen Persistenzmechanismus, und ist dementsprechend erst spät in einem Angriff relevant. Durch das Auslesen der Active Directory Datenbank ist es möglich, an den Kennwort-Hash des

Key-Distribution-Center Accounts zu gelangen. Mithilfe dessen werden alle Ticket-granting-Tickets verschlüsselt, was bedeutet, dass ein Angreifer sich beliebige Tickets ausstellen lassen kann.

Zuletzt wird das „Kerberroasting“ noch behandelt, welches unter Umständen ein Sicherheitsrisiko darstellt. Aufgrund der Funktionsweise von Kerberos verschlüsseln Benutzer und/oder Computer die einen Dienst (SQL, HTTP etc.) bereitstellen (und somit das Service Principal Name Attribut gesetzt haben) ein Ticket-Granting-Service Ticket mit ihrem Passworthash. Es ist dabei egal, ob das Objekt einen tatsächlichen Dienst bereitstellt oder nicht, solang das Service Principal Name Attribut gefüllt ist.

Jeder authentifizierte Benutzer kann nun ein TGS-Ticket für diesen Dienst anfragen, auch wenn er nicht die Absicht hat diesen Dienst tatsächlich zu benutzen. Dadurch ist es einem Angreifer möglich, das Kennwort des Benutzers bzw. Computers mittels Bruteforcing oder Wörterbuchattacken zu erraten. Dies setzt voraus, dass ein entsprechend schwaches Kennwort gewählt wurde.

5.2.3 Verschiedenes

Um noch ein alltägliches Beispiel in das Labor zu integrieren, wird das Thema „Password Spraying“ behandelt. Hierbei handelt es sich um das Vorgehen des automatisierten Ausprobierens bekannter Passwörter bei einer vielen oder allen Accounts einer Umgebung. Anders als bei einem Bruteforce-Angriff wird hier nicht ein oder mehrere wenige Accounts gezielt angegriffen um das Passwort zu erraten, sondern so viele Accounts wie möglich mit wenigen, bekannten Passwörtern ins Visier zu nehmen. Es ist auch heutzutage noch ein großes Problem, dass Benutzer entweder unsichere oder bekannte Kennwörter verwenden, und dementsprechend ein leichtes Ziel darstellen.

Diese Art von Angriff wird in den Folien zwar nicht explizit erwähnt, stellt jedoch einen guten Einstieg in die Thematik dar und sensibilisiert für die Benutzung sicherer Kennwörter.

5.3 Walkthrough

Dieser Teil stellt dar, wie die einzelnen Aufgaben konzipiert und gelöst werden sollen. Der Ablauf ist in Abbildung 2 visualisiert. Ziel des Labors ist es, die Grundlagen der praktischen Anwendungen der Tools und Sicherheitslücken näher zu bringen. Diese sind zwar nicht gerade kompliziert, können jedoch mit begleitenden Aufgaben wie zum Beispiel beobachten des Netzwerkverkehrs, oder Analyse der Eventlogs ergänz werden.

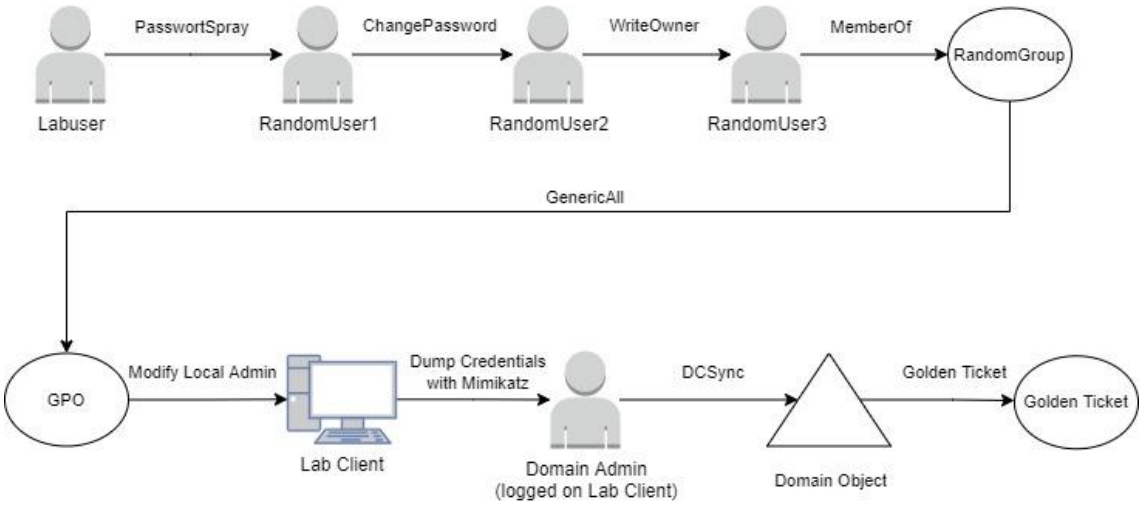

Abbildung 2: Visualisierung des Laborablaufs

Der Labuser ist der Einstiegspunkt des Labors, die Zugangsdaten werden bereitgestellt. Mittels eines PasswortSpray Angriffs werden die Zugangsdaten von „RandomUser1“ bekannt. Der tatsächliche Name des Accounts ist in diesem Fall irrelevant, da dieser bei der Einrichtung zufällig vergeben wird. Dieser besitzt die Möglichkeit, das Passwort für den Benutzer „RandomUser2“ zu verändern. Durch das Ändern des Passwortes auf einen neuen Wert, ist es möglich sich mit diesem Benutzer anzumelden beziehungsweise seine Identität anzunehmen. Weiterhin hat der dieser Benutzer die Möglichkeit, den Besitzer des nächsten Benutzers zu ändern. Dadurch ergibt sich die Möglichkeit, die Access Control List anzupassen. Doch anstatt hier lediglich wieder das Kennwort zu ändern, soll nur die Möglichkeit geboten werden, einen Service Principal Name hinzuzufügen. Hierdurch ergibt sich die Möglichkeit eines Kerberroasting Angriffes. Durch Bereitstellen einer Wordlist, in der das Kennwort aufgeführt ist, ist es möglich via eines Wörterbuchangriffs das Passwort des Accounts zu erlangen. Nun besitzt dieser Benutzer die Berechtigungen, Mitglieder zu der Gruppe „RandomGroup“ hinzuzufügen. Auch hier ist der Name nicht relevant und wird zufällig bei der Einrichtung generiert. Diese Gruppe besitzt die Berechtigung ein Gruppenrichtlinienobjekt zu modifizieren, die auf den „Lab Client“ gelinkt ist, wodurch es möglich ist, einen Benutzer zu den lokalen Administratoren hinzuzufügen. Dies ist notwendig, um anschließend mittels Mimikatz den NTLM Hash des Domain Admins auszulesen, welcher auf dem „Lab Client“ angemeldet ist. Dies wird sichergestellt, in dem ein Scheduled Task konfiguriert wird, der alle 5 Minuten einen Befehl im Benutzerkontext des Domain Admins ausführt. Nun ist man in der Lage via DCSync auf die komplette Active Directory Datenbank zuzugreifen, welches zum nächsten Punkt führt: Durch das Auslesen des „krbtgt“ Account Hashes ist es möglich, ein sog. Golden Tickets zu erstellen. Dieses Ticket kann für den Domain Admin ausgestellt werden und hat eine Gültigkeit von 10 Jahren, wodurch ein Angreifer die notwendige Persistenz erhält, um sich unbefristet in der Umgebung aufzuhalten.

6 Ausblick

Die aktuellen Inhalte vermitteln die Grundlagen was sowohl die Funktionsweise des Active Directories angeht als auch offensive Maßnahmen, die in der Praxis gängig sind. Aufgrund des zeitlich limitierenden Faktors konnten jedoch nicht alle Themenbereiche erfasst, und manche auch nur knapp behandelt werden.

Für die Zukunft ist es denkbar, weitere Inhalte in den Kurs aufzunehmen die entweder ausgelassen oder auch nur angeschnitten wurden. Möglich wäre folgende Auswahl an weiteren Themen.

6.1 Architektur/Funktionsweise

Speziell in diesem Bereich besteht noch einiges an Potential. Es besteht die Möglichkeit, näher auf die Funktionsweise von LDAP einzugehen, welches die Grundfunktionalität zum Abfragen von Daten bereitstellt. Auch wenn die Grundzüge der Vererbung und Objektinstanzen erläutert wurden, besteht noch die Möglichkeit diese Themen weiter zu vertiefen, als auch neue Bereiche wie LDAP Filter, das Datenbankschema, Protokolldetails, und die Namespace Struktur mit aufzunehmen. Diese sind zwar nicht unmittelbar notwendig für ein grundlegendes Verständnis der Technologie, aber für tiefergehende Einblicke doch unverzichtbar.

Weiterhin ist auch der Replikationsmechanismus im Active Directory überhaupt nicht aufgenommen worden, da dies ein durchaus komplexes Themengebiet ist, und nicht unmittelbar für Angriffe relevant ist. Dennoch ist die Funktionsweise ein relevanter Bestandteil für das Active Directory, und spielt ebenfalls eine wichtige Rolle, um resiliente Active Directory Umgebungen zu entwerfen und umzusetzen.

Ebenfalls wurden Vertrauensstellungen zwischen verschiedene Domänen beziehungsweise Forests auch nicht in diesen Kurs integriert, da diese einerseits in kleinen Umgebungen so gut wie nicht vorkommen, als auch in Angriffsszenarien relativ komplexe Szenarien einnehmen und dementsprechend schwer zu vermitteln sind.

Zuletzt wäre es ebenfalls sinnvoll die Integration und Funktionsweise von DNS im Zusammenhang mit dem Active Directory näher zu bringen. Durch die enge Verzahnung beider Komponenten ist es wichtig, zu verstehen wie diese miteinander Wechselwirken und welche Funktionen sie genau einnehmen. Weiterhin ist die Authentifizierungsarchitektur innerhalb von Windows ein wichtiger Bestandteil in der modernen Windowssicherheit, und sollte ebenfalls seinen Platz in diesem Kurs finden. Denn um zu verstehen, wie die Zugangsdaten in Windows verwendet werden, spielt eine essenzielle Rolle, um

einen Missbrauch von Zugangsdaten zu erkennen, und wie beispielsweise das Auslesen von Zugangsdaten funktioniert.

6.2 Technische und Organisatorische Maßnahmen/Hardening

Bisher wurden in diesem Kurs lediglich die Funktionalitäten der Active Directory Komponenten, und deren gängigen Angriffe skizziert. Um ein holistisches Bild zu schaffen, wäre es ebenfalls wichtig, die Absicherung einer solchen Umgebung detailliert zu erläutern. Eine bekannte Sicherheitslücke kann mit gängigen Tools leicht ausgenutzt werden, aber ein sicheres und stabiles System zu entwerfen und zu deployen gehört zu den Anspruchsvolleren Aufgaben, die auch in der Industrie sehr gefragt sind.

Es sollten also Themen nähergebracht werden, die diese Bereiche genauer behandeln. Darunter zählen beispielsweise die Enhanced Security Admin Environment oder das Tiering Konzept eines Active Directory. Diese Konzepte setzen jedoch tiefergehende Kenntnisse im Active Directory Design voraus, weswegen diese, wie zuvor angesprochen, ebenfalls vermittelt werden müssen.

6.3 Eventlogging / Detection

Ein weiterer wichtiger Bestandteil sollte das Erkennen und Aufspüren von Angriffen selbst werden. Es ist nicht ausreichend ein System sicher zu gestalten, da ein genügend motivierter Angreifer früher oder später eine Sicherheitslücke findet. Das kontinuierliche Monitoring ist wichtig, um Angriffe frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten. Dieser Themenkomplex ist aufgrund seiner Vielschichtigkeit jedoch nicht zu unterschätzen. Es bedarf einer genauen Analyse welche Ereignisse protokolliert, wie diese gespeichert, und was für eine Art von Security Incidence and Monitoring (SIEM) Lösung tatsächlich in Frage kommt. Daran gebunden sind ebenfalls Fragen wie, was bei einem Auftreten eines bestimmten Events unternommen werden muss, wie die genaue Analyse von statten geht, und welche Art von Maßnahmen eingeleitet werden sollen.

6.4 Andere Produkte des Active Directory Ökosystems

In diesem Kurs wurde lediglich das als Active Directory bekannte Active Directory Domain Services Produkt von Microsoft behandelt, doch das gesamte Ökosystem von Microsoft ist wesentlich reichhaltiger.

Beispielsweise existieren noch die Zertifikatsdienste, Federation Services, oder Cloud-Dienste. Diese bieten aufgrund ihrer Komplexität zwar genug Inhalt, um eigene Kurse zu

entwerfen, jedoch könnten die Grundzüge der Funktionsweisen dargestellt werden, um einen Eindruck davon zu erhalten. Auch im Zusammenspiel mehrerer Produkte ergeben sich dann Angriffsszenarien, die bei alleiniger Betrachtung eines Produkts nicht funktionieren.

7 Feedback und Lessons Learned

Die Studienarbeit war für mich eine gute Möglichkeit, meine Kenntnisse im System-/Netzwerkadministrationsbereich, als auch im Active Directory Bereich zum einen anzuwenden als auch zu vertiefen. Durch das Umstrukturieren in einen Kurs, der sich an Studenten ohne Vorwissen in diesem Bereich richtet, war es nötig einiges neu zu formulieren und einfach verständlich zu machen. Während dieses Prozesses konnten einige Themenbereiche selbst weiter vertieft und besser verstanden werden.

Dieser Strukturierungs- und auch Darstellungsprozess in PowerPoint Folien stellte sich als große Herausforderung heraus. Es ist ein großer Unterschied zwischen guten Folien gesehen zu haben, und selbst entsprechende Folien zu entwerfen, da hier Erfahrung vonnöten ist, die ich bisher noch nicht sammeln konnte. Viele Faktoren beeinflussen die Güte der Folien, wie zum Beispiel die richtige Wahl und Positionierung der Bilder, knappe, aber dennoch präzise Formulierungen, bis hin zur Schriftart und Größe. Aber auch die korrekte Strukturierung, Organisation und Vermittlung der Inhalte ist von entscheidender Bedeutung, um die Studenten an die jeweiligen Themenbereiche heranzuführen. Auch sinnvoll gestaltete Beispiele helfen dabei, das Wissen zu visualisieren und zu vermitteln, da so die „trockene“ Theorie in reale Praxis überführt, und entsprechend verknüpft werden kann. Dementsprechend war, und ist es weiterhin, ein laufender Prozess die Folien zu überarbeiten und zu verbessern.