Technische
Hochschule
Rosenheim

Fakultät für Informatik

Studiengang Informatik Master

Domain Trust Discovery

Seminar wissenschaftliches Arbeiten

von

Christian Pritzl

Datum der Abgabe: 28.06.2021

Erstprüfer: Prof. Dr. Reiner Hüttl

ERKLÄRUNG

Ich versichere, dass ich diese Arbeit selbstständig angefertigt, nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Rosenheim, den 28.06.2021

Christian Pritzl

Kurzfassung

Domain Trust Discovery ist eine der aktuell 27 Techniken, welche die The MITRE Corporation in ihrer ATT&CK Matrix unter der Taktik „Discovery“ aufführt. Mittels entsprechender Werkzeuge ist es einem Angreifenden möglich, die, als Domain Trusts bezeichneten, Vertrauensbeziehungen im Verzeichnisdienst Active Directory zu nutzen, um Informationen über das Angriffsziel zu sammeln. Da diese Werkzeuge in der Regel auf Schnittstellen und Methoden basieren, die standardmäßig auf einer Windows Server Instanz vorhanden sind und grundlegende Funktionen einer Active Directory ausnutzen, ist eine gezielte Abwehr oder Entdeckung einer Domain Trust Discovery schwer möglich. Die folgende Arbeit ordnet Domain Trust Discovery zunächst anhand von Beispielen in den Ablauf eines Angriffs ein. Anschließend klärt sie wichtige Begriffe im Umfeld von Active Directory, die nötig sind um das Konzept von Domain Trusts zu verstehen. Eine Übersicht über dieses Konzept sowie seine Ausprägungen, die in einer Active Directory verwendet werden können, werden im Anschluss erläutert. Im nächsten Schritt erfolgt eine Vorstellung gängiger Werkzeuge sowie zugrunde liegender Methoden des Serverbetriebssystems, auf welchen diese Werkzeuge basieren, um eine Domain Trust Discovery durchzuführen. Im anschließenden Kapitel wird anhand eines Beispiels das praktische Vorgehen bei einer Domain Trust Discovery aus Sicht des Angreifenden beschrieben. Abschließend folgt ein Einblick, welche Möglichkeiten Administrierende zur Verfügung stehen, um Domain Trust Discovery in einem Netzwerk zu erschweren und den gewonnenen Informationsgehalt zu minimieren.

Schlagworte: Domain Trust Discovery, Domain Trust, Active Directory Domain Services, Powershell, MITRE ATT&CK

Abkürzungsverzeichnis

ADDS Active Directory Domain Services 4
AD Active Directory iii
AES Advanced Encryption Standard 8
API Application Programming Interface 11
CVE Common Vulnerabilities and Exposures 6
DACL Discretionary Access Control List 6
DMZ Demilitarisierte Zone 19
DNS Domain Name System 6
GUID Global Unique Identifier 13
IaaS Infrastructure as a Service 1
LDAP Lightweight Directory Access Protocol 11
NIST National Institute of Standards and Technology 19
NT New Technology 13
SID SecurityID 6
TDO Trust Domain Object 6

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung und Abgrenzung

Unter der Bezeichnung „Discovery“ mit der ID TA0007 wurde die MITRE ATT&CK Matrix im Februar 2019 um Techniken aus dem Bereich der Informationsgewinnung über das Zielsystem beziehungsweise –netzwerk erweitert. Die Liste 1.1 bietet eine Übersicht über den aktuellen Stand der 27 Techniken, die unter Discovery zusammengefasst werden. In Abgrenzung zu TA0043 Reconnaissance hat der Angreifende bereits Zugriff auf die Zielumgebung erhalten. Bevor der Angreifende zum Angriff übergeht, können diese Techniken helfen, die Umgebung zu analysieren und potentielle Schwachstellen im Zielsystem zu identifizieren. Relevante Informationen reichen dabei von Benutzerkonten auf einem lokalen System oder in einer Domäne, E-Mailkonten, installierte Anwendungen und Programme oder im Browser abgelegte Lesezeichen bis hin zu entsprechenden Passwordpolicies. Im Netzwerkbereich werden beispielsweise Trust-Beziehungen in Domänen oder Netzwerkservices aufgeführt. Auch Informationen über verwendete Cloud-Infrastruktur in einer Infrastructure as a Service (IaaS)-Umgebung oder Sandboxumgebungen, wie virtuelle Maschinen, können für Angreifende interessant sein.

Da im Rahmen von Discovery in der Regel betriebssystemabhängige Systemwerkzeuge zum Einsatz kommen, ist es für Administrierende schwierig, Systeme und Netzwerke gezielt abzusichern beziehungsweise verdächtiges Verhalten festzustellen.[1] [2]

1 [34]
2 [29]

Discovery 1.1 Aktuelle Techniken der Taktik Discovery in MITRE ATT&CK [34]

- T1087 Account Discovery
- T1010 Application Window Discovery
- T1217 Browser Bookmark Discovery
- T1580 Cloud Infrastructure Discovery
- T1538 Cloud Service Dashboard
- T1526 Cloud Service Discovery
- T1613 Container and Resource Discovery
- T1482 Domain Trust Discovery
- T1083 File and Directory Discovery
- T1046 Network Service Scanning
- T1135 Network Share Discovery
- T1040 Network Sniffing
- T1201 Password Policy Discovery
- T1120 Peripheral Device Discovery
- T1069 Permission Groups Discovery
- T1057 Process Discovery
- T1012 Query Registry
- T1018 Remote System Discovery
- T1518 Software Discovery
- T1082 System Information Discovery
- T1614 System Location Discovery
- T1016 System Network Configuration Discovery
- T1049 System Network Connections Discovery
- T1033 System Owner/User Discovery
- T1007 System Service Discovery
- T1127 System Time Discovery
- T1497 Virtualization/Sandbox Evasion

2 Technischer Hintergrund und Hinführung

Das folgende Kapitel führt die Taktik Domain Trust Discovery der Technik Discovery ein und nennt eine Reihe von aktuellen Angriffen, bei denen Domain Trust Discovery zum Einsatz gekommen ist. Anschließend wird eine technische Grundlage zu den Themen AD und Domain Trust geschaffen, welche erforderlich sind, um zu verstehen wie Domain Trust Discovery abläuft. Anschließend werden einige sicherheitsrelevante Punkte genannt und hinterfragt, die dazu dienen, Domain Trust Discovery für einen Angreifenden zu erschweren.

2.1 Relevanz und aktuelle Beispiele

Unter der ID T1482 fasst die MITRE ATT&CK Matrix verschiedene Vorgehensweisen sowie Verteidigungs- und Erkennungsstrategien im Zusammenhang mit der Enumeration von sogenannten Domain Trusts zusammen.[1] Diese sind ein Konzept aus der Microsoft Windows AD, dem Verzeichnisdienst von Windows Server, welche in Kapitel 2.2 genauer vorgestellt werden. Domain Trusts etablieren Vertrauensbeziehungen zwischen einzelnen Komponenten der AD und stellen somit eine kritische Komponente bei der Enumeration, also dem Sammeln von Informationen, einer AD dar. Dies verursacht in der Regel noch keinen Schaden, bietet Administrierenden allerdings die Möglichkeit einen Angriff zu erkennen. Näheres hierzu in Kapitel 4. Sobald Zugriff auf das Unternehmensnetzwerk erlangt werden konnte, ist es über Kompromittierung der AD prinzipiell möglich, volle Kontrolle über das Organisationsnetzwerk zu erlangen. Ein prominentes Beispiel ist die Schadsoftware „Emotet“ , welche das universelle Angriffswerkzeug „Trickbot“ nachlädt. Trickbot nutzt zum enumerieren von Domain Trusts Komponenten des Powershell-Frameworks Empire sowie das Kommandozeilenwerkzeug Nltest.[2]

2015 wurde der Deutsche Bundestag Opfer eines Angriffs mit Emotet. Über die Kompromittierung der Domänenadministratoraccounts war es den Angreifenden möglich, sich im Netzwerk auszubreiten. Obwohl die Netzwerke der einzelnen

1 [14]
2 [35]

Bundestagsfraktionen von einander getrennt sind, bestand über Domain Trusts eine gemeinsame Vertrauensbeziehung zum Netzwerk des Bundestages.[3] Im Jahr 2019 wurde der Heinz Heise Verlag, beziehungsweise die Heise Gruppe, ebenfalls Opfer eines Angriffs mit Emotet. Auch hier wurde Trickbot nachgeladen, um Informationen über das Netzwerk zu sammeln und sich dort auszubreiten. Als Konsequenz wurde entschieden ein komplett neues Netz mit neuer AD zu erstellen.[4]

2.2 Domain Trust im Kontext von Active Directory

Als Active Directory Domain Services (ADDS), kurz AD, wird der Verzeichnisdienst für Netzwerkressourcen, Benutzerkonten und Zugriffsrechten innerhalb eines auf Windows Server basierenden Unternehmensnetzwerkes bezeichnet.[5] Domain Trusts sind ein Konzept um Vertrauensbeziehungen zwischen verschiedenen Organisationseinheiten zu erstellen. Unternehmen oder Organisationen, deren Netzwerk aus mehr als einer Domäne besteht, bekommen durch Domain Trusts die Möglichkeit, Ressourcen und Services zwischen diesen Domänen zu teilen und diese authentifizierten Anwendern beziehungsweise Diensten zur Verfügung zu stellen.[6]

2.2.1 Überblick Active Directory

Eine AD dient der Nachbildung der Struktur einer Organisation und bietet die Möglichkeit, Netzwerkressourcen beziehungsweise –objekte zentral zu administrieren. Einzelne Organisationsbereiche werden dabei über sogenannte „Domänen“ von einander abgetrennt.

Die Domäne stellt innerhalb einer AD die kleinste Organisationseinheit dar, siehe Abbildung 2.2 Nummer 3, und umfasst mindestens einen Domänencontroller. Da sie gemeinsam administrierte Objekte wie PCs oder Drucker, Sicherheitsrichtlinien und Vertrauensbeziehungen über physikalische Orte hinweg zusammenfassen, werden Domänen auch als Containerobjekte bezeichnet. Eine Domäne stellt dabei eine Grenze für Authentifizierung und Autorisierung dar.

Mehrere Domänen können zu einer hierarchischen Baumstruktur, einem sogenannten „Tree“ zusammengefasst werden, siehe Abbildung 2.2 Nummer 2. Jede neu hinzugefügte Domäne wird automatisch zu einem Kind der Wurzeldomäne eines Trees. Da Domänen

3 [10]
4 [30]
5 [36]
6 [8]

innerhalb eines Trees allerdings eigenständig bleiben, werden Administrationsrechte nicht automatisch von Kinddomänen an die Wurzel übertragen. Zwischen den Domänen eines Trees werden automatisch sogenannten „Kerberos Two Way Transitive Trusts“ , siehe Tabelle 2.1, eingerichtet, die ein Vertrauen auch über nicht direkt verbundenen Domänen hinweg ermöglichen und somit automatisch Zugriff auf Ressourcen freigeben.[7]

Mehrere Trees werden zu einem sogenannte „Forest“ zusammengefasst, siehe Abbildung 2.2 Nummer 1. Dieser ist die größte Organisationseinheit einer AD-Architektur und bildet dabei eine vollständige AD-Instanz ab. Die Grenze eines Forest stellt hierbei, laut der Definition von Microsoft, die Grenze zur vertrauensunwürdigen Außenwelt dar, womit erst zwischen Forests Vertrauensbeziehungen explizit erstellt werden müssen.[8] Microsoft bezeichnet einen Forest folglich auch als „Security Boundary“ .[9] Der standardmäßig erstellte Authentifizierungspfad innerhalb eines Forest wird in Abbildung 2.1 dargestellt.

2.2.2 Überblick Domain Trust

Microsoft unterscheidet verschiedene Arten von Vertrauensbeziehungen, die entweder standardmäßig, beispielsweise beim Erstellen einer Domäne, oder explizit, beispielsweise bei der Anbindung einer externen Ressource, vom Administrierenden erstellt werden müssen. Domain Trusts können entweder als unidirektionale One-Way-Trusts in eine Richtung etabliert werden oder in beide Richtungen als bidirektionale Two-Way-Trusts. Um Vertrauensbeziehungen mit geringem Aufwand erweitern zu können, gibt es sogenannte transitive Trusts, die ähnlich einer Verkettung funktionieren. Wenn *Domäne A* einer *Domäne B* vertraut und diese wiederum einer *Domäne C*, dann vertraut *Domäne A* auch *Domäne C*. Analog können auch nicht-transitive Trusts erstellt werden, um genau diese Art von Verkettung zu verhindern.[10]

Der Tabelle 2.1 lassen sich alle Arten von Domain Trusts, welche aktuell in einer AD erstellt werden können, entnehmen. Bei der Nomenklatur ist zu beachten, dass die Richtung der Vertrauensbeziehungen entgegengesetzt zur Zugriffsrichtung läuft. Das bedeutet bei einem One-Way-Trust vertraut *Domäne A* einer *Domäne B*, womit Rechner aus *Domäne B* auf Ressourcen aus *Domäne A* zugreifen können, aber nicht umgekehrt. Solche Vertrauensbeziehungen unterliegen allerdings auch Einschränkungen. Ein Domänenadministrator ist nicht automatisch auch Administrator einer anderen,

7 [11]
8 [22]
9 [9]
10 [6]

vertrauenswürdigen Domäne. Ein solches Recht muss aus Sicherheitsgründen explizit gesetzt werden.

Technisch werden die Vertrauensbeziehungen jeweils von einem sogenannten Trust Domain Object (TDO) repräsentiert, welches Attribute, wie den Domain Name System (DNS)-Namen der Domäne, die SecurityID (SID) der Domäne und die Art und Transitivität der Vertrauensbeziehung speichert. Innerhalb eines Forest haben alle Domänen Zugriff auf die TDOs des Forest und können somit alle verfügbaren Vertrauensbeziehungen auslesen. TDOs werden dabei in den sogenannten „Global Catalog“ repliziert, welcher Kopien von AD-Objekten enthält, um beispielsweise bei domänenübergreifenden Suchvorgängen nicht über die jeweiligen Domänencontroller vorgehen zu müssen. Grundsätzlich wird hierfür kein dedizierter Server benötigt, da jeder Domänencontroller die Funktion des Global Catalog übernehmen kann. Da der sogenannte „ntSecurityDescriptor“ eines jeden AD-Objekts von einem authentifizierten Anwender gelesen werden kann, ist es möglich, über entsprechende Vertrauensbeziehungen, Discretionary Access Control List (DACL) Einträge zu finden, die sich über Domänen hinweg erstrecken. Somit lässt sich feststellen, auf welche Objekte in einer anderen Domäne Zugriff besteht.[11]

2.3 Absicherung von Domain Trusts

Wie in Kapitel 2.2 gezeigt, handelt es sich bei Vertrauensbeziehungen zwischen einzelnen Komponenten einer AD um kritische Komponenten. Bei der Einrichtung dieser Beziehungen sollten Sicherheitsbedenken folglich eine tragende Rolle spielen. Im Folgenden werden einige generelle Richtlinien genannt, die eine Enumeration erschweren und somit die Quantität an Informationen einschränken können, die bei Domain Trust Discovery ermittelt wird.

Laut Definition von Microsoft stellt der Forest die Grenze der automatisch erstellten Vertrauensbeziehungen dar, was als „Security Boundary“ bezeichnet wird. Um Forests miteinander in Beziehung zu setzen, müssen Vertrauensbeziehungen explizit vom Administrierenden erstellt werden, innerhalb eines Forests geschieht dies jedoch implizit. Dies muss kritisch hinterfragt werden, da so bereits ein kompromittiertes Objekt innerhalb einer Domäne die Sicherheit des gesamten Forest gefährden kann. Beispielsweise Drucker sind hierfür aufgrund alter Protokolle anfällig.[12] Die Common Vulnerabilities and Exposures

11[22]
12[38]

Tabelle 2.1 Übersicht der möglichen Typen von Vertrauensbeziehungen in einer AD, [7]

Trust Typ	**Transitivität und Richtung**	**Beschreibung**
Parent & child	Transitiv bidirektional	standardmäßig bei Kinddomäne, Authentifizierungsanfragen fließen aufwärts von Subdomänen durch Elterndomänen zu Trusted-Domäne
Tree-root	Transitiv bidirektional	standardmäßig bei Erstellung von Domaintree in existierendem Forest
External	Nontransitiv uni- / bidirektional	Ermöglicht Zugriff von Außen in Windowsdomäne, oder auch falls zugreifende Domäne in nicht vertrauenswürdigen Forest
Realm	(Non) Transitiv uni- / bidirektional	Ermöglicht Beziehung zwischen Windows Domäne und nicht-Windows Kerberos Realm (zB. Linux)
Forest	Transitiv uni- / bidirektional	Ermöglicht Teilen von Ressourcen zwischen Forests, standardmäßig unidirektional
Shortcut	Transitiv uni- / bidirektional	Verkürzung der Loginzeit zwischen zwei Domänen in einem Windows Server Forest

(CVE)-2019-0683[13] beschreibt exemplarisch eine Möglichkeit zur Rechteausweitung innerhalb eines kompromittierten Forests mittels Drucker. Grundsätzlich sollten aus diesem Grund Vertrauensbeziehungen nur eingerichtet werden, sofern und solange eine entsprechende Notwendigkeit besteht und dann vorzugsweise unidirektional, um die Navigation innerhalb der AD einzuschränken.

Da Benutzer aus vertrauten Domänen Teil der „AUTHENTICATED USERS“ Gruppe sind, sollte diese Gruppe nicht dazu verwendet werden, Zugriffsberechtigungen zu erteilen. Damit Administrationsrechte nur innerhalb einer Domäne gelten, dürfen Administrationskonten nur in der jeweiligen Domäne existieren und der Zugriff nicht über Vertrauensbeziehungen hinweg erstellt werden.

Trusts sollten generell für eine Verschlüsselung mittels Advanced Encryption Standard (AES)-Algorithmus konfiguriert werden. Anstelle von externen Trusts sollten Foresttrusts konfiguriert werden, da diese Kerberosauthentifzierung verwenden. Kerberos ist das moderne Standardprotokoll für Authentifizierungsprozesse in der AD.[14] [15]

Ein Angreifender, der in Besitz eines Domänen- oder Enterpriseadministratoraccounts gelangt ist, kann Netzwerkauthentifizierungsanfragen überwachen und somit die SID abgreifen. Diese ermöglicht eine eindeutige Identifizierung von Anwendern, Gruppen, Rechnern und Domänen in einer AD. Jede SID ist dabei über die DACL eines Objekts in der Domäne mit entsprechenden Zugriffsrechten auf dieses Objekt verknüpft. Da der sogenannte „ntSecurityDescriptor“ eines jeden AD-Objekts einer Domäne von einem authentifizierten Anwender gelesen werden kann, ist es möglich, über entsprechende Vertrauensbeziehungen, DACL Einträge zu finden, die sich über Domänen hinweg erstrecken. Somit lässt sich feststellen auf welche Objekte in einer anderen Domäne Zugriff besteht. Mittels SID-Filtern kann verhindert werden, dass ein Anwender seine SID aus Domäne A verwendet, um Zugriffe in Domäne B zu erlangen. Dabei werden beim Zugriff über eine Vertrauensbeziehung auf eine vertrauende Domäne aus dem Zugriffstoken alle SIDs entfernt, die nicht aus der vertrauenden Domäne stammen. Dabei wird implizit die sogenannte „SID-Historie“ deaktiviert, welche es ermöglicht zusätzliche, beliebige SIDs an einen Zugriffstoken anzufügen.[16][17] Microsoft hat dies als potentielle Gefahr identifiziert und SID-Filterung standardmäßig für externe Trusts und Foresttrusts aktiviert.[18]

13[13]
14[8]
15[12]
16[12]
17[39]
18[5]

Interessanterweise ist dabei die Filterung für Vertrauensbeziehungen zwischen Forests standardmäßig stringenter als die Filterung bei einer externen Vertrauensbeziehung. Dies lässt sich über das Trustattribut „TREAT_AS_EXTERNAL“ anpassen.[19]

19[26]

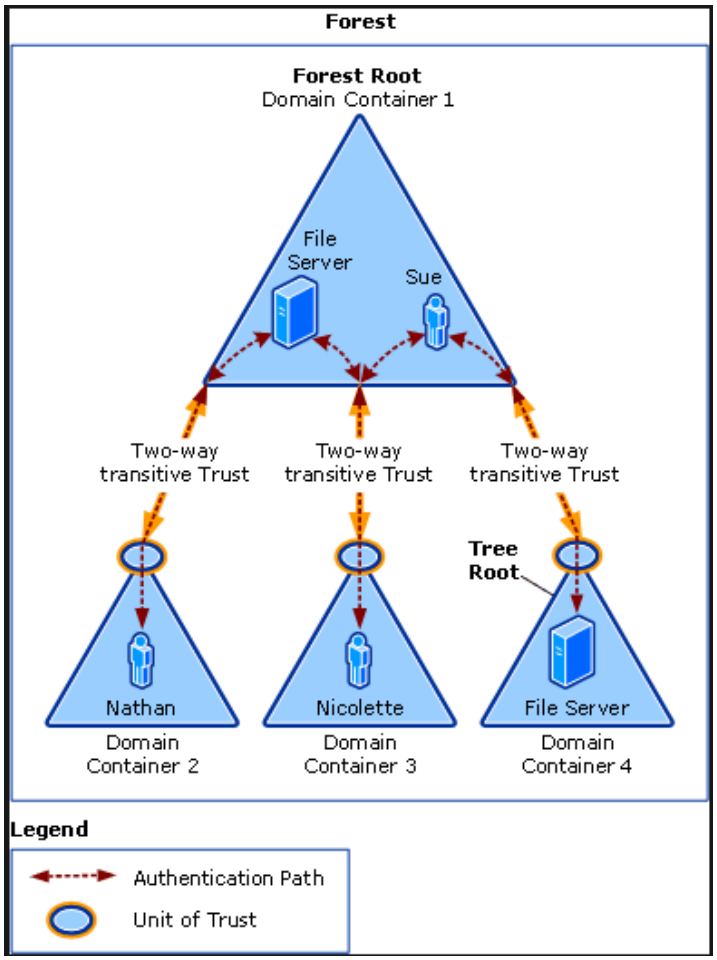

Abbildung 2.1 Standardauthentifizierungspfade innerhalb eines Forest [9]

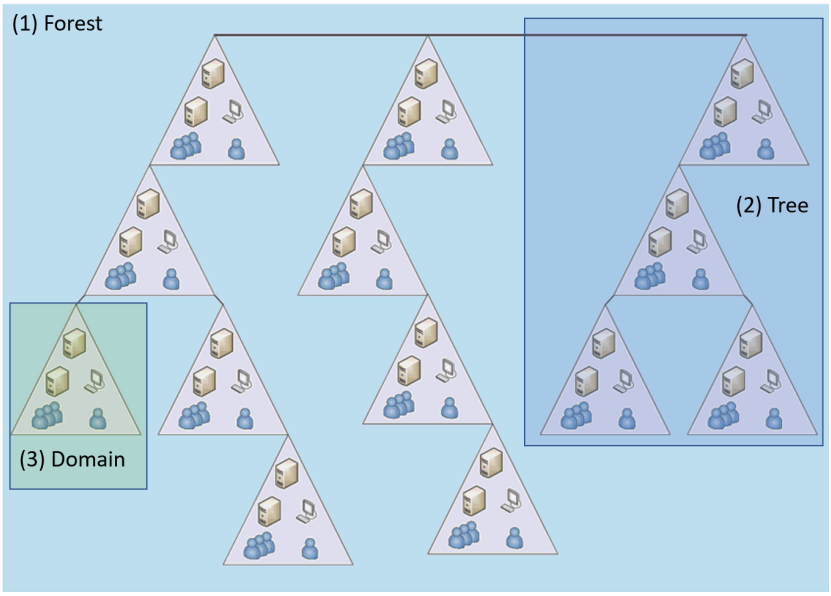

Abbildung 2.2 Übersicht Active Directory Domain, Tree und Forest, bearbeitet [11]

3 Vorgehen und Durchführung

Im folgenden Kapitel wird das theoretische Wissen aus dem vorhergehenden Kapitel 2 genutzt, um anhand eines Beispiels zu erläutern, wie und warum Domain Trust Discovery funktionieren kann. Hierzu werden zunächst gängige Werkzeuge und Methoden vorgestellt. Anschließend wird die in Abbildung 3.4 gezeigte Domäne mittels des quelloffenen Post-Exploitation Werkzeugs PowerView enumeriert. In Kapitel 4 wird dieser Vorgang referenziert, um Möglichkeiten zur Mitigation vorzustellen.

3.1 Vorstellung gängiger Werkzeuge und Methoden

Es gibt aktuell drei grundsätzliche Möglichkeiten in einer AD Domain Trusts zu enumerieren. Generell gilt für alle vorgestellten Methoden, dass das Ergebnis abhängig davon ist, in welcher Richtung die Enumeration durchgeführt wird, da Vertrauensbeziehungen nicht bidirektional sein müssen.[1] [2]

- .NET-Methoden, beispielsweise aus dem Namensraum *System.DirectoryServices.ActiveDirectory.Domain*[3]
- Aufruf der Win32 Application Programming Interface (API) über *DSEnumerateDomainTrusts()*[4]
- Lightweight Directory Access Protocol (LDAP) Queries [5]

Im Folgenden werden diese anhand von Aufrufen auf die Domäne sub.dev.testlab.local vorgestellt. Diese Methoden werden normalerweise nicht direkt verwendet, sondern durch entsprechende Anwendungen abstrahiert. Gängige Post-Exploitation Frameworks auf Basis von Powershell sind Empire[6], PowerSploit/PowerView[7] oder PoshC2[8]. Auch das

1 [20]
2 [32]
3 [15]
4 [25]
5 [23]
6 [27]
7 [18]
8 [17]

```
PS C:\Users\localadmin\Documents> $ENV:USERDNSDOMAIN
SUB.DEV.TESTLAB.LOCAL
PS C:\Users\localadmin\Documents> Get-DomainTrust -NET

SourceName            TargetName          TrustType TrustDirection
----------            ----------          --------- --------------
sub.dev.testlab.local dev.testlab.local ParentChild  Bidirectional
sub.dev.testlab.local external.local       External       Outbound
```

Abbildung 3.1 Ausgabe der PowerView-Methode Get-DomainTrust -NET [20]

administrative Kommandozeilenwerkzeug Nltest kann zur Enumeration von Domain-Trusts genutzt werden.[9] Der Vorteil der nltest.exe liegt darin, dass sie als Bestandteil von Windows Server verfügbar ist, sobald AD-Komponenten installiert sind.[10] Ein weiteres gängiges Werkzeug ist das freie Kommandozeilenwerkzeug AdFind, welches verschiedene Programme, wie zum Beispiel ldapsearch, search.vbs, ldp, dsquery und dsget, zum Abfragen von Domain Trusts kombiniert. AdFind muss allerdings explizit installiert werden, was entsprechende Rechte auf dem Server voraussetzt.[11] Da diese Methoden Informationen in unterschiedlicher Detailtiefe und Präsentationsform zurückliefern, ist es von Vorteil Methoden zu kombinieren und somit einen umfangreicheren Überblick über die Architektur der Vertrauensbeziehungen zu erhalten.

3.1.1 Domain Trust Enumeration mit .NET

Als „.NET“ bezeichnet Microsoft seine plattformübergreifende Entwicklungsplattform, welche aktuell in Version 5 vorliegt.[12] Für Domain Trust Discovery ist insbesondere die Domain-Klasse im Namensraum *System.DirectoryServices.ActiveDirectory* von Interesse, da sie eine AD repräsentiert und entsprechende Methoden zur Verwaltung verfügbar macht.[13] Abbildung 3.1 zeigt die Ausgabe einer Enumeration mit der PowerView-Methode *Get-DomainTrust -NET*, welche intern die .NET-Methode *[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().GetAllTrustRelationships()* verwendet. Diese Methode liefert im Vergleich zu den anderen vorgestellten Vorgehensweisen, vergleichsweise wenig Daten zurück. Der Vorteil liegt hier mehr in der übersichtlichen Präsentationsform.[14]

9 [3]
10 [4]
11 [21]
12 [24]
13 [15]
14 [20]

3.1.2 Domain Trust Enumeration mit Win32 API

Bei Win32 handelt es sich um die 32-bit Version der Windows API, eingeführt mit Windows New Technology (NT), welche eine Schnittstelle für Entwickler zum Betriebssystem Microsoft Windows bietet. Da die Windows API sowohl für Desktop als auch für Server existiert, verfügt sie über Methoden zum interagieren mit AD. Die aktuelle Implementierung setzt dabei mindestens Windows Server 2008 als Plattform voraus. ADs lassen sich über die Methode *DsEnumerateDomainTrustsA()*, definiert im Header *dsgetdc.h*, enumerieren. Beim Aufrufer muss es sich um einen authentifizierten Domänenbenutzer handeln.[15] Im Erfolgsfall wird eine Struktur vom Typ *DS_DOMAIN_TRUSTSA* zurückgeliefert, welche Informationen über die Zieldomäne, wie die SID und Global Unique Identifier (GUID), sowie den Typ und Richtung der Vertrauensbeziehung beinhaltet. Abbildung 3.2 zeigt die Ausgabe einer Enumeration mit der PowerView-Methode *Get-DomainTrust -API*, welche intern auf diesen API-Aufruf zurückgreift. Im Vergleich zur Ausgabe der .NET-basierten Methode aus Kapitel 3.1.1 lässt sich erkennen, dass hier deutlich mehr Informationen über die untersuchte Vertrauensbeziehung zurückgeliefert wird. Dieser API-Aufruf wird von Blodhound/SharpHound2 sowie mutmaßlich auch von Nltest verwendet.[16] [17]

3.1.3 Domain Trust Enumeration mit LDAP

Bei LDAP handelt es sich um ein auf TCP/IP basierendes Netzwerkprotokoll, welches Möglichkeiten bietet, sich mit über dem Internet verteilten Verzeichnisdiensten zu verbinden und diese zu durchsuchen. Vereinfacht ausgedrückt beinhaltet dabei AD eine Implementierung von LDAP mit zusätzlichen Funktionen und Komponenten, wie das Authentifizierungsprotokoll Kerberos.[18] Da Domain Trusts in AD als TDOs gespeichert werden und somit für alle Domänen innerhalb eines Forest lesbar sind, vergleiche Kapitel 2.2, lassen sich über eine LDAP-Query mit Filter auf *objectClass=trustedDomain* entsprechende Informationen über die Vertrauensbeziehungen auslesen. Dieser Ansatz wird standardmäßig in der aktuellen Version von PowerView eingesetzt. Der Methodenaufruf Get-DomainTrust liefert die in Abbildung 3.3 gezeigten Informationen zurück.[19]

15[25]
16[20]
17[16]
18[2]
19[20]

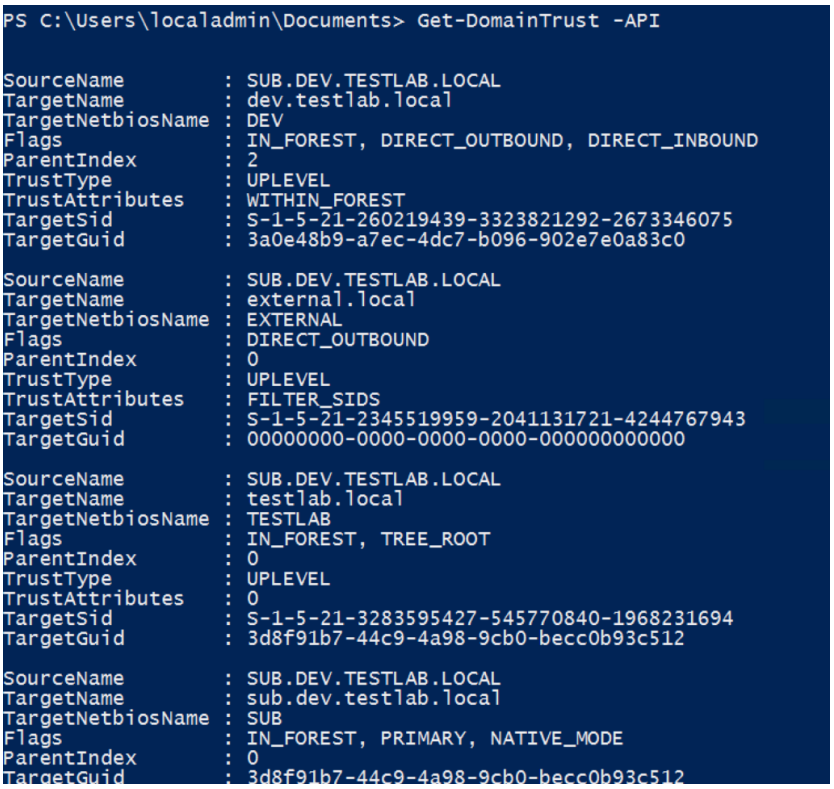

Abbildung 3.2 Ausgabe der PowerView-Methode Get-DomainTrust -API [20]

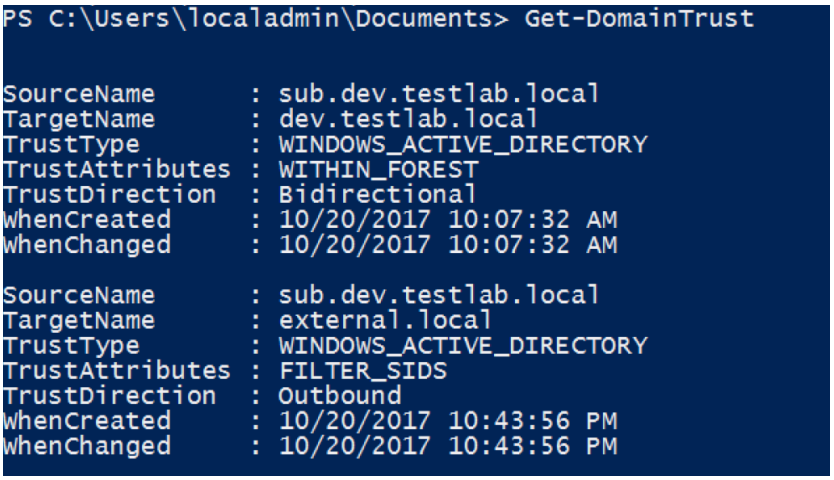

Abbildung 3.3 Ausgabe der PowerView-Methode Get-DomainTrust [20]

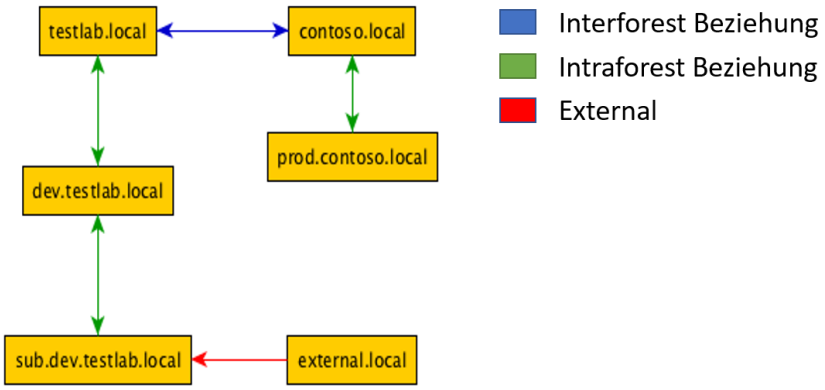

Abbildung 3.4 Ausgabe von TrustVisualizer, angewendet auf die Beispieldomäne sub.dev.testlab.local, Screenshot bearbeitet [20]

3.1.4 Visualisierung von Domain Trusts

Um die extrahierten Informationen einer Enumeration grafisch aufzubereiten, kann beispielsweise das Python-basierte Werkzeug TrustVisualizer eingesetzt werden.[20] Abbildung 3.4 zeigt die entsprechende Visualisierung der Beispieldomäne sub.dev.testlab.local.

3.2 Durchführung Domain Trust Discovery

Für die Durchführung der Domain Trust Discovery auf das Zielnetzwerk aus Abbildung 3.4 wird das Werkzeug PowerView verwendet, welches Teil des Post-Exploitation Frameworks PowerSploit ist.[21] MITRE listet PowerSploit unter der ID S0194 als quelloffenes Offensive-Security-Framework für die Windowsplattform auf.[22] PowerView kommt dabei zur sogenannten „Network Situational Awareness “ also der Situationsanalyse innerhalb der Netzwerkumgebung, wie zum Beispiel der Analyse von Domain Trusts, zum Einsatz. Standardmäßig verwendet PowerView LDAP-Queries um Domain Trusts zu analysieren. Der initiale Zugriff auf das Netzwerk wurde im vorliegenden Beispiel über einen kompromittierten Account in der Domäne *external.local* hergestellt.

Im ersten Schritt wird versucht eine Übersicht aller bestehenden Domain Trusts zu erstellen. Hierzu wird die aktuelle Domäne *sub.dev.testlab.local* nach Vertrauensbeziehungen zu anderen Domänen durchsucht. Mittels des Kommandos *Get-DomainTrust -Domain sub.dev.testlab.local* lassen sich aufgrund dieser Beziehung alle direkten

20[19]
21[18]
22[28]

Vertrauensbeziehungen enumerieren, die sub.dev.testlab.local mit anderen Domänen hat. Siehe hierzu Abbildung 3.3. Abhängig von den zurück erhaltenen Vertrauensbeziehungen lässt sich dieses Kommando rekursiv auf die Ergebnisse anwenden, um weitere potentielle Ziele zu identifiziert oder, falls bereits ein Ziel existiert, einen potentiellen Angriffspfad zu erstellen.

Um darüber hinausgehend weitere Beziehungen innerhalb des kompromittierten Forest aufzudecken, wird mittels des Kommandos *Get-DomainTrust -SearchBase „gc://sub.dev.testlab.local“* der globale Katalog zur Informationsgewinnung herangezogen. In diesem sind, wie in Kapitel 2.2 beschrieben, alle TDOs des Forest repliziert. Abbildung 3.5 zeigt die entsprechende Ausgabe, rot eingerahmt ist dabei die Domäne *contoso.local*, welche über eine interforest Beziehung, vergleiche die blaue Kante in der Abbildung 3.4, eine Zugriffsmöglichkeit auf einen zweiten Forest ermöglichen kann.

Da, wie in Tabelle 2.1 aufgeführt, externe Trusts implizit nicht-transitiv sind, könnte für einen Zugriff auf *contoso.local* mittels des Kommandos *Get-DomainForeignGroupMember -Domain sub.dev.testlab.local* geprüft werden, ob es Anwender, Gruppen oder Rechnern (sogenannte „Security Principals“) gibt, die Zugriff auf Ressourcen in der Ausgangsdomäne haben. Die Abbildung 3.6 zeigt die entsprechende Ausgabe, dieser lässt sich im zweiten roten Kasten auch das Übersetzen einer SID in einen Benutzernamen mittels des Kommandos *<SID> | ConvertFrom-SID* entnehmen.

Das Kommando *Get-DomainForeignUser* wird ausgeführt, um zu ermitteln ob Anwender aus *sub.dev.testlab.local* Mitgliedschaften in anderen Gruppen des Forests haben. Abbildung 3.7 [23] lässt sich beispielsweise entnehmen, dass der Nutzer „subuser1“ Teil der „DevUniversalGroup“ ist. Mittels *Get-DomainForeignGroupMember -Domain <Domäne>* lassen sich anschließend auch die Gruppen der Domänen *dev.testlab.local* und *testlab.local* prüfen. Lokale Administratorgruppen oder solche mit Einträgen in den DACLs interessanter Objekte stehen dabei im Fokus. Die Gruppenzugehörigkeiten lassen sich hierbei in drei Kategorien aufteilen. „Domain Local Groups“ beinhalten Anwender sowohl aus dem aktuelle Forest als auch aus anderen Forests. „Global Groups “ ermöglichen keine Mitgliedschaften über Domänen hinweg und sind in diesem Fall folglich irrelevant für das weitere Vorgehen. „Universal Groups“ , wie die genannte „DevUniversalGroup“ aus Abbildung 3.7, können jeden Anwender aus dem eigenen Forest als Mitglied haben. Über das Auslesen des ntSecurityDescriptor lassen sich DACL Einträge finden, die sich über Domänen hinweg erstrecken womit sich letztendlich feststellen lässt, auf welche Objekte in

23[20]

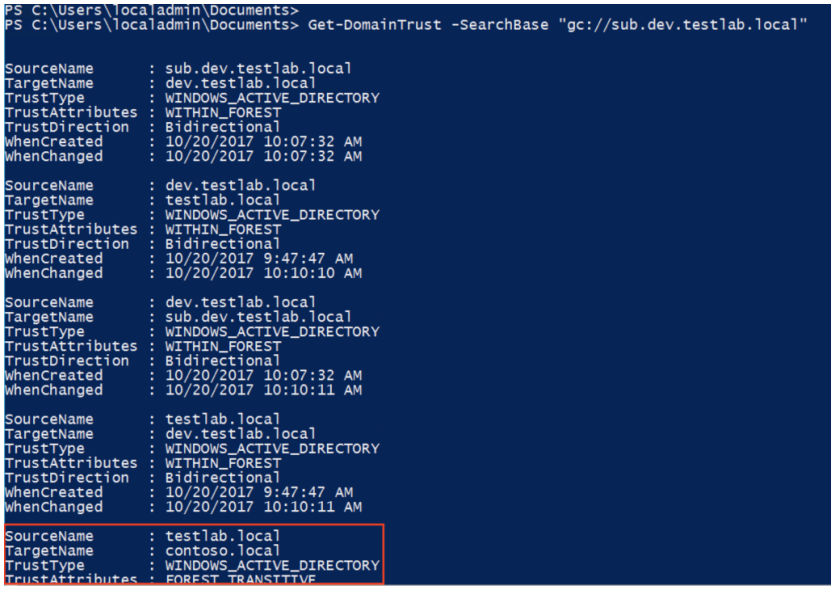

Abbildung 3.5 Ausgabe der Suche über den Global Catalog der Beispiel AD [20]

einer anderen Domäne Zugriff besteht. Hierzu wird das Kommando *Get-DomainObjectACL -Domain <foreign.domain>* ausgeführt.[24]

Somit wäre im Beispielfall der komplette Forest, ausgehend von einer kompromittierten externen Domäne aus, aufgedeckt. Für einen potentiellen Angriff steht nun eine Übersicht über die Architektur der AD, sowie die enthaltenen Nutzeraccounts und Services zur Verfügung.

24[20]

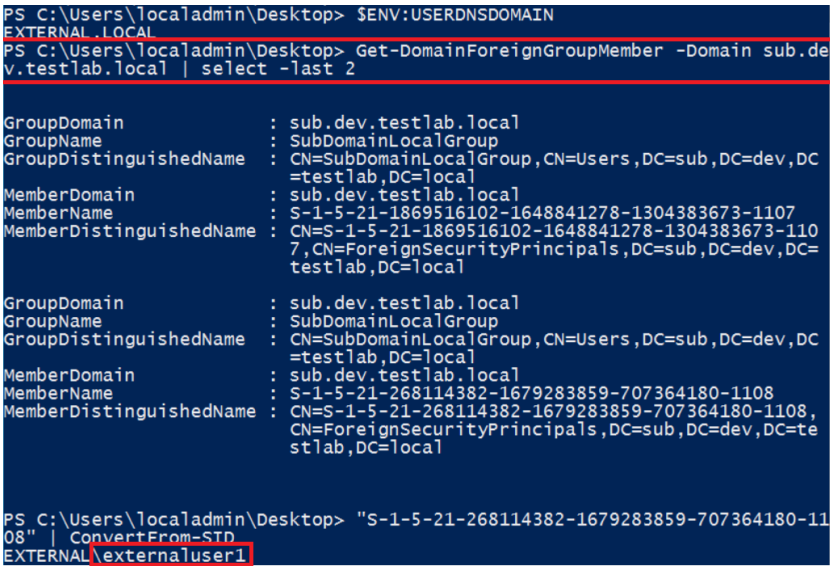

Abbildung 3.6 Ausgabe von Get-DomainForeignGroupMember, bearbeitet [20]

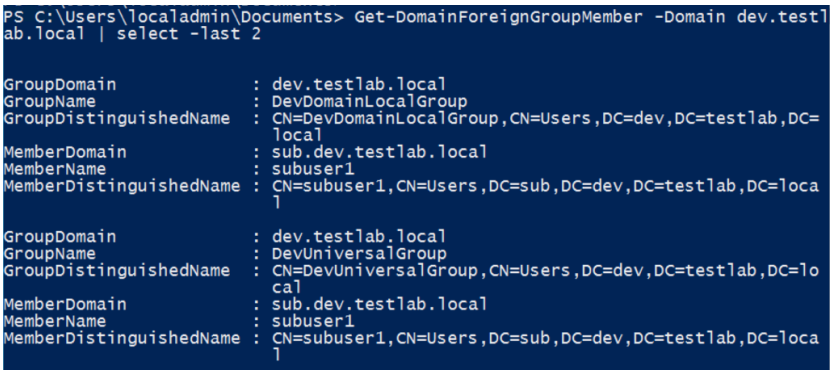

Abbildung 3.7 Ausgabe von Get-DomainForeignUser [20]

4 Mitigation und Entdeckung

Durch entsprechend sorgfältige Implementierung der Vertrauensbeziehungen lässt sich die Angriffsoberfläche bereits deutlich reduzieren.

Da ein vollständiger Verzicht auf Domain Trusts in einem modernen Unternehmensnetzwerk kaum vertreten ist, listet die ATT&CK-Datenbank aktuell „Audit“ und „Netzwerksegmentierung“ unter dem Stichwort „Mitigations“ auf.[1]. Die Unterteilung eines Netzwerkes in einzelne Segmente, welche beispielsweise über eine Demilitarisierte Zone (DMZ) verbunden sind, ist eine grundsätzliche Anforderung an die Sicherheitsarchitektur eines Netzwerkes, welche unter anderen vom National Institute of Standards and Technology (NIST) in der Publikation 800-82 beschrieben wird.[2] Mittels Netzwerksegmentierung kann die Qualität der extrahierten Informationen im Falle einer Domain Trust Discovery eingeschränkt werden. Angewendet auf das Beispiel aus Kapitel 3.2 zeigt sich, dass für die Enumeration von *contoso.local* ausgehend von *testlab.local* ein anderer Ansatz über die Benutzergruppen verwendet werden musste, da zwischen diesen beiden Domänen ein nicht-transitiver externer Trust existiert.

Auch sollten Vertrauensbeziehungen nur dort etabliert werden, wo sie notwendig sind. Kritisch zu berücksichtigen ist auch, ob bidirektionale Vertrauensbeziehungen für den jeweiligen Anwendungsfall nötig sind oder ob restriktiver vorgegangen werden kann. Solche Überprüfungen können durch regelmäßige Audits erreicht werden. AD bietet eine Reihe von Auditfunktionen, die beispielsweise auf Lesezugriffe auf Objekte, Systemevents und Prozessüberwachung abzielen.[3]

Da Domain Trusts ein grundsätzlicher Bestandteil einer AD sind, existieren native Werkzeuge und Schnittstellen um diese zu verwalten. Angreifende, die auf diese Möglichkeiten zurückgreifen, lassen sich nur eingeschränkt von autorisierten Anwendern und Diensten unterscheiden. Ergänzend zu den von MITRE genannten Punkten kann die Analyse von Logs als weitere Möglichkeit zur Mitigation genannt werden. Insbesondere

1 [33]
2 [31]
3 [1]

LDAP-Queries, welche standardmäßig Port 389 beziehungsweise verschlüsselt Port 636 nutzen, lassen sich im Netzwerklog erkennen. Die exemplarische Enumeration aus Kapitel 3.2 mittels PowerView hätte sich so identifizieren lassen. Auch Kommandozeilenwerkzeuge wie Nltest oder AdFind können über verdächtige Aufrufparameter in den Prozesslogs identifiziert werden.

„Discovery“ ist oftmals generell nur ein Teilbereich eines komplexeren Angriffs, da, wie in Kapitel 1 erwähnt, der Angreifende bereits Zugriff auf das Zielnetzwerk erlangt haben muss. Folglich sollten bereits verdächtige Aktivitäten aufgefallen sein. Etwa 85% aller Angriffe wurden allerdings erst nach einer Zeit von mehreren Wochen entdeckt, obwohl in 84% der Fälle entsprechende Hinweise in den Logs vorhanden gewesen wären.[4]

Domain Trust Discovery lässt sich folglich aktuell nicht sinnvoll verhindern, allerdings kann durch entsprechende Aufmerksamkeit bereits bei der Erstellung und Wartung der Netzwerke der Erfolg einer Enumeration deutlich eingeschränkt werden. Bei der Erstellung und Auswertung der Logeinträge kann ein Angriff während einer Enumeration entdeckt und entsprechend reagiert werden.

4 [37]

5 Fazit

Das Thema Domain Trust Discovery nimmt in der öffentlichen Wahrnehmung im Themenbereich IT-Sicherheit nur eine kleine Rolle ein. Obwohl entsprechende Werkzeuge existieren, die auch von Schadsoftware eingesetzt werden, ist die Forschungslage relativ dünn. Dies kann durch die Rechercheergebnisse zur Erstellung dieser Arbeit bestätigt werden.

Die vorgestellten Beispiele und Werkzeuge zeigen, dass der Aufwand zur Durchführung einer Enumeration durch einen Angreifenden relativ gering ist, sobald eine Domäne kompromittiert wurde. Zur Interpretation und Weiterverarbeitung der zurückgelieferten Ergebnisse gehört allerdings Wissen über den internen Aufbau einer AD und der zugehörigen Attribute.

Da sich die Techniken von Domain Trust Discovery den Sinn und Zweck dieses Verzeichnisdienstes zu Nutzen machen, ist es für Administrierende schwer sie vollständig zu unterbinden. Allerdings kann über entsprechende Verfahren, wie Netzwerksegmentierung und regelmäßige Audits der Vertrauensbeziehungen, die Qualität der gewonnenen Informationen eingeschränkt werden. Durch Logging und Monitoring innerhalb der AD erhalten Administrierende die Chance einen Angriff anhand der Discovery-Tätigkeiten zu entdecken.

Die Zukunft wird zeigen, ob das Thema Domain Trust Discovery mit dem Wechsel der AD in cloudbasierte Umgebungen an Bedeutung gewinnen wird und ob sich neue Möglichkeiten zur Enumeration ergeben werden.

Literatur

[1] Archiveddocs. *Active Directory Domain Services (AD DS) Auditing Step-by-Step Guide*. Hrsg. von Microsoft Corporation. 2012. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731607(v=ws.10) (besucht am 29. 05. 2021).

[2] Archiveddocs. *Active Directory Search and Publication Technologies: Active Directory*. Hrsg. von Microsoft Corporation. 2021. URL: https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc775686(v=ws.10) (besucht am 18. 04. 2021).

[3] Archiveddocs. *Nltest*. Hrsg. von Microsoft Corporation. 2016. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731935(v=ws.11) (besucht am 29. 05. 2021).

[4] Archiveddocs. *Nltest*. Hrsg. von Microsoft Corporation. 2021. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731935(v=ws.11) (besucht am 11. 04. 2021).

[5] Archiveddocs. *Security Considerations for Trusts: Domain and Forest Trusts*. Hrsg. von Microsoft. 2014. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)?redirectedfrom=MSDN#w2k3tr_trust_security_zyzk (besucht am 05. 04. 2021).

[6] Archiveddocs. *Trust Technologies: Domain and Forest Trusts*. Hrsg. von Microsoft Corporation. 2009. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759554(v=ws.10)?redirectedfrom=MSDN (besucht am 10. 04. 2021).

[7] Archiveddocs. *Trust types: Active Directory*. Hrsg. von Microsoft Corporation. 2011. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc775736(v=ws.10) (besucht am 20. 04. 2021).

[8] Archiveddocs. *What Are Domain and Forest Trusts? Domain and Forest Trusts*. Hrsg. von Microsoft Corporation. 2014. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757352(v=ws.10)?redirectedfrom=MSDN (besucht am 10. 04. 2021).

[9] Archiveddocs. *What Are Domains and Forests?: Active Directory*. Hrsg. von Microsoft. 2014. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)?redirectedfrom=MSDN (besucht am 05. 04. 2021).

[10] Anna Biselli. *Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ*. 2016. URL: https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#protokoll_iuk_6_20150512 (besucht am 03. 04. 2021).

[11] Ulrich B. Boddenberg. *Rheinwerk Computing :: Windows Server 2012 R2 - 8 Active Directory-Domänendienste*. 2014. URL: https://openbook.rheinwerk-verlag.de/windows_server_2012r2/08_001.html#dodtp350e4541-4eb5-44c4-87a6-1398bac8ad4a (besucht am 31. 03. 2021).

[12] Enno Rey Christoph Kuderna. "ERNW WHITEPAPER 67: ACTIVE DIRECTORY TRUST CONSIDERATIONS". In: (2018). URL: https://static.ernw.de/whitepaper/ERNW_Whitepaper67_ADTrustConsiderations.pdf (besucht am 03. 04. 2021).

[13] *CVE - CVE-2019-0683*. 2018. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0683 (besucht am 05. 04. 2021).

[14] *Domain Trust Discovery, Technique T1482 - Enterprise | MITRE ATT&CK®*. 2021. URL: https://attack.mitre.org/versions/v8/techniques/T1482/ (besucht am 31. 03. 2021).

[15] Dotnet-bot. *Domain Klasse (System.DirectoryServices.ActiveDirectory)*. Hrsg. von Microsoft Corporation. 2021. URL: https://docs.microsoft.com/de-de/dotnet/api/system.directoryservices.activedirectory.domain?view=net-5.0 (besucht am 11. 04. 2021).

[16] GitHub. *BloodHoundAD: SharpHound - DomainTrustEnumerations.cs*. 2021. URL: https://github.com/BloodHoundAD/SharpHound (besucht am 18. 04. 2021).

[17] GitHub. *nettitude/PoshC2*. 2021. URL: https://github.com/nettitude/PoshC2 (besucht am 11. 04. 2021).

[18] GitHub. *PowerShellMafia/PowerSploit*. 2021. URL: https://github.com/PowerShellMafia/PowerSploit (besucht am 11. 04. 2021).

[19] GitHub - Will Schroeder. *HarmJ0y/TrustVisualizer*. 2021. URL: https://github.com/HarmJ0y/TrustVisualizer (besucht am 18. 04. 2021).

[20] harmj0y - Will Schroeder. *A Guide to Attacking Domain Trusts*. Hrsg. von Will Schroeder. 2017. URL: http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/ (besucht am 24. 03. 2021).

[21] joeware.net. *AdFind*. 2021. URL: http://www.joeware.net/freetools/tools/adfind/ (besucht am 23. 05. 2021).

[22] Justin Hall. *How trust relationships work for resource forests in Azure Active Directory Domain Services*. Hrsg. von Microsoft Corporation. 2021. URL: https://docs.microsoft.com/de-de/azure/active-directory-domain-services/concepts-forest-trust (besucht am 31. 03. 2021).

[23] LDAP.com. *LDAP.com*. 2021. URL: https://ldap.com/ (besucht am 29. 05. 2021).

[24] Microsoft. *NET | Free. Cross-platform. Open Source*. 2021. URL: https://dotnet.microsoft.com/ (besucht am 11. 04. 2021).

[25] Mikben. *DsEnumerateDomainTrustsA function (dsgetdc.h) - Win32 apps*. Hrsg. von Microsoft Corporation. 2018. URL: https://docs.microsoft.com/de-de/windows/win32/api/dsgetdc/nf-dsgetdc-dsenumeratedomaintrustsa?redirectedfrom=MSDN (besucht am 18. 04. 2021).

[26] Openspecs-office. *[MS-ADTS]: trustAttributes*. Hrsg. von Microsoft Corporation. 2021. (Besucht am 29. 05. 2021).

[27] PowerShell Empire. *PowerShell Empire*. 2021. URL: http://www.powershellempire.com/ (besucht am 11. 04. 2021).

[28] *PowerSploit, Software S0194 | MITRE ATT&CK®*. 2021. URL: https://attack.mitre.org/versions/v8/software/S0194/ (besucht am 24. 04. 2021).

[29] Tripwire Researcher. "The MITRE ATT&CK Framework: Discovery". In: *Tripwire* (2020). URL: https://www.tripwire.com/state-of-security/mitre-framework/the-mitre-attck-framework-discovery/ (besucht am 29. 03. 2021).

[30] Jürgen Schmidt. "Trojaner-Befall: Emotet bei Heise". In: *heise Online* (2019). URL: https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html (besucht am 03. 04. 2021).

[31] Keith Stouffer u. a. *Guide to Industrial Control Systems (ICS) Security*. 2015. DOI: 10.6028/NIST.SP.800-82r2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (besucht am 29. 05. 2021).

[32] The MITRE Corporation. *Discovery, Tactic TA0007 - Enterprise | MITRE ATT&CK®*. 17 October 2018. URL: https://attack.mitre.org/versions/v8/tactics/TA0007/ (besucht am 28. 03. 2021).

[33] The MITRE Corporation. *Domain Trust Discovery, Technique T1482 - Enterprise | MITRE ATT&CK®*. 2021. URL: https://attack.mitre.org/versions/v9/techniques/T1482/ (besucht am 23. 05. 2021).

[34] The MITRE Corporation. *MITRE ATT&CK®: ATT&CK Matrix for Enterprise*. 2021. URL: https://attack.mitre.org/ (besucht am 28. 03. 2021).

[35] *TrickBot, Software S0266 | MITRE ATT&CK®*. 2021. URL: https://attack.mitre.org/versions/v8/software/S0266/ (besucht am 03. 04. 2021).

[36] Frank Ully. "Himmelsgeschenk". In: *Heise* 2020.10 (2020). URL: https://www.heise.de/select/ix/2020/10/2007210021036488235 (besucht am 03. 04. 2021).

[37] Verizon Communications Inc. "Verizon-Data-Breach-Report-2012". In: (2012), S. 3–53. URL: https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf (besucht am 29. 05. 2021).

[38] Will Schroeder. *Not A Security Boundary: Breaking Forest Trusts*. 2018. URL: https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/ (besucht am 29. 05. 2021).

[39] Will Schroeder. *The Trustpocalypse*. 2015. URL: http://www.harmj0y.net/blog/redteaming/the-trustpocalypse/ (besucht am 29. 05. 2021).