txOne networks | Keep the Operation Running

Q2 2023 EDITION

A Practical Model for Quantifying the Risk of Active Directory Attacks

TXOne Threat Research

Authors: Mars Cheng, Dexter Chen

Contents

Executive Summary

Active Directory is commonly used as the backbone of most enterprise networks. If it were to be compromised, attackers would be capable of gaining full control over the entire organization. Despite the significant potential impact, most defenders are unaware of the numerous attack vectors for Active Directory. Attackers can leverage overlooked attack vectors to breach the network and carry out malicious activities. Even if defenders are aware of potential vulnerabilities, they may not be able to prioritize their responses effectively if they are unclear about the severity of each attack vector. Given the high stakes involved, it is therefore critical that defenders have a comprehensive understanding of the various attack vectors for Active Directory.

We have developed a practical model for quantifying the risk of each attack vector in order to simultaneously increase visibility of potential attack vectors and properly prioritize which vector or path should be addressed first. We have also developed a way to quantify the risk of an attack path that is chained together by multiple attack vectors. This enables defenders to comprehensively evaluate the overall risk and mitigate AD attack surface risks in order of their risk result, reducing both the time and manpower needed to fend off AD attacks. By implementing these measures, defenders can better protect their networks against malicious activities and ensure that their organization’s sensitive data remains secure.

Introduction to Defense Challenges of AD

Active Directory Overview

Microsoft's Active Directory (AD) is an essential and ubiquitous component of IT infrastructure nowadays, serving as the backbone of identity and access management (IAM) in Windows-based environments which is used to manage computers and other devices on a network. It provides a centralized location for storing information about users, groups, computers, and other network resources, allowing administrators to manage access to these resources from a single location.

Over 90% of companies in the Global Fortune 1000[1] use AD widely for several vital functionalities, including centralized authentication and authorization, policy enforcement, and network resources management. These functionalities are supported by several AD services and technologies, such as Domain Service for storing AD data and Kerberos for user authentication. We have selected the following feature services provided by Microsoft for a closer look.

- **Active Directory Domain Services (AD DS)**

  Active Directory Domain Services is a server role in Active Directory that allows admins to manage and store information about resources from a network. It is also utilized to store information about network objects, such as user accounts and shared resources, and make this information available. Active Directory uses a structured data storage system to organize this information and integrates security by authenticating logons and controlling access to directory resources. This allows administrators to manage data and organization throughout the network with a single logon and allows authorized users to access resources anywhere on the network. Policy-based administration eases the management of complex networks.[2]

- **Active Directory Federation Service (AD FS)**

  Active Directory Federation Service (AD FS) enables federated identity and access management by securely sharing digital identity and entitlement rights across security and enterprise boundaries. AD FS extends the ability to use single sign-on functionality available within a single security or enterprise boundary to internet-facing applications. This enables customers, partners, and suppliers to have a streamlined user experience while accessing the web-based applications of an organization.[3]

- **Active Directory Certificate Services (AD CS)**

  AD CS enables the creation of Public Key Infrastructure (PKI) as well as the management of certificates, which can be used for encrypting and digitally signing electronic documents, emails, and messages.[4]

- **Active Directory Rights Management (AD RMS)**

  AD RMS can enhance your organization's security strategy by protecting sensitive documents and emails with encryption that is persistent regardless of where a file goes or how it is transported (Information Rights Management, IRM).

  Through IRM policies, individuals and administrators can specify access permissions for documents, workbooks, and presentations. This prevents unauthorized people from printing, forwarding, or copying sensitive information. Once access to a file has been restricted using IRM, access and usage restrictions are enforced no matter where the information's access point may be. This is because the permission to access a file is stored within the document file itself.[5]

In summary, Active Directory (AD) provides a range of management mechanisms, such as DS, CS, FS, and RMS, for the convenience of those in charge of the system. While it is widely adopted and used, one might wonder if there are truly no security issues with these widely used mechanisms. Can users actually use these services safely with no concerns about potential attacks?

Threats in Active Directory

In this session, we will explore the security and threat landscape of AD. According to our analysis, AD is the pathway to the crown jewel. As mentioned earlier, compromising AD grants access to almost all, if not all, systems, applications, and resources within the enterprise network. It should come as no surprise then, that AD has been the specific target in an estimated 90% of cyberattacks in the last several years.[6] With such a high rate, we must investigate what happened to AD. Here we summarize some attack incidents and how AD is leveraged by attackers to inflict devastating damage:

1. **Leveraging Group Policy for Ransomware Deployment**

   Today's threat groups are aware of how important Active Directory (AD) is in the enterprise. They are savvy and have cunningly learned how to abuse the Group Policy (GPO) mechanism to deploy ransomware. Their goal is to spread and execute the ransomware by compromising the domain controller. The ransomware is placed on the domain machine within the scope of GPO, maximizing its potential damage.

   To provide a clear analysis, Figure 1 shows the attack process of commonly targeted ransomware using GPO, and Figure 2 shows how Lockbit 2.0 embedded the group policy abuse into the ransomware. In the first stage, the attacker's goal is to take down domain administrators, or accounts or services that have domain controller permissions, in order to penetrate the enterprise center. Once they've gained entry, the attacker may use various methods, such as establishing C&C, abusing GPO to spread ransomware, and even stealing data before moving onto blackmail and other malicious behaviors. Table 1 lists recent security incidents related to this type of attack.

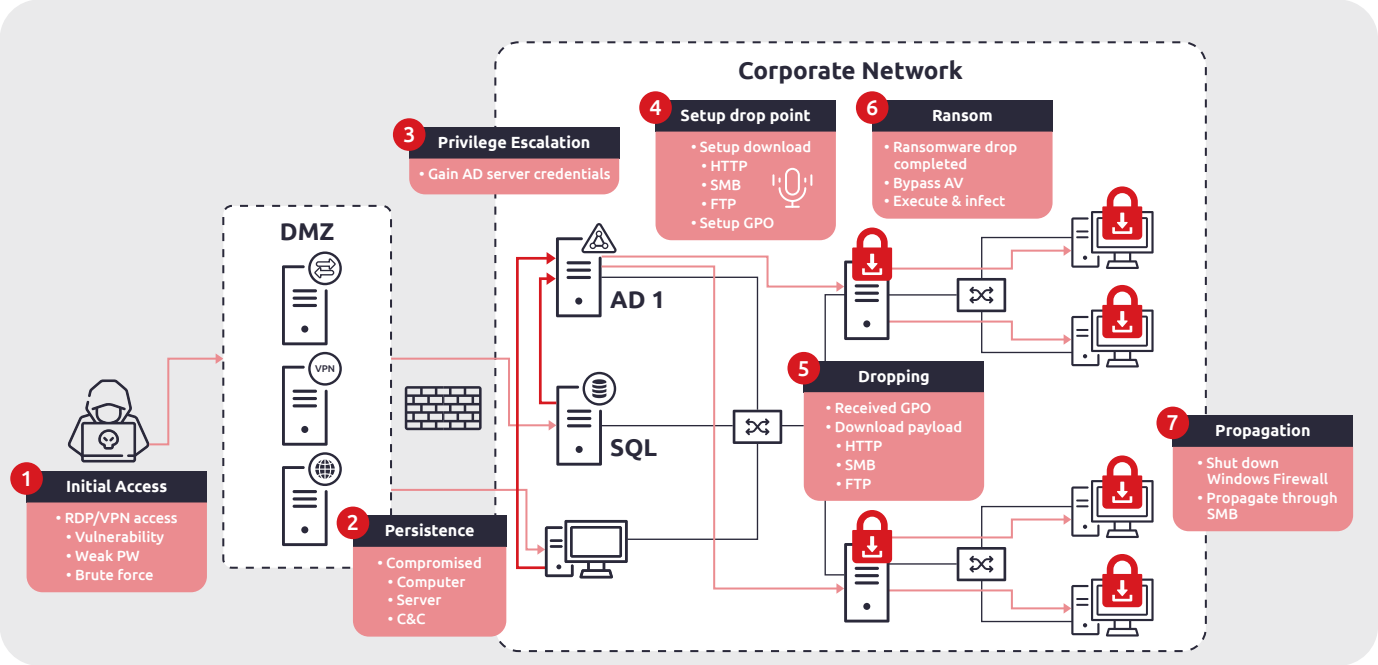


Figure 1: Targeted Ransomware Attack with GPO Case Study

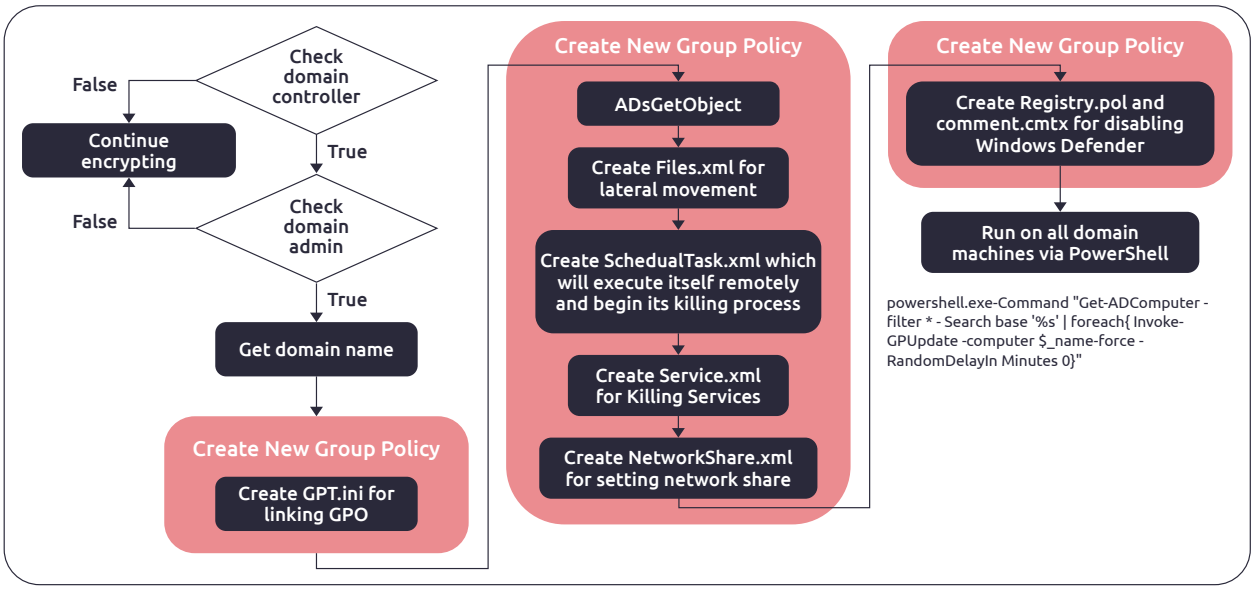


Figure 2: Lockbit 2.0 Ransomware with GPO

Table 1: Ransomware Incidents That Leveraged GPO

Name	Started from	References
LockBit2.0	2021	[7]
LockBit3.0	2022	[8]
Darkside	2021	[9]
BlackMatter	2021	[10]
Lockergoga	2019	[11]
Ryuk	2019	[12]
SaveTheQueen	2020	[13]
Bumblebee	2022	[14]
Quantum	2022	[14]
Conti	2021	[14]
Black Basta	2022	[15]
HermeticWiper	2022	[16]
HermeticRansom	2022	[16]

2. Leveraging AD Misconfigurations to Take Over the Entire Domain

Thus far, attackers have been pleased to find that they can easily exploit windows servers or domain controllers. However, as we mentioned earlier, enterprises often list domain controllers as Tier 1 assets, and they will patch up vulnerabilities as quickly as possible. Therefore, it is very unrealistic for attackers to use various techniques to attack AD over an extended period of time. Furthermore, attackers often examine whether there are any functions or features in AD itself that they can abuse. The vulnerabilities in AD's services would typically be fixed in due course, so attackers will instead seek out and exploit improperly configured settings as their pathway of attack. This approach has become so common that the misuse of misconfigurations have become a mainstream tactic for malicious actors today.

Thus, attackers are constantly compromising AD by taking advantage of opportunities unique to AD. Given that AD comprises several services and components, the mechanisms behind them can often be abused for various attack techniques which we define as AD attack vectors. These AD attack vectors take advantage of designated mechanisms when some prerequisites are met (such as a configuration setting enabled, or domain privileges granted), providing attackers with opportunities for credential access, privilege escalation, or persistence. For example, domain privileges granted to a user could allow privilege escalation that leads to full control of the entire AD or the Kerberos authentication. AD supports complex administration configuration for provided functionalities as well as corresponding services and technologies. For these configuration settings, when the corresponding security implications for potential impact are not fully understood, these configurations usually remain indefinitely until an attacker abuses them. When a configuration can be abused for an attack technique, this is often considered a misconfiguration.

More specifically, MITRE ATT&CK has no documented evidence that these techniques have happened. In other words, the blue team lacks visibility and detection capabilities for numerous AD configuration abuses. Naturally, these aren't recorded in MITRE ATT&CK. This is the largest gap between attackers and defenders today. There are many such AD techniques, also known as AD attack vectors.

Challenges for AD Defense

At this point, you might be wondering: Given the severe potential consequences of AD attacks and threats, what precisely are defenders up against? After extensive research, we have identified that there are three major challenges that defenders face when securing Active Directory.

1. **Visibility of Potential Attack Vectors**

   Before taking any action, the objective needs to be established. However, defenders often lack insight into potential attack vectors, and do not fully understand the security implications of administrative configurations. Attackers can often compromise AD from available attack vectors that go undetected by defenders since each administration configuration, from a wide variety of AD functionalities with corresponding services and technologies, present an angle from which attackers can compromise AD. Thus, the visibility for defenders needs to cover all the potential attack vectors. Without comprehensive coverage, blind spots for AD attacks will persist. So, even if defenders have some degree of visibility, if it is only partial, the attacker can still compromise AD. In short, incomplete visibility makes securing AD impossible since it is then impossible to completely unearth the precise misconfigurations that led to the AD compromise.

   Moreover, even having visibility of all AD attack vectors (techniques) in MITRE ATT&CK is not enough to build visibility of all attack vectors in the AD environment. For example, the AD CS attack was proposed to be added in August 2021 (as shown in Figure 3), but it was not added by MITRE until August 2022 (as shown in Figure 4). This kind of delay can also result in a lack of visibility.

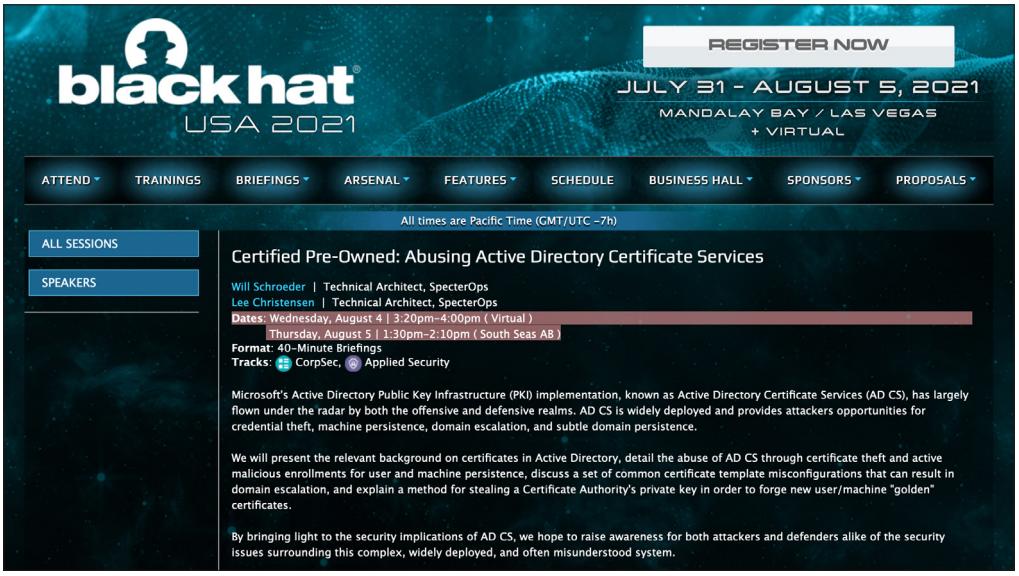
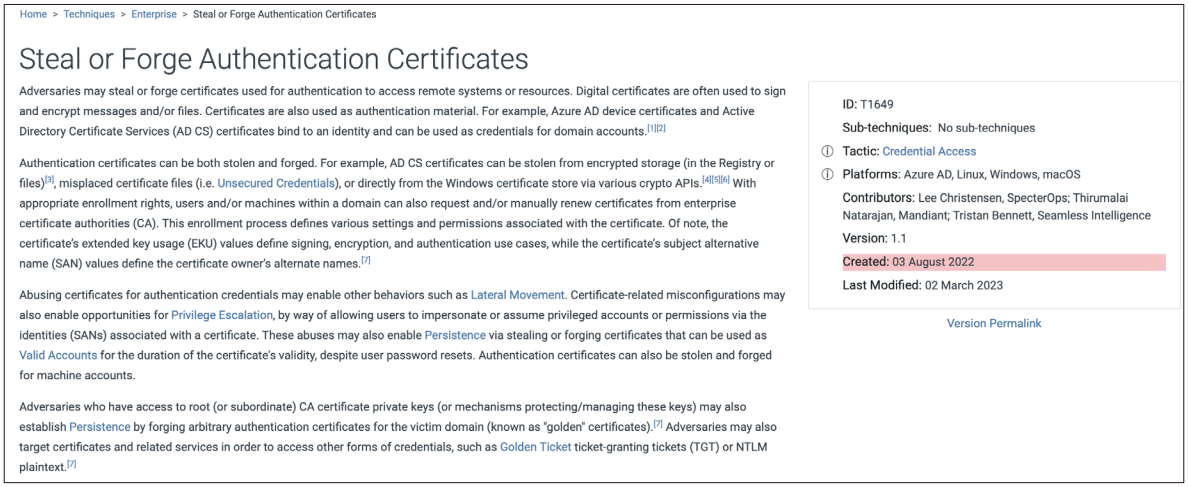


Figure 3: Certified Pre-Owned: Abusing Active Directory Certificate Services[17]



Home > Techniques > Enterprise > Steal or Forge Authentication Certificates

Steal or Forge Authentication Certificates

Adversaries may steal or forge certificates used for authentication to access remote systems or resources. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. For example, Azure AD device certificates and Active Directory Certificate Services (AD CS) certificates bind to an identity and can be used as credentials for domain accounts.[1][2]

Authentication certificates can be both stolen and forged. For example, AD CS certificates can be stolen from encrypted storage (in the Registry or files)[3], misplaced certificate files (i.e. Unsecured Credentials), or directly from the Windows certificate store via various crypto APIs.[4][5][6] With appropriate enrollment rights, users and/or machines within a domain can also request and/or manually renew certificates from enterprise certificate authorities (CA). This enrollment process defines various settings and permissions associated with the certificate. Of note, the certificate's extended key usage (EKU) values define signing, encryption, and authentication use cases, while the certificate's subject alternative name (SAN) values define the certificate owner's alternate names.[7]

Abusing certificates for authentication credentials may enable other behaviors such as Lateral Movement. Certificate-related misconfigurations may also enable opportunities for Privilege Escalation, by way of allowing users to impersonate or assume privileged accounts or permissions via the identities (SANs) associated with a certificate. These abuses may also enable Persistence via stealing or forging certificates that can be used as Valid Accounts for the duration of the certificate's validity, despite user password resets. Authentication certificates can also be stolen and forged for machine accounts.

Adversaries who have access to root (or subordinate) CA certificate private keys (or mechanisms protecting/managing these keys) may also establish Persistence by forging arbitrary authentication certificates for the victim domain (known as "golden" certificates).[7] Adversaries may also target certificates and related services in order to access other forms of credentials, such as Golden Ticket ticket-granting tickets (TGT) or NTLM plaintext.[7]

ID: T1649
Sub-techniques: No sub-techniques
Tactic: Credential Access
Platforms: Azure AD, Linux, Windows, macOS
Contributors: Lee Christensen, SpecterOps; Thirumalai Natarajan, Mandiant; Tristan Bennett, Seamless Intelligence
Version: 1.1
Created: 03 August 2022
Last Modified: 02 March 2023

Version Permalink

Figure 4: MITRE - Steal or Forge Authentication Certificates[18]

2. Priority for Taking Action

We assumed that once defenders were equipped with complete visibility of potential attack vectors, defenders can finally start taking action to secure them. However, defenders would later find enormous attack vectors in the environment and be clueless about which one they should start defending first. Since the AD attack vectors are derived from mechanism abuse, misconfigurations gradually increase along with the size and complexity of the enterprise network environment. As every defense-related action may take up huge amounts of resources, enormous attack vectors are challenging for the defenders as they attempt to distribute their limited resources in the most efficient way possible (we believe that the resources for an enterprise's security are limited, and proper allocation of resources is necessary to maximize the benefits and effectiveness).

Without understanding the true severity of each attack vector, defenders cannot judge which attack vectors should receive which level of priority. Additionally, the AD environment and configuration of each enterprise are different, thus even if two enterprises have the same attack vector, they may not have the same priority level or severity of impact. Therefore, attackers will still have a chance to compromise AD attack vectors before defenders can get to them. Resources might also be spent trying to mitigate various risks, without any meaningful defenses being constructed to protect AD.

3. Insufficient Comprehensiveness in Attack Vector Risk Evaluation

However, having the knowledge of the risk level for each attack vector and its priority level in and of itself is not enough. Despite being a low-risk attack vector that has low priority for defense action, several of these attack vectors can be chained together to cause even higher risk severity from the perspective of the attack path. There could be some restrictive factors or excessive costs in a specific attack vector that creates risk that cannot be effectively mitigated without further analysis. Therefore, a comprehensive risk assessment is also required.

In short, even though we know how to detect and defend against the attack vectors, the follow-up questions are (1) Which AD attack vector should be prioritized for mitigation? (2) Which AD attack path should be prioritized for mitigation? These are key points of this white paper that we will explore next.

Deep Dive Active Directory Risk Model

To solve the aforementioned challenges when attempting to secure AD, we propose a Risk Quantification Model for AD attack vectors and attack paths that can be chained by them that can provide the priority for the defender an answer as to which vector or path should be mitigated first. This AD risk quantification model is designed for AD especially. Our two main tenets in creating this model were to adapt it closely to the real AD environment and to make it user-friendly.

To begin with, in this model, an attack vector inventory is developed that can be referenced by defenders as a basis from which they can identify the potential security risk. Next, based on the numbered list of attack vectors in the environment, defenders can use this model to quantify the risk and thus prioritize the work in order of great severity or urgency, addressing the most high-risk threats first and efficiently focusing their efforts. In addition to quantifying the risk of AD attack vectors, we also propose an approach to evaluate the attack paths based on the quantification result to enable comprehensiveness.

In the following sections, we will introduce the structure, core concepts, and how to use this AD risk quantification model by taking attack vectors and paths from real life as examples, so that everyone can get started quickly and conveniently.

Introduction of AD Attack Vectors and Risk Model

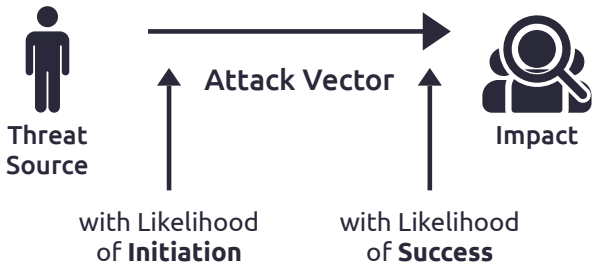


Figure 5: Attack Vector Risk Overview

We designed this model based on the NIST 800-30,[19] taking the risk from a threat source initiating an attack vector that causes some impact when successful. Before further analysis, we define some key terms as follows.

- **Threat Source:** Attacker with a certain amount of access to the assessing object who initiates the attack vector in question.
- **Attack Vector:** The attack technique that abuses Active Directory services or components. These long-lasting AD attack vectors, or attack techniques, are our focus. The attack vector itself does not contain any AD or Windows Server related vulnerabilities; it is only based on abuse-related techniques.

And you may be wondering, what is the relationship between attack vectors and MITRE techniques? In fact, it is roughly the same, except that our vector will contain many techniques that are as yet undefined by MITRE, such as ACL abuse or delegation, etc.

- **Impact:** Harm or damage that will be inflicted once an attack vector succeeds.

After establishing the relationship between the attack vector, threat source, and impact, we will proceed onto risk calculation. In this white paper, we basically use two formulas which we will explain in detail.

$$Risk = Likelihood \times Impact$$

$$Likelihood = (Threat\ Initiation \times Threat\ Occurrence) \pm Predisposing\ Condition$$

- **Risk:** The definition of risk we use is based on its definition in the NIST 800-30, ergo: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence".[19]
- **Likelihood:** Probability level of the attacker initiating an attack vector and succeeding in their intended impact.
  - » **Threat Initiation (T.I.):** Probability of the attacker initiating an attack vector.
  - » **Threat Occurrence (T.O.):** Probability of the initiated attack vector causing an impact.
  - » **Predisposing Condition (P.D.):** Variables affect the threat occurrence in the environment under assessment.

The risk value is produced by a threat source initiating an attack vector that causes some impact once it has succeeded. Next, we will analyze in detail the definition and calculation of threat initiation, threat occurrence, predisposing condition, impact, likelihood, and risk.

Threat Initiation: To adapt to the characteristics of the domain, we define threat initiation as a coverage percentage of accounts (accounts having the access rights / all the accounts in the domain) that have the right to initiate the attack vector. This risk factor serves to reflect the uncertainty of an adversary controlling any of the accounts able to initiate an attack vector.

In Active Directory, domain accounts are granted rights that can be abused by attackers for various attack vectors. The number of this domain account is calculated for threat initiation. Two types of accounts are included in total. The correspondence between qualitative values and threat Initiation is shown in Table 2. The output of threat initiation will be semi-qualitative values between 1 to 5.

1. User Account
2. Computer Account

Table 2: (Semi-) Qualitative Values and Description of Threat Initiation (T.I.)

Qualitative Values	Semi-Quantitative Values	Description
Very High (VH)	5	Coverage percentage of accounts able to initiate the Attack Vector ≥ 90%
High (H)	4	Coverage percentage of accounts able to initiate the Attack Vector from 70% to 89%
Moderate (M)	3	Coverage percentage of accounts able to initiate the Attack Vector from 25% to 69%
Low (L)	2	Coverage percentage of accounts able to initiate the Attack Vector from 0% to 24%
Very Low (VL)	1	There is no account able to initiate the Attack Vector

Threat Occurrence: Determines the success rate of an initiated attack vector causing impact. These risk factors serve to reflect the uncertainty of some attack vectors that are not guaranteed to be successful once initiated. The correspondence between qualitative values and threat occurrence is shown in Table 3. The output of threat occurrence will be semi-qualitative values between 1 to 5.

Table 3: (Semi-) Qualitative Values and Description of Threat Occurrence (T.O.)

Qualitative Values	Semi-Quantitative Values	Description
Very High (VH)	5	The success rate for initiated Attack Vector is 100%
High (H)	4	The success rate for initiated Attack Vector is from 70% to 99%
Moderate (M)	3	The success rate for initiated Attack Vector is from 30% to 69%
Low (L)	2	The success rate for initiated Attack Vector is from 0% to 29%
Very Low (VL)	1	The success rate for initiated Attack Vector is 0%

Predisposing Condition: Variables that affect the success rate of initiating an attack vector in the environment being assessed. This risk factor serves to reflect the uncertainty of some attack vectors that are not guaranteed to be successful once initiated. The most intuitive understanding is that the environment configurations of different companies vary. The correspondence between items, adjust value, description, and predisposing condition is shown on Table 4. The output of predisposing condition will be an adjusted value between ±1 to ±5.

Table 4: Items, Adjust Value, and Description of Predisposing Condition (P.D.)

Items	Adjust Value	Description
Setting Affects the Attack Vector	±5	Affects the success rate of the attack vector e.g., Kerberos encryption type
Detection Mechanism for the Attack Vector	±2	Allows blue team to spot the attack e.g., Audit Policy – Auth events, logon events, access events
Organization Security Policy	±1	Requirements that are not stringently applied e.g., Recommending that passwords not only meet the requirement but avoid the use of weak passwords, such as “Passw0rd!”
Self-Defined	± (1-5)	Organization may define additional items to serve its needs

Likelihood: After the level of threat initiation, threat occurrence, and the predisposing condition is determined, we can calculate the likelihood by using the matrix shown in Figure 6 and Figure 7, and calculate the likelihood via Figure 6 which places the number between 1 to 25. From there, use the mapping table via Figure 7 to get the final qualitative value. The output of likelihood will be one of {VL, L, M, H, and VH}.

$$Likelihood=(\ T.I.\ \times\ T.O.)\pm P.D.$$

Threat Initation	Threat Occurence				
	Very Low	Low	Moderate	High	Very High
Very High (VH)	5	10	15	20	25
High (H)	4	8	12	16	20
Moderate (M)	3	6	9	12	15
Low (L)	2	4	6	8	10
Very Low (VL)	1	2	3	4	5

Figure 6: Likelihood Matrix - I

Qualitative Values	Semi-Quantitative Values
Very High (VH)	20-25
High (H)	15-19
Moderate (M)	10-14
Low (L)	5-9
Very Low (VL)	1-4

Figure 7: Likelihood Matrix - II

Impact: Once an attack vector is initiated and succeeds, the magnitude of harm is determined by the level of domain access to the attacker. The correspondence between qualitative values and impact is shown in Table 5. The output of impact will be semi-qualitative values between 1 to 5.

Table 5: (Semi-) Qualitative Values and Description of Impact

Qualitative Values	Semi-Quantitative Values	Description
Very High (VH)	5	Directly or indirectly obtain usable Domain administrative access e.g., “domain admins”, “domain controller”
High (H)	4	Directly or indirectly obtain usable Domain privileged access for domain management e.g., “DNS Admins”, “Account Operator”, “Backup Operator”
Moderate (M)	3	Directly or indirectly obtain usable access from account serving applications e.g., database domain accounts, IIS service accounts
Low (L)	2	Directly or indirectly obtain usable general user or computer account access
Very Low (VL)	1	Directly or indirectly obtain any of the above access but it is not usable

Risk: After analyzing the likelihood and impact based on real-life scenarios, we can calculate the final risk based on the matrix shown in Figure 8 and Figure 9, and calculate the risk via Figure 8, which produces the original risk number between 1 to 25, and use the mapping table via Figure 9 to calculate the final risk level. The output of risk will be one of {VL, L, M, H, and VH}.

$$Risk = Likelihood \times Impact$$

Likelihood	Impact				
	Very Low	Low	Moderate	High	Very High
Very High (VH)	5	10	15	20	25
High (H)	4	8	12	16	20
Moderate (M)	3	6	9	12	15
Low (L)	2	4	6	8	10
Very Low (VL)	1	2	3	4	5

Figure 8: Risk Matrix - I

Qualitative Values	Semi-Quantitative Values
Very High (VH)	20-25
High (H)	15-19
Moderate (M)	10-14
Low (L)	5-9
Very Low (VL)	1-4

Figure 9: Risk Matrix – II

Applying Attack Vectors to the Risk Model

In the previous session, we discussed the details of the entire AD risk model. Next, we will use two real cases which include Kerberoasting and ACL abuse to demonstrate how to use this model and calculate the corresponding risk value.

1. Kerberoasting

- **Kerberoasting Definition:** Based on MITRE ATT&CK, Kerberoasting is an attack technique that *"abuse[s] a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force"*.[20] When Service Principal Name (SPN) is set on a domain user account, every domain user with a valid TGT can request the service ticket which has a portion encrypted by its password hash. This encrypted portion allows the attacker to use brute force in an attempt to decrypt the password.

In the following section, we will dissect each component one by one and calculate the risk. In the risk assessment, we need to point out that our risk assessment objectives are to limit the scope, the attack vector/path, the environment configuration, and the user/computer etc. The objective below is an example we used to assess the Kerberoasting risk.

- **Risk Assessment (RA) Objective:** We performed a Kerberoasting risk assessment for the entire domain with the default domain environment configuration settings. To assess this attack vector, the assessing object is the domain users with the SPN set. The assumption of this assessment example is that password policy, such as complexity and renewal period default settings, and service ticket encryption, enables and supports RC4.
- **Threat Initiation (T.I.) Analysis:** Kerberoasting is done by requesting a service ticket to use brute force to decrypt a password with a TGT. Attackers can use any domain user account for TGT, so the coverage percentage of accounts is 100%. Based on Table 2, the value for this risk factor is 5.
- **Threat Occurrence (T.O.) Analysis:** Since a Kerberoasting attack is based on brute forcing the password, the success rate is determined by whether attackers can crack the password within the valid period. The default Active Directory setting used and password policy requires a password to have a length of 7 and maximum age of 42 days with a combination of 93 characters (ASCII Code between 33~126).

  1. Upper or lowercase letters (a-zA-Z)
  2. Numeric characters (0-9)
  3. Non-alphanumeric characters

  So, the number of all possible password combinations is 93^7. When using a graphic card 2080ti that has 641.1 MH/s (443.81ms) hash rate for RC4 encryption,[21] we can calculate that the time required for all password combinations is around 65 days. The success rate is 42/65 ≅ 0.646 (65%) which corresponds to Moderate and a value of 3 based on Table 3.

- **Likelihood Calculation:** After analysis of threat initiation and threat occurrence, we can calculate the likelihood. For this attack vector assessment, the likelihood numeric value is 15 with a risk level high based on Figure 6, and the qualitative value is H based on Figure 7.

$$5\ (T.I.)\ x\ 3\ (T.O.) = 15\ (H)$$

- **Impact Calculation:** The impact is determined by the account privilege level of the domain user account and service account. Based on Table 5, we use the matrix to calculate the risk of Kerberoasting and use two accounts as examples (domain administrator and MSSQL account). If the privilege of the account cracked by Kerberoasting attack is at the level of domain administrator, corresponding to Table 5, the impact is 5 (VH) because they have the authority to influence operation of the entire domain. If the authority of the cracked account is at the MSSQL service account level, its authority pertains to specific application services, so the impact is 3 (M).
- **Risk Calculation:** Following the likelihood and impact, we can directly calculate risk as shown in Table 6. Under the same likelihood, the calculated risks are relatively different because of the different impacts.

Table 6: Kerberoasting Risk by Different Privilege Levels

	Likelihood	Impact	Description	Risk
Domain Administrator	15 -> 4(H)	5 (VH)	Domain Administrative Access	20 (VH)
MSSQL Service Account	15 -> 4(H)	3 (M)	Account Serving Application	12 (M)

- **With Predisposing Condition:** While not completely practical, it is possible to disable RC4 for Kerberos ticket encryption and we add this to the RA objective. After changing to these configuration settings, the service ticket that was leveraged for brute forcing the password has a stronger encryption type, such as AES 128 and AES 256, lowering the likelihood of a Kerberoasting attack vector. Based on Table 4, these configuration settings lower the success rate of the attack vector. So, it is minus the likelihood for 5 numeric values. We also calculate the corresponding likelihood such as in Table 7, as the P.D. lowers the likelihood, the risk value is also lowered according to it and as shown in Table 8.

Table 7: Likelihood of Kerberoasting with Predisposing Condition

T.I.	T.O.	P.D.	Likelihood
5 (VH)	3 (M)	-5	10 -> 3 (M)

Table 8: Kerberoasting Risk with Predisposing Condition by Different Privilege Levels

	Likelihood	Impact	Description	Risk
Domain Administrator	10 -> 3(M)	5 (VH)	Domain Administrative Access	15 (H)
MSSQL Service Account	10 -> 3(M)	3 (M)	Account Serving Application	9 (L)

2. ACL Abuse

- **ACL Abuse Definition:** ACL abuse refers to the types of attack techniques in AD that, in order for the attacker to achieve lateral movement, abuse the rights granted to a principal controlled by the attacker. In Active Directory, every resource, such as a domain account, domain group, or organizational unit is managed and stored as a domain object. These domain objects grant principals access rights (ACL) which fall into two categories.
  - » **Generic Rights** - Generic rights allow complete control over that domain object which includes object-specific rights such as writeOwner, writeDacl,genericWrite, genericAll, or WriteProperty.
  - » **Object-Specific Rights** – Object-specific rights allow specific rights on the domain object to be configured.

Depending on the type of domain object, there are different implementations for ACL abuse shown in Table 9.

Table 9: Domain Object Type and ACL Abuse

Object Type	ACL Abuse Type
User Account	Force changes the password by targeted attack Set the SPN to enable Kerberoasting attack Disable pre-authentication for AS-REP roasting Set certificate for Kerberos authentication using PKINIT
Computer Account	Configure resource-based constrained delegation Read local administrator password Configure certificate for Kerberos authentication using PKINIT
Domain Group	Add member to whom rights can be granted of that domain group
Organizational Unit (OU)	Add additional ACL with inheritance flag specified on the OU object for controlling the contained objects
Group Policy Object	Configure the policy settings for compromising the accounts applied by the group policy
Domain Object	Ability to perform domain replication (DCSync)
Certificate Template Object	Configure vulnerable templates for attacker to abuse

- **Risk Assessment (RA) Objective:** We perform ACL abuse risk assessment for domain accounts that have been granted certain ACLs with domain default settings. To assess this attack vector, we assessed an AD domain object that grants certain rights to another principal. The assumption of this assessment example is that an attacker may compromise any account that has been granted the ACL rights which can be abused to control our assessing object. We would perform ACL abuse risk assessment on {dexter, administrator}@corp.local and ACL {User-Force-Change-Password, GeneralAll} with the default domain environment configuration.
- **Threat Initiation Analysis:** The T.I. is determined by the coverage percentage of the account granted with ACL.

- **Threat Occurrence Analysis:** When an ACL is configured that grants a right to a principal, the attacker can easily abuse this right. So, the success rate is 100% with corresponding numeric value 5 and level very high (VH).
- **Case 1: User user01 is granted ACL permission with User-Force-Change-Password to user dexter.** This ACL is an object-specific right that permits resetting a password on a user account.[22] Attacker controlled an account user01 that was granted this ACL to change the password of the user dexter account, compromising it without knowing the original password. The schematic diagram is shown in Figure 10.

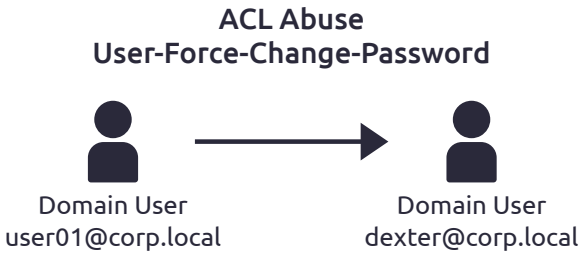


Figure 10: ACL Abuse for User-Force-Change-Password

  - » **Threat Initiation Analysis:** This ACL is granted to one user only. So, based on the table for threat initiation, the account coverage is less than 25 percent (<25%) which corresponds to numeric value 2 and the level is low (L).
  - » **Threat Occurrence Analysis:** The success rate is 100% with corresponding numeric value 5 and level very high (VH).
  - » **Likelihood Calculation:** After the principal granted this ACL is calculated, we have the value for threat initiation with only one account found. Based on the table, we calculate the likelihood is equal to 10 numeric values which corresponds to 3 and the level is moderate (M).
  - » **Impact Calculation:** The domain object that grants the ACL is a normal user account (dexter@corp.local). So, based on the table, the impact is equal to 2 numeric values and the level is 2 low (L).
  - » **Risk Calculation:** Following likelihood 3 (M) and impact 2 (L), we can directly calculate Risk 6 (L) as shown in Table 11.

Table 10: ACL Abuse Likelihood for User-Force-Change-Password

T.I.	T.O.	Likelihood
2 (L)	5 (VH)	10 -> 3 (M)

Table 11: ACL Abuse Risk for User-Force-Change-Password

ACL Abuse of	Likelihood	Impact	Description	Risk
dexter@corp.local	3 (M)	2 (L)	General user or computer account access	6 (L)

- **Case 2: Everyone within the domain group is granted ACL permission with GenericAll to user dexter.** This ACL is a generic right that grants principals full control of the object itself. An attacker controlling a principal granted this right can do whatever it wants to the object and are thus able to abuse or compromise it in various ways. A schematic diagram is shown in Figure 11.

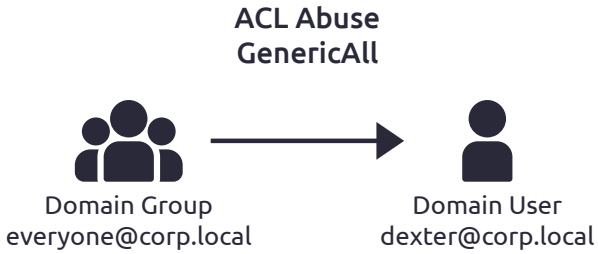


Figure 11: ACL Abuse for GenericAll to user dexter

» **Threat Initiation Analysis:** "Everyone" is a special group that exists by default in the domain. As the name indicates, this group contains every authenticated user and all guest accounts.[23] So, when the ACL is granted to this domain, the account coverage is 100%, which corresponds to numeric value 5 and qualitative level is very high (VH) for threat initiation based on Table 2.

» **Threat Occurrence Analysis:** The success rate is 100% with corresponding numeric value 5 and level very high (VH).

» **Likelihood Calculation:** Based on Table 12, we calculate the likelihood as equal to numeric value 25 which corresponds to 5, and level very high (VH).

» **Impact Calculation:** If the domain object granted the ACL is the same as our previous example, the impact of a general user account for impact is equal to numeric value 2 and level is low (L).

» **Risk Calculation:** Following Likelihood 5 (VH) and Impact 2 (L), we can directly calculate risk 10 (M), as shown in Table 13.

Table 12: ACL Abuse Likelihood for GenericAll

T.I.	T.O.	Likelihood
5 (VH)	5 (VH)	25 -> 5 (VH)

Table 13: ACL Abuse Risk for GenericAll

ACL Abuse of	Likelihood	Impact	Description	Risk
dexter@corp.local	5 (VH)	2 (L)	General user or computer account access	10 (M)

- **Case 3: Domain group IT is granted ACL permission with GenericAll to domain administrator.** This is a common situation in practice, and many groups related to the IT department will be included as the domain administrator and have complete access rights in order to facilitate related maintenance operations.

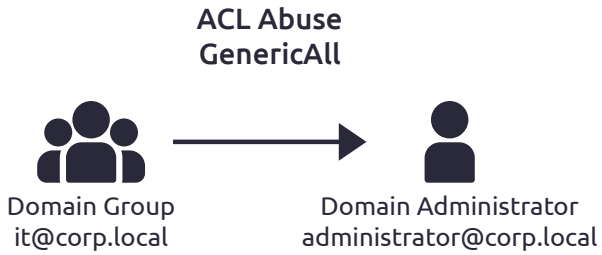


Figure 12: ACL Abuse for GenericAll to domain administrator

  - » **Threat Initiation Analysis:** Assuming this is a user-created domain group with 30% account coverage, the T.I. value is 3 and level is moderate (M).
  - » **Threat Occurrence Analysis:** The success rate is 100% with corresponding numeric value 5 and level very high (VH).
  - » **Likelihood Calculation:** Based on Table 14, we calculate the likelihood as equal to numeric value 15 which corresponds to 4 and level is high (H).
  - » **Impact Calculation:** The domain object grants the ACL to a default domain account. Since it has domain administrative access, the numeric value of impact is 5 and level is very high (VH).
  - » **Risk Calculation:** Following likelihood 4 (VH) and impact 5 (VH), we can directly calculate that the risk value is 20 (VH), as shown in Table 15.

Table 14: ACL Abuse Likelihood for GenericAll to Domain Administrator

T.I.	T.O.	Likelihood
3 (M)	5 (VH)	15 -> 4 (H)

Table 15: ACL Abuse Risk for GenericAll to Domain Administrator

ACL Abuse of	Likelihood	Impact	Description	Risk
administrator@corp.local	4 (VH)	5 (VH)	Domain administrative access	20 (VH)

Applying Attack Paths to the Risk Model

Why do we need attack path assessments?

Considering a single attack vector on its own will not provide a sufficient enough evaluation of an all-terrain AD attack. An attack path that causes devastating impact can form from multiple low risk attack vectors. In terms of the attack path, the risk level is calculated by assessing the attack path as a whole for corresponding likelihood and impact. To reflect the real status of an attack path, we slightly modified the definitions of risk factors for attack vectors.

An example can be seen for two attack vectors below in Figure 13 and Figure 14. Assuming there are multiple domain users that have local admin rights on a domain computer - wks01 as Figure 13, while this domain computer has an ACL right - GenericAll, granted to the domain administrator as Figure 14. This would mean that multiple domain users can obtain domain admin permission in this indirect way and, from there, take over the entire domain. Through the risk assessment for these two attack vectors, we find that the risk for the first one is 6 (L) and the second one is 15 (H). This situation clearly shows that the risk of the first attack vector that can indirectly control domain admin is low, but in fact, another vector further along the chain can achieve a high-risk effect, which is why we believe that evaluating an attack vector on its own does not suffice. Clearly, the risk is not fully recognized with this scenario. Therefore, it is also necessary to assess the risk for the attack path along with the attack vector.

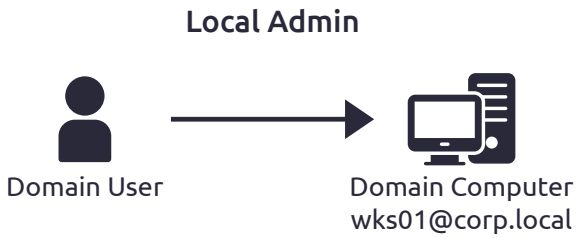


Figure 13: Attack Vector Example Vectors – I

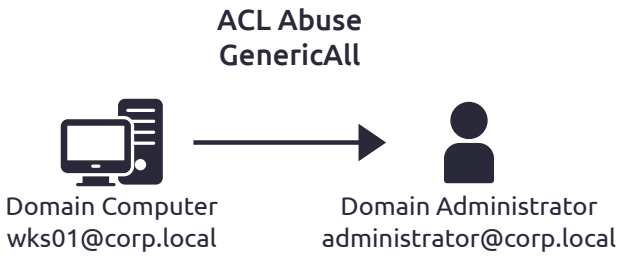


Figure 14: Attack Vector Example Vectors - II

Attack Path Risk Assessment Method

Due to the difference between evaluating the attack vector and the attack path, we will explain the relevant definitions here again, and the definitions of some nouns may be slightly different from the previous ones.

- **Threat Initiation (T.I.):** In terms of the attack path, the attacker can compromise any node in the path and proceed to the end of it to achieve the objective. Therefore, for percentage coverage, we enumerate the accounts that can initiate any of the attack vectors in the path. These enumerated accounts in the path reflect the initiation likelihood of the attacker compromising one of them, allowing the attacker to follow this attack path until they achieve the end objective. The number of enumerated accounts is then used to calculate the percentage coverage for T.I. value. One thing that needs to be noted is that the same account may be able to initiate multiple attack vectors in a path. Therefore, when counting the number of enumerated accounts, duplicate accounts need to be removed.
- **Threat Occurrence (T.O.):** In the attack path, the attackers needs to succeed in the last attack vector in the path in order to achieve its objective. Therefore, T.O. is defined by the success rate of the last attack vector.
- **Likelihood:** For a comprehensive assessment of the likelihood of the attack path, all attack vectors need to be included. The likelihood calculation is the same as shown previously in Figure 6 and Figure 7, but the definitions for T.I. and T.O. have been modified.
- **Impact:** For the impact from an attack path, we will take the highest impact value from the attack vectors in the path. The impact for the attack path is defined this way to reflect the level of domain access possible for an attacker to obtain.
- **Risk:** The attack path risk calculation method is the same as the attack vector using the matrix as shown in Figure 8 and Figure 9.

Attack Path Assessment

The evaluation definition and concept of the attack path have been explained. Next, let us use actual cases to substantiate your understanding and apply it. As shown in Figure 15, we have an attack path containing 4 attack vectors from domain user with local admin to the DCSync permission to the domain controller.

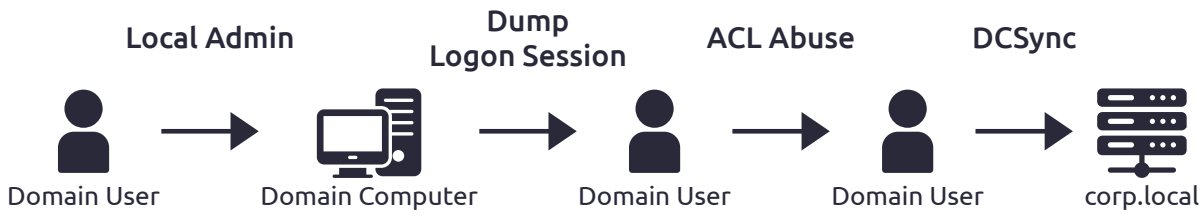


Figure 15: Attack Path Assessment Example

- **Attack Vectors Overview**
  - » **Local Admin:** Principals in the local administrators' group can be leveraged by the attacker for remote command execution through protocols like SMB and WMI.
  - » **Dump Logon Session:** When domain computer systems contain a user logon session, the credentials can be dumped from LSASS memory with elevated access.
  - » **ACL Abuse:** Same as the previous description on 3.2.2 ACL Abuse.
  - » **DCSync:** A variant of ACL abuse/specific privilege with domain admin which allows an attacker to leverage the domain replication rights granted in order to simulate the behavior of a domain controller (DC) and thus retrieve password hashes and credentials via domain replication.
- **Risk Assessment (RA) Objective:** We perform a risk assessment for an attack path in the entire domain. The objective is to assess any attack paths that match the scenario described in Figure 15 and evaluate all conditions of the entire domain that match the path with default settings.
- **Threat Initiation Analysis:** For this example, we enumerated the accounts for each attack vector as shown in Table 16, and in this attack path example, we assume a simulated environment that has 1000 domain accounts. 156 domain accounts are able to initiate one of the attack vectors in this path, so the account coverage rate is 156/1000=15.6%. Based on Table 2, we have a T.I. value of 3 at level M.

Table 16: Attack Path Assessment - Domain Accounts Enumeration

Attack Vector	Accounts able to initiate the attack vector	Enumerated Accounts Description
Local Admin	35	Number of members in the administrators group
Dump Logon Session	40	Number of accounts that can remotely access the computer system. e.g., "Remote Desktop User", "Remote Management Users"
ACL Abuse	66	Number of accounts having ACL rights on the domain object
DCSync	15	Number of accounts having domain replication rights

- **Threat Occurrence Analysis:** For the attack path shown in Figure 15, the attack vector DCSync is the last one in this path. In other words, an attacker is required to initiate DCSync and successfully obtain the credentials from it before achieving the objective. Therefore, the T.O. value is according to the success rate of DCSync attack vector. Assuming there is no predisposing condition, the success rate for DCSync is 100%. Therefore, according to Table 3, we have a T.O. value of 5 and level of VH.
- **Likelihood Calculation:** After the values of T.I. and T.O. are obtained, we calculate the likelihood by 3 x 5 =15 (H) as shown in Table 17.

Table 17: Attack Path Assessment Example - Likelihood Calculation

Total Accounts	Sum of Accounts from Each Attack Vector	Coverage Percentage	T.I.	T.O.	Likelihood
1000	156	15.6	3 (M)	5 (VH)	15 (H)

- **Impact Analysis:** From the attack path defined in this scenario example, we can find that the DCSync attack vector has the highest impact for a numeric value of 5 and a very high (VH) level, according to Table 5.
- **Risk Calculation:** After obtaining the value for likelihood and impact, we calculate the risk for this attack path scenario, and arrive at risk level 20 (VH) by multiplying 4 x 5. This means this attack path is very high (VH).

Table 18: Attack Path Assessment Example - Risk Calculation

Total Accounts	Likelihood	Impact	Risk
1000	4 (H)	5 (VH)	20 (VH)

After assessing the risk for an attack path from the entire domain, there is still a question remaining. In this path, which attack vector needs to be mitigated first? To solve this, we would also like to assess each attack vector within this path and understand the risk in the context of the attack path for the RA objective.

- **Assess Each Attack Vector Within the Attack Path:** Since we are assessing the attack vector in the context of the path, the RA Objective has changed. That is to say, we must adjust the evaluation limit of the RA objective to adapt to the attack path and conduct a risk assessment for each attack vector, so as to specifically analyze which vector is the riskiest in this path and should therefore take highest priority.
  - » **Local Admin**
    - **RA Objective:** Based on 156 abused domain accounts that fits this path, the risk is that an attacker can abuse local admin privileges to the domain computer.
    - **Threat Initiation Analysis:** We have 35 users who can initiate the local admin attack vector. To calculate the percentage coverage, we will use 156, as this is the number of users in this entire path according to the RA objective. Based on Table 2, the account coverage is 35/156 - 22% which corresponds to 2 numeric values and the level is low (L).

- **Threat Occurrence Analysis:** When the attacker can abuse local admin privileges, the success rate is 100% with corresponding numeric value 5 and level very high (VH).
- **Likelihood Calculation:** As shown in Table 19, we calculate that the likelihood is equal to 10 (2 x 5) numeric values which corresponds to 3 and the level is moderate (M).
- **Impact Analysis:** Of the 35 users with local admin privileges, they are local admin of 60 domain computers, and the highest privilege provides service. Based on Table 5, servers as targets have an impact equal to numeric value 3 and the level is moderate (M).
- **Risk Calculation:** After obtaining the value for likelihood and impact, we calculate the risk as shown in Table 20.

Table 19: Likelihood Calculation for Local Admin

T.I.	T.O.	Likelihood
2 (L)	5 (VH)	10 -> 3 (M)

Table 20: Risk Calculation for Local Admin

Likelihood	Impact	Risk
3 (M)	3 (M)	9 (L)

» **Dump Logon Session**

- **RA Objective:** Under this attack path, the attacker proceeds from the attack vector of local admin (35 users are local admin to 60 computers) to perform dump logon session in the computers.
- **Threat Initiation Analysis:** In this example, we later found that there are 60 computers from the previous attack vector and 30 of them have been evaluated with some logon sessions. Based on Table 2, the account coverage is 30/60 - 50% which corresponds to numeric value 3 and the level is moderate (M).
- **Threat Occurrence Analysis:** The success rate is 100% with corresponding numeric value 5 and level very high (VH).
- **Likelihood Calculation:** As shown in Table 21, we calculate the likelihood is equal to 15 (3 x 5) numeric values which corresponds to 3 and the level is moderate (M).
- **Impact Analysis:** Among 30 domain computers with 40 logon sessions, all sessions are regular domain users. Based on Table 5, regular domain users have an impact equal to 2 numeric values, and the level is low (L).

- **Risk Calculation:** After obtaining the value for likelihood and impact, we calculate the risk as shown in Table 22.

Table 21: Likelihood Calculation for Logon Session

T.I.	T.O.	Likelihood
3 (M)	5 (VH)	15 -> 4 (H)

Table 22: Risk Calculation for Logon Session

Likelihood	Impact	Risk
4 (H)	2 (L)	8 (L)

» **ACL Abuse**

- **RA Objective:** Under this attack path, the attacker proceeds from the attack vector of dump logon sessions (30 domain computers to 40 logon sessions) to perform ACL abuse.
- **Threat Initiation Analysis:** In this example, we later found that there are 40 logon session users (each logon session is a user) from the previous attack vector and 30 of them have abusable ACL. Based on Table 2, the account coverage is 30/40 - 75% which corresponds to 4 numeric values and the level is high (H).
- **Threat Occurrence Analysis:** The success rate is 100% with corresponding numeric value 5 and level very high (VH).
- **Likelihood Calculation:** As shown in Table 23, we calculate the likelihood as equal to 20 (4 x 5) numeric value which corresponds to 5 and the level is very high (VH).
- **Impact Analysis:** Among 40 logon session users, 30 users have abusable ACL, and the highest abusable privilege is DCSync with 10 users which allows user/attack to sync domain database data. Based on Table 5, the user that has DCSync is equivalent to having administrative rights. So, the impact is equal to the numeric value 5 and the level is very high (VH).
- **Risk Calculation:** After obtaining the value for likelihood and impact, we calculate the risk as shown in Table 24.

Table 23: Likelihood Calculation for ACL Abuse

T.I.	T.O.	Likelihood
4 (H)	5 (VH)	20 -> 5 (VH)

Table 24: Risk Calculation for ACL Abuse

Likelihood	Impact	Risk
5 (VH)	5 (VH)	25 (VH)

» **DCSync**

- **RA Objective:** Under this attack path, the attacker proceeds from the attack vector of ACL abuse (30 abusable ACLs from 40 logon session users) to perform DCSync.
- **Threat Initiation Analysis:** In this example, we later found that there are 30 users from the previous attack vector and 10 of them have the right to initiate DCSync. Based on Table 2, the account coverage is 10/30 - 33% which corresponds to 3 numeric values and the level is moderate (M).
- **Threat Occurrence Analysis:** The success rate is 100% with corresponding numeric value 5 and level very high (VH).
- **Likelihood Calculation:** As shown in Table 25, we calculate the likelihood is equal to 15 (3 x 5) numeric value which corresponds to 3 and the level is moderate (M).
- **Impact Analysis:** Based on Table 5, DCSync can obtain every domain account credential. So, the impact is equal to 5 numeric values and the level is very high (VH).
- **Risk Calculation:** After obtaining the value for likelihood and impact, we calculate the risk as shown in Table 26.

Table 25: Likelihood Calculation for DCSync

T.I.	T.O.	Likelihood
3 (M)	5 (VH)	15 -> 4 (H)

Table 26: Risk Calculation for DCSync

Likelihood	Impact	Risk
4 (H)	5 (VH)	20 (H)

From the above attack path example scenario, we can produce the following table for the risk of each vector. From this table, we can clearly see the highest risk attack vector in the path that needs to be prioritized for taking action first. ACL abuse should be the first priority on this path, and DCSync will be second. On the premise of knowing which attack path has the highest risk, we can effectively provide suggestions so that enterprises can quickly arrange the priority of their countermeasures.

Table 27: Assessment Example for Each Vector in Attack Path

Attack Vector	Likelihood	Impact	Risk
Local Admin	3 (M)	3 (M)	9 (L)
Dump Logon Session	4 (H)	2 (L)	8 (L)
ACL Abuse	5 (VH)	5 (VH)	**25 (VH)**
DCSync	4 (H)	5 (L)	20 (H)

Risk Evaluation and Mitigation Strategy

After calculating the quantified risk for the attack vector or attack path, the numeric risk value can then be used for prioritization. In this section, we introduce a strategy for risk mitigation based on the quantified value from a risk assessment.

From the attack vectors' assessment, it is obvious that the areas with the highest risk value would be prioritized. However, there may be constraints for the enterprise network environment. For example, IT users would probably require elevated rights for server administration even though this right enables an attack vector. Therefore, after risk assessment, we can have two categories as options for a mitigation strategy.

- **Risk Avoidance**

  Remove the configuration settings completely, if possible, e.g., SPN property. After assessing the attack vector, we may find that the prioritized one is from an account that does not require this configuration setting or access rights. Therefore, we can safely remove it as a way of neutralizing this attack vector without disrupting the normal running operation.

- **Risk Reduction:** Lower the likelihood or impact when an attack vector cannot be completely avoided.
  - » **Likelihood – Threat Initiation:** This can be done by reducing the number of accounts that can initiate an attack vector. Accounts should be removed when it does not need to have access rights or configuration settings.
  - » **Likelihood – Threat Occurrence:** For some attack vectors, such as Kerberoasting, we can try to decrease the success rate by enhancing password complexity of the attack vector.
  - » **Likelihood – Predisposing Condition:** Another way of reducing the likelihood is to enable predisposing condition. Based on Table 4, we can also enforce the detection mechanism or establish a security policy.
  - » **Impact:** The overall risk can be reduced even further through the target of the attack vector. Based on Table 5, we can see that the severity depends on the privilege of the target account. Therefore, we can remove privilege from this target account.

Conclusion

In this whitepaper, we provided an overview of the looming threat to AD, analyzed challenges to AD defense, and proposed a risk quantification model that specifically focuses on attack vectors and attack paths. Defenders can use this model to quantify the risk of attack vectors after enumeration to solve the previously described challenge of proper prioritization. In addition, our proposed risk model also quantifies the risk for the attack path to address the deficiency of comprehensiveness that comes from only assessing the attack vectors in isolation.

The results of risk quantification can serve as the basis for prioritizing various mitigation measures. We anticipate that this method will optimize the use of corporate security resources and maximize benefits, thereby contributing to a secure corporate network.

References

1 "Active Directory Holds the Keys to your Kingdom, but is it Secure?," [Online]. Available: https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/. [Accessed 28 5 2023].

2 "Active Directory Domain Services Overview," [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. [Accessed 28 5 2023].

3 "AD FS Overview," [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview. [Accessed 28 5 2023].

4 "Active Directory Certificate Services Overview," [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11). [Accessed 28 5 2023].

5 "Active Directory Rights Management Services Overview," [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831364(v=ws.11). [Accessed 28 5 2023].

6 "Researchers Explore Active Directory Attack Vectors," 2021. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/researchers-explore-active-directory-attack-vectors/d/d-id/1340902.

7 "Active Directory is Now in the Ransomware Crosshairs," [Online]. Available: https://www.tenable.com/blog/active-directory-is-now-in-the-ransomware-crosshairs. [Accessed 28 5 2023].

8 "Threat Alert: Cortex vs. LockBit 3.0," [Online]. Available: https://www.paloaltonetworks.com/blog/security-operations/threat-alert-cortex-vs-lockbit-3-0/. [Accessed 28 5 2023].

9 "Darkside Ransomware Attack and Domain Compromise," [Online]. Available: https://www.sentinelone.com/blog/darkside-ransomware-attack-and-domain-compromise/. [Accessed 28 May 2023].

10 "Active Directory is Now in the Ransomware Crosshairs," [Online]. Available: https://www.tenable.com/blog/active-directory-is-now-in-the-ransomware-crosshairs. [Accessed 28 May 2023].

11 "Spyware Stealer Locker Wiper: LOCKERGOGA Revisited," [Online]. Available: https://pylos.co/wp-content/uploads/2020/04/Spyware_Stealer_Locker_Wiper-_LockerGoga_Revisited.pdf. [Accessed 28 May 2023].

12 "Ransomware Attacks on Active Directory," [Online]. Available: https://www.imanami.com/how-ransomware-attacks-on-active-directory-and-azure-ad/. [Accessed 28 May 2023].

13 "A Queen's Ransom: Varonis Uncovers Fast-Spreading "SaveTheQueen" Ransomware," [Online]. Available: https://www.varonis.com/blog/save-the-queen-ransomware. [Accessed 28 May 2023].

14 "Microsoft Active Directory as a Prime Target for Ransomware Operators," [Online]. Available: https://www.sentinelone.com/blog/microsoft-active-directory-as-a-prime-target-for-ransomware-operators/. [Accessed 28 May 2023].

15 "Ransomware Spotlight - Black Basta," [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta. [Accessed 28 May 2023].

16 "HermeticWiper and HermeticRansom delivered via Active Directory GPO," [Online]. Available: https://www.acronis.com/en-us/cyber-protection-center/posts/hermeticwiper-and-hermeticransom-delivered-via-active-directory-gpo/. [Accessed 28 May 2023].

17 "Certified Pre-Owned: Abusing Active Directory Certificate Services," [Online]. Available: https://www.blackhat.com/us-21/briefings/schedule/index.html#certified-pre-owned-abusing-active-directory-certificate-services-23168. [Accessed 28 May 2023].

18 "Steal or Forge Authentication Certificates," [Online]. Available: https://attack.mitre.org/techniques/T1649/. [Accessed 28 May 2023].

19 "SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments," NIST, 2012.

20 [Online]. Available: https://attack.mitre.org/techniques/T1558/003/.

[21] "Gigabyte RTX 2080ti Hashcat Benchmarks," [Online]. Available: https://gist.github.com/binary1985/c8153c8ec44595fdabbf03157562763e. [Accessed 28 May 2023].

[22] [Online]. Available: https://learn.microsoft.com/en-us/windows/win32/adschema/r-user-force-change-password.

[23] "Special identity groups," [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-special-identities-groups#everyone.

[24] "Nobelium APT uses new backdoor to steal data from AD FS servers," 2021. [Online]. Available: https://www.cybersecurity-help.cz/blog/2332.html.

[25] "Indicators of Compromise Associated with LockBit 2.0," 2022. [Online]. Available: https://www.ic3.gov/Media/News/2022/220204.pdf.

Copyright © 2023 TXOne Networks. All rights reserved.

txone.com