Pentesting Active Directory - Part 2 | Access Control, Users, KRGBT, Golden ticket attack

- 21 days ago

Let’s learn about Authentication, Authorization, Access Control, Users, KRGBT, Golden ticket attack and more.

Active Directory (AD) authentication is a Windows-based system that enables organizations to authenticate and authorize users, endpoints, and services in the AD environment. AD authentication offers centralized control over user and device configurations, as well as streamlined user and rights management through the use of AD Group Policy. It also provides single sign-on (SSO) functionality, allowing users to authenticate once and then access any authorized corporate resource in the domain.

AD authentication replaces the easily exploitable LAN Manager (LM) and NT LAN Manager (NTLM) protocols, which were used in earlier versions of Windows operating systems. LM used a fragile cryptography scheme that could be easily cracked by modern processors, while NTLM improved upon this with stronger cryptography but lacked mutual authentication and smart card authentication services.

AD authentication supports two standards: Kerberos and Lightweight Directory Access Protocol (LDAP).

Kerberos Protocol

In a Kerberos-based AD authentication, users log in once to access enterprise resources. Instead of transmitting login credentials over the network, as was the case with LM and NTLM, the Kerberos system generates a session key for the user and a token containing the user's access policies and rights. The user must first authenticate themselves to a key distribution center (KDC), which is a trusted third party consisting of an authentication server (AS) and a ticket granting server (TGS). The AS encrypts the user's login credentials and sends a ticket granting ticket (TGT) to the user. The user then transmits the TGT to the TGS along with an authorization request to access the target resource on the server. The TGS issues a token to the client that is encrypted with a key shared between the target server and TGS. Finally, the client transmits the token to the target server, which decrypts it to allow the client to access resources for a limited time.

Lightweight Directory Access Protocol

LDAP is an open source and cross-platform protocol that provides AD authentication services. There are two options associated with LDAP-based authentication in AD: simple authentication, which relies on login credentials to create a request to the server, and simple authentication and security layer (SASL), which uses other authentication services such as Kerberos to connect to the LDAP server.

Aside from Kerberos and LDAP, AD uses several other authentication methods, including:

LAN Manager (LM) Hash

The LM hash is an older and less secure hashing method used in Windows operating systems prior to Windows NT. It is considered weak due to its case-insensitive nature and its limitation to 14 characters or less, which are split into two 7-character parts, hashed separately, and concatenated. This vulnerability makes LM hashes susceptible to brute force and rainbow table attacks. While modern Windows systems no longer use LM hashes by default, they may still be present in some legacy systems.

NT LAN Manager (NTLM) Hash

The NTLM hash is an improvement over LM and was introduced in Windows NT. This hashing method is case-sensitive and supports password lengths up to 128 characters. Although more secure than LM, NTLM still has some vulnerabilities, such as susceptibility to pass-the-hash attacks, which allow an attacker to impersonate a user without knowing their plaintext password.

NT LAN Manager version 1 (NTLMv1)

NTLMv1 is an authentication protocol that uses a challenge-response mechanism. When a client attempts to access a resource, the server sends a challenge (a random 8-byte number). The client encrypts this challenge using their NTLM hash and sends the response back to the server. The server then verifies the response by comparing it to its stored hash of the user's password. While NTLMv1 is an improvement over LM and NTLM, it is still vulnerable to various attacks, including man-in-the-middle and relay attacks.

NT LAN Manager version 2 (NTLMv2)

NTLMv2 is an updated version of the NTLMv1 authentication protocol and was introduced in Windows NT 4.0 SP4. It enhances security by adding a client challenge and server timestamp to the authentication process. This addition helps protect against man-in-the-middle and relay attacks. However, NTLMv2 is still susceptible to pass-the-hash attacks and is considered less secure than Kerberos.

The table below compares these hashes and protocols and highlights that, although not perfect, Kerberos is often the preferred authentication protocol when possible.

Protocol	Technique	Mutual Authentication	Message Type	Trusted Third Party
NTLM	Symmetric key cryptography	No	Random number	Domain Controller
NTLMv1	Symmetric key cryptography	No	MD4 hash, random number	Domain Controller
NTLMv2	Symmetric key cryptography	No	MD4 hash, random number	Domain Controller
Kerberos	Symmetric key cryptography & asymmetric cryptography	Yes	Encrypted ticket using DES, MD5	Domain Controller,/Key Distribution Center (KDC)

AD Domain Users

Domain users, as opposed to local users, enjoy access to a variety of resources within the domain, such as file servers, printers, and intranet hosts, based on the privileges assigned to their user account or the group they belong to. Unlike local users, domain user accounts can log in to any host within the domain. For more information on different types of Active Directory accounts, you can explore various resources online. One account that merits special attention is the KRBTGT account(Kerberos Ticket-Granting Ticket).

The KRBTGT account is a local account that is integrated within the Active Directory infrastructure. It serves as a service account for the Key Distribution service, which is responsible for authentication and granting access to domain resources. However, the KRBTGT account is often targeted by attackers due to the potential for granting them unrestricted access to the domain if compromised.

Attackers can exploit the KRBTGT account for privilege escalation and persistent access using techniques such as the Golden Ticket attack. In a Golden Ticket attack, the attacker gains access to the KRBTGT account’s hash, which allows them to create forged Kerberos tickets. These tickets grant the attacker access to any resource within the domain, effectively giving them full control.

To protect the KRBTGT account and the Active Directory domain from such attacks, it is essential to implement strong security measures, such as:

1. Regularly updating the KRBTGT account password, while ensuring that the password is complex and not easily guessable.
2. Employing monitoring and intrusion detection systems to detect any unusual activities or access attempts related to the KRBTGT account.
3. Implementing the principle of least privilege, granting users and groups only the necessary permissions to perform their tasks.
4. Enforcing strong password policies and multi-factor authentication (MFA) across the domain.
5. Conducting regular security audits and vulnerability assessments to identify and remediate potential security risks.

Exploit KRBTGT account - The Golden Ticket attack

- Initial compromise: Attackers first gain a foothold within the network, usually by exploiting a vulnerability or using phishing techniques to obtain valid credentials.

- Privilege escalation: Once inside, attackers work on escalating their privileges by targeting accounts with higher access levels, such as domain administrators.

- Extracting KRBTGT hash: After gaining domain administrator privileges, attackers can access the Active Directory database (NTDS.DIT file) and extract the KRBTGT account’s NTLM hash.
    - **Access the Active Directory Domain Controller**: After gaining domain administrator privileges, attackers can access the domain controller, which hosts the Active Directory database (NTDS.DIT file) that contains the KRBTGT account information.
    - **Locate the NTDS.DIT file:** The NTDS.DIT file is typically located in the “%SystemRoot%\NTDS” folder on the domain controller.

- **Copy the NTDS.DIT file**: Attackers would need to copy the NTDS.DIT file to a location where they can safely work with it. They may use tools like the Volume Shadow Copy Service (VSS) or ntdsutil to create a copy of the NTDS.DIT file without disrupting the domain controller’s operation.

How to access the Domain Controller(DC) using ntdsutil

- Log in to the domain controller with an account that has administrative privileges.
- Open an elevated Command Prompt (right-click on Command Prompt and select "Run as administrator").
- Enter `ntdsutil` in the Command Prompt and press Enter.
- At the `ntdsutil` prompt, type `snapshot` and press Enter.
- At the `snapshot` prompt, type `activate instance ntds` and press Enter.
- Now, create a snapshot by typing `create` and pressing Enter. You should see a message indicating that the snapshot was created successfully.
- To list available snapshots, type `list all` and press Enter. **Note the GUID of the snapshot you just created.**
- Exit the `snapshot` and `ntdsutil` prompts by typing `quit` and pressing Enter at each prompt.
- Mount the snapshot by running the following command in the elevated Command Prompt:

  ```
  ntdsutil snapshot "mount {<Snapshot_GUID>}"
  ```

  Replace `<Snapshot_GUID>` with the GUID you noted in step 7.
- You'll see a message indicating the snapshot was mounted successfully and the path to the mounted snapshot. Navigate to the mounted snapshot directory, where you can access the NTDS.DIT file without affecting the domain controller's operation.
- Copy the **NTDS.DIT** file and the **SYSTEM** registry hive (located in `%SystemRoot%\System32\config`) to a secure location for further analysis.

        - After you’ve finished copying the files, unmount the snapshot by running the following command in the elevated Command Prompt:

          ```
          ntdsutil snapshot "unmount {<Snapshot_GUID>}"
          ```

          Replace `<Snapshot_GUID>` with the GUID you noted in step 7.

    - **Extract the KRBTGT account’s NTLM hash**: With the NTDS.DIT file in hand, attackers can use a tool like Mimikatz, a popular post-exploitation tool, to parse the file and extract the KRBTGT account’s NTLM hash.
        - Once you have both files (NTDS.dit and SYSTEM), you can use the Mimikatz tool to extract the KRBTGT account’s NTLM hash. Download and run Mimikatz on a system where you can safely work with the files.
        - In Mimikatz, use the following commands to extract the KRBTGT account’s NTLM hash:

          ```
                  # Load the necessary Mimikatz module
                  privilege::debug

                  # Parse the SYSTEM registry hive to get the boot key
                  lsadump::lsa /inject /system:<path_to_SYSTEM_hive>

                  # Parse the NTDS.dit file with the boot key to get the
          KRBTGT hash
                  lsadump::lsa /inject /ntds:<path_to_NTDS_dit> /system:
          <path_to_SYSTEM_hive>
          ```

          Replace `<path_to_NTDS_dit>` and `<path_to_SYSTEM_hive>` with the correct paths to the files on your system.

        - After running these commands, Mimikatz will display information about all the accounts in the Active Directory database, including the KRBTGT account. Look for the KRBTGT account’s NTLM hash in the output.

- Creating forged Kerberos tickets: Using the extracted KRBTGT hash, attackers can generate forged Kerberos tickets, known as “Golden Tickets.” These tickets grant the attacker access to any resource within the domain, essentially providing them with full control.

- Maintaining persistence: The Golden Ticket attack enables attackers to maintain persistence within the network, even if passwords are reset or the attackers' original access point is discovered and removed.

Local accounts

When it comes to Windows-based systems, local user accounts are stored directly on the server or workstation. These accounts can be assigned rights either individually or through group membership, but it's important to note that these rights will only apply to that particular host and won't carry over to other systems in the domain. Despite being considered security principals, local user accounts are only able to manage access and secure resources on a standalone host.

There are several default local user accounts created during a Windows installation, including:

- The Administrator account, which is the first account created and has the SID S-1-5-domain-500. This account has complete control over most resources on the system, and while it can't be deleted or locked, it can be disabled or renamed. Windows 10 and Server 2016 disable the built-in administrator account and create another local account in the administrator group during setup.
- The Guest account, which is disabled by default. This account is meant to allow temporary access for users without a registered account on the computer, but due to the security risk of anonymous access, it is recommended to leave this account disabled.
- The SYSTEM account, or NT AUTHORITY\SYSTEM, is a default account installed and used by the operating system to perform internal functions. Unlike the Root account on Linux, this is a service account and doesn't run in the same context as a regular user. Many processes and services run under the SYSTEM context, and while it doesn't have a profile, it has permissions over most everything on the host and cannot be added to any groups. By default, it has Full Control permissions to all files on a Windows system.
- The Network Service account, which is a predefined local account used by the Service Control Manager for running Windows services. This account presents credentials to remote services when a service is running in its context.
- The Local Service account, which is another predefined local account used by the Service Control Manager for running Windows services. This account is configured with minimal privileges and presents anonymous credentials to the network.

To gain a comprehensive understanding of how these various accounts work together within an individual Windows system and across a domain network, it is recommended to thoroughly study Microsoft's documentation on local default accounts.

79%

Create your account today and explore more content on this platform. You can also start blogging and be inspiration for others 😎

8 days later

admiralarjun changed the title to **Pentesting Active Directory - Part 2 | Access Control, Users, KRGBT, Golden ticket attack** 13 days ago.