علیرضا رضایی

تحقیق جلسه هشتم

Resources

https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

https://infosecwriteups.com/kerberos-authentication-in-active-directory-2dc4af232f65

Kerberos Authentication

Kerberos is an authentication protocol that is used to verify the identity of a user or host. This topic contains information about Kerberos authentication in Windows Server 2012 and Windows 8.

Feature description

The Windows Server operating systems implement the Kerberos version 5 authentication protocol and extensions for public key authentication, transporting authorization data, and delegation. The Kerberos authentication client is implemented as a security support provider (SSP), and it can be accessed through the Security Support Provider Interface (SSPI). Initial user authentication is integrated with the Winlogon single sign-on architecture.

The Kerberos Key Distribution Center (KDC) is integrated with other Windows Server security services that run on the domain controller. The KDC uses the domain's Active Directory Domain Services database as its security account database. Active Directory Domain Services is required for default Kerberos implementations within the domain or forest.

The below mentioned ports are used for Active Directory authentication:

- UDP port 389: LDAP.
- TCP port 53: DNS.
- TCP, UDP port 88: Kerberos.
- TCP, UDP port 445: SMB over IP.

Practical applications

The benefits gained by using Kerberos for domain-based authentication are:

Delegated authentication.

Services that run on Windows operating systems can impersonate a client computer when accessing resources on the client's behalf. In many cases, a service can complete its work for the client by accessing resources on the local computer. When a client computer authenticates to the service, NTLM and Kerberos protocol provide the authorization information that a service needs to impersonate the client computer locally. However, some distributed applications are designed so that a front-end service must use the client

computer's identity when it connects to back-end services on other computers. Kerberos authentication supports a delegation mechanism that enables a service to act on behalf of its client when connecting to other services.

Single sign on.

Using Kerberos authentication within a domain or in a forest allows the user or service access to resources permitted by administrators without multiple requests for credentials. After initial domain sign on through Winlogon, Kerberos manages the credentials throughout the forest whenever access to resources is attempted.

Interoperability.

The implementation of the Kerberos V5 protocol by Microsoft is based on standards-track specifications that are recommended to the Internet Engineering Task Force (IETF). As a result, in Windows operating systems, the Kerberos protocol lays a foundation for interoperability with other networks in which the Kerberos protocol is used for authentication. In addition, Microsoft publishes Windows Protocols documentation for implementing the Kerberos protocol. The documentation contains the technical requirements, limitations, dependencies, and Windows-specific protocol behavior for Microsoft's implementation of the Kerberos protocol.

More efficient authentication to servers.

Before Kerberos, NTLM authentication could be used, which requires an application server to connect to a domain controller to authenticate every client computer or service. With the Kerberos protocol, renewable session tickets replace pass-through authentication. The server is not required to go to a domain controller (unless it needs to validate a Privilege Attribute Certificate (PAC)). Instead, the server can authenticate the client computer by examining credentials presented by the client. Client computers can obtain credentials for a particular server once and then reuse those credentials throughout a network logon session.

Mutual authentication.

By using the Kerberos protocol, a party at either end of a network connection can verify that the party on the other end is the entity it claims to be. NTLM does not enable clients to verify a server's identity or enable one server to verify the identity of another. NTLM authentication was designed for a network environment in which servers were assumed to be genuine. The Kerberos protocol makes no such assumption.