Authentication Methods for E-commerce Website Security

Todd M. Hammond

Pace University

Introduction to Cybersecurity Fall 2024 72308 - CYB 611- 72308 - 202470

Jeytha Sahana Venkatesh Babu

October 24, 2024

New Technology LAN Manager(NTLM)

Purpose

NTLM provides a challenge-response authentication protocol primarily based on messages to authenticate client messages and ensure integrity. NTLM authentication is an authentication protocol used to verify access and security of the systems through access channels. NTLM authentication is an authentication protocol that consists of the Windows Msv1_0.dll. Other NTLM authentication protocols include LAN Manager versions 1 and 2 and NTLM versions 1 and 2. NTLM protocols are embedded in applications. The caller sends parameters to NTLM, which then replies with an authentication method that the caller would use in its own messages that are to be used for transmission(*NTLM*, 2023).

Fundamentals

The protocols are in place and required to authenticate users and systems based on the challenge and response mechanism that verifies that the server and domain controller the user is using is through the proper channel of authentication and that the user knows the password associated with an account. When the NTLM protocol is used, a resource server must take actions to verify the identity of a computer or user whenever a new access token is needed- Contact a domain authentication service on the domain controller for the computer's or user's account domain, if the account is a domain account. Authentication is ensured in three major steps as follows:

NEGOTIATE_MSG: To begin the communication client sends the message (Request) to the server to access the service. In this message, the client specifies its supported NTLM options to the server.

CHALLENGE_MSG (Server to Client): This message is sent by the server to the client to challenge the client to prove their identity. This message is generated by the server in response to the client's negotiated message.

AUTHENTICATE _MSG (Client to Server): This message is sent from client to server in response to the challenge given by the server.(Bhandari et al., 2014)

Strengths

NTLM has its own set of benefits and strengths for which it is preferred for usage first would be connection-less authentication Which means a user can use authentication without a connection to a domain controller this is especially helpful in environments that contain limited network infrastructure. Following this NTLM can authenticate the identity of the target server even if it is not known and this is suitable for diverse network configuration. It is also versatile and it avoids sharing of passwords over the network since it uses a challenge/response mechanism to authenticate users. The NTLM is also considered extremely flexible since it integrates with other protocols and is also helpful for file sharing. Further, It is considered compatible with Linux and permits, Linux to use NTLM proxies through tools like CNTLM and NTLM Authorization Proxy Server (APS). These advantages help act as a strong suit for security measures for the online t initially starting out, especially for startups since it ensures that SMB (Server Message Block) communications are signed and authenticated, making it more difficult for attackers to intercept or modify traffic. This helps the integrity of communications and data within companies. NTLM's automatic authentication mechanism, designed for convenience within Active Directory environments, allows users to access network resources such as shared folders or printers without repeated credential prompts; a convenience that comes with security trade-offs.

Application

The new technology LAN manager contains a set of security protocols that is developed and published by Microsoft. It is essentially helpful for ensuring internal security and implementing zero trust strategy within and is primarily used to authenticate the identity of the users and to ensure the integrity and confidentiality of the company the system and of the users. The NTLM authentication is developed to be used in Logging Authentication on non-domain controllers (*NTLM Explained: Definition, Protocols & More | CrowdStrike*, 2019). It is a great way for companies that are small-scale working on expansions or startups whose majority workforce and revenue is dependent on online sales and for those companies who majorly run business as online storefronts.

Weakness

Along with the strengths NTLM also comes with its own set of weaknesses starting with NTLMv1 hashes are always the same length and are not salted, making them easy to crack. NTLM also is not very efficient when it comes to authentication because it only provides the feature of one-way authentication which means that the client can verify the identity of the server but the server cannot verify the identity of the client which would conclude it lacks mutual authentication. When a user logs into a Windows system, their credentials (username and hashed password) are stored in memory. During their session, these stored credentials are used for authentication requests to network resources using NTLM. This automatic authentication occurs without the system verifying the legitimacy of the network resource because the network is treated as inherently trustworthy, which could lead to inadvertent leakage of NTLM credentials, making them vulnerable to theft or misuse

Security Risks

NTLM's one-way authentication process allows attackers to impersonate a server and intercept or alter communications between the client and the server. (Yoad Dvir, 2024). Further Attackers can extract NTLM hashes from the memory of authenticated machines and use them to impersonate users without knowing their passwords since NTLM uses outdated hashing and encryption algorithms that make it more prone to cryptographic attacks. The use of weaker algorithms, such as MD4 and DES, makes NTLM hashes make way for further attacks, especially creating the vulnerability to brute-force attacks. Then there is another form of security risk called the NTLM relay attacks that occurs since attackers can intercept authentication traffic between a client and a server and redirect the user's credentials to a different server they control (Yoad Dvir, 2024)

KERBEROS

Purpose

Kerberos is a computer network authentication protocol that uses trusted third-party and secret-key cryptography to verify user identities and authenticate client-server applications(Bhandari et al, 2014). The Kerberos protocol is developed primarily to provide authentication service. It also is used to provide integrity and confidentiality of data that is exchanged between the client and server. Kerberos allows a process that runs on behalf of a user and to prove its identity to a verifier without sending data across the network that might allow an attacker or the verifier to impersonate the principal(Jason Gerend, 2021).

Fundamentals

Whenever a client authenticates itself to a new verifier it relies on the authentication server to generate a new encryption key and distribute it securely to both parties. This new encryption key is called a session key and the Kerberos ticket is used to distribute it to the verifier. The Kerberos ticket is a certificate issued by an authentication server and encrypted using the server key. Initially, a client presents its identity to the server using the ticket, which contains the principal, authenticator, and service principal. Issuing of tickets is provided by the Key Distribution Center (KDC). The KDC Stores the secret keys of clients and servers in the Database. These keys serve the client and server for the authenticity of the tickets they receive. It is important to note that a ticket's lifetime is limited, i.e., it eventually expires(Neuman & Ts'o, 1994). The Kerberos model consists of a KDC, which consists of three components: the Authentication Server, which serves as the authentication part of the Kerberos environment; the ticket provider for the environment, called the Ticket-Granting Server; and finally, the Database, which is the primary storage component of the secret keys of clients and servers of Kerberos. (Bhandari et al., 2014)

Strengths

Kerberos has several strengths that make it efficient for authentication. it uses symmetric encryption to safeguard data exchanges between the client and the server, including the authentication process itself. The keys used for encryption are never transmitted across the network, reducing the chance of interception. The interoperability feature supports different types of systems and platforms, including Windows, Unix, and Linux. (Hill, n.d.). Mutual authentication is another feature that strengthens the purpose of using Kerberos which allows the client and server to verify identities of each other. This is extremely helpful to

prevent and reduce the risk of man-in-the-middle attacks. When Kerberos is needed to be updated to increase load it can be scaled to handle authentication requests. Further, the single sign-on capability helps users authenticate only once and gain access to various services thereby reducing the issue of password fatigue that leads users to adopt insecure practices due to an overload of passwords(*Kerberos Authentication Protocol - Article*, 2024). As pointed out above the strengths Kerberos holds, include a great feature for startups to incorporate into their work culture, which allows employees the ease to remember only a single password allowing them to gain access to the company services the same time providing safety by ensuring the safe passage of data and facilitating viable communication between client and user.

As pointed out in the above section, highlighting the strengths Kerberos holds, it is a great feature for startups to incorporate into their work culture, that allows employees the ease to remember only a single password allowing them to gain access to the company services at the same time providing safety by ensuring the safe passage of data and facilitating viable communication between client and user.

Application

In terms of authentication, Kerberos ensures that both users and services are securely authenticated using tickets, removing the need to repeatedly transmit passwords over the network. This minimizes the risk of credential theft during authentication processes. Next in terms of authorization, Kerberos works with access control mechanisms, where once a user is authenticated, their permissions are checked based on the tickets issued. Regarding network security, Kerberos also plays a critical role by preventing replay and man-in-the-middle attacks. It encrypts all authentication exchanges, ensuring secure communication and protecting against unauthorized access within the network. These aspects help ensure a

company's data is secure and its integrity is maintained. Especially for companies that have an online database and rely on e-commerce revenue generation and also those that have online transactions enabled. Further, it is a great feature for startups to incorporate into their work culture, that allows employees the ease to remember only a single password allowing them to gain access to the company services at the same time providing safety by ensuring the safe passage of data and facilitating viable communication between client and users.

Weakness

Kerberos is not beneficial if the host is not trustworthy. Otherwise, the intruder can use the host as a key to get authentic. An intruder can impersonate by obtaining an IP address for that server. Although Kerberos has been proven quite capable in a lot of aspects it comes with its limitations and vulnerabilities Because Kerberos was initially designed for use within a single domain, establishing cross-realm trust relationships between different administrative domains, can be complex to set up and manage. It is challenging to integrate with systems and services that do not support Kerberos. Kerberos is not effective against password-guessing attacks; if a user chooses a poor password, then an attacker guessing that password can impersonate the user. Kerberos also works on time synchronisation hence between the client, and server, if the clocks are too far out of sync, authentication requests may fail, leading to access issues. Kerberos also depends heavily on the availability and security of the KDC; if the KDC becomes compromised or unavailable, the entire authentication system can be disrupted. Kerberos is not considered helpful if the host is not trustworthy since the intruder can use the host as a key to get authentic. An intruder can impersonate by obtaining an IP address for that server.

Security Risks

Roasting attacks are a major source of threat for Kerberos, first would be the AS-REQ Roasting where the attacker creates a duplicate of a Kerberos ticket-granting ticket (TGT) using credentials that have been compromised, with this fake TGT, the attacker can impersonate any user in the domain, second being Kerberoasting, the attacks work by leveraging the Kerberos authentication to perform a variety of tasks such as Scan Active Directory (AD) for users with a Service Principal Name (SPN), a unique identifier that helps to authenticate that user into a specific account. Post which the attacker can also move laterally within the network unchecked, request, extract tickets and decrypt them for password information and steal other critical data(*Harmj0y – Harmj0y*, 2014). Another form of attack would be ticket abuse There are three different types first would be the golden ticket where the attacker creates a duplicate of a Kerberos ticket-granting ticket (TGT) using credentials that have been compromised, with this fake TGT, the attacker can impersonate any user in the domain. Second is the silver Ticket when the attacker forges service tickets (TGS) since these tickets access a particular service, such as SQL or HTTP, the attacker easily impersonates a legitimate user(ActiveDirectorySecurity et al., 2015). Third would be, pass-the-Ticket when the attacker steals a legitimate Kerberos ticket from memory and uses it to authenticate to systems without needing the user's password(*Redirect Notice*, 2024)

Lightweight Directory Access Protocol (LDAP)

Purpose

The Lightweight Directory Access Protocol (LDAP) is a vendor-neutral software protocol that is used to look for information or devices within a network; it is a protocol that helps users find data about organisations, persons, etc. LDAP has two main goals: to store data in the LDAP directory and authenticate users to access the directory, it is designed to

deliver fast READ performance. LDAP is majorly designed to build central authentication servers. These servers contain usernames and passwords for all the users within a network. Applications irrespective of their types and services can connect to the LDAP server to authenticate and authorise users.

Fundamentals

There is a multi-step process involved in connecting to an LDAP directory and completing a request. It includes establishing a secure connection. It is essential that a user has pre-installed the LDAP client on the device they are using. This client is also required to establish a secure connection with an LDAP directory by utilising services such as secure sockets layer or transport layer security by submitting a query. The query is submitted to an application, to perform actions for example it could be looking up an email address or connecting to a printer. The application accesses the LDAP client and sends the user's distinguished name (DN) and password to the LDAP directory server for authentication, thereafter authenticating and authorising the user. The LDAP directory then decides and determines that the user has correct credentials, and identifies, in particular, the user group they have been given permission to access and the operations that group is authorised to perform. After the query is considered complete, the directory returns information to the user, providing the necessary service that was requested. Hence ending the session, the user disconnects from the LDAP directory and the session ends(*Lightweight Directory Access Protocol (LDAP)*, 2019).

Strengths

LDAP's major strength lies in securing information in an organised and secure manner. Further LDAP protects Passwords through regular updates passwords ensuring they are strong, long, and unique, so that security of personal information is achieved. LDAP also verifies the identity of the person who is requesting information this method provides a foundational level of security and it also helps in eliminating a layer of access management and ensures that there is an enhancement in encryption security for the company's and organisation's safety. LDAP Deletes Sensitive Information When It Is No Longer Needed This is accomplished by using SSL/TLS encryption and adding an extra layer of protection to the information that is shared via LDAP. Additionally, LDAP helps backup critical files when you install other security extensions along with using this protocol(*What Is LDAP and How Does It Benefit Your Business?* 2022).

Application

The most common LDAP use cases would include startups or companies that have already established a strong foothold or legacy companies, which would have a lot of backend data, especially those that have a huge database and lots of inventory as well as merchandise/client/customer information that requires safekeeping since LDAP provides a central location for accessing and managing directory services. LDAP enables organisations to store, manage, and secure information about the organisation, its users, and assets–like usernames and passwords. This helps reduce the complexity of storage access by providing structural segmentation of information, and it can be extremely useful for corporations, and startups as they grow and acquire more user data and assets. LDAP also functions as an identity and access management (IAM) for ensuring the company's internal security solution that targets user authentication, supports Kerberos, single sign-on (SSO), Simple

Authentication Security Layer (SASL), and Secure Sockets Layer (SSL)(*What Is Lightweight Directory Access Protocol (LDAP) Authentication?* 2022).

Weakness

The application probably isn't secure enough to be touching credentials and despite this flaw, The LDAP server cannot enforce the security of the authentication mechanism used to obtain the credentials. While utilising LDAP for authentication, the user must disclose their secret to a 3rd party, for them to replay that secret against the LDAP directory. Another major weakness lies in the fact that managing an Active Directory in a large distributed environment, is quite difficult itself and even more so to determine when services are using an active directory as an LDAP directory, and how the application administrators have configured their LDAP client. Further, an application using LDAP for authentication will forever be limited to usernames and passwords(link et al., 2018).

Security Risks

Considering the weakness possessed by LDAP there is a major security risk called LDAP injection which is a type of attack where code is injected through a web application in order to access sensitive information in an LDAP directory. The injected code is said to consist of LDAP metacharacters that perform the function of modifying legitimate requests from LDAP clients to achieve malicious objectives. The repercussions resulting in this injection attack include data breach, user privilege escalation, or account hijacking. This attack is orchestrated by attackers when servers do not validate the legitimacy of LDAP client requests, which allows uninterrupted access to cyber attackers for liberal communication within the LDAP servers(*What Is LDAP? How It Works, Uses and Security Risks in 2022 | UpGuard*, n.d.)

References

ActiveDirectorySecurity, S. M. in, Security, M., Reading, T., & Reference, T. (2015, November 17). *How Attackers Use Kerberos Silver Tickets to Exploit Systems*. Active Directory Security. https://adsecurity.org/?p=2011

Bhandari, R., Kumar, N., & Sharma, S. (2014). Analysis of Windows Authentication Protocols: NTLM and Kerberos. *ResearchGate*. https://doi.org/10.13140/2.1.2087.5528

harmj0y – harmj0y. (2014). Rssing.com. https://harmj4.rssing.com/chan-30881824/all_p5.html

Hill, P. (n.d.). *Kerberos interoperability issues*. Retrieved October 19, 2024, from https://www.usenix.org/legacy/events/lisa-nt00/hill/hill.pdf

Jason Gerend. (2021, July 29). *Kerberos Authentication Overview*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

Kerberos authentication protocol - Article. (2024, March 20). Sailpoint.com. https://www.sailpoint.com/identity-library/kerberos-authentication-protocol

Lightweight Directory Access Protocol (LDAP). (2019, June 21). GeeksforGeeks. https://www.geeksforgeeks.org/lightweight-directory-access-protocol-ldap/

link, G., Facebook, Twitter, Pinterest, Email, & Apps, O. (2018, March 14). *The LDAP "authentication" anti-pattern*. https://blog.lithnet.io/2018/03/the-ldap-authentication-anti-pattern.html

Neuman, B. C., & Ts'o, T. (1994). Kerberos: an authentication service for computer networks. *IEEE Communications Magazine*, *32*(9), 33–38. https://doi.org/10.1109/35.312841

NTLM. (2023, March 24). Wikipedia. https://en.wikipedia.org/wiki/NTLM

NTLM Explained: Definition, Protocols & More | CrowdStrike. (2019). Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/windows-ntlm/

OWinfreyATL. (2024, July 15). *Delegation and roles in entitlement management - Microsoft Entra ID Governance*. Microsoft.com. https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-delegate

Security Risks of NTLM: Confronting Realities Outdated Protocols | Whitepaper | CrowdStrike. (2022, March 17). Crowdstrike.com. https://www.crowdstrike.com/resources/white-papers/the-security-risks-of-ntlm/

What are the advantages and disadvantages of using Kerberos authentication over other access control methods? (n.d.). Www.linkedin.com. https://www.linkedin.com/advice/0/what-advantages-disadvantages-using-kerberos-authentication

What is LDAP (Lightweight Directory Access Protocol)? (n.d.). SearchMobileComputing. https://www.techtarget.com/searchmobilecomputing/definition/LDAP

What Is LDAP and How Does It Benefit Your Business? (2022, January 17). Helpy.io. https://helpy.io/blog/what-is-ldap-and-how-does-it-benefit-your-business/

What is LDAP? How it Works, Uses and Security Risks in 2022 | UpGuard. (n.d.). Www.upguard.com. https://www.upguard.com/blog/ldap

What is lightweight directory access protocol (LDAP) authentication? (2022, June 3). Www.redhat.com. https://www.redhat.com/en/topics/security/what-is-ldap-authentication

Yoad Dvir. (2024, August 15). *The End of an Era: Understanding the Security Risks of NTLM*. Silverfort; Silverfort. https://www.silverfort.com/blog/understanding-the-security-risks-of-ntlm/

(2024). Nccgroup.com. https://www.nccgroup.com/us/research-blog/detecting-and-hunting-for-the-petitpotam-ntlm-relay-attack/