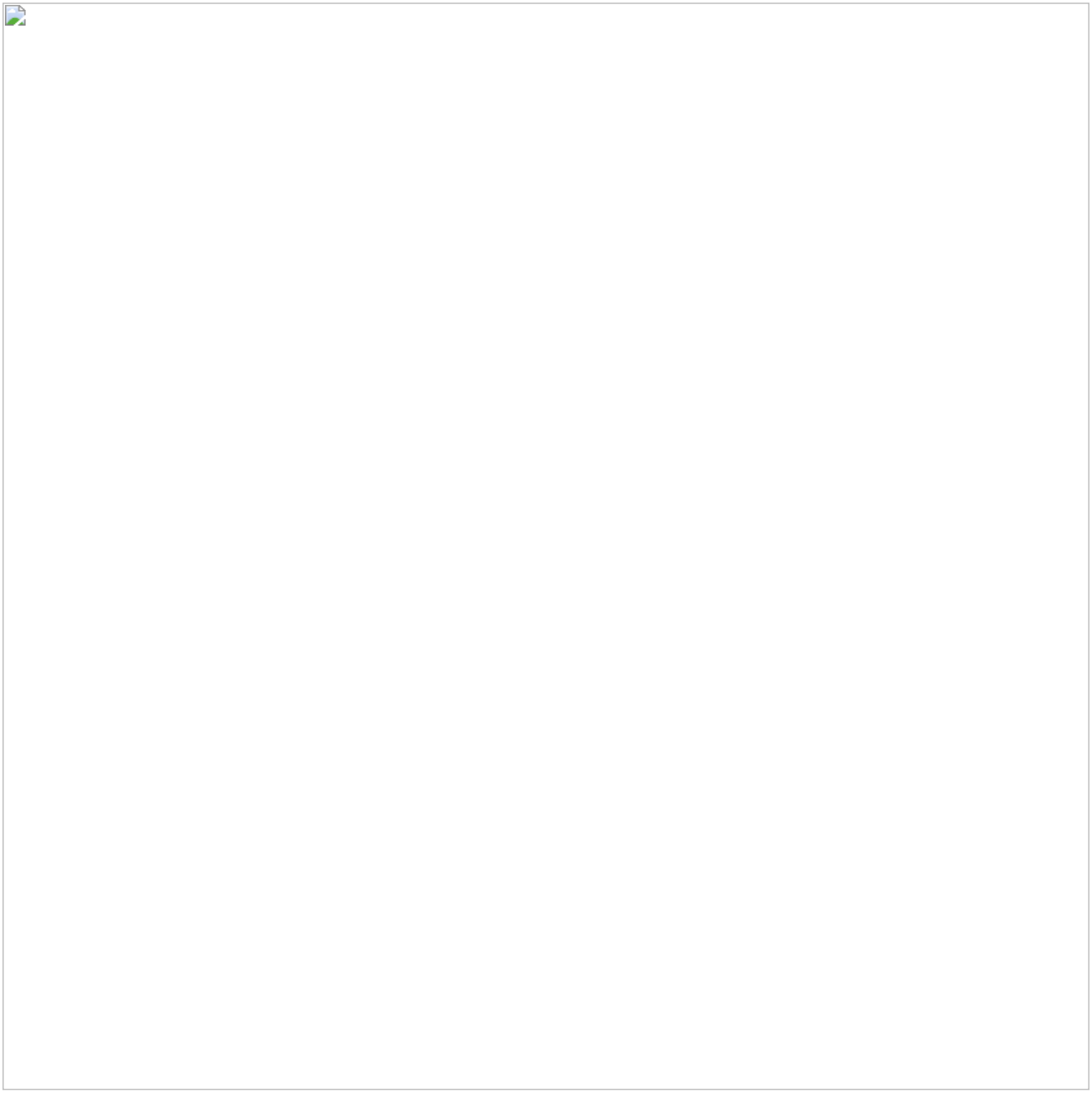
Authentication protocols and avoiding downgrade attacks

crowe.com/cybersecurity-watch/authentication-protocols-avoiding-downgrade-attacks



Strengthening authentication protocols is critical for protecting networks from backward compatibility.

Authentication protocols are a crucial component of security systems because they grant only authorized individuals or entities access to resources. Because of their function, authentication protocols are a popular attack vector, so they continue to evolve to incorporate enhanced security features. Despite improvements, however, some organizations still allow backward compatibility to older protocols, which can leave them vulnerable. Organizations can strengthen their security posture by strengthening challenge-response protocols or implementing more secure token- or ticket-based authentication protocols.

Evolution of authentication protocols

Authentication protocols in Microsoft Windows™ have undergone a significant transformation throughout the years, from less secure protocols to more robust and sophisticated mechanisms. The LAN Manager (LM) authentication protocol came first. Due to its limited character set and its use of weak cryptographic algorithm, LAN Manager was fairly easy to crack.

As security concerns mounted, a more formidable approach was introduced with the implementation of New Technology (NT) LAN Manager (NTLM) authentication protocols. NTLM introduced the NT hash, a relatively stronger hashing algorithm than the one used in LM. NTLMv1 (officially Net-NTLMv1) of the protocol uses the NT or LM hash through a challenge-response mechanism between a server and a client. The server authenticates the client by sending an 8-byte random number as the challenge, and the client returns a 24-byte result of the computation using the NT or LM hash and challenge. The server verifies that the client has computed the correct result and, therefore, the authenticity of the client.

However, because of the outdated encryption algorithm and poor implementation of session authenticity validation, NTLMv2 (officially Net-NTLMv2) was introduced in 1996 as an improved version of the NTLMv1 protocol, with the similar challenge-response mechanism but stronger algorithms and two changes. The first change was including a time stamp into the encryption step, and the second change was that the target server would also generate a variable-length challenge instead of providing the 8-byte challenge. Nonetheless, because NTLMv2 still used the challenge-response mechanism, it remained vulnerable by design.

With the launch of Microsoft Windows 2000, Kerberos became the default authentication protocol in the Windows environment. Researchers at the Massachusetts Institute of Technology developed Kerberos in the 1980s. Kerberos is a ticket-based protocol that uses a trusted third-party authentication service that supports multifactor authentication and uses mutual authentication. During authentication, Kerberos looks for tickets instead of passwords to authenticate and authorize, and then it stores specific tickets for each session on the end user's device. Despite its superiority, however, it still is not yet the de facto standard because of backward compatibility concerns with older systems.

Downgrade attacks

New vulnerabilities emerge every day. However, not all cyberattacks employ the latest techniques and exploits and not all vulnerabilities can be patched.

Downgrade attacks take advantage of a system's backward compatibility to force it into less secure modes of operation by using deprecated protocols or mechanisms. The older the protocols are, the more effective a downgrade attack can be.

It's important to keep in mind, however, that balancing security with usability is always a delicate tradeoff. Any backward compatibility mechanism can provide a convenient bridge between legacy systems and modern machines but serve as a time machine for malicious actors to travel back in time to exploit the deprecated protocols.

Supporting NTLM security

Although replaced by Kerberos as the primary authentication protocol, the NTLM suite remains broadly deployed in the Windows environment and includes the LM, NTLMv1, and NTLMv2 protocols. To support any legacy system or solve compatibility issues, Microsoft has provided backward compatibility for authentication protocols via the "LAN Manager authentication level" policy setting, which is used to determine which challenge-response authentication protocol should be used for network logons.

This setting offers five levels, and higher levels require stricter authentication protocols. From zero to five, each level affects the authentication protocol that clients use, the session security level that the computers negotiate, and the authentication level that servers accept.

Downgrade attack mechanics

NTLMv1 downgrade attack methodology is not complex or fancy. The following attack steps are simple below:

1. Configure and start a listener tool to receive and capture traffic
2. Coerce authentication from the target system
3. Negotiate a weaker authentication setting

4. Crack the captured downgraded hash

How NTLMv1 downgrade attacks work

Source: Crowe analysis, April 2024

If the target system has set the LAN Manager authentication level lower than five, then malicious actors can coerce an NTLMv1 authentication request from the target system to their workstation and capture the insecure NTLMv1 hash. An attacker can simply use the responder tool and set the "--lm" flag to force an LM downgrade. This action essentially asks the target server to please use the weakest authentication setting as it is all that the attacker machine supports.

Once the NTLMv1 hash is captured, an attacker can crack the hash by breaking it down into its cryptographic keys and guessing every possible option. With readily available consumer-level hardware or cloud resources combined with open source tools, this action can be accomplished in a reasonable amount of time, typically a few days, but with a 100% success rate.

To make the password crack process run faster, threat actors can set a static challenge during capture (such as 1122334455667788) to replace the default random challenge included in protocol negotiation. It should be noted that Microsoft introduced extended session security as a stopgap solution to the NTLMv1 authentication protocol that

prevents this. However, the responder tool also has a “--disable-ess” flag that aims to disable this protection. In this way, the static challenge allows threat actors to crack the captured NTLMv1 hash using a precomputed rainbow table in seconds.

Other downgrade attack goals

Cracking the hash is not the only goal for an NTLM downgrade attack. The ultimate purpose of such an attack is to lower the security measures to a deprecated outdated protocol such that threat actors can use N-day (known) vulnerabilities to bypass certain security settings. Even though NTLM is vulnerable by design, the additional layers of security of server message block (SMB) signing and lightweight directory access protocol (LDAP) signing can confirm the authenticity and origin of packets to prevent relay attacks. The signature cannot be stripped in transit because NTLM includes a message integrity code (MIC) for the full NTLM negotiation.

With the downgrade to NTLMv1, malicious actors – and penetration testers – can exploit the authentication as NTLMv1 doesn’t support computing a MIC. Tooling already exists to support this exploitation due to a previous vulnerability, CVE-2019-1040 (NoMIC), in which relay attacks could be conducted despite message signing being in place. In this way, any SMB-related protocols can be relayed to a domain controller to perform SMB- and LDAP-related attacks, such as domain enumeration, credential harvesting, and resource-based constrained delegation.

Mitigation techniques

Understanding how downgrade attacks work is critical for security teams to be able to determine the best method to prevent them. Because downgrade attacks focus on exploiting the enabled backward compatibility, one direct way to mitigate the risk is to set the LM authentication level in the environment to level five. Level five permits only NTLMv2 and refuses NTLMv1 and LM algorithms. To prevent this setting from breaking anything, security teams can enable and review logs to determine which systems (if any) in the environment might be using legacy forms of authentication. By requiring only NTLMv2 with strong passwords, security teams can make it much more difficult for attackers to crack the password.

Although NTLMv2 was an improvement over NTLMv1 and LM, in that it used a higher-level cryptographic algorithm (HMAC-MD5) with protection from replay attacks, the core challenge-response mechanism did not change. This lack of change left NTLMv2 exposed to other NTLMv1 vulnerabilities, including relay attacks.

Microsoft introduced Kerberos authentication as a more secure protocol and has set it as the default authentication protocol over NTLMv2. Kerberos uses a ticketing server rather than pass-through authentication, which disallows hashed passwords from being transported insecurely over the network, as they could be with NTLM authentication. Additionally, Kerberos supports mutual authentication, which allows the client and server to authenticate each other and help make attacks like NTLM’s pass-the-hash or relaying more difficult in Kerberos. Although legacy applications and functions might prevent comprehensive adoption, organizations should aim to use Kerberos-only authentication (or passwordless authentication) wherever possible.

Authentication protocol vigilance

Given that threat actors continue to target authentication protocols, organizations need to remain vigilant about how users and entities authenticate to their networks. By incorporating enhanced security features, removing backward compatibility, and addressing vulnerabilities in legacy systems, organizations can better protect their users, data, and networks.