ForeScout™

CounterACT® and Pass-the-Hash (PtH)

CounterACT Technical Notes

Version 1.0

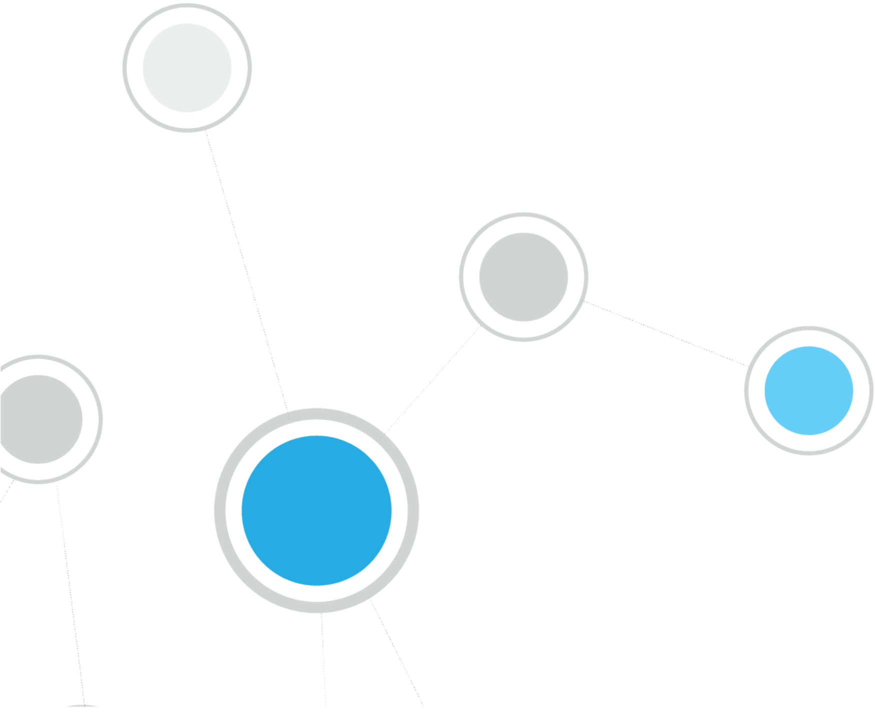

Table of Contents

Summary

When an endpoint connects to the network, ForeScout CounterACT® employs several techniques to perform deep endpoint inspection remotely. CounterACT uses Microsoft's NTLMv1 & v2 protocols to authenticate to Windows® endpoints.

🗎 *NTLMv1 is considered outdated and not secure. ForeScout recommends working with NTLMv2.*

In non-CounterACT environments, use of the NTLM protocol inherently exposes networks to a Pass-the-Hash (PtH) attack. In this attack scenario, a rogue user redirects or reuses password hashes in an attempt to spoof a legitimate and authenticated user and to gain fraudulent access to endpoints on the network.

ForeScout has analyzed PtH attack vectors and has concluded that CounterACT does not introduce a PtH threat to Windows endpoints on the customer network.

Technical Details

During an "Interactive" logon (a.k.a. "Logon locally" or Logon Type #2), the hash of the logon password is saved on the endpoint. In a PtH attack, a rogue user having local administrative rights can capture the logon password hash. When the captured hash is of a Domain user, the attacker can reuse the hash to authenticate to other machines in the Domain. As a result, the attacker may gain access to other machines and servers in the organization and spread the attack further.

CounterACT does not expose endpoints to this type of attack. The CounterACT HPS Inspection Engine uses a "Network" logon (Logon Type #3) to authenticate to endpoints. This logon type does not leave the password hash in the admitted endpoint's memory and thus does not expose it to rogue users who may have gained control over the endpoint.

Another PtH attack vector is relevant when the CounterACT HPS Inspection Engine uses the NTLM protocol to authenticate to endpoints while the attacker has access to network traffic. In this scenario, a rogue user listens to the challenge-response authentication hash in an attempt to bypass CounterACT. It is important to understand that CounterACT does not transmit the NTLM-hash of the user password over the wire. In addition, the CounterACT administrator can select NTLMv2 which is more secure than NTLMv1 in several ways. One of the key differences is that NTLMv2 adds a client challenge. Breaking NTLMv2 by sniffing traffic is rendered impractical when using a good password policy with a client challenge. With NTLMv2, CounterACT authentication is not only protected from PtH attacks, but also combats dictionary and brute-force attacks more effectively. For more information about PtH attacks see:

https://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf

Table 6 on page 40 indicates which credentials are reusable for the various logon types. Note that other authentication protocols, including SSH and TLS, are not vulnerable to PtH attacks.

Protocol Abbreviations

Abbreviation	Protocol
NTLM	MS NT LAN Manager
SSH	Secure Shell
TLS	Transport Layer Security

Legal Notice

2018-04-10 09:21