Forescout

Pass-the-Hash (PtH)

Technical Note

Forescout version 8.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-03-20 14:40

Table of Contents

Summary **4**

Technical Details **4**

Protocol Abbreviations **5**

Additional Forescout Documentation **5**

Documentation Downloads ..... **Error! Bookmark not defined.**
Documentation Portal ..... **Error! Bookmark not defined.**
Forescout Help Tools ..... **Error! Bookmark not defined.**

Summary

When an endpoint connects to the network, the Forescout® platform employs several techniques to perform deep endpoint inspection remotely. The Forescout platform 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 *NTLMv1 is considered outdated and not secure.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-Forescout 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 the Forescout platform 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.

The Forescout platform does not expose endpoints to this type of attack. The Forescout 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 Forescout 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 the Forescout platform. It is important to understand that the Forescout platform does not transmit the NTLM-hash of the user password over the wire. In addition, the Forescout 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, Forescout 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

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).