I am AD FS and so can you: Attacking Active Directory Federated Services

Archived: 2026-04-06 03:18:13 UTC

Go back

With the rise in popularity of enterprise cloud applications - email, data processing, and data warehousing for example - organizations find themselves contending with the need to securely share identity information with their cloud service providers. This talk explores one common model for this, Active Directory Federated Services, and how it can be exploited by attackers to access cloud applications as any user, without knowing their password and without MFA.

DESCRIPTION

This talk will take attendees on a tour of one of the most popular federated authentication solutions, **Active Directory Federated Services (AD FS)**. We will cover AD FS basics, reconnaissance (both pre and post-exploitation), various post-exploitation attacks, and lastly defense.

This work was inspired by CyberArk's "Golden SAML" research blog. It expands on the work by giving a more detailed view of AD FS, how an attacker might reconnoiter and attack AD FS, and a more service provider agnostic tooling to forge SAML tickets.

Introduction

In the last few years we have witnessed a paradigm shift in how enterprises think of the cloud. Hailed for its low-cost and low-complexity, organizations have moved a large amount of enterprise functions into the cloud. This decentralized approach required a new model for authentication and authorization - organizations needed a way to securely share identity information with cloud-based partners.

We begin by giving an overview of Microsoft's solution to this problem, **Active Directory Federated Services (AD FS)**. Throughout the talk we will use one of the most common use-cases for AD FS, authenticating users to Office 365 as a teaching example; however, our tooling and techniques can be applied to any federated application.

Reconnaissance

First, we will talk about some common ways you can identify if an organization is using AD FS, and some key information to extract from it once identified. This reconnaissance phase is from the point-of-view of an external attacker with no credentials:

- Identification of external AD FS proxies (using the Office 365 portal and/or DNS is usually enough)
- Internal hostnames and AD names that the AD FS proxies expose

- MFA providers that the organization may use
- Authentication methods accepted by AD FS (by requesting special metadata XML files)

Attacks

We now move on to attacks against AD FS in particular. All of these attacks are from a **post-exploitation** standpoint. That is we assume the attacker has already compromised the victim's internal network, and is seeking to move into one or more of an organization's cloud applications. Notably, *none* of these attacks require Domain Administrator rights, yet could give an attacker access to any application as any user and bypass MFA! We begin by talking about identifying the internal AD FS servers:

- Using DNS to identify the AD FS farm internally
- Using Active Directory to identify the AD FS farm
- Using Active Directory to identify the AD FS account

Once we have identified the AD FS farm we must compromise a server and pull key information from it:

- Acquiring and decrypting the AD FS signing material
- Listing relying trusts (i.e. applications that trust AD FS to share identity information)
- Obtaining the access policies and AD FS claims that a service (cloud app) is expecting

Finally we will demonstrate our **new tool** in action. Using the extracted information, our tool will generate a **forged SAML token** as an arbitrary user that can then be used to authenticate to Office 365 without knowledge of that user's password. This attack also **bypasses any MFA** requirements. We will show how the tool can be used to create SAML tokens for arbitrary apps, given a template.

Bonus!

We will also demonstrate how an attacker could implant a **persistent backdoor** into AD FS to bypass authentication for specific users. This attack will demonstrate code that can be placed on the AD FS server to bypass authentication and/or the two-factor step of an AD FS server using Duo's AD FS plugin. Essentially the code looks for specific username/password combinations and, when present authenticates the user regardless of password or MFA validity.

Defense and Detection

We will wrap up the talk by going over some ways organizations can better defend their AD FS environment. The concepts here are fairly simple:

- AD FS farms should be treated with the same level of concern as your domain controllers (i.e. they should be tier 0 devices)
- Some additional steps you can take with policies and claims to make tokens harder to forge (this will depend a lot on the relying party, but we will use Office 365 as an example)
- If you really want, use an HSM to store your signing keys

Source: https://www.troopers.de/troopers19/agenda/fpxwmn/