4 Service Account Attacks and How to Protect Against Them

blog.netwrix.com/2023/02/24/protecting-service-accounts

Jeff Warren

Whether you realize it or not, service accounts represent a major risk to your data security. This article explains the fundamentals of service accounts and how attackers can exploit them so you can prevent yours from being compromised.

Handpicked related content:

Active Directory Security Best Practices

What is a service account?

A service account is an account used to run services or applications, rather than being used interactively by administrators or business users. Service accounts often have privileged access to computers, applications and data, which makes them highly valuable to attackers.

What makes securing service accounts so difficult?

Because service accounts are not tied directly to a human, they must be treated differently from other accounts. One important example is password policies. It may be acceptable to require very long and complex passwords for service accounts because you don't have to worry about a human forgetting them.

On the other hand, it is hard to set password expiration policies because resetting a service account password may break an application. That means that once a service account's password is compromised by an attacker, it is unlikely to change for a long time, if ever.

How do attackers take advantage of service accounts?

Attackers use multiple tactics to compromise service accounts and misuse their privileged access. This series of blog posts details some of the most common ones:

What can you do to protect service accounts?

There are measures you can take to prevent the misuse and compromise of service accounts. They include restricting these accounts from interactive logons and automating password management.

How can Netwrix help?

It’s really hard to detect a service account attack, but the Netwrix Active Directory security solution delivers the comprehensive visibility you need to secure your Active Directory environment from end to end. It will enable you to:

- Uncover security risks in Active Directory and prioritize your mitigation efforts.
- Harden security configurations across your IT infrastructure.
- Promptly detect and contain even advanced threats, such as DCSync, NTDS.dit password extraction and Golden Ticket attacks.
- Respond to known threats instantly with automated response options.
- Minimize business disruptions with fast Active Directory recovery.

Jeff Warren