DAMP

The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification.

This project contains several files that implement host-based security descriptor "backdoors" that facilitate the abuse of various remotely accessible services for arbitrary trustees/security principals.

tl;dr - this grants users/groups (local, domain, or 'well-known' like 'Everyone') of an attacker's choosing the ability to perform specific administrative actions on a modified host without needing membership in the local administrators group.

Note: to implement these backdoors, you need the right to change the security descriptor information for the targeted service, which in stock configurations nearly always means membership in the local administrators group.

More information:

- An ACE in the Hole - Stealthy Host Persistence via Security Descriptors
- The Unintended Risks of Trusting Active Directory

Authors: @tifkin_, @enigma0x3, and @harmj0y.

License: BSD 3-Clause

Remote Registry

Add-RemoteRegBackdoor.ps1

Add-RemoteRegBackdoor

Implements a new remote registry backdoor that allows for the remote retrieval of a system's machine and local account hashes, as well as its domain cached credentials.

RemoteHashRetrieval.ps1

Get-RemoteMachineAccountHash

Abuses the ACL backdoor set by Add-RemoteRegBackdoor to remotely retrieve the local machine account hash for the specified machine.

Get-RemoteLocalAccountHash

Abuses the ACL backdoor set by Add-RemoteRegBackdoor to remotely retrieve the local SAM account hashes for the specified machine.

Get-RemoteCachedCredential

Abuses the ACL backdoor set by Add-RemoteRegBackdoor to remotely retrieve the domain cached credentials for the specified machine.