



**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.