DATA SHEET

Trustwave SpiderLabs® Active Directory Review

ACTIVE DIRECTORY IS THE HEART OF AN ORGANIZATION; MAKE SURE IT'S SECURE

Operation issues and technical debt are the primary, root cause issue for data breaches. Active Directory (AD) is the beating heart of an organization and is ultimately where malicious threat actors, internal or external, will focus their efforts. The advantages of AD compromise to an attacker mean unlimited access to all internal resources, accounts and workstations.

Why Trustwave SpiderLabs?

Our comprehensive and best of breed AD review methodology will simulate real life attacks that Advanced Persistent Threats are using to compromise global organizations. Our methodology ensures that defense in depth and resiliency are integral factors of your AD design to slow attackers down, create detection points for your internal team and protect critical assets. AD is a complex infrastructure and to ensure a comprehensive view the SpiderLabs methodology covers four key categories.

1 Managing Domains and Forests

We focus on the configuration of Forest to Forest and Forest to Domain relationships and identify issues with Trusts, protocol configuration and control of core assets such as Domain Controllers.

- Configuration of Active Directory forest and domain configuration (red forest).
  - › Network Isolation
  - › Privileged Access Workstations
- Domain Functional Level
- Active Directory trust configuration and security
- Forest and Domain Trust Directions
- Protocol Signing (SMB, LDAP)
- Organizational Units
- Network footprint of domain controllers
  - › Netsessionenum resilience, if any

2 Controlling the Endpoints

The endpoints are the initial foothold for an attacker and therefore how these are managed and controlled can be an effective layer in disrupting attackers. We review how these are managed, what policies are applied to endpoints and how local access is logged.

- Patch Management Policy across the Windows estate
- Server Baselines
- Domain Password policy configuration
- Password hash storage techniques (LM/NTLM):
  - › AD password review
- Security Group Policy Review
- Security Template Baselines
- Auditing and Logging
- Group Policy Objects
- Whitelisting

3 User Access Controls

Users need access to network assets and we examine the user permissions, explicit and implicit group membership and local administrative controls.

- User Access Rights and Privileges
- Group Memberships
- Delegated Administrative Rights
- Local Administrative Controls
- Kerberos
- DACLs/ACEs

4 Attackers Toolbox

This area of the service analyses how an attacker can enumerate the directory and identify privilege escalation routes.

- Domain Enumeration
- Service Account Passwords
- Token Impersonation
- Privilege Escalation
- Data Access

For more information: www.trustwave.com