SERVICE DESCRIPTION

SpiderLabs Active Directory Review

Service Scope

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 a malicious threat actor, either 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.

Our comprehensive and best of breed AD review methodology simulates real life attacks Advanced Persistent Threats (APTs) to compromise target organizations. Through our mature methodology, we ensure that defense-in-depth and resiliency are integral factors of your AD design to slow down attackers. Additionally, our team assist in creating detection points for internal teams, in order to protect critical assets. In order to ensure comprehensive coverage, the SpiderLabs methodology covers four key categories.

Managing Domains and Forests

Our approach is to 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. Coverage of the following key areas is assured:

- 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

Controlling Endpoints

Endpoints often provide the initial foothold for an attacker and therefore how these are managed and controlled can be an effective layer in disrupting attackers. As part of the assessment, a review is conducted to describe how these are currently managed, what policies are applied to endpoints and how local access is logged. Key areas covered by this assessment are:

- Patching 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

User Access Controls

Users need access to network assets, however, the access rights should not be overly permissive. This area of the assessment provides an examination of user permissions, explicit and implicit group membership and local administrative controls. Additional key areas of investigation include:

- User access rights and privileges
- Group Memberships
- Delegated Administrative Rights
- Local Administrative Controls
- Kerberos
- DACLs/ACEs

Attackers Toolbox

In addition, analysis of how an attacker can enumerate the directory and identify privilege escalation routes is included as part of the assessment. Key areas that are covered include:

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

Deliverables and Outputs

The report will be both strategic and tactical in nature, presented in a drill down format that will be highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.