Securing AD DS

Eli Chang

MSSA Cohort #2

Lab Summary 7

3/14/2020

Securing AD DS

The security team in the company found some possible security issues on AD DS. The administrators should improve security and monitor authentication against the enterprise AD DS domain. They should enforce it for all user accounts and password policies. The admins also deploy and configure RODCs to support AD DS authentication; they evaluate gMSA usage for the test server. The maximum password age is 60 days for all users and 30 days for IT administrators, and the minimum is one day for both groups. The length should be eight characters for all users and ten characters in IT admins.

Security Risks against Domain Controllers

Domain controllers contain essential resources and information that could be dangerous if security beaches compromised. There are several risks, including network security, authentication attacks, the elevation of privilege, DoS attack, operating system, operational risks, and physical security threats. Configuring security settings is essential to protect them from security threats. The security settings could be found in the address under computer configuration\policies\windows settings by setting account policies, local policies, event log configuration, restricted groups, secure system services, Windows Firewall with advanced security, public key policies and advanced auditing. In the lab, some of these options are utilized, but other options are also useful to improve the security level for the domain controllers.

Account Security Implementation

In password policies, there are ways to set password requirements by settings in enforcing password history, maximum password age, minimum password age, minimum password length, and password complexity requirements. By enabling these options, the security would improve because it is more challenging to find complicated passwords. Also, account

lockout policies could utilize for the users so that the accounts could be locked automatically after a specific number of attempts as the admins set them up. The duration, threshold, and resetting counter after could be configured as well.

Audit Authentication Implementation

Auditing is also an essential component for security so that the admins could monitor and identify any issues requiring further investigations. The account login and audit logon events sound similar terms, but AD DS/ domain controllers authenticate the accounts, whereas logon events could be used in the user's system. In the account logon event, there are four different audit settings: credential validation, Kerberos service ticket operations, other account logon events, and Kerberos authentication services.