THREAT DETECTION BYPASS TECHNIQUES IN ACTIVE DIRECTORY

Active Directory (AD) plays a critical role in modern IT environments, managing users, computers, and security policies. As a result, it has become a primary target for attackers. One of the more advanced tactics used by adversaries is bypassing threat detection mechanisms to maintain persistence and escalate privileges within the AD environment.

Below are some advanced techniques commonly used to bypass detection in Active Directory.

1. DCShadow Attacks

DCShadow is an advanced attack technique where an adversary registers a rogue domain controller (DC) within the AD environment.

This rogue DC can push changes to AD objects without being detected by conventional security monitoring tools, as the updates are processed through legitimate replication mechanisms. Detecting this attack requires advanced logging and monitoring of DC registrations and replication activities.

2. Golden Ticket Attacks

Golden Ticket attacks exploit vulnerabilities in the Kerberos authentication system by compromising the key of the KRBTGT account.

Once compromised, attackers can forge a Kerberos Ticket-Granting Ticket (TGT), granting them access to any service within AD. These tickets appear legitimate, making them difficult to detect through standard monitoring solutions.

Mitigation strategies involve frequent password changes for the KRBTGT account and monitoring TGT activity for anomalies.

3. SID History Injection

Security Identifier (SID) History Injection is a technique used to elevate privileges across domains by injecting previously used SIDs into a user's SID history attribute. This manipulation allows attackers to inherit permissions from other accounts or domains. Detecting SID history injection requires monitoring changes to SID history attributes and auditing for unusual account activities.

4. AdminSDHolder Exploitation

The AdminSDHolder object in AD is responsible for protecting privileged accounts by ensuring that specific security descriptors are applied regularly. Attackers can abuse this mechanism to apply persistent administrative rights to their account. This technique is particularly dangerous as it grants attackers continuous access, even if their original point of compromise is mitigated. Mitigating this threat requires regular audits of AdminSDHolder and monitoring for unauthorized changes to security descriptors.

5. Event Log Tampering

Event logs are essential for detecting malicious activities. However, attackers often tamper with these logs by clearing them or modifying specific entries to cover their tracks. While event log tampering can be detected through careful auditing and monitoring of log retention policies, advanced attackers may still find ways to obfuscate their activity. Enforcing secure logging practices and using centralized log collection tools can help mitigate this risk.

Understanding these advanced threat detection bypass techniques is crucial for defenders tasked with securing Active Directory environments. Organizations should focus on implementing strong monitoring, auditing, and proactive threat hunting to detect and mitigate these sophisticated attacks.