DynamicPacks Technologies SmartProfiler leverages MITRE ATT&CK Framework fo Active Directory Forests

Applying the MITRE ATT&CK Framework to your Active Directory environment can significantly enhance the security posture of your Active Directory Forest including the threats identified by ANSSI organization.

California City, California Jun 5, 2023 (Issuewire.com) - DynamicPacks Technologies

Evaluating the security and risk associated with Active Directory involves assessing the capabilities of your chosen Active Directory assessment tool to conduct a comprehensive analysis of vulnerabilities and risks. This assessment encompasses various aspects, including Lan Manager Hashes, SMB Signing, LDAP Signing, NT4Crypto, accounts with blank passwords, accounts utilizing SPNs, unauthenticated domain controllers and servers, credential caching in RODC, duplicate SPNs, unprivileged accounts with excessive permissions on OUs, non-default principal accounts with full control or write permission on critical directory objects, anonymous access to AD, and many other AD security tests.

The MITRE ATT&CK framework has gained widespread adoption across industries due to its ability to help organizations map out the tactics and techniques employed by adversaries. The MITRE ATT&CK

Matrix provides comprehensive details about attacker behavior, including tactics, techniques, and sub-techniques. It elucidates the attackers' objectives and how they intend to achieve them.

The current version of the MITRE ATT&CK framework comprises 14 tactics, 191 techniques, and 385 sub-techniques. Each technique offers specific insights into attacker operations, such as required privileges, identification of associated commands, and more.

Attackers utilize various techniques to exploit Active Directory systems. For instance, the "Network Logon Script" technique involves adversaries leveraging network logon scripts executed during logon initialization to establish persistence. These scripts can be assigned using AD or Group Policy Objects (GPOs). In the "Rogue Domain Controllers" technique, adversaries register rogue domain controllers and replicate the entire Active Directory database. The "Domain Account" technique involves attempts to create a domain account to maintain access to victim systems. Active Directory Domain Services manage domain accounts, configuring access and permissions across systems and services within the domain. Understanding these tactics and techniques enables proactive measures to safeguard your AD environment.

For instance, some accounts may possess constrained authentication delegations to domain controller services, granting the subject account the ability to elevate privileges on the domain controller. This allows the account to authenticate to a Kerberos service with the identity of a third-party user who has authenticated to that account. If such delegations are authorized for privileged resources like domain controllers, it enables account privilege elevation and compromises the entire forest.

Another MITRE technique involves attackers manipulating permissions on the AdminSDHolder object, which are periodically copied to all protected AD objects. By default, only privileged objects possess access rights to the AdminSDHolder object. This mechanism safeguards the most privileged Active Directory users and groups from accidental misconfigurations. Modifying default permissions on the AdminSDHolder object is strongly discouraged, and removing dangerous permissions is recommended to restore the object to its default state.

MITRE also explains how attackers exploit administrators who utilize weak password policies, facilitating brute force attacks. Brute force tools can instantly crack passwords with a length of seven characters. Apart from the risks associated with compromised accounts, weak password policies pose challenges in terms of regulatory compliance. It is advisable to enforce a password policy for privileged accounts, setting a minimum password length of eight characters.

SmartProfiler for Active Directory leverages the MITRE ATT&CK Framework to assess critical and high threats identified by MITRE within an Active Directory Forest. This tool is specifically developed to support both the MITRE ATT&CK and ANSSI frameworks. SmartProfiler enables comprehensive health checks, misconfiguration assessments, and security and risk evaluations for multiple Active Directory forests. With a broad range of 168 tests covering both MITRE and ANSSI frameworks, SmartProfiler provides valuable insights into the health, security, and risk posture of your Active Directory infrastructure. Notably, SmartProfiler offers a more extensive set of tests compared to MITRE and ANSSI, encompassing 168 tests across all relevant categories, while MITRE and ANSSI offer only 87 tests. Our Active Directory Experts have meticulously designed the additional 81 tests in SmartProfiler to ensure comprehensive coverage of every aspect of your Active Directory environment.

Key features of SmartProfiler include a Multi-AD Forest Assessment tool specifically designed for MSP/CSPs to conduct AD Assessments for their customers, a dashboard and Bird's eye view to display issues and status, and the ability to generate a report with impact assessments and recommended

actions for issue resolution.

Learn more about SmartProfiler for Active Directory here:

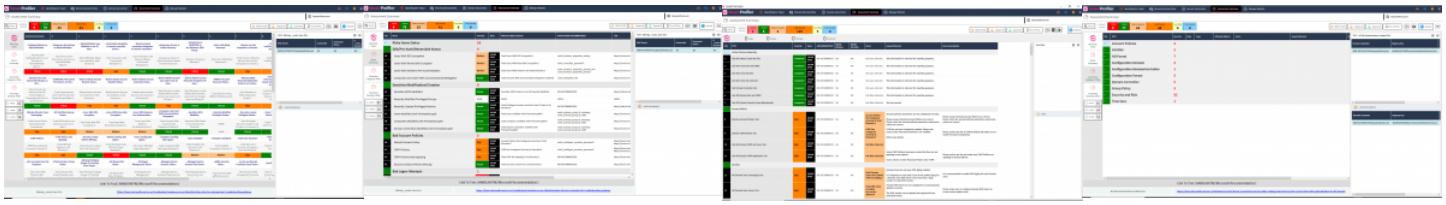
https://microsoft-assessment.com/smartprofiler-active-directory-assessment

Here are the tests executed by Smart Profiler for Active Directory:

https://microsoft-assessment.com/blog/active-directory-security-and-health-testsand-recommendations-from-vendors-2

Importance of Active Directory health and configuration checks as part of AD Security Assessment:

https://microsoft-assessment.com/blog/importance-of-health-and-configuration-checks-as-part-of-active-directory-security-assessment/



Media Contact

DynamicPacks Technologies

Host@Microsoft-Assessment.com

9739930908

A2507 Genesis Eco

Source : DynamicPacks Technologies Private Limited

See on IssueWire