Active Directory (AD) has become a primary target for attackers launching identity-centric attacks. Fortunately, there are several tools available to help enterprise security teams get clearer visibility into their AD instances and address any vulnerabilities they may find. One popular tool in use by analysts is Attack Path graphs, which can be used to show the possible paths an attacker can take to escalate privileges. Attack Path graphs are crafted to show known attacks, whereas closing vulnerabilities eliminates both these and, often, unknown vectors, too.

Consequently, Attack Paths are an incomplete representation of the actual AD security situation. Graphs showing how a potential attacker could exploit vulnerabilities can be misleading and can cloud the fact that the best way to guard against the next attack is often to fix vulnerabilities that the next attacker will exploit. Due to this, Attack Paths are best used as a decision-making tool to help prioritize vulnerabilities that can be fixed in priority order.

AD Security Assessments and Attack Paths

Let’s examine another simple Attack Path.

Case Study: Credentials Cracking

In our first example, a compromised standard user ‘Bob’ happens to be a member of a larger Engineering group, which is a subset of a CAD group. If Bob is removed from the larger Engineering group, along with all the others that may also be nested, the compromised standard user would no longer be a Domain Admin.

By following the mitigation steps and best practice recommendations of an AD security assessment tool, an administrator can eliminate the potential Attack Path of an attacker and prevent them from exploiting these misconfigurations and vulnerabilities.

Conclusion

While Attack Paths are interesting graphs that can enlighten administrators as to how potential attacks can take place on the network, they are no substitute for a proactive approach that eliminates known vulnerabilities and enforces best practices. Attack Paths are crafted to show known attacks, whereas closing vulnerabilities eliminates both these and, often, unknown vectors, too.