

TOP 5 ACTIVE DIRECTORY PENTESTING TOOLS



TCM
SECURITY

INTRODUCTION

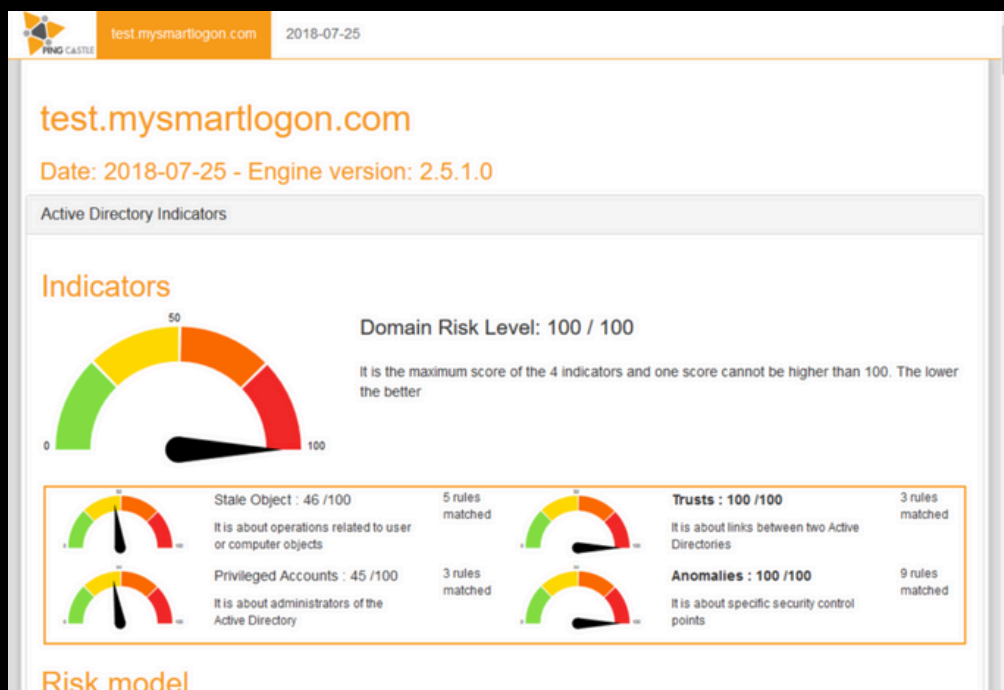
Are you on the road to becoming a penetration tester? Understanding Active Directory and how it is vulnerable to attackers is a crucial skill when it comes to infiltrating corporate networks. More than **95% of Fortune 1000 companies rely on AD** for their business environments, meaning it's a critical skill for network pentesters master. In this article, we look at some of our favorite tools for Active Directory pentesting and how you can use them.



certifications.tcm-sec.com

PINGCASTLE

PingCastle is an Active Directory scanning tool that can be used to rapidly identify AD vulnerabilities and risks. This open source tool delivers a comprehensive Health Check report that can be used to prioritize attack vectors and also delivers nice visuals that are great to include in client reports.



certifications.tcm-sec.com

IDAPDOMAINDUMP

Idapdomaindump is a Python tool used to extract and dump data from AD via LDAP. It's used for domain enumeration and reconnaissance, and can be very helpful during the early stages of an internal penetration test. It provides a clear, structured output of AD objects like users, groups, and computers without needing elevated privileges.



certifications.tcm-sec.com

BLOODHOUND

BloodHound is an open source tool that helps map out and analyze relationships and permissions within an AD environment. It's a very powerful tool that can help us discover potential paths for privilege escalation and lateral movement in an environment.

PLUMHOUND

PlumHound is usually used in combination with BloodHound to make sense of large datasets by organizing, scoring, and prioritizing attack paths. In large environments with thousands of objects, PlumHound can help security teams remediate any vulnerabilities identified by BloodHound.

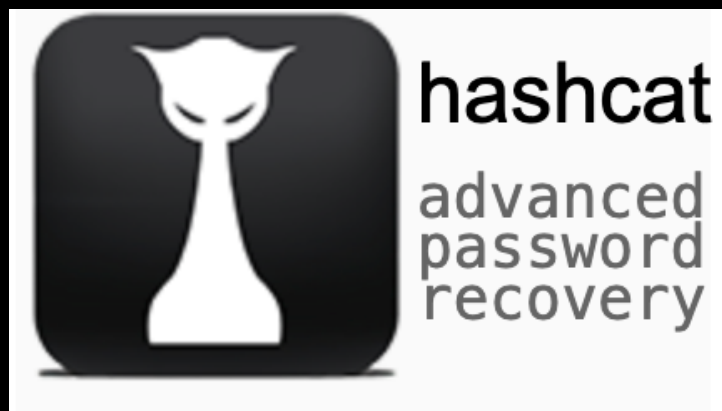


certifications.tcm-sec.com

HASHCAT

Once we obtain hashed credentials from a tool like Responder, we can use another tool to crack them.

Hashcat is a powerful password cracking tool that can take those hashes and deliver user credentials and passwords that can be used to gain access to user accounts or systems.



certifications.tcm-sec.com

WANT TO LEARN MORE ABOUT ACTIVE DIRECTORY?



Join our one day **Hacking (and Defending) Active Directory** class! Get hands-on, real world experience using these tools and prepare for a career as a penetration tester. Find out for yourself why this is our most popular live training class!



certifications.tcm-sec.com