Attacking and Defending Active Directory – Beginners Edition Bootcamp

Objective

Active Directory drives enterprises! Used by more than 90% of Fortune 1000 companies, the all-pervasive AD is the focal point for adversaries. Still, when it comes to AD security, there is a large gap of knowledge which security professionals and administrators struggle to fill.

This class is designed to help security professionals to understand, analyze and practice threats and attacks in a modern Active Directory environment. The course and the lab are based on our years of experience of making and breaking Windows and AD environments and teaching security professionals.

We cover topics like AD enumeration, trusts mapping, domain privilege escalation, domain persistence, Kerberos based attacks (Golden ticket, Silver ticket and more), ACL issues, SQL server trusts, Defenses and bypasses of defenses.

Whether you are a beginner, a red teamer or penetration tester or a blue teamer, the course has something for everyone!

Course Content:

The course is split in four modules across four weeks:

- Module 1 - Active Directory Enumeration and Local Privilege Escalation
    - Enumerate useful information like users, groups, group memberships, computers, user properties, trusts, ACLs etc. to map attack paths!
    - Learn and practice different local privilege escalation techniques on a Windows machine.
    - Hunt for local admin privileges on machines in the target domain using multiple methods.
    - Abuse enterprise applications to execute complex attack paths that involve bypassing antivirus and pivoting to different machines.

- Module 2 – Lateral Movement, Domain Privilege Escalation and Persistence
    - Learn to find credentials and sessions of high privileges domain accounts like Domain Administrators, extracting their credentials and then using credential replay attacks to escalate privileges, all of this with just using built-in protocols for pivoting.
    - Learn to extract credentials from a restricted environment where application whitelisting is enforced. Abuse derivative local admin privileges and pivot to other machines to escalate privileges to domain level.
    - Understand the classic Kerberoast and its variants to escalate privileges.

- Understand and exploit delegation issues.
- Learn how to abuse privileges of Protected Groups to escalate privileges.
- Abuse Kerberos functionality to persist with DA privileges. Forge tickets to execute attacks like Golden ticket and Silver ticket to persist.
- Subvert the authentication on the domain level with Skeleton key and custom SSP.
- Abuse the DC safe mode Administrator for persistence.
- Abuse the protection mechanism like AdminSDHolder for persistence.

- Module 3 - Domain Persistence, Dominance and Escalation to Enterprise Admins
  - Abuse minimal rights required for attacks like DCSync by modifying ACLs of domain objects.
  - Learn to modify the host security descriptors of the domain controller to persist and execute commands without needing DA privileges.
  - Learn to elevate privileges from Domain Admin of a child domain to Enterprise Admins on the forest root by abusing Trust keys and krbtgt account.
  - Execute intra-forest trust attacks to access resources across forest.
  - Abuse database links to achieve code execution across forest by just using the databases.

- Module 4 - Defenses – Monitoring, Architecture Changes, Bypassing Advanced Threat Analytics and Deception
  - Learn about useful events logged when the discussed attacks are executed.
  - Learn briefly about architecture changes required in an organization to avoid the discussed attacks. We discuss Temporal group membership, ACL Auditing, LAPS, SID Filtering, Selective Authentication, credential guard, device guard (WDAC), Protected Users Group, PAW, Tiered Administration and ESAE or Red Forest.
  - Learn how Microsoft's Advanced Threat Analytics and other similar tools detect domain attacks and the ways to avoid and bypass such tools.
  - Understand how Deception can be effective deployed as a defense mechanism in AD.

Prerequisites:

- Basic understanding of Active Directory.
- Ability to use command line tools.