Attacking and Defending Active Directory – Advanced Edition Bootcamp

Objective

If you want to improve your Active Directory and Red Team skills, this is the class for you. If you have already done our Basic bootcamp and/or cleared CRTP, this is the next level.

This advanced class is designed to help security professionals to understand, analyze and practice threats and attacks in a modern, multi-forest Active Directory environment with fully patched Server 2019 machines. The course and the lab are based on our years of experience of making and breaking Windows and AD environments and teaching security professionals.

In addition to popular TTPs, we will see how they change when we have to attack across forest trusts. We will see how to abuse or bypass modern Windows features and defenses like Advanced Threat Analytics, LAPS, JEA, RBCD, WDAC, AWL, CLM, virtualization and more.

Whether you are a red teamer or seasoned 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
    - Introduction to Active Directory
    - Introduction to Attack methodology and tradecraft
    - Domain Enumeration (Attacks and Defense)
    - Enumerating information that would be useful in attacks with leaving minimal footprint on the endpoints
    - Understand and practice what properties and information to look for when preparing attack paths to avoid detection
    - Enumerate trust relationships within and across forests to map cross trust attack paths
    - Learn and practice escalating to local administrator privileges in the domain by abusing OU Delegation, Restricted Groups, LAPS, Nested group membership and hunting for privileges using remote access protocols
    - Credential Replay Attacks

- Module 2
    - Abusing on-prem MS Exchange for privilege escalation and extracting emails and sensitive information from mailboxes

- Evading application whitelisting (WDAC)
- Domain Privilege Escalation by abusing Unconstrained Delegation. Understand how unconstrained delegation is useful in compromising multiple high privilege servers and users in AD
- Abusing Constrained Delegation for Domain Privilege Escalation by impersonating high privilege accounts
- Using ACL permissions to abuse Resource-based Constrained Delegation
- Domain Persistence Techniques

- Module 3
  - Advanced Cross Domain attacks. Learn and practice attacks that allow escalation from Domain Admins to Enterprise Admins by abusing MS Products and delegation issues.
  - Lateral movement from on-prem to Azure AD by attacking Hybrid Identity infrastructure.
  - Advanced Cross Forest attacks. Execute attacks like abuse of Kerberoast, SID Filtering misconfigurations etc. across forest trusts forests and understand the nuances of such attacks.
- Module 4
  - Abusing SQL Server for cross forest attacks
  - More on advanced Cross Forest attacks like abuse of Foreign Security Principals, ACLs etc.
  - Abusing PAM trust and shadow security principals to execute attacks against a managed forests.
  - Detections and Defenses (Red Forest, JEA, PAW, LAPS, Selective Auth, Deception, App Whitelisting, ATA, Tiered Administration)
  - Bypassing defenses like Advanced Threat Analytics, Protected Users Group, WDAC etc.

What participants will get:

- Access to online labs for one month beginning which starts with the bootcamp.
- Class spread over four live sessions of about 3 hours each on weekends.

Why this course:

The course enables you to:

- Any TTP covered in the course will be usable for years to come as it uses fully patched Server 2019 machines.
- Sharpen your AD security skills by applying them to a unique multi-forest environment.
- Understand that getting Domain Admin privileges is just the beginning of Enterprise compromise, even in Active Directory!

- Abuse or bypass modern Windows features like LAPS, JEA, RBCD, WDAC, AWL, CLM, virtualization and more.

Prerequisites:

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