Practical Active Directory

Exploitation and Investigation Training Course

This course offers a well-rounded approach to understanding, identifying and addressing common vulnerabilities present in modern Active Directory environments, as experienced by Banshie operators through decades of offensive testing and forensic examinations.

In this condensed training program, **Banshie invites** IT administrators, network engineers, network security, SOC, and internal security testing staff to explore and learn about practical offensive security testing techniques, tailored for Active Directory environments.

Participants will **gain** practical experience in various attack methods, including:

Password spraying

Kerberos delegation attacks (constrained delegation, resource-based constrained delegation, unconstrained delegation)

Credential dumping

Lateral movement

And explore contemporary means of bypassing security controls

Attendees will **learn** to identify and exploit these vulnerabilities, enabling them to discover similar issues in their own Active Directory setups, and proactively secure and mitigate these as well as explore and investigate potential past exploitation attempts.

Information and Registration

Duration: 3 day course from 9:00 to 16:00 (last day from 9:00 to 13:30)

Price: DKK 24.950,-
(See website for early bird discount)

Location: Edison Huset – Holmbladsgade 133, 2300 København S

Registration: click here

The core components of this training course:

1.Practical Attack Techniques:
Explore practical attack methodologies targeting Active Directory. Learn how attackers leverage common vulnerabilities to compromise AD environments.

2.Operationalizing Attacks:
Understand the process of operationalizing attacks against Active Directory. Gain insights into the attacker's mindset and methods to effectively simulate real-world threats.

3.Vulnerability Assessment:
Master the art of identifying, assessing and exploiting common vulnerabilities and pick the low-hanging fruits within Active Directory. Acquire skills to discover, prioritize and remediate these vulnerabilities in your organization.

4.Logging and Investigation:
Navigate through environments with varying levels of logging to investigate attacks. Learn how to interpret logs and reconstruct attack sequences for effective incident response and uncover potential gaps in your current detection and telemetry stack.

Course Providers

TRESCHOW×SON

Banshie