Offensive Security & Attack Lifecycle Workshop/LAB

Hands-On Red Team Tactics, Techniques, and Procedures (TTPs)

Target Audience:	CISOs, Security Architects, Network Engineers, Security Engineers. No hacking experience required! Some basic understanding of Windows, Active Directory, Linux and Networking is assumed.
Duration:	4-6 Hours (Hands-on Technical Lab and Workshop)
Focus Area:	Offensive Cyber Operations, Adversary Mindset, Attack Surface Exploitation
Format:	On-site workshop for max 15 attendees. (English, Swedish or Spanish).
Requirements:	Internet access. Attendees bring their own laptops. No software installation is required.

Objective

To prepare our defenses, we need to understand our adversary. We must understand the intruders' techniques, using stealthy living-off-the-land techniques for compromise, lateral movement and persistence.

This 6-hour practical workshop/lab provides security architects and network engineers with operational exposure to understand the complete Attack Kill Chain from an adversary perspective.

Practical Exercises

Attendees will operate within an isolated lab environment, systematically executing each phase of the attack Lifecycle:

- **Reconnaissance & OSINT:** Conducting initial target intelligence gathering using Open-Source Intelligence (OSINT) techniques to map infrastructure, employee footprints, and attack surfaces.
- **Initial Access & Endpoint Compromise:** Executing targeted spear-phishing scenarios and leveraging client-side vulnerability exploits to achieve initial arbitrary code execution.
- **Privilege Escalation:** Identifying local system misconfigurations and vulnerable kernel/service constructs to escalate privileges from standard user to administrative/SYSTEM levels.
- **Internal Pivoting & Lateral Movement:** Utilizing compromised endpoints as network pivots to route traffic, scan internal subnets, and move laterally across segmented trust zones.
- **Credential Harvest & Social Engineering:** Deploying social engineering vectors and credential sniffing tactics to capture high-privilege Domain Admin credentials.
- **Active Directory & Domain Controller Exploitation:** Extracting password hashes directly from the Active Directory database (NTDS.dit) on compromised Domain Controllers.
- **Pass-the-Hash & Kerberos Ticket Attacks:** Executing Pass-the-Hash (PtH) techniques and forging Kerberos Ticket Granting Tickets (Golden Tickets) for unrestricted domain authority.
- **Fileless Persistence Architecture:** Establishing covert, fileless persistence mechanisms on target hosts to maintain long-term command and control (C2) without disk-backed payloads