Cyberdefense

Training Catalogue

Knowledge is power

HA 4.01 | Windows Attack & Defense

Overview

This training will familiarize system administrators and security professionals with modern Windows attacks and best security practices, such as Windows security components, network interception, Active Directory mapping, privilege escalation, lateral movements, credentials theft and common persistence techniques. After covering a large attack overview, the course introduces associated counter-measures such as credentials protection and much more. After the workshop, members will understand how to protect their infrastructure against modern attacks. Hands-on: This class is practice-oriented, lectures present realworld attacks that participants put into practice in various labs.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

- **Comfortable with command line (Linux)**
- **Some experience with Windows environments**
- **Some experience with pentesting & hacking tools**

Level 3

2 days

French or English

Course Modules

Network access to initial account

- Windows network protocols poisoning (LLMNR, NetBIOS, DHCPv6)
- Initial network discovery (nmap port scan)

Active Directory mapping

- Active directory enumeration (Bloodhound, PingCastle)
- Kerberos authentication
- Common domain password extraction techniques (GPP passwords, Kerberoast, ASREPRoast)

Lateral movement

- Kerberos delegation (Unconstrained, constrained, ressource-based)
- NTLM authentication and cross-protocol relay attacks
- Ways to coerce a machine account NTLM authentication and abuse it (Printer Bug, PetitPotam, ntlmrelayx)

Windows credentials dumping

- Windows credentials storage (SAM, LSA secrets, LSASS, etc.)

Getting access to a key asset

- From RDP access to administrator
- Abusing impersonation privileges in Windows services

Domain compromise and persistence

- Domain credentials storage
- Kerberos Silver/Golden tickets

Bonus

- Physical device security (BitLocker and known attacks)
- LSA protection (how it works and how it can be bypassed)
- Credential Guard (how it works and how it can be bypassed)