Training sheet
Security for an internal network based on Active Directory

CONTACT FOR THIS TRAINING

Miora RAHARINIRINA
Almond Institute coordinator
almond.institute@almond.eu
07 64 42 71 56

- Version 1.0
- 08/12/2023

Security for an internal network based on Active Directory

Course overview

The aim of this training course is to learn and understand the most common techniques used to compromise an Active Directory environment, their causes, and how to remedy them. The course simulates an internal penetration test, from connecting the workstation without a valid domain account, to the total compromise of the forest by obtaining the company's administrator privileges. Several techniques will be presented and explained for each stage of this compromise, with most participants putting the attacks into practice.

01. **Know the main vulnerabilities** associated with internal networks based on Active Directory

02. **Detecting the presence** of faults

03. **Acquire good** administration security **practices**

Security for an internal network based on Active Directory

Useful informations

Who should attend?

- Team of system and network administrators
- Information systems security team
- User support team

Entry requirements

- Computer basics: Networking (protocols, OSI model, etc.), Active Directory environment and Windows operating system

Method of assessment

Course validation through practical exercises. Completion of a final online questionnaire covering all the concepts learned.

How and when to access

The participant is considered registered when:

- The prerequisites and needs are identified and validated
- The training agreement is signed

Registration requests can be sent up to 10 working days before the start of the training.

Accessibilité

Que vous soyez reconnu en situation de handicap ou pas, rendre notre formation accessible à toutes et à tous fait partie de notre engagement.

Si vous avez besoin d'une compensation ou adaptation pour le contenu, les supports, le « lieu », le matériel utilisé, les horaires, le rythme, **nous sommes à votre écoute.**

Security for an internal network based on Active Directory

Face-to-face and distance learning

Course curriculum

Day 1	Day 2	Day 3
→ **Introduction: why target Active Directory** → **Authentication protocols (NTLM and Kerberos)** → **Main application protocols (LDAP, SMB and RDP)** → **Obtaining a first domain account** ▪ Techniques : Obtain an NTLM response with network poisoning: ARP, DHCPv4/v6, LLMNR, NBT-NS, mDNS / Break or relay this NTLM response / Get a list of users (via relay, NULL sessions, Kerbrute), to set up password spraying or ASREPRoasting. / Network enumerations: web applications and network services ▪ Tools: Responder / Impacket / Bettercap / Mitm6 / Kerbrute / Wireshark ▪ Additional access via a domain account	→ **Obtain local administrator rights on machines** ▪ Techniques : NTLM to LDAP authentication relays (RBCD, Shadow Credentials), ADCS and SMB / Kerberoast / Local elevation of privileges (PrivescCheck) / Downgrade NTLMv1 / Update faults (PrintNightmare, MS17-010) / Unencrypted disk on user workstation ▪ Tools : BloodHound / Pingcastle /Impacket / PrivescCheck ▪ Additional access with local administrator access	→ **Raising domain privileges** ▪ Techniques : Lateral movements (WMI, SMB, WinRM) / Administrator sessions open on machines / Extraction of passwords from service accounts and scheduled tasks / Extraction of cached password fingerprints / Kerberos delegations / ADCS certificate templates / Update defaults (ZeroLogon, SamAccountName Spoofing, Certifried) / Intra-forest privilege elevation: child domain to parent domain ▪ Tools : Rubeus / Impacket / Certipy / → **Attacking approval relationships** ▪ Techniques : SID Filtering / TGT Delegation / Password reuse / Inter-forest accounts in administration groups

Training benefits

- → Training provided by an Active Directory security expert who has carried out numerous internal intrusion tests.
- → Practical exercises carried out by participants themselves.

Price and informations

- → **Duration:** 3 days
- → **Price:** 2750€ excl. tax.
- → **Financing:** OPCO support