INFOSECTRAIN

ACTIVE DIRECTORY PENTEST

COURSE CONTENT

sales@infosectrain.com | www.infosectrain.com

Course Content

1. Course Introduction and Overview
2. Active Directory Overview
3. Physical, Logical Active Directory Components
4. Building Active Directory Lab
5. Attacking Active Directory
6. Post-Compromise Enumeration
7. Post-Compromise Attacks
8. Post Exploitation

ACTIVE DIRECTORY PENTEST

- Course Introduction and Overview
- Active Directory Overview
- Physical, Logical Active Directory Components
- Building Active Directory Lab

Attacking Active Directory

- Introduction
- LLMNR Poisoning Overview
- Capturing NTLMv2 Hashes with Responder
- Password Cracking with Hashcat
- LLMNR Poisoning Defenses
- SMB Relay Attacks Overview
- Quick Lab Update
- Discovering Hosts with SMB Signing
- SMB Relay Attack Demonstration
- SMB Relay Attack Defenses
- Gaining Shell Access

Post-Compromise Enumeration

- Introduction
- PowerView Overview
- Domain Enumeration with PowerView
- Bloodhound Overview and Setup
- Grabbing Data with Invoke-Bloodhound
- Enumerating Domain Data with Bloodhound

Post-Compromise Attacks

- Introduction
- Pass the Hash / Password Overview
- Installing crackmapexec
- Pass the Password Attacks

- Dumping Hashes with secretsdump.py
- Cracking NTLM Hashes with Hashcat
- Pass the Hash Attacks
- Pass Attack Mitigations
- Token Impersonation Overview
- Token Impersonation with Incognito
- Token Impersonation Mitigation
- Kerberoasting Overview
- Kerberoasting Walkthrough
- Kerberoasting Mitigation
- GPP / cPassword Attacks Overview
- Abusing GPP: Part 1
- Abusing GPP: Part 2
- Mimikatz Overview
- Credential Dumping with Mimikatz
- Golden Ticket Attacks

Post Exploitation

- Introduction
- File Transfers Review
- Maintaining Access Overview
- Pivoting Lab Setup
- Pivoting Walkthrough
- Cleaning Up

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com