FORENSICS INTRODUCTION

Forensics Introduction 14 hours of content | 50 hours of practice | Final Project

1. Introduction to Windows Server Environments

- What is virtualization?
- Installing a virtual environment with VBox
- Defining networks in virtualization
- Creating a virtual machine
- Installing Windows Server 2016
- What is a Domain Controller?
- Initial configuration for a DC
- Installing AD DS on a DC
- Installing a Windows 10 client
- Connecting a client to a domain
- Managing and defining GPO
- Creating and managing groups
- Creating and managing users in a domain
- DNS Record Types
- DNS Zones
- Backup policies
- Defining shared folders
- Installing DHCP service
- What is the DHCP service?

2. Data and File Storage

- Memory management methods
- Types of memory
- Methods of file storage in the system
- File deletion process
- Files and their uses
- File signatures (Fingerprints)
- File permissions and uses

3. ProDiscover - Windows

- NAT
- SYSLOG
- SSH
- Attacks on files
- Attacks on network services
- Using Access Lists
- Working with Port Security
- How to secure the network

4. AutoPsy - Linux

- Kali Linux Forensics
- Opening a project and case files
- Extracting data from images
- AutoPsy definitions
- AutoPsy results
- Generating a forensic report
- Practice lab

5. Memory Forensics - Volatility

- Volatility Intro
- Volatility over Windows
- Volatility over Linux
- Memory analysis
- Practice lab

6. Forensics Capabilities

- Email analysis
- File tracking
- Printer forensics
- WiFi profile extraction
- WiFi signal extraction
- Printer signal extraction
- Identifying suspicious files
- Practice lab

7. Sysinternals Suite

- Autorun
- Process Monitor
- ProcDump
- PsServices
- RamMap
- RegDelNull
- TCPView
- ProcMon
- PsLoggedOn
- PsList

8. OSINT (Open Source Intelligence)

- Maltego
- Shodan
- Google Dorks
- The Harvester
- Whois
- Open Source tools for OSINT