



14 שעות תוכן

88 שיעורים

50 שעות מעבדה

מעבדות תירגול

Forensics

Introduction

2. אחסון מידע וקבצים

- אופן ניהול הזיכרון.
- סוגי זכרונות.
- אופן איחסון הקבצים במערכת.
- תהליך מחיקת קבצים.
- קבצים ושימושים.
- חתימות קבצים (Fingerprints).
- הרשאות קבצים ושימושים.

3. ProDiscover - Windows

- NAT
- SYSLOG
- SSH
- התקפות על מתגים.
- התקפות על שירותי רשת.
- שימוש ב Access List.
- עבודה עם Port Security.
- כיצד לאבטח את הרשת.

4. AutoPsy - Linux

- Kali Linux Forensics
- פתיחת פרוייקט וקבצי Case
- חילוץ מידע מתמונות
- הגדרות AutoPsy
- תצוגת AutoPsy
- הוצאת דו"ח פורנזי
- מעבדת תירגול

1. מבוא לסביבות ווינדוס אירגוניות

- מהי וירטואליזציה.
- התקנת סביבת וירטואליזציה VBox.
- הגדרות תקשורת בוירטואליזציה.
- יצירת מכונה וירטואלית.
- התקנת Server Windows 2016
- מהו Domain Controller.
- הגדרות מקדימות ל- DC
- התקנת AD DS על DC.
- התקנת קליינט Windows 10.
- צירוף קליינט לדומיין.
- ניהול הגבלות ו GPO
- יצירה וניהול של קבוצות.
- יצירה וניהול של משתמשים בדומיין
- DNS Record Types
- DNS Zones
- שימור כתובות
- הגדרת טווחי כתובות
- התקנת שירותי DHCP
- מהו שירותי DHCP

5. חקירת זיכרון Volatility

- Volatility Intro
- Volatility over Windows
- Volatility over Linux
- ניתוח זיכרון
- מעבדות תירגול

Sysinternals Suite .7

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

Forensics Capabilities .6

- ניתוח מיילים (Email Analysis)
- מעקב קבצים
- פורנזיקה על דפדפנים
- חשיפת פרופילי WiFi
- חילוץ סיסמאות WiFi
- חילוץ סיסמאות מדפדפנים
- אימות קבצים זדוניים
- מעבדות תירגול

OSINT .8

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

AFE
Security Trainings

CERTIFICATE
OF APPRECIATION

IS PRESENTED TO

Amir Shweika

This certificate of completion is given to you for your outstanding
achievement of the Forensics introduction course
which consists of 14 Hours of Content and 50 Hours of practice.

19/2021
DATE


SIGNATURE
Amir Bar-El
CEO

