Cybersecurity Fundamentals & Ethical Hacking

კურსის ხანგრძლივობა: 19 ლექცია, 38 საათი.

კურსის მიზანი: პროგრამის მიზანია, მონაწილეები მოამზადოს კომპიუტერული უსაფრთხოების სფეროში მუშაობისთვის, მათ შორის ეთიკური ჰაკინგის დარგში. კურსი უზრუნველყოფს როგორც თეორიულ, ისე პრაქტიკულ ცოდნას, რომელიც დაეხმარება მონაწილეებს შეიძინონ უნარები და ცოდნა მოწყვლადობების გამოვლენაში, მათ ექსპლოატაციაში და უსაფრთხოების გეგმარებაში. პროგრამა ყურადღებას ამახვილებს არა მხოლოდ ტექნიკურ უნარებზე, არამედ იმაზე, რომ მონაწილე იყოს მზად იაზროვნოს როგორც ეთიკურმა ჰაკერმა. ეს გულისხმობს, უსაფრთხოების გამოწვევებზე მეტყველების და სისტემის უსაფრთხოების, ჰაკერის თვალით დანახვის უნარის განვითარებას.

აუცილებელი მოთხოვნები: პროგრამის დაწყებისთვის წინასწარი ცოდნა არ არის აუცილებელი, თუმცა სასურველია, მონაწილეს ქონდეს ზოგადი გაგება IT ინფრასტრუქტურის და მონაცემთა უსაფრთხოების შესახებ. განსაკუთრებით მნიშვნელოვანია ეთიკური ჰაკინგის პრაქტიკისა და უსაფრთხოების საკითხებში მუშაობისადმი სურვილი და ინტერესი.

კურსის შედეგები: კურსის დასრულების შემდეგ, მონაწილეები შეძლებენ, რომ მიღებული ცოდნით დამოუკიდებლად განახორციელონ შეტევები და აღმოაჩინონ მოწყვლადობები, ასევე, მოახდინონ უსაფრთხოების შეფასებები და შეიმუშავონ უსაფრთხოების სტრატეგიები. ეს კურსი არა მხოლოდ მათი ტექნიკური უნარების გაძლიერებას უზრუნველყოფს, არამედ მყარ საფუძველს უქმნის მათ, მომავალი კარიერული წინსვლისთვის.

შეხვედრა 1 - COURSE INTRODUCTION & CYBERSECURITY BASICS

- Understanding Cybersecurity & Ethical Hacking
- Web Application Security Overview (OWASP Top 10)
- Legal & Ethical Considerations

შეხვედრა 2 - KALI LINUX BASICS

- Installing & Configuring Kali Linux
- Linux Commands for Penetration Testing
- Networking, File System, and Permissions

შეხვედრა 3 - OPEN-SOURCE INTELLIGENCE (OSINT)

- What is OSINT & How It's Used in Cybersecurity
- Finding Publicly Available Information (Google Dorking, Social Media)
- Hands-on: Using OSINT Tools

შეხვედრა 4 - PHISHING OVERVIEW & PHISHING ATTACKS

- Understanding & Exploiting Phishing Attacks
- Creating and Simulating Phishing Attacks

- Mitigating Phishing Attacks

შეხვედრა 5 - BURP SUITE BASICS

- Setting Up Burp Suite for Web Security Testing
- Intercepting & Modifying HTTP Requests
- Using Burp Suite Tools

შეხვედრა 6 - WIRELESS PENETRATION TESTING

- Introduction to Wireless Security & Encryption (WEP, WPA, WPA2)
- Cracking Wi-Fi Networks
- Rogue Access Points & Evil Twin Attacks

შეხვედრა 7 - VULNERABILITY SCANNING & EXPLOITATION

- Introduction to Vulnerability Scanning
- Automated vs. Manual Vulnerability Discovery
- Exploiting Vulnerabilities Using Metasploit

შეხვედრა 8 - INTRODUCTION TO WEB APPLICATION ATTACK TYPES

- Overview of Common Web Attacks (SQLi, XSS, CSRF, etc.)
- How Web Vulnerabilities Are Exploited
- OWASP Top 10 & Industry Trends

შეხვედრა 9 - INFORMATION DISCLOSURE

- Leaking Sensitive Data via Headers, Comments, and APIs
- Directory Listing & Backup File Exposure
- Secure Data Handling

შეხვედრა 10 - CROSS-SITE SCRIPTING (XSS) & CSRF

- Understanding XSS (Reflected, Stored, DOM-based)
- Exploiting XSS
- Understanding CSRF & Exploiting CSRF Vulnerabilities
- Mitigating XSS & CSRF
- DOM Manipulation & DOM XSS

შეხვედრა 11 - SQL INJECTION (SQLI)

- Understanding SQL Injection Types (Error-Based, Blind, Time-Based)
- Exploiting SQLi with Burp Suite
- Bypassing Authentication & Extracting Data
- SQL Injection Prevention

შეხვედრა 12 - CLICKJACKING ATTACKS

- Understanding Clickjacking and its Impact
- Exploiting Clickjacking with HTML & CSS
- Clickjacking Prevention Techniques

შეხვედრა 13 - SERVER-SIDE REQUEST FORGERY (SSRF)

- Understanding SSRF and Common Exploits
- SSRF in Cloud & Internal Network Attacks

- Preventing SSRF

შეხვედრა 14 - PATH TRAVERSAL ATTACKS

- Exploiting Path Traversal to Access Restricted Files
- Directory Traversal Attacks & Bypasses
- Preventing Path Traversal Attacks

შეხვედრა 15 - ACCESS CONTROL VULNERABILITIES

- Exploiting Broken Access Controls
- Privilege Escalation (Horizontal & Vertical)
- Secure Access Control Best Practices

შეხვედრა 16 - FILE UPLOAD VULNERABILITIES

- Unrestricted File Upload & Remote Code Execution
- Bypassing File Upload Restrictions
- Securing File Uploads

შეხვედრა 17 - JWT (JSON WEB TOKEN) ATTACKS

- Understanding JWT Authentication
- JWT Signature Forgery & Token Manipulation
- Securing JWT Implementations

შეხვედრა 18 - FINAL EXAM (CTF CHALLENGE)

- Practical CTF Lab: Exploiting a Web Application
- Identifying & Reporting Vulnerabilities
- Securing the Application from Attacks

შეხვედრა 19 - CAREER ADVICE & NEXT STEPS

- Final Exam Overview
- Career Paths in Cybersecurity (Penetration Testing, SOC Analyst, Bug Bounty)
- Building a Cybersecurity Portfolio (Write-ups, GitHub, LinkedIn)
- Networking & Finding Job Opportunities