HACKERU

Offensive Security Ethical Hacking

CB109

05
Days

Offensive Security Ethical Hacking

Outline

This course delves into the minds of criminal hackers to give students a sense of how black hat hackers think, what their intentions are, and what they do to implement their intentions. Students will learn how to execute and defend against social engineering attacks, network attacks, application attacks, and cryptographic attacks. Hands-on labs provide students with methods, tools, knowledge, and skills to discover and exploit system vulnerabilities. This course constitutes additional preparation for the CompTIA Security+, C|EH, and CySA+ certification exams.

Target Audience

The course is suitable for system administrators, network administrators and engineers, web developers, and security professionals. Any other cyber professional with a desire to study the subject of information security can participate in the course as well. In addition, it is ideal for blue team candidates who want to understand how malicious cyber attackers think.

Prerequisites

Before attending this course, students must have the following technical knowledge:

- Background in security or information systems.
- Knowledge of TCP/IP and experience with networking.
- Knowledge of operating systems (Linux and Windows).

Objectives

Upon course completion, participants will be able to:

- Understand security terms in depth.
- Understand attack vectors for common network services, and their mitigation.
- Have an awareness of how hackers use social engineering to hack systems.
- Understand policies and procedures that can be implemented to proactively deal with known strategies.

Content

Day 1

Module 01

Introduction to Ethical Hacking

- Fundamentals
- Ethics
- Malware
- Cyber Attack Cycle

Day 1

Module 02

Network Scanning

- Network Scanning Definition
- Nmap Overview
- Nmap Scanning Types
- Additional Tools

Day 1

Module 03

MITM Attacks

- MITM
- ARP Poisoning
- DNS Poisoning
- Port Stealing
- SSL Stripping

Day 2

Module 04

Brute-Force

- Fundamentals
- Offline Password Cracking
- Online Password Attacks

Day 2

Module 05

Social Engineering

- Introduction
- Social Engineering Toolkit
- SE Additional Tools

Day 3

Module 06

Infrastructure Attacks

- Metasploit
- Reverse Shell
- Lateral Movement

Day 3

Module 07

Windows Privilege Escalation

- Windows Privileges
- Windows Local PE
- Post Exploitation

Day 3

Module 08

Linux Privilege Escalation

- Linux Local PE
- Linux Remote PE

Day 4

Module 09

Web Application Security Fundamentals

- Understanding HTTP
- Burp Suite

Day 4

Module 10

XSS & File Inclusion

- Client-Side Web languages
- Cross-Site Scripting
- Session Hijacking
- XSS Mitigations
- Local File Inclusion

Day 5

Module 11

SQL Injection

- Introduction to Databases
- SQLi

Day 5

Module 12

Vulnerability Scanners & Reporting

- Automated Scanning
- Vulnerability Scanners
- PT Report Subjects
- Regulations

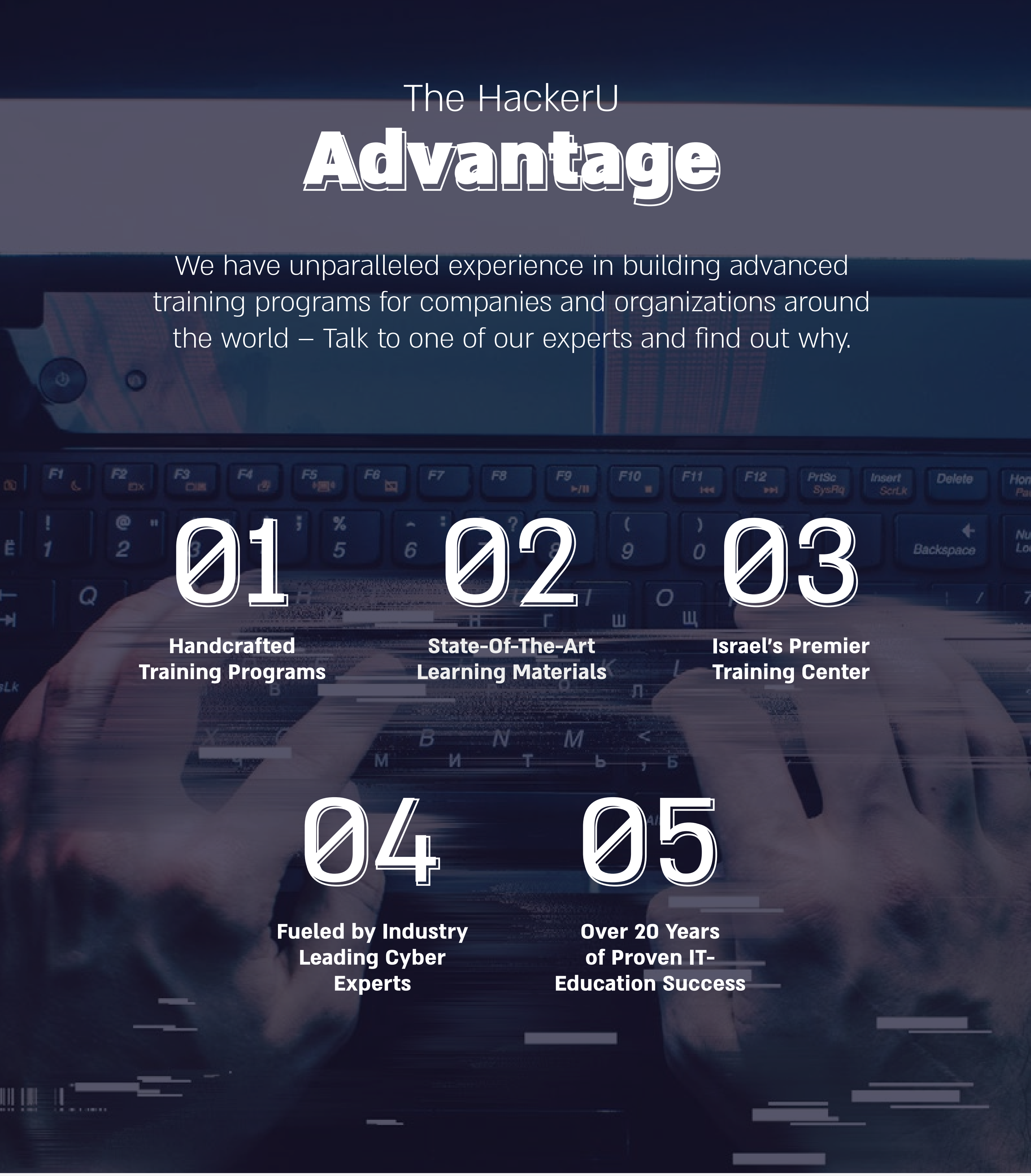
Day 5

Module 13

Final Project

- Final Project Scenarios

> **Execute and defend** against social engineering attacks, network attacks, application attacks, and cryptographic attacks"



The HackerU

Advantage

We have unparalleled experience in building advanced training programs for companies and organizations around the world – Talk to one of our experts and find out why.

01

Handcrafted Training Programs

02

State-Of-The-Art Learning Materials

03

Israel's Premier Training Center

04

Fueled by Industry Leading Cyber Experts

05

Over 20 Years of Proven IT-Education Success

Info@hackerupro.com

www.hackerupro.com