HACKERU

Advanced Infrastructure Attacks

CR109

05
Days

Advanced Infrastructure Attacks

Outline

IT and security teams are responsible for meeting cyber challenges that involve the technical layer of the organization. This course is designed to help such teams build and maintain secure networks and systems, protect data, implement vulnerability management programs, initiate strong access control measures, regularly monitor and test networks, and maintain consistent information security policies. This course also introduces various attack vectors that can be used by pen testers to breach internal systems.

Target Audience

This course was designed for:

- Personnel with IT background, skill, and experience, and high-level knowledge of both Linux and Windows operating systems.
- Personnel with knowledge of information security, computer networking & common protocols.
- Personnel with an understanding of security-related terms.

Prerequisites

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

- Basic knowledge of the Linux OS.
- Basic knowledge of the Windows OS.
- Basic knowledge of networking.

Objectives

Upon completing this course, graduates will be able to:

- Enumerate an organization.
- Perform lateral movement in a network.
- Gather information about an organization via LDAP.
- Bypass security measures.
- Collect users and passwords over a network.
- Exploit common protocols.
- Use PowerShell as a weapon.

Content

Day 1 **Module 01**
Enumerating an Organization

- Windows domain environment
- Domain enumeration techniques
- Manual enumeration
- Automatic enumeration

Day 1 **Module 02**
Lateral Movement

- Manual Lateral Movement
- PsExec
- WMI
- WinRM
- Pass the Hash

Day 2 **Module 03**
SMB Relay & Responder

- Broadcasting
- LLMNR Manipulation
- Hash Evolution
- Responder
- SMB Relay
- Inveigh

Day 2 **Module 04**
PowerShell as a Weapon

- PowerShell Fundamentals
- PowerShell ISE
- PowerShell Modules
- Attack with PowerShell
- PowerShell to EXE

"**build and maintain** secure networks and systems, **protect data** and implement vulnerability management programs"

Day 3

Module 05
Office Exploitation

- Macro & VBA
- Word Exploitation
- Excel as a weapon
- PowerPoint exploit
- Macro Obfuscation
- SFX
- Social Engineering technique

Day 3

Module 06
Exploiting Services

- Basic Enumeration
- Vulnerability search
- Services features
- SearchSploit
- Misconfiguration bugs
- RDP Enumeration

Day 4

Module 07
Veil Framework & Obfuscation

- What is obfuscation?
- Types of obfuscation
- Packing
- Various tools
- Tools comparison
- Multi-layered obfuscation

Day 4

Module 08
Reverse Shell & Tunneling

- Shell
- Reverse Shell
- Remote connections
- Firewall Evasion
- ICMP Tunneling
- SSH Tunneling
- DNS Tunneling

Day 5

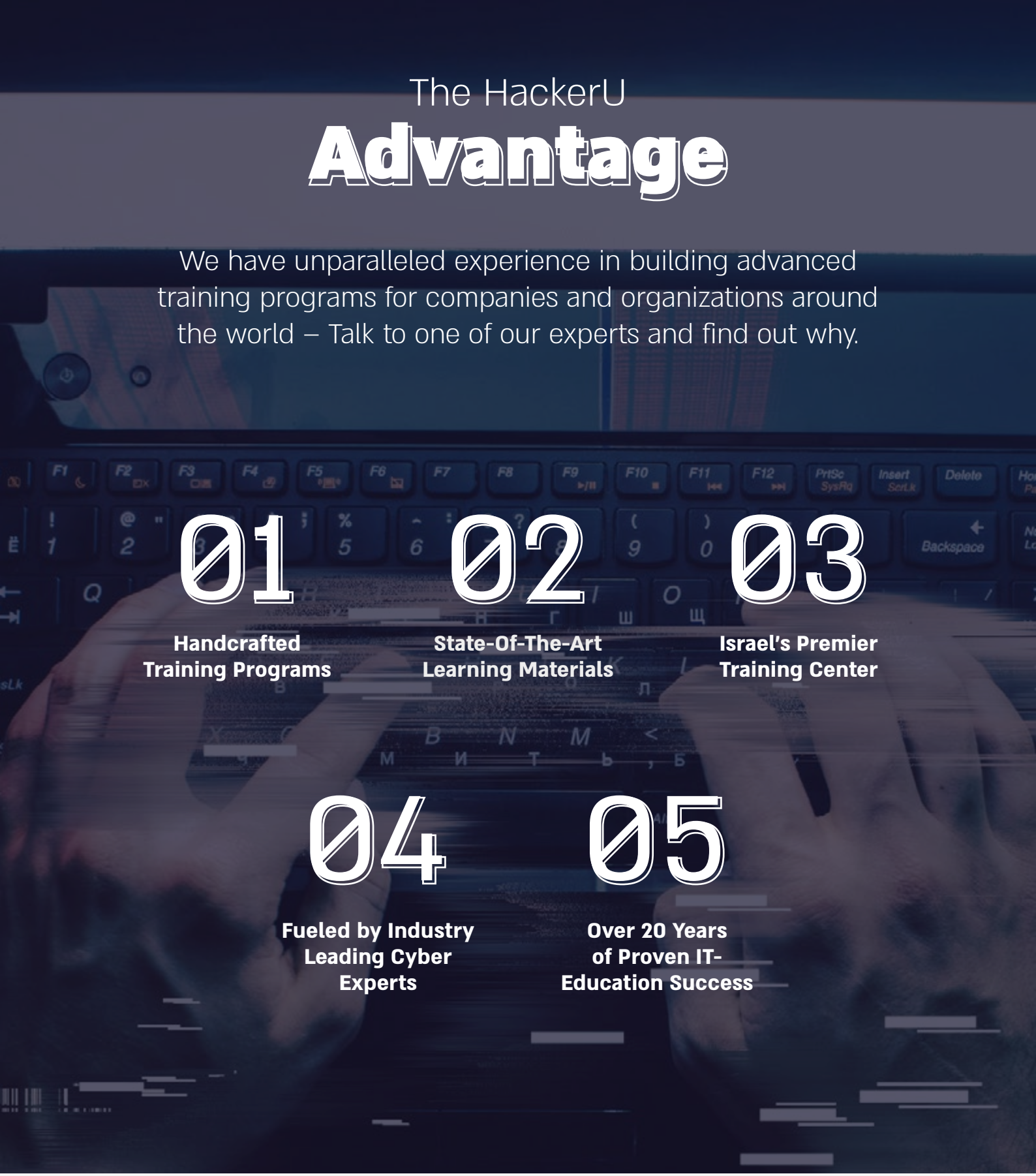
Module 09
Kerberoasting & Pass the Ticket

- Kerberos Authentication
- Kerberos Traffic Analysis
- Kerberoasting
- Pass the Ticket
- Golden Ticket
- Domain Replications

Day 5

Module 10
Challenge

- The students will receive a challenge and will try to hack according to the learning material to the targeted machine/services.



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

hackerupro.com