Summer Infrastructure Pentesting Bootcamp

CQURE

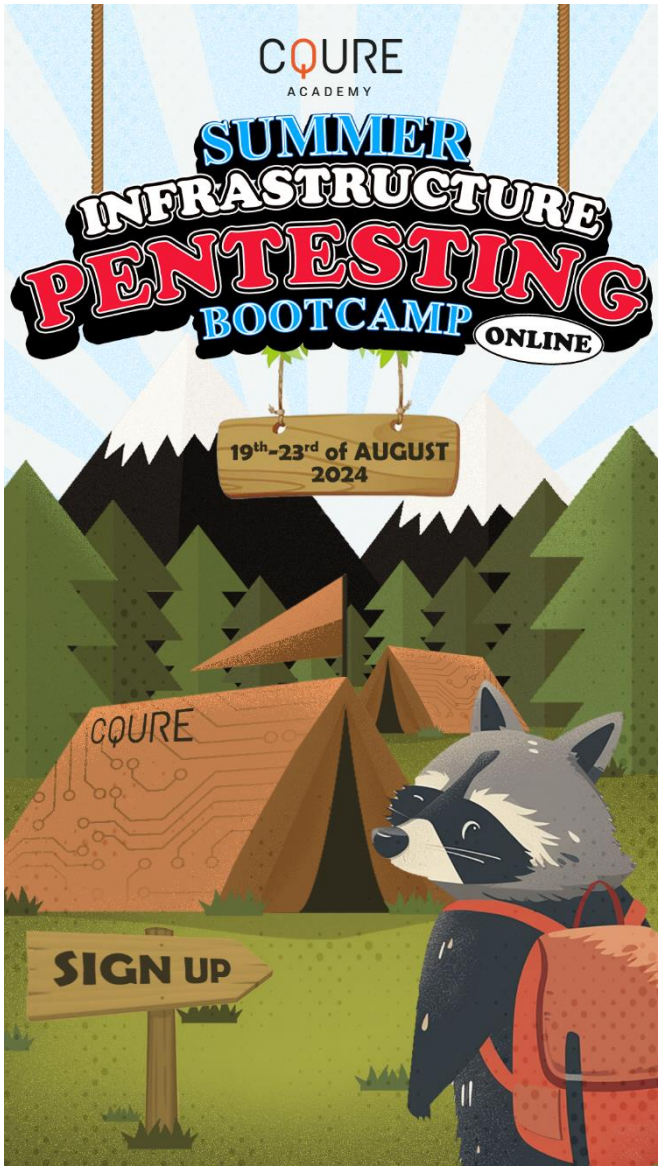
Warsaw New York Dubai Zug

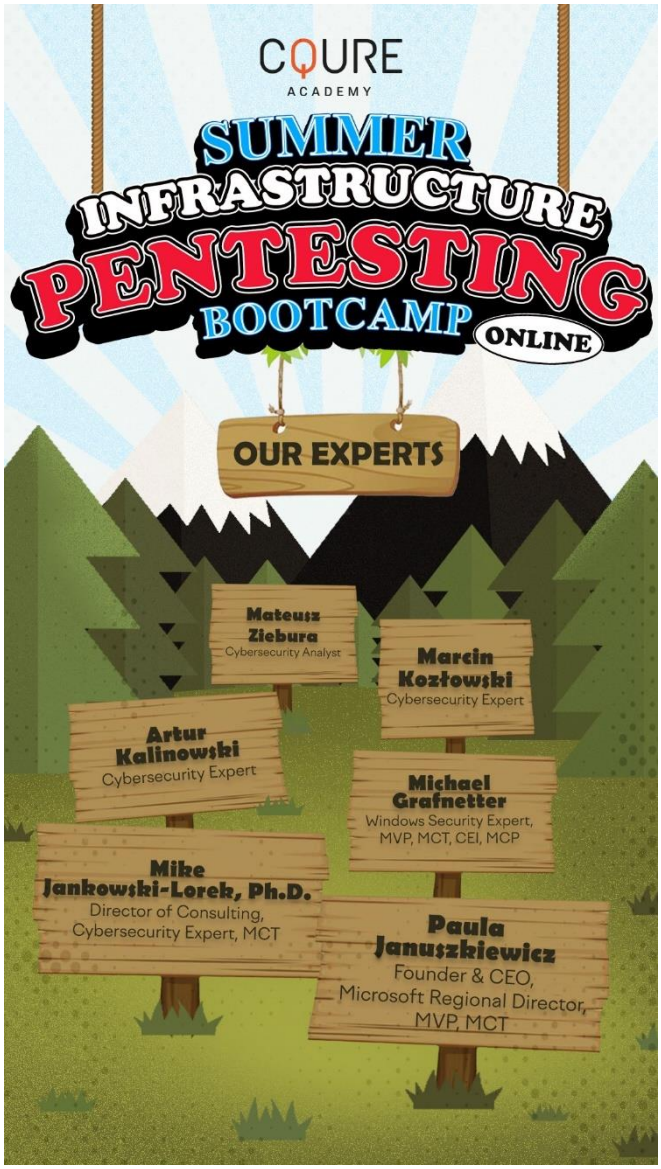
info@cqure.pl

www.cqure.pl
www.cqureacademy.com

What is Summer Infrastructure Pentesting Bootcamp

The Summer Infrastructure Pentesting Bootcamp is an intensive, five-day training program running from August 19th to August 23rd, 2024, designed for cybersecurity professionals, IT professionals and IT geeks. This hands-on course, offering 7.5 hours of daily training, focuses on advanced techniques in network defense, vulnerability hunting, and exploitation, specifically targeting Active Directory and Windows services. Ideal for penetration testers, security analysts, and IT administrators, the bootcamp provides practical experience with the latest cybersecurity tools and methodologies, ensuring participants can effectively enhance organizational security against sophisticated cyber threats.





Who is it for

Penetration Tester: Experienced in performing authorized simulated attacks to identify vulnerabilities and seeking to deepen your skills in advanced network and system exploitation.

Security Analyst: Responsible for monitoring, analyzing, and defending against security threats and looking to enhance your ability to identify and mitigate complex vulnerabilities.

IT Professional: Managing and securing IT infrastructure, eager to learn cutting-edge techniques to protect your organization's assets from sophisticated cyber attacks.

Cybersecurity Professional: Focused on safeguarding organizational data and systems, aiming to stay ahead of the latest threats and improve your defensive strategies.

Geeks with an IT Background: Excited to start an adventure in the cybersecurity pentesting field, ready to dive deep into hands-on learning and practical application of advanced pentesting techniques.

Key takeaways

In-depth knowledge of reconnaissance and enumeration: You'll will learn how to map and analyze networks to spot vulnerabilities and potential entry points.

Advanced skills in vulnerability & threat hunting: Gain expertise in using cutting-edge tools and techniques to find, understand, and exploit system weaknesses.

Mastery of Active Directory (AD) and Azure Entra ID exploitation: Discover sophisticated attack and defense tactics for identity based attacks.

Proficiency in advanced Windows services attacks: Learn how to exploit and defend against attacks on critical Windows services and infrastructure.

Expertise in enterprise exploitation and post-exploitation techniques:Understand how to exploit key enterprise services and maintain persistence within compromised networks.

Practical experience with the latest cybersecurity tools and methodologies Hands-on training with various tools, ready for real-world application.

Agenda

DAY 1: Mastering Reconnaissance and Enumeration

Module 1. Reconnaissance Techniques

a) Review of goals for testing
b) Mastering scanning tools
c) Attacking password authentication
d) Executing initial access techniques
e) Network traffic sniffing and analysis
f) Covert channel delivery and exfiltration

Module 2: Operating system oriented environment enumeration

a) Understanding Windows & Linux network architecture
b) Enumerating Windows domains and workstations
c) Identifying high value targets (users, admins, devices etc.)
d) Identifying roles of different machines (Domain Controllers, File Servers, etc.)
e) Utilizing Nmap for operating system-specific scans
f) Accessing sensitive data

Daily Summary: Discussing possible points of entry and mitigation strategies.

DAY 2: Mastering Hunting for Vulnerabilities

Module 3: Hunting for Vulnerabilities

a) Discovering live systems
b) Getting information from open ports
c) Misusing typical services NetBIOS, SMB, and other
d) Metasploit and other tools
e) Automation techniques
f) Mastering Powershell / Powersploit
g) Manipulating SMB, RDP, and other protocols for control and data exfiltration

Daily Summary: Discussing vulnerability management and possible mitigations.

DAY 3: Mastering identity attacks and protocol flows

Module 4: Attacks on NTLM: Execution and Mitigations

a) Understanding and exploiting NTLM
b) Pass-The-Hash
c) Over-Pass-The-Hash
d) NTLM relay
e) NTLM attacks detections
f) Hardening NTLM authentication

Module 5: Attacks on Kerberos authentication: Execution and Mitigations

a) Understanding and exploiting Kerberos
b) Core concepts (tickets, keys, SPN)
c) Authentication flow
d) PKIinit
e) Refreshing PAC
f) Authentication Monitoring

Module 6: Attacks against Kerberos tickets: Execution and Mitigations

a) Pass-The-Ticket
b) Silver ticket
c) Golden ticket
d) Keberoasting

Daily Summary: Discussing identity protection techniques.

DAY 4: Advanced attacks on Active Directory and Entra ID

Module 7: Advanced AD Attacks: Execution and Mitigations

a) DCSync
b) DCShadow
c) NGC/shadow credentials
d) Advanced persistence techniques
e) Skeleton Key
f) Windows Hello for Business Security,
g) AdminSDholder
h) Offline access attacks
i) Decrypting secrets with DPAPI and DPAPI-NG
j) Attacks against smart card authentication

Module 8: Azure and Entra ID pivoting

a) Cloud enumeration
b) On-prem to cloud pivoting
c) Cloud to on-prem pivoting
d) Entra ID security review
e) Stealing Entra ID tokens
f) Entra ID MFA and FIDO2 auditing
g) Entra ID application security
h) Catching signs of attack on-prem and in the Cloud

Daily Summary: Discussing security features and misconfigurations that help or lead to attacks.

DAY 5: Mastering Enterprise Exploitation, Post-Exploitation and Pivoting

Module 9: Mastering Exploitation of Enterprise Services

a) Exploiting PKI services
b) Exploiting MSSQL Severs
c) Exploiting IIS
d) Exploiting ADFS
e) Bypassing application whitelisting

Module 10: Mastering Persistence and Lateral Movement

a) Techniques for lateral movement recap
b) BITS Jobs
c) Boot or Login Autostart Execution
d) Boot or Login Initialization Scripts
e) Browser Extensions
f) Compromising Software Binary
g) Event-Triggered Execution
h) External Remote Services
i) Hijack Execution Flow
j) Office Application Startup
k) Scheduled Task/Job
l) Server Software Component
m) Traffic Signaling
n) Persistence through Registry keys
o) Malicious services
p) Fileless malware

Daily Summary: Discussing mitigations and monitoring capabilities.

CQURE

Warsaw New York Dubai Zug

info@cqure.pl

www.cqure.pl www.cqureacademy.com