PEN-300 - Advanced Evasion Techniques and Breaching Defenses (ETBD/OSEP)

Varighed: 5 Days **Kursus Kode: GK840105** **Leveringsmetode: Company event (Firmakursus)**

Beskrivelse:

Building on the skills acquired in PEN-200, OffSecs PEN-300 course explores advanced penetration testing techniques against hardened targets. Learners gain hands-on experience bypassing security defenses and crafting custom exploits in real-world scenarios, enhancing their expertise in ethical hacking and vulnerability assessment.
This course culminates in a challenging exam, leading to the OffSec Experienced Penetration Tester (OSEP) certification. Achieving the OSEP certification distinguishes professionals with advanced penetration testing skills, making them highly sought-after experts in securing organizations from sophisticated threats.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Målgruppe:

The PEN-300 course is ideal for experienced penetration testers and security professionals seeking to master advanced penetration testing methodologies, ultimately earning the OSEP certification. While completion of PEN-200 (Penetration Testing with Kali Linux) is not a formal prerequisite, it is highly recommended due to the advanced nature of PEN-300.

Agenda:

- Upon completing PEN-300 and successfully passing the OSEP exam, youll have mastered advanced penetration testing skills, including:
- In-depth vulnerability analysis and exploitation
- Custom exploit development
- Bypassing modern security defenses
- Exploiting authentication and authorization flaws
- Attacking Active Directory and cloud environments
- Post-exploitation techniques for maintaining access and escalating privileges

Forudsætninger:

While there are no formal certification prerequisites, a strong understanding of operating systems, networking, and scripting (e.g., Python, Bash) is highly recommended. Additionally, familiarity with the concepts and techniques covered in PEN-200 (Penetration Testing with Kali Linux) is highly recommended for success in this course.

- GK840104 - PEN-200 - Penetration Testing with Kali Linux (PWK/OSCP)

Test og certificering

Indhold:

Evasion Techniques and Breaching Defenses: General Course Information

- About the PEN-300 Course
- Provided Material
- Overall Strategies for Approaching the Course
- About the PEN-300 VPN Labs
- About the OSEP Exam

Operating System and Programming Theory

- Programming Theory
- Operating System and Programming Theory
- Client-Side Code Execution with Office

Client-Side Code Execution with Office

- Will You Be My Dropper
- Phishing with Microsoft Office
- Keeping Up Appearances
- Executing Shellcode in Word Memory
- PowerShell Shellcode Runner
- Keep That PowerShell in Memory
- Talking to the Proxy

Client-Side Code Execution with Windows Script Host

- Creating a Basic Dropper in JScript
- JScript and C#
- In-memory PowerShell Revisited

Process Injection and Migration

- Finding a Home for Our Shellcode
- DLL Injection
- Reflective DLL Injection
- Process Hollowing

Introduction to Antivirus Evasion

- Antivirus Software Overview
- Simulating the Target Environment
- Locating Signatures in Files
- Bypassing Antivirus with Metasploit
- Bypassing Antivirus with C#
- Messing with Our Behavior
- Office Please Bypass Antivirus
- Hiding PowerShell Inside VBA

Advanced Antivirus Evasion

- Intel Architecture and Windows 10
- Antimalware Scan Interface
- Bypassing AMSI With Reflection in PowerShell
- Wrecking AMSI in PowerShell
- UAC Bypass vs Microsoft Defender
- Bypassing AMSI in JScript

Application Whitelisting

- Application Whitelisting Theory and Setup
- Basic Bypasses
- Bypassing AppLocker with PowerShell
- Bypassing AppLocker with C#
- Bypassing AppLocker with JScript

Bypassing Network Filters

- DNS Filters
- Web Proxies
- IDS and IPS Sensors
- Full Packet Capture Devices
- HTTPS Inspection
- Domain Fronting
- DNS Tunneling

Linux Post-Exploitation

- User Configuration Files
- Bypassing AV
- Shared Libraries

Kiosk Breakouts

- Kiosk Enumeration
- Command Execution
- Post-Exploitation
- Privilege Escalation
- Windows Kiosk Breakout Techniques

Windows Credentials

- Local Windows Credentials
- Access Tokens
- 3 Kerberos and Domain Credentials
- Processing Credentials Offline

Windows Lateral Movement

- Remote Desktop Protocol
- Fileless Lateral Movement

Linux Lateral Movement

- Lateral Movement with SSH
- DevOps
- Kerberos on Linux

Microsoft SQL Attacks

- MS SQL in Active Directory
- MS SQL Escalation
- Linked SQL Servers

Active Directory Exploitation

- AD Object Security Permissions
- Kerberos Delegation
- Active Directory Forest Theory
- Burning Down the Forest
- Going Beyond the Forest
- Compromising an Additional Forest

Combining the Pieces

- Enumeration and Shell
- Attacking Delegation
- Owning the Domain

Trying Harder: The Labs

- Real Life Simulations
- Wrapping Up

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre