أسم البرنامج : أخصائي اختبار الاختراق RED TEAM – Penetration Tester Workshop

P

برنامج "Red Team - Real Penetration Testing Workshop" هو برنامج تدريبي متخصص مهني يستهدف تطوير مهارات مختبري الاختراق (Penetration Testers) من خلال تعريفهم بأحدث الممارسات والتقنيات في مجال الأمن السيبراني . يتميز البرنامج بأنه يقدم تجربة تعلم عملية وحيّة، حيث يتم التدريب في بيئة عمل فعلية لضمان اكتساب المشاركين الخبرة اللازمة لتنفيذ مهام اختبار الاختراق بنجاح.

في إطار البرنامج، سيتعرف المشاركون على أساسيات اختبار الاختراق وأهم أدوات وتقنيات هذا المجال. سيتم تناول مواضيع مثل فهم طبيعة أنظمة المعلومات، تقييم مستوى الأمان، وتحديد الثغرات والضعف الموجودة في الأنظمة. بالإضافة إلى ذلك، سيتعلم المشاركون طرق اكتشاف واستغلال هذه الثغرات لاختبار مدى قوة الأنظمة والشبكات المستهدفة.

كما سيتعلم المشاركون في الورشة كيفية تنفيذ عمليات الاختراق بطريقة قانونية وأخلاقية، وفقًا للقواعد والمعايير المعترف بها دوليا و عمل التقارير الفنية . يتضمن البرنامج أيضاً تطبيق عملي على سيناريوهات حقيقية، والتي تتيح للمشاركين فرصة لاختبار مهاراتهم واكتساب ثقة أكبر في قدراتهم كمختبري اختراق.

في نهاية البرنامج، سيكون المشاركون قادرين على تنفيذ اختبارات الاختراق بشكل فعّال واحترافي، ومواجهة التحديات الأمنية المعقدة في مجال المعلومات. هذا يجعل "Red Team - Real Penetration Testing Workshop" خياراً مثالياً .

|  |  |
| --- | --- |
| Red Team | **أسم البرنامج** |
| Penetration Testing | **الوظيفة المؤهل لها الدارس** |
| 80 ساعة (محاضرتين أسبوعيا) | **مدة البرنامج** |
| OSCP or EC Council CEH 12 | **الاختبار الدولي** |
| أون لاين | **تنقيذ البرنامج** |
| الرسوم 5 ألاف ريال بدلا من 10 ألاف غير شامل ضريبة القيمة المضافة بخصم 50% خلال فترة التسجيل الاولي  السعر يشمل الرخص اللازمة **بالإضافة إلى خصم 50% على رسوم الاختبار الدولي** | **رسوم البرنامج** |
| 14 يوما | **فترة السماح بالاسترداد** |
| شهادة حضور من مركز المبدعون  شهادة خبرة مهنية من شركة انفوسيك | **شهادات البرنامج** |
| محاضر معتمد | **المحاضر** |
| أساسيات الشبكات (سيتم تخصيص أول أسبوعين في التدريب لدورة مكثفة في الأساسيات) | **المؤهلات اللازمة** |
| 27 | **عدد المعامل والسيناريوهات التي سيتم التدريب عليها** |

**Advanced Red Team Training: Techniques and Tools for Offensive Security**

**Module 1:** Introduction to Red Teaming

* Red Team Fundamentals
* Red Team Engagements
* Red Team Threat Intel
* Red Team OPSEC
* Intro to C2

**Module 2**: Reconnaissance and Footprinting

* Passive and active reconnaissance techniques
* Open-source intelligence (OSINT) gathering
* Target enumeration and identification
* footprinting techniques and tools
* Advanced Foot-Printing techniques

**Module 3**: Scanning and Enumeration

* Port scanning and service enumeration
* Tips for Awesome Scanning
* Version Scanning with Nmap
* False-Positive Reduction
* Netcat for the Pen TesterGetting the Most Out of Nmap
* Faster Scanning with Masscan
* OS Fingerprinting, Version Scanning In-Depth, Netcat for Penetration Testers, and EyeWitness
* Nmap In-Depth: The Nmap Scripting Engine
* Advanced scanning and enumeration techniques.

**Module 4:** Exploitation and Post-Exploitation

* Gaining Initial Access
* Password Guessing, Spraying, and Credential Stuffing
* Exploitation and Exploit Categories
* Exploiting Network Services and Leveraging Meterpreter
* Command and Control Frameworks and Selecting the One for You
* Using the Adversary Emulation and Red Team Framework
* Post-Exploitation with [PowerShell] Empire
* Payload Generation in Metasploit and Silver
* Post-Exploitation
* Assumed Breach Testing
* Situational Awareness on Linux and Windows
* Extracting Useful Information from a Compromised Windows Host

**Module 5**: Privilege Escalation, Persistence, and Password Attacks

* Privilege Escalation Methods and Techniques on Windows and Linux
* Persistence and Maintaining Access
* Password Attack Tips
* Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems
* Extracting Hashes and Passwords from Memory with Mimikatz Kiwi
* Effective Password Cracking with John the Ripper and Hashcat

**Module 6:** Lateral Movement and Reporting

* Lateral Movement
* Running Commands Remotely
* Anti-Virus and Evasion of Defensive Tools
* Application Control Bypasses Using Built-In Windows Features
* Implementing Port Forwarding Relays via SSH
* Pivoting through Target Environments with C2
* Effective Reporting and Business Communication

**Module 7:** Compromising Active Directory

* Active Directory Basics
* Breaching Active Directory
* Enumerating Active Directory
* Lateral Movement and Pivoting
* Exploiting Active Directory
* Persisting Active Directory
* Credentials Harvesting

**Module 8** : Network Security Evasion

* Network Security Solutions and Evasion
* Firewalls Evasion
* Sandbox Evasion

**Module 9**: Use cases

* Real Scenarios and use cases

**Module 10** Exam preparation

* Professional Exam preparation.
* Red Team Capture-the-Flag

# Module 5: Web Application Attacks

* SQL injection and other web-based vulnerabilities
* Cross-site scripting (XSS) and Cross-site request forgery (CSRF)
* Exploiting file upload and file inclusion vulnerabilities
* Web application enumeration and exploitation techniques
* Advanced web application attacks techniques

# Module 6: Wireless and Social Engineering Attacks

* Wireless security fundamentals
* Wi-Fi hacking and cracking techniques
* Social engineering techniques and tools
* Physical security and social engineering attacks