Cyber Security and Technology

Crack the Code Cyber Security Mastery

Code: 259001

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

In an increasingly digital world, the battlefield is no longer just physical—it's virtual. Cyber threats evolve at an unprecedented pace, targeting everything from critical national infrastructure to personal data. The ability to understand, defend against, and ethically counteract these threats is not just a technical skill; it's a critical business imperative. This course is designed to demystify the complex world of cybersecurity, moving from foundational concepts to advanced offensive and defensive techniques.

"Crack the Code" is a hands-on, immersive experience that takes participants on a journey through the mind of both a defender and an attacker. You will learn to think like a hacker to better defend your organization, mastering the tools and strategies used by professionals to protect systems, data, and reputations in a landscape of constant cyber warfare.

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a binder containing a copy of the presentation
- slides and handouts
- Post-assessment

Course Objectives

Upon completion of this course, participants will be able to:

- **Analyze the Cyber Threat Landscape:** Identify current and emerging threats, threat actors, and their methodologies.
- **Conduct Vulnerability Assessments and Penetration Testing:** Utilize ethical hacking techniques to proactively identify and exploit system vulnerabilities in a controlled environment.
- **Implement Robust Defensive Strategies:** Design and configure network defenses, including firewalls, intrusion detection/prevention systems (IDS/IPS), and access controls.
- **Respond to Security Incidents:** Execute a structured incident response plan to detect, contain, eradicate, and recover from a security breach.
- **Apply Core Security Principles:** Implement the principles of confidentiality, integrity, and availability (CIA triad) across IT infrastructure.
- **Develop a Security-First Mindset:** Make risk-based decisions and effectively communicate cyber risks to technical and non-technical stakeholders.

Who Should Attend?

This course is designed for IT professionals and others responsible for protecting digital assets.

- **IT Administrators, Network Engineers, and Systems Analysts**
- **Aspiring Security Analysts, SOC Analysts, and Security Consultants**
- **IT Managers and Risk & Compliance Officers**
- **Software Developers** interested in building secure applications (DevSecOps)
- **Senior Management** seeking to understand cyber risk (optional high-level track)

Course Outline

Day 1: Foundations – The Hacker's Mindset & Reconnaissance

Morning:

- **Module 1: The Cyber Security Universe:** Introduction to the course, the threat landscape, and the ethics of ethical hacking.
- **Module 2: The CIA Triad & Security Fundamentals:** Confidentiality, Integrity, Availability. Introduction to cryptography.

Afternoon:

- **Module 3: Footprinting and Reconnaissance:** Passive and active information gathering techniques (OSINT).
- **Lab 1: The Art of Discovery:** Using tools like whois, nslookup, and theHarvester to profile a target.
- **Day 1 Recap: Knowing your enemy and yourself.**

Day 2: Scanning & Vulnerability Analysis

Morning:

- **Module 4: Network Scanning Methodologies:** Identifying live hosts, open ports, and running services.
- **Module 5: Enumeration:** Extracting valuable information about users, groups, and network resources.

Afternoon:

- **Module 6: Vulnerability Assessment:** Introduction to vulnerability scanners.
- **Lab 2: Mapping the Attack Surface:** Using tools like **Nmap** and **Nessus** to scan a network and analyze results for weaknesses.
- **Day 2 Recap: Finding the open doors.**

Day 3: Gaining Access – Exploitation

Morning:

- **Module 7: Introduction to Exploitation:** Understanding exploits, payloads, and Metasploit.
- **Module 8: Web Application Attacks:** OWASP Top 10 deep dive (e.g., SQL Injection, Cross-Site Scripting – XSS).

Afternoon:

- **Module 9: Password Attacks & Social Engineering:** Techniques and defenses.
- **Lab 3: The Controlled Breach:** Using a framework like **Metasploit** to exploit a known vulnerability and gain initial access on a target machine.
- **Day 3 Recap: Cracking the code and crossing the threshold.**

Course Outline

Day 4: Post-Exploitation & Defense-in-Depth

Morning:

- **Module 10: Post-Exploitation Techniques:** What to do after gaining access? Privilege escalation, persistence, and lateral movement.
- **Module 11: Building the Defense: Security Architecture:** Principles of defense-in-depth, zero trust, and segmentation.

Afternoon:

- **Module 12: Defensive Tools of the Trade:** Configuring firewalls (iptables), IDS/IPS (Snort), and antivirus solutions.
- **Lab 4: Fortifying the Castle:** Hardening a system based on the vulnerabilities found earlier. Configuring a firewall to block attack vectors.
- **Day 4 Recap: Holding the fort and building stronger walls.**

Day 5: Incident Response & Capstone Challenge

Morning:

- **Module 13: The Incident Response Lifecycle:** Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
- **Module 14: Digital Forensics Fundamentals:** Live vs. dead box analysis, log analysis, and evidence handling.

Afternoon:

- **Capstone Activity: The Cyber Range Exercise:** Teams are placed in a simulated corporate network. One team plays as Red Team (attackers) and another as Blue Team (defenders).
  - **Red Team:** Objective: Breach the system and exfiltrate data.
  - **Blue Team:** Objective: Defend the network, detect the intrusion, and respond accordingly.
- **Hot Wash Debrief:** Teams present their strategies, findings, and lessons learned.
- **Course Conclusion:** Review, career pathways, and awarding of certificates

المقدمة

في عالمٍ رقميٍّ متزايد، لم تعد ساحة المعركة ماديةً فحسب، بل أصبحت افتراضية. تتطور التهديدات السيبرانية بوتيرةٍ غير مسبوقة، مستهدفةً كل شيء، من البنية التحتية الوطنية الحيوية إلى البيانات الشخصية. إن القدرة على فهم هذه التهديدات والدفاع عنها ومواجهتها أخلاقياً ليست مجرد مهارةٍ تقنية؛ بل هي ضرورةٌ أساسيةٌ للأعمال. صُممت هذه الدورة لتوضيح عالم الأمن السيبراني المعقد، بالانتقال من المفاهيم الأساسية إلى التقنيات الهجومية والدفاعية المتقدمة.
"فكّ الشفرة" تجربة عملية وغامرة تأخذ المشاركين في رحلة عبر عقلية كلٍّ من المدافع والمهاجم. ستتعلم كيف تفكر كهاكر لتدافع عن مؤسستك بشكل أفضل، وتتقن الأدوات والاستراتيجيات التي يستخدمها المحترفون لحماية الأنظمة والبيانات والسمعة في ظلّ حرب سيبرانية متواصلة.

طريقة التدريب

- التقييم المسبق
- تدريب جماعي مباشر
- استخدام أمثلة واقعية ودراسات حالة وتمارين
- مشاركة ونقاش تفاعلي
- عرض تقديمي باستخدام باور بوينت، وشاشة LCD، ولوح ورقي
- أنشطة واختبارات جماعية
- يحصل كل مشارك على ملف يحتوي على نسخة من العرض التقديمي
- شرائح ومطبوعات
- التقييم اللاحق

أهداف الدورة

عند الانتهاء من هذه الدورة، سيكون المشاركون قادرين على:

- **تحليل مشهد التهديدات السيبرانية:** تحديد التهديدات الحالية والناشئة، والجهات الفاعلة في التهديد، ومنهجياتها.
- **إجراء تقييمات الثغرات الأمنية واختبار الاختراق:** استخدم تقنيات القرصنة الأخلاقية لتحديد نقاط الضعف في النظام واستغلالها بشكل استباقي في بيئة خاضعة للرقابة.
- **تنفيذ استراتيجيات دفاعية قوية:** تصميم وتكوين دفاعات الشبكة، بما في ذلك جدران الحماية، وأنظمة الكشف عن التطفل/الوقاية منه (IDS/IPS)، وضوابط الوصول.
- **الاستجابة لحوادث الأمن:** تنفيذ خطة منظمة للاستجابة للحوادث من أجل الكشف عن خرق أمني واحتوائه والقضاء عليه والتعافي منه.
- **تطبيق مبادئ الأمن الأساسية:** تنفيذ مبادئ السرية والنزاهة والتوافر (ثالوث الأمن الأساسي) عبر البنية التحتية لتكنولوجيا المعلومات.
- **تطوير عقلية الأمن أولاً:** اتخاذ قرارات تعتمد على المخاطر والتواصل بشكل فعال بشأن المخاطر السيبرانية مع أصحاب المصلحة التقنيين وغير التقنيين

من ينبغي أن يهتم؟

تم تصميم هذه الدورة التدريبية لمحترفي تكنولوجيا المعلومات وغيرهم من المسؤولين عن حماية الأصول الرقمية.

- **مسؤولو تكنولوجيا المعلومات ومهندسو الشبكات ومحللو الأنظمة**
- **محللو الأمن الطموحون، ومحللو مركز العمليات الأمنية، ومستشارو الأمن**
- **مديري تكنولوجيا المعلومات ومسؤولي المخاطر والامتثال**
- **مطورو البرامج** المهتمون ببناء تطبيقات آمنة (DevSecOps)
- **الإدارة العليا** تسعى إلى فهم المخاطر السيبرانية (مسار اختياري رفيع المستوى)

محتويات الكورس

اليوم الأول الأساسيات - عقلية الهاكر والاستطلاع

صباح:

- **الوحدة 1: عالم الأمن السيبراني:** مقدمة عن الدورة، ومشهد التهديدات، وأخلاقيات القرصنة الأخلاقية.
- **الوحدة الثانية: ثالوث وكالة المخابرات المركزية وأساسيات الأمن:** السرية، والنزاهة، والتوافر. مقدمة في التشفير.

بعد الظهر:

- **الوحدة 3: البصمة والاستطلاع:** تقنيات جمع المعلومات السلبية والإيجابية (OSINT).
- **المختبر 1: فن الاكتشاف:** استخدام أدوات مثل nslookup، whois، و theHarvester لتحديد ملف تعريف الهدف.
- **ملخص اليوم الأول: معرفة عدوك ومعرفة نفسك**

اليوم الثاني المسح وتحليل الثغرات الأمنية

صباح:

- **الوحدة 4: منهجيات مسح الشبكة:** تحديد المضيفين المباشرين والمنافذ المفتوحة والخدمات قيد التشغيل.
- **الوحدة 5: الترقيم:** استخراج معلومات قيمة حول المستخدمين والمجموعات وموارد الشبكة.

بعد الظهر:

- **الوحدة 6: تقييم الثغرات الأمنية:** مقدمة إلى ماسحات الثغرات الأمنية.
- **المختبر 2: رسم خريطة لسطح الهجوم:** استخدام أدوات مثل **Nmap** و **Nessus** لمسح الشبكة وتحليل النتائج بحثًا عن نقاط الضعف.
- **ملخص اليوم الثاني: العثور على الأبواب المفتوحة**

اليوم الثالث الوصول - الاستغلال

صباح:

- **الوحدة 7: مقدمة عن الاستغلال:** فهم الاستغلالات والحمولات والاستغلال الخبيث.
- **الوحدة 8: هجمات تطبيقات الويب:** تحليل متعمق لأفضل 10 هجمات وفقًا لـ OWASP (على سبيل المثال، حقن SQL، و XSS – Cross-Site Scripting).

بعد الظهر:

- **الوحدة 9: هجمات كلمة المرور والهندسة الاجتماعية:** التقنيات والدفاعات.
- **المختبر 3: الاختراق المتحكم فيه:** استخدام إطار عمل مثل **Metasploit** لاستغلال ثغرة أمنية معروفة والحصول على وصول أولي إلى جهاز مستهدف.

محتويات الكورس

اليوم الرابع مرحلة ما بعد الاستغلال والدفاع المتعمق

صباح:

- **الوحدة ١٠: تقنيات ما بعد الاستغلال:** ما العمل بعد الحصول على حق الوصول؟ تصعيد الامتيازات، والمثابرة، والحركة الجانبية.
- **الوحدة 11: بناء الدفاع: بنية الأمن:** مبادئ الدفاع المتعمق، والثقة الصفرية، والتجزئة.

بعد الظهر:

- **الوحدة 12: أدوات الدفاع التجارية:** تكوين جدران الحماية (iptables)، وIDS/IPSs (Snort)، وحلول مكافحة الفيروسات.
- **المختبر الرابع: تحصين النظام:** تعزيز النظام بناءً على الثغرات الأمنية المكتشفة سابقًا. تكوين جدار حماية لصد هجمات النواقل.
- **ملخص اليوم الرابع: الحفاظ على الحصن وبناء جدران أقوى**

اليوم الخامس الاستجابة للحوادث وتحدي المشروع النهائي

صباح:

- **الوحدة 13: دورة حياة الاستجابة للحوادث:** التحضير، والتحديد، والاحتواء، والاستئصال، والتعافي، والدروس المستفادة.
- **الوحدة 14: أساسيات الطب الشرعي الرقمي:** تحليل الصندوق الحي مقابل الصندوق الميت، وتحليل السجلات، ومعالجة الأدلة.

بعد الظهر:

- **نشاط التخرج: تمرين النطاق السيبراني:** تُوزّع الفرق في شبكة شركة محاكاة. يلعب فريق كفريق أحمر (مهاجمون) وآخر كفريق أزرق (مدافعون).
  - **الفريق الأحمر:** الهدف: اختراق النظام واستخراج البيانات.
  - **الفريق الأزرق:** الهدف: الدفاع عن الشبكة، واكتشاف الاختراق، والرد وفقًا لذلك.
- **إحاطة سريعة:** تقدم الفرق استراتيجياتها ونتائجها والدروس المستفادة.
- **خاتمة الدورة:** المراجعة والمسارات المهنية ومنح الشهادات

Terms & Conditions

Complete & Mail to future centre or email

Info@futurecentre.com

Cancellation and Refund Policy

Delegates have 14 days from the date of booking to cancel and receive a full refund or transfer to another date free of charge. If less than 14 days' notice is given, then we will be unable to refund or cancel the booking unless on medical grounds. For more details about the Cancellation and Refund policy, please visit
https://futurecentre.net/

Registration & Payment

Please complete the registration form on the course page & return it to us indicating your preferred mode of payment. For further information, please get in touch with us

Course Materials

The course material, prepared by the future centre, will be digital and delivered to candidates by email

Certificates

Accredited Certificate of Completion will be issued to those who attend & successfully complete the programme.

Travel and Transport

We are committed to picking up and dropping off the participants from the airport to the hotel and back.

Registration & Payment

Complete & Mail to future centre or email

Info@futurecentre.com

Registration Form

- Full Name (Mr / Ms / Dr / Eng) .....
- Position .....
- Telephone / Mobile .....
- Personal E-Mail .....
- Official E-Mail .....
- Company Name .....
- Address .....
- City / Country .....

Payment Options

- ☐ Please invoice me
- ☐ Please invoice my company

Course Calander:

- 05/01/2026 - 09/01/2026 Click Now
- 25/05/2026 - 29/05/2026 Click Now
- 12/10/2026 - 16/10/2026 Click Now

VENUES

- LONDON
- BARCELONA
- KUALA LUMPER
- AMSTERDAM
- DAMASCUS
- ISTANBUL
- SINGAPORE
- PARIS
- DUBAI

OUR PARTNERS

THANK YOU

CONTACT US

+963 112226969

+963 953865520

Info@futurecentre.com

Damascus - Victoria - behind Royal Semiramis hotel

FUTURE CENTRE
مركز المستقبل

futurecentre.net