

# From Novice to Ninja

Cyber Security and Technology

Comprehensive Cyber Security  
Training From Novice to Ninja

Code: 259006



FUTURE CENTRE  
مركز المستقبل



futurecentre.net



## Course Introduction

Cybersecurity is no longer a niche field—it's a critical discipline essential for safeguarding personal, organizational, and national digital assets. Comprehensive Cyber Security Training: From Novice to Ninja is designed to take learners with little or no prior experience on a journey to cybersecurity mastery. This course balances foundational principles with advanced offensive and defensive techniques, ensuring participants gain both the theoretical knowledge and hands-on skills needed to protect systems, detect threats, and respond to incidents like a seasoned professional. Whether you're starting a new career or elevating your existing skills, this training provides the roadmap to become a cybersecurity ninja.

## 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:

1. **Understand core cybersecurity concepts**, including threats, vulnerabilities, attacks, and countermeasures.
2. **Perform basic to advanced penetration testing** using industry-standard tools.
3. **Implement defensive security measures** such as firewalls, IDS/IPS, and endpoint protection.
4. **Detect, analyze, and respond to security incidents** effectively.
5. **Secure networks, cloud environments, and applications.**
6. **Develop and enforce cybersecurity policies** aligned with best practices and compliance requirements.

## Who Should Attend?

This course is ideal for:

- **Beginners** aspiring to enter the cybersecurity field.
- **IT professionals** transitioning into security roles.
- **System/network administrators** looking to enhance security skills.
- **Developers** interested in secure coding and application security.
- **Students and career-changers** seeking practical cybersecurity knowledge.

# Course Outline

## Day 1: Cybersecurity Fundamentals

- **Module 1:** Introduction to Cybersecurity: Importance, Key Terms, and the Threat Landscape
- **Module 2:** Core Principles: CIA Triad, Authentication, Authorization, and Accounting
- **Module 3:** Common Threats: Malware, Phishing, Social Engineering, and Insider Threats
- **Hands-On Lab:** Setting Up a Virtual Lab Environment (VirtualBox/Kali Linux)
- **Quiz:** Fundamentals Assessment

## Day 2: Network Security and Defense

- **Module 4:** Networking Basics for Security: TCP/IP, Subnetting, and Protocols
- **Module 5:** Network Defense Tools: Firewalls, IDS/IPS, and VPNs
- **Module 6:** Wireless Security: Securing Wi-Fi Networks and IoT Devices
- **Hands-On Lab:** Configuring Firewall Rules and Analyzing Network Traffic with Wireshark
- **Case Study:** Real-World Network Breach Analysis

## Day 3: Ethical Hacking and Penetration Testing

- **Module 7:** Introduction to Ethical Hacking: Reconnaissance, Scanning, and Enumeration
- **Module 8:** Vulnerability Assessment and Exploitation
- **Module 9:** Web Application Security: OWASP Top 10 (SQL Injection, XSS, CSRF)
- **Hands-On Lab:** Conducting a Pen Test on a Vulnerable Web App (e.g., OWASP Juice Shop)
- **Workshop:** Writing a Penetration Testing Report

# Course Outline

## Day 4: Incident Response and Digital Forensics

- **Module 10:** Incident Response Lifecycle: Preparation, Detection, Containment, Eradication, Recovery
- **Module 11:** Digital Forensics: Data Acquisition, Analysis, and Evidence Handling
- **Module 12:** Malware Analysis: Static and Dynamic Techniques
- **Hands-On Lab:** Simulated Incident Response and Forensic Investigation
- **Group Exercise:** Responding to a Ransomware Attack

## Day 5: Advanced Topics and Capstone Project


- **Module 13:** Cloud Security: Best Practices for AWS/Azure
- **Module 14:** Security Governance: Policies, Compliance (GDPR, HIPAA), and Risk Management
- **Module 15:** Career Pathways in Cybersecurity: Certifications and Next Steps
- **Capstone Project:** Designing and Implementing a Secure Network Architecture
- **Course Wrap-Up:** Q&A, Certificates, and Guidance for Further Learning



## المقدمة

لم يعد الأمن السيبراني مجالاً متخصصاً، بل أصبح تخصصاً بالغ الأهمية لحماية الأصول الرقمية الشخصية والتنظيمية والوطنية. صُمم برنامج "التدريب الشامل في الأمن السيبراني: من المبتدئ إلى الخبير" ليأخذ المتدربين ذوي الخبرة المحدودة أو المعدومة في رحلة نحو إتقان الأمن السيبراني. يوازن هذا البرنامج بين المبادئ الأساسية والتقنيات الهجومية والدفاعية المتقدمة، مما يضمن للمشاركين اكتساب المعرفة النظرية والمهارات العملية اللازمة لحماية الأنظمة، واكتشاف التهديدات، والاستجابة للحوادث باحترافية عالية. سواء كنت تبدأ مسيرة مهنية جديدة أو تُطوّر مهاراتك الحالية، يوفر لك هذا التدريب خارطة الطريق لتصبح خبيراً في الأمن السيبراني.

## 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:
1. فهم مفاهيم الأمن السيبراني الأساسية ، بما في ذلك التهديدات والثغرات والهجمات والتدابير المضادة.
  2. قم بإجراء اختبارات الاختراق من الأساسية إلى المتقدمة باستخدام أدوات قياسية في الصناعة.
  3. تنفيذ تدابير أمنية دفاعية مثل جدران الحماية، وأنظمة الكشف عن التسلل/منع التسلل، وحماية نقاط النهاية.
  4. اكتشاف الحوادث الأمنية وتحليلها والاستجابة لها بشكل فعال.
  5. الشبكات الآمنة والبيئات السحابية والتطبيقات .
  6. تطوير وتنفيذ سياسات الأمن السيبراني بما يتماشى مع أفضل الممارسات ومتطلبات الامتثال

## من ينبغي أن يهتم؟

- هذه الدورة مثالية ل:
- المبتدئين الطامحين لدخول مجال الأمن السيبراني.
  - محترفي تكنولوجيا المعلومات ينتقلون إلى الأدوار الأمنية.
  - مسؤولو النظام/الشبكة الذين يتطلعون إلى تعزيز مهاراتهم الأمنية.
  - المطورون المهتمون بالترميز الآمن وأمان التطبيقات.
  - الطلاب والراغبون في تغيير مسارهم المهني والذين يبحثون عن المعرفة العملية في مجال الأمن السيبراني.

# محتويات الكورس

## اليوم الأول أساسيات الأمن السيبراني

- الوحدة 1: مقدمة في الأمن السيبراني: الأهمية والمصطلحات الرئيسية ومشهد التهديدات
- الوحدة 2: المبادئ الأساسية: ثالوث وكالة المخابرات المركزية، والمصادقة، والتفويض، والمحاسبة
- الوحدة 3: التهديدات الشائعة: البرامج الضارة، والتصيد الاحتيالي، والهندسة الاجتماعية، والتهديدات الداخلية
- ورشة عمل عملية: إعداد بيئة مختبر افتراضي (VirtualBox/Kali Linux)
- اختبار: تقييم الأساسيات

## اليوم الثاني أمن الشبكات والدفاع عنها

- الوحدة 4: أساسيات الشبكات للأمان: TCP/IP، والتقسيم الفرعي للشبكات، والبروتوكولات
- الوحدة 5: أدوات الدفاع عن الشبكة: جدران الحماية، وأنظمة كشف التسلل/منع التطفل، وشبكات VPN
- الوحدة 6: الأمان اللاسلكي: تأمين شبكات Wi-Fi وأجهزة إنترنت الأشياء
- مختبر عملي: تكوين قواعد جدار الحماية وتحليل حركة مرور الشبكة باستخدام Wireshark
- دراسة حالة: تحليل اختراق الشبكة في العالم الحقيقي

## اليوم الثالث الاختراق الأخلاقي واختبار الاختراق

- الوحدة 7: مقدمة في الاختراق الأخلاقي: الاستطلاع والمسح والحصص
- الوحدة 8: تقييم نقاط الضعف والاستغلال
- الوحدة 9: أمان تطبيقات الويب: أفضل 10 نقاط وفقاً لـ OWASP (حقن SQL، XSS، CSRF)
- مختبر عملي: إجراء اختبار اختراق على تطبيق ويب معرض للخطر (على سبيل المثال، OWASP Juice Shop)
- ورشة عمل: كتابة تقرير اختبار الاختراق

## محتويات الكورس

### اليوم الرابع الاستجابة للحوادث والتحليلات الجنائية الرقمية

- الوحدة 10: دورة حياة الاستجابة للحوادث: التحضير، والكشف، والاحتواء، والاستئصال، والتعافي
- الوحدة 11: الطب الشرعي الرقمي: الحصول على البيانات وتحليلها ومعالجة الأدلة
- الوحدة 12: تحليل البرامج الضارة: التقنيات الثابتة والديناميكية
- مختبر عملي: محاكاة الاستجابة للحوادث والتحقيق الجنائي
- تمرين جماعي: الاستجابة لهجوم برامج الفدية

### اليوم الخامس مواضيع متقدمة ومشروع التخرج

- الوحدة 13: أمان السحابة: أفضل الممارسات لـ AWS/Azure
- الوحدة 14: حوكمة الأمن: السياسات والامتثال (اللائحة العامة لحماية البيانات، وقانون التأمين الصحي المحمول والمساءلة)، وإدارة المخاطر
- الوحدة 15: المسارات المهنية في مجال الأمن السيبراني: الشهادات والخطوات التالية
- مشروع التخرج: تصميم وتنفيذ بنية شبكة آمنة
- ملخص الدورة: الأسئلة والأجوبة، والشهادات، والإرشادات لمزيد من التعلم

# 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:



09/02/2026 - 13/02/2026

[Click Now](#)



29/06/2026 - 03/07/2026

[Click Now](#)



16/11/2026 - 20/11/2026

[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](mailto:Info@futurecentre.com)

 Damascus - Victoria - behind Royal Semiramis hotel



**FUTURE CENTRE**  
مركز المستقبل



[futurecentre.net](http://futurecentre.net)