CORSO CYBERSECURITY ETHICAL HACKER v12

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: INTRODUCTION TO ETHICAL HACKING

- Information Security Overview
- Cyber Kill Chain Concepts
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Information Security Laws and Standards

MODULO 2: FOOTPRINTING AND RECONNAISSANCE

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

MODULO 3: SCANNING NETWORKS

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Draw Network Diagrams

MODULO 4: ENUMERATION

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques
- Enumeration Countermeasures

MODULO 5: VULNERABILITY ANALYSIS

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Solutions and Tools
- Vulnerability Assessment Reports

MODULO 6: SYSTEM HACKING

- System Hacking Concepts
- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

MODULO 7: Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Fileless Malware Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software

MODULO 8: SNIFFING

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning
- Sniffing Tools Countermeasures
- Sniffing Detection Techniques

MODULO 9: SOCIAL ENGINEERING

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Countermeasures

MODULO 10: DENIAL-OF-SERVICE

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- DoS/DDoS Attack Tools
- Countermeasures
- DoS/DDoS Protection Tools

MODULO 11: SESSION HIJACKING

- Session Hijacking Concepts Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures

CORSO CYBERSECURITY ETHICAL HACKER v12

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

- IDS, IPS, Firewall, and Honeypot Concepts
- IDS, IPS, Firewall, and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

MODULO 13: HACKING WEB SERVERS

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Tools
- Countermeasures
- Patch Management
- Web Server Security Tools

MODULO 14: HACKING WEB APPLICATIONS

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks, and Web Shell
- Web Application Security

MODULO 15: SQL INJECTION

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Countermeasures

MODULO 16: HACKING WIRELESS NETWORKS

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Countermeasures
- Wireless Security Tools

MODULO 17: HACKING MOBILE PLATFORMS

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

CONTATTI

info@nexsys.it

www.nexsys.it

MODULO 18: IOT AND OT HACKING

- IoT Hacking
- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures
- OT Hacking
- OT Concepts
- OT Attacks
- OT Hacking Methodology
- OT Hacking Tools
- Countermeasures

MODULO 19: CLOUD COMPUTING

- Cloud Computing Concepts
- Container Technology
- Serverless Computing
- Cloud Computing Threats
- Cloud Hacking
- Cloud Security

MODULO 20: CRYPTOGRAPHY

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Countermeasures

APPENDIX A: ETHICAL HACKING ESSENTIAL CONCEPTS

- Operating System Concepts
- File Systems
- Computer Network Fundamentals
- Basic Network Troubleshooting
- Virtualization
- Network File System (NFS)
- Web Markup and Programming Languages
- Application Development Frameworks and Their Vulnerabilities
- Web Subcomponents
- Database Connectivity

APPENDIX B: ETHICAL HACKING ESSENTIAL CONCEPTS

- Information Security Controls
- Network Segmentation
- Network Security Solutions
- Data Leakage
- Data Backup
- Risk Management Concepts
- Business Continuity and Disaster Recovery
- Cyber Threat Intelligence
- Threat Modeling
- Penetration Testing Concepts
- Security Operations
- Forensic Investigation
- Software Development Security
- Security Governance Principles
- Asset Management and Security

CORSO CYBERSECURITY ETHICAL HACKER v12

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

OVERVIEW DEL CORSO

Il corso Cybersecurity Ethical Hacker forma i professionisti che desiderano utilizzare gli strumenti impiegati dagli hacker ma con scopi eticamente corretti. Durante il corso, i partecipanti avranno l'opportunità di acquisire conoscenze di base e di approfondire argomenti specifici in tema cybersecurity, con particolare attenzione ai temi di Vulnerability Assessment, Penetration Test, Malware Analysis, Incident Response e Digital Forensics. Durante la formazione saranno presentate e praticate, attraverso simulazioni di scenari reali, tecniche di ethical hacking e di security assessment. Inoltre, sarà dedicato spazio all'analisi dettagliata, modulo per modulo, delle contromisure di sicurezza adottabili in contesti specifici.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- IT manager;
- CIO e Responsabili di funzione IT;
- Professionisti IT sistemisti, amministratori di sistema, ingegneri di rete e sviluppatori che vogliono approfondire le conoscenze sulla sicurezza informatica e proteggere i sistemi dalle minacce informatiche;
- Responsabili della sicurezza informatica: CISO, security architects, security specialists, malware analysts, security consultants, security engineers e security administrators;
- Penetration testers e ethical hackers.

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Raccogliere informazioni di Intelligence;
- Scansionare reti e computer;
- Sfruttare vulnerabilità software e web application;
- Usare tecniche di evasione dei firewall;
- Usare tecniche di evasione degli antivirus;
- Effettuare attacchi su reti wireless;
- Analizzare la non-sicurezza nel mondo IOT;
- Sviluppare le security policy aziendali.

Scopri di più sul corso Cybersecurity Ethical Hacker V12.

CONTATTI

✉ info@nexsys.it

www.nexsys.it