CYBER SECURITY PROGRAMS

5 day training programs

The 5 day training programs is geared to prepare the participant for taking the Security+ exam. The online exam can be taken at Etisalat Academy's Pearson VUE test center.

CompTIA

اتصالات
etisalat

أكاديمية اتصالات
etisalat academy
Skills | Solutions | Results

CYBER SECURITY PROGRAMS

CompTIA Security+™ Certification

CompTIA Security+ certification designates knowledge-able professionals in the field of security, one of the fastest-growing fields in IT.
Our CompTia Security+ training will provide you the necessary knowledge and skills in the following areas

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data and host security
- Access control and identity management
- Cryptography

The 5 day training program is geared to prepare the participant for taking the Security+ exam. The online exam can be taken at Etisalat Academy's Pearson VUE test center.

CompTIA Advanced Security Practitioner

(CASP) certification designates IT professionals with advanced-level security skills and knowledge.
The 5 day training course will provide knowledge and skills in enterprise security; risk management; research and analysis; and integration of computing, communica-tions, and business disciplines. It covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. It involves applying critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

CompTIA Storage+ Certification

The CompTIA Storage+ Powered by Storage Networking Industry Association (SNIA) certification is designed to validate foundational knowledge for storage networking professionals seeking to demonstrate their competency in storage networking and information management.
The CompTIA Storage+ Powered by SNIA certification covers the knowledge and skills required to configure basic networks to include archive, backup, and restoration technologies. Additionally, the successful candidate will be able to understand the fundamentals of business continuity, application workload, system integration, and storage/system administration, while performing basic troubleshooting on connectivity issues and referencing documentation

Certification: GPEN

Global Information Assurance Certification Penetration Tester (GPEN)
The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test.
The five day training course will equip you with the knowledge and skills in :

- Network Penetration Testing: Planning, Scoping, and Recon
- Network Penetration Testing: Scanning
- Network Penetration Testing: Exploitation and Post Exploitation
- Network Penetration Testing: Password Attacks
- Network Penetration Testing: Wireless and Web Apps
- Penetration Testing Workshop & Capture the Flag Event

Certification: GXPN

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
Security personnel whose job duties involve assessing target networks, systems and applications to find vulner-abilities. The 5 day GXPN training course provides the knowledge, skills, and ability to conduct advanced penetration tests, how to model the abilities of an advanced attacker to find significant security flaws in systems, and demonstrate the business risk associated with these flaws. It focuses on important topics in IT Security such as:

- Network Attacks for Penetration Testers
- Crypto, Network Booting Attacks, and Escaping Restricted Environments
- Python, Scapy, and Fuzzing
- Exploiting Linux for Penetration Testers
- Exploiting Windows for Penetration Testers
- Capture the Flag

CompTIA Security+

CompTIA Security+™ Certification

Introduction

Security affects all areas of business, not just the IT department. In addition to a firm's loss of income and employee productivity, a security breach can cost a business its reputation. Demonstrating that you can stay ahead of the ever-changing security issues is a key marketable skill in today's job market. CompTIA Security+ certification validates experienced technical knowledge of security as it relates to the overarching subject matter areas.

Preparing for the Security+ Exam:

The Candidates may choose to prepare for the CompTIA Security+ exam by taking the CompTIA Security+ course in Etisalat Academy

Course Contents:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data and host security
- Access control and identity management
- Cryptography

Expected Accomplishments:

- Proactively implement sound security protocols to mitigate security risks
- Quickly respond to security issues
- Retroactively identify where security breaches may have occurred
- Design the network, onsite or in the cloud, with security in mind

Prerequisites:

- Working knowledge of TCP/IP
- No prior programming knowledge is required for the course.

Training Course for the Certification Exam:	Course Duration:	Course Provider:
Security+	5 Days	Etisalat Academy

☎ +971 4 264 4444 🖷 +971 4 264 8888 ✉ info@etac.ae

CompTIA Advanced Security Practitioner

CompTIA Advanced Security Practitioner

Introduction

The CompTIA Advanced Security Practitioner certification is an international, vendor-neutral exam that proves competency in enterprise security; risk management; research and analysis; and integration of computing, communications, and business disciplines.

The exam covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. It involves applying critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

Course Contents:

- Enterprise Security
- Risk Management, Policy / Procedure and Legal
- Research and Analysis
- Integration of Computing, Communications and Business Disciplines

Expected Accomplishments:

- Distinguish which cryptographic tools and techniques are appropriate for a given situation.
- Distinguish and select among different types of virtualized, distributed and shared computing
- Integrate hosts, networks, infrastructures, applications and storage into secure comprehensive solutions
- Given a scenario, distinguish and select the method or tool that is appropriate to conduct an assessment
- Analyze the security risk implications associated with business decisions
- Execute and implement risk mitigation strategies and controls
- Explain the importance of preparing for and supporting the incident response and recovery process
- Implement security and privacy policies and procedures based on organizational requirements
- Analyze industry trends and outline potential impact to the enterprise
- Carry out relevant analysis for the purpose of securing the enterprise
- Explain the security impact of inter-organizational change
- Select and distinguish the appropriate security controls with regard to communications and collaboration
- Explain advanced authentication tools, techniques and concepts
- Carry out security activities across the technology life cycle

Prerequisites:

- Working knowledge of TCP/IP
- CompTIA Security+ training is recommended

Training Course for the Certification Exam:	Course Duration:	Course Provider:
CompTIA Advanced Security Practitioner	5 Days	Etisalat Academy

CompTIA Storage+ Certification

CompTIA Storage+ Certification

Introduction

The CompTIA Storage+ Powered by Storage Networking Industry Association (SNIA) certification is designed to validate foundational knowledge for storage networking professionals seeking to demonstrate their competency in storage networking and information management.

The CompTIA Storage+ Powered by SNIA certification covers the knowledge and skills required to configure basic networks to include archive, backup, and restoration technologies. Additionally, the successful candidate will be able to understand the fundamentals of business continuity, application workload, system integration, and storage/system administration, while performing basic troubleshooting on connectivity issues and referencing documentation.

Preparing for the GXPN Exam:

The Candidates may choose to prepare for the CompTIA Storage+ Certification exam by taking the Etisalat Academy Training Course: CompTIA Storage+ Certification

Course Contents:

- Storage Components
- Connectivity
- Storage Management
- Data Protection
- Storage Performance

Expected Accomplishments:

- Be able to validate knowledge, skills and abilities in all major aspects of storage networking technologies (software and hardware).
- Understand the operations of major technologies, standards, protocols, and interconnects in the operation of networked storage, and to understand how to optimize those elements for superior performance.
- Leverage storage networking technologies to provide data protection, backup, fault tolerance, and disaster recovery/business continuity services for the organization.
- Understand and deploy the attributes of various types of network storage that enable an organization to deploy the optimum storage solution for the business need, (e.g. data management, file services, messaging, structured and unstructured data, data under regulatory compliance requirements, or archival storage needs).

Prerequisites:

- The exam is targeted toward IT storage professionals with at least twelve months of experience. Though it is not required, CompTIA A+, CompTIA Network+ or CompTIA Server+ certification is recommended.

Training Course for the Certification Exam:	Course Duration:	Course Provider:
CompTIA Storage+ Certification	5 Days	Etisalat Academy

Global Information Assurance Certification Penetration Tester (GPEN)

Global Information Assurance Certification Penetration Tester (GPEN)

Introduction

The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test.

Preparing for the GPEN Exam:

No specific training course is a required prerequisite for the exam . However, the Candidates may choose to prepare for the GPEN exam by taking the SANS Training Course: SEC560: Network Penetration Testing and Ethical Hacking.

Exam Information:

- 1 proctored exam
- 115 questions
- Time limit of 3 hours
- Minimum Passing Score of 74%

Course Contents:

- Network Penetration Testing: Planning, Scoping, and Recon
- Network Penetration Testing: Scanning
- Network Penetration Testing: Exploitation and Post Exploitation
- Network Penetration Testing: Password Attacks
- Network Penetration Testing: Wireless and Web Apps
- Penetration Testing Workshop & Capture the Flag Event

Prerequisites:

- Working knowledge of TCP/IP, cryptographic routines (DES, AES, and MD5); and the Windows and Linux command lines.
- No prior programming knowledge is required for the course.

Expected Accomplishments:

- Develop tailored scoping and rules of engagement for penetration testing.
- Conduct detailed reconnaissance using document metadata, search engines, etc
- Utilize scanning tools such as Nmap.
- Choose and properly execute Nmap Scripting Engine scripts.
- Configure and launch a vulnerability scanner such as Nessus.
- Analyze the output of scanning tools
- Utilize the Windows and Linux commands
- Configure an exploitation tool such as Metasploit to scan & exploit
- Conduct comprehensive password attacks against an environment, including automated password guessing
- Utilize wireless attack tools for Wifi networks.
- Launch web application vulnerability scanners such as ZAP.

Training Course for the Certification Exam:	Course Duration:	Course Provider:
SEC560: Network Penetration Testing and Ethical Hacking	5 Days	SANS

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

Introduction

Security personnel whose job duties involve assessing target networks, systems and applications to find vulnerabilities. The GXPN certifies that candidates have the knowledge, skills, and ability to conduct advanced penetration tests, how to model the abilities of an advanced attacker to find significant security flaws in systems, and demonstrate the business risk associated with these flaws.

Preparing for the GXPN Exam:

No specific training course is a required prerequisite for the exam . However, Candidates may choose to prepare for the GXPN exam by taking the SANS Training Course: SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking.

Exam Information:

- 1 proctored exam
- 75 questions
- Time limit of 3 hours
- Minimum Passing Score of 66%

Course Contents:

- Network Attacks for Penetration Testers
- Crypto, Network Booting Attacks, and Escaping Restricted Environments
- Python, Scapy, and Fuzzing
- Exploiting Linux for Penetration Testers
- Exploiting Windows for Penetration Testers
- Capture the Flag

Expected Accomplishments:

- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse engineer vulnerable code to write custom exploits

Prerequisites:

- Working knowledge of TCP/IP, cryptographic routines (DES, AES, and MD5); and the Windows and Linux command lines.
- SEC560: Network Penetration Testing and Ethical Hacking

Training Course for the Certification Exam:	Course Duration:	Course Provider:
SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking	5 Days	SANS

Etisalat Academy is the largest single-source provider of training and development solutions in the Middle East. For 30 years we have been providing consultancy and human capital development services to telecoms, government agencies, oil & gas companies, financial institutions and organizations across all industries and business sectors. Our solutions range from training and development programs in business, technology and leadership, to consultancy services in the areas of recruitment, team building, performance management, assessment centers and career development. Based in the United Arab Emirates and operating a 1,200,000 square feet training facility in Dubai, our partner network spans five continents and delivers world class training solutions to customers in many countries.

Training & Development

Seminars & Events

Corporate Facilities

Accommodation on Campus

Sports & Leisure Club

اتصالات
etisalat

أكاديمية اتصالات
etisalat academy
Skills | Solutions | Results

P.O. Box 99100 | Al Muhaisnah | Dubai | U.A.E.
Emirates Road (E311) | Exit 60
Phone +971 4 264 4444 | Fax +971 4 264 8888
info@etac.ae | www.etac.ae