Network Security Course

Distance Learning

G-CITI CAMPUS

Changing Lives Through Technology

What is Network Security?

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system.
It protects your computer network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Why study Network Security?

Network Security is one of the most important aspects to consider when working over the internet, LAN or other method, no matter how small or big your business is. While there is no network that is immune to attacks, a stable and efficient network security system is essential to protecting client data. A good network security system helps businesses reduce the risk of falling victim to data theft and sabotage. Once data is transferred from one company to another, the risk of data theft exists! Therefore we need Network Security staff to serve as a policeman over the internet to ensure that data travels safely.

ITS (Information Technology Specialist) Network security helps protect the organization workstations from harmful cyber attacks. It also ensures that shared data is kept safe and secure. Network security infrastructure provides several levels of protection to prevent attacks by breaking down information into numerous parts, encrypting these parts and transmitting them through independent paths thus preventing cases like eavesdropping. Company Data is crucial to protect, as it has become the currency of communication and transactions within the 4th Industrial Revolution!

Becoming a Networking Security Engineer will enhance the chances of your employability in the Information technology industry. As you have completed your ITS networking Certificate   Highlighting yourself as someone who strives for positive change, as well as an eagerness to learn the latest technologies could take you a long way in your career.

Why study ITS Databases at G-CITI Campus?

G-CITI Campus is a South African Accredited and Global / International IT College, that offers both qualifications and certifications in IT Training. With over 10 000 students completing a wide variety of Global / International Certifications, G-CITI Campus has become the leading IT College to obtain credentials in preparation for the 4th Industrial Revolution and the Digital Economy.

IT SPECIALIST EXAM OBJECTIVES

Our innovative approach to learning and skills development will help students go beyond what they have signed up for! Providing a holistic approach to learning and Job Readiness, we ensure a quality level of the services we offer With its course offerings, G-CITI Campus offers a range of partners, such as CompTIA, Microsoft, Adobe, ITS, Cert Nexus and Cisco, G-CITI Campus offers both online learning subscriptions, exam vouchers and simulation labs to enable students to learn online, conduct digital assessments and conduct vendor certifications online.

Boosting your technical skills by understanding the world of nNetworking Security and how it applies to your business and job role, or the career of your dreams, is one of the many reasons to upskill in this field. All of the modules on the course speak directly to the skills that employers are actively seeking within the Networking Security Development sector.

Studying ITS (Information Technology Specialist) Networking Security with G-CITI Campus through Distance Learning, will enable you to be prepared for the professional use of Networking as well as understanding how it is important for an organization.

Also, we have a range of **ITS** Certificates where the networking   is part of a family of certifications. See more certifications on our website: www.gciticampus.academy under **Distance Learning**

Potential Career Opportunities in Network Security

- Network Security Consultant
- Information Security Analyst
- Network Manager
- Network Technical Engineer

COST OF THE COURSE

WAS R 4 990.00 | NOW R 2 950.00

Deposit: R 2000.00

Balance: R 950.00 *(To be paid before undertaking final exam)*

Use the banking Details below for any payment

Bank Name: FNB
Account Name: Genesis CITI
Account Nr: 62563325755
Account Type: Cheque
Branch: Epping
Branch Code: 200810

Deposit Reference: ID Number

What is included in the course fees

Please, be aware that all course materials are only offered online. In other words, you will not be receiving any hard copies of the textbook, and you will need to access all the required content through your online classroom, where you'll be able to find the following course content:

- A digital textbook (PDF) focused on all the content you'll need to pass the exam successfully
- Videos and Learning material to ensure you are covered to understand practical concepts
- Practice files OR quizzes to accompany the step-by-step exercises in your textbook
- A PDF summary of everything you've covered in the textbook
- A study guide and exercise files to help you with your exam prep
- A set of mock exams to be covered before undertaking global exams.

This Course Fee includes your Certiport exam voucher.

Network Security

1. Defense in Depth

1.1 Identify core security principles

- Confidentiality, integrity, availability, non-repudiation, threat, risk, vulnerability, principle of least privilege, attack surfaces including IoT

1.2 Define and enforce physical security

- Site security, computer security, removable devices and drives, mantraps

1.3 Identify security policy types

- Administrative controls, technical controls

1.4 Identify attack types

- Buffer overflow, viruses, polymorphic viruses, worms, Trojan horses, spyware, ransomware, adware, rootkits, backdoors, zero day attacks/vulnerabilities, denial-of-service (DoS) attacks, common attack methods, types of vulnerability, cross-site scripting (XSS), SQL injection, brute force attack, man-in-the-middle (MITM) and man-in-the-browser (MITB), social engineering, keyloggers (software and hardware), logic bombs

1.5 Identify backup and restore types

- Full, incremental, differential

2. Operating System Security

2.1 Identify client and server protection

- Separation of services, hardening, patch management, reducing the attack surface, group policy (gpupdate and gpresult), secure dynamic Domain Name System (DNS) updates, User Account Control (UAC), keeping client operating system and software updated, encrypting offline folders, software restriction policies

2.2 Configure user authentication

- Multifactor authentication, enforcing password policies, remote access, using secondary sign-on to perform administrative tasks (Run As, sudo), domain and local user and group creation, Kerberos

2.3 Manage permissions in Windows and Linux

- File and folder permissions, share permissions, inheritance, moving or copying files within the same disk or on another disk, multiple groups with different permissions, take ownership, delegation

2.4 Facilitate non-repudiation using audit policies and log files

- Types of auditing, what can be audited, enabling auditing, what to audit for specific purposes, where to save audit information, reviewing log files

2.5 Demonstrate knowledge of encryption

- File and folder encryption, how encryption impacts moving/copying files and folders, drive encryption, TPM, secure communication processes (email, texting, chat, social media), virtual private network (VPN) encryption methods, public key/private key, certificate properties and services, Bitlocker

INFORMATION
TECHNOLOGY
SPECIALIST

3. Network Device Security

3.1 Implement wireless security

- Wireless security types (strength of encryption), service set identifiers (SSIDs), MAC filtering, default configuration (OOBE)

3.2 Identify the role of network protection devices

- Purpose of firewalls, hardware vs. software firewalls, network vs. host firewalls, stateful vs. stateless firewall inspection, security baselines, intrusion detection system (IDS), intrusion prevention system (IPS), security information and event manager (SIEM), content filtering, blacklisting/whitelisting

3.3 Identify network isolation methods

- Routing, honeynet, perimeter networks (DMZ), NAT/PAT, VPN, IPsec, air gap network, DirectAccess, virtual LAN (VLAN)

3.4 Identify protocol security concepts

- Tunneling, DNSSEC, network sniffing, well-known ports (FTP, HTTP, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LDAPS, SNMP, SMTP, IMAP, SFTP)

4. Secure Computing

4.1 Implement email protection

- Antispam, spoofing, phishing, and pharming, client protection, user training

4.2 Manage browser security

- Browser settings, cache management, private browsing

4.3 Install and configure anti-malware and antivirus software

- Installing, uninstalling, reinstalling, and updating; remediation, scheduling scans, investigating alerts

INFORMATION
TECHNOLOGY
SPECIALIST