Unit 29: Network Security

Unit code	**M/618/7443**
Unit level	**5**
Credit value	**15**

Introduction

‘Who is accessing my network?’ ‘A bank was hacked last week, did you hear about that?’ ‘Last night I blocked my neighbours from accessing their internet because they did not have a Wireless Equivalent Protection (WEP) or WPA (Wi-Fi Protected Access) key on their wireless.’ It is estimated that network security (NS) breaches occur every second worldwide, from small home networks to massive corporate networks. The cost to businesses is in billions, if not trillions. There are several methods, techniques and procedures that need to be implemented on a network in order for it to be ‘secure’. Sometimes basic procedures such as locking your network room, changing your password regularly, and putting a password on all your network devices, are all that is needed to achieve some basic network security.

This unit introduces students to the fundamental principles of network security practices. As systems administration and management are important tasks in the day-to-day functioning and security of information systems, poor or improper practices can lead to loss of data, its integrity, performance reductions, security breaches and total system failure. Special planning and provision need to be made for ongoing support of systems and networks, which account for a significant proportion of the IT budget. With the widespread use of computers and the internet for business customers and home consumers, the topic of security continues to be a source for considerable concern.

Among the topics included in this unit are: historical network security principles and associated aspects such as firewalls, routers, switches, MD5, SSL, VPN, AES, SHA-1/2, RSA, DES, 3DES; different types of public and private key cryptography such as Caesar cipher, IPsec; types of attacks that can be carried out on a network and methods of preventing attacks such as man-in-the-middle (MITM) (eavesdropping), Denial of Service (DoS), Distributed Denial of Service (DDoS) (ping); certificate authority (CA); ‘The Cloud’ security aspects and associated counter-measures such public cloud, private cloud, hybrid cloud, community cloud, Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), phishing, spoofing, DNS attack, SQL injection, Media Access Control (MAC) address spoofing/control. Firewalls and other Gateways can be used as a tool for Intrusion Detection and Prevention as they can be situated on the perimeter of the Network to provide security.

On successful completion of this unit, students will be able to confidently discuss several types of network security measures and associated protocols, and cryptographic types and configuration settings of network security environments.

They will also be able to test the security of a given network to identify and fix vulnerabilities. As a result, they will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Examine network security principles, protocols and standards

LO2 Design a secure network for a corporate environment

LO3 Configure network security measures for the corporate environment

LO4 Undertake the testing of a network using a Test Plan.

Essential Content

LO1 Examine network security principles, protocols and standards

The history of network security:

Formation and role of Computer Emergency Response Team (CERT), common and advanced cyber security threats and techniques, e.g. malware, DoS etc, network vulnerabilities, threat actors, threat actor tools, threat actor motivations and opportunities.

Network security devices:

Security frameworks, Authentication, Authorisation, Accounting (AAA), historical network security principles and associated physical and virtual aspects such as firewalls, routers and switches.

Network security protocols:

MD5, SSL, VPN, AES, SHA-1/2, RSA, DES, 3DES, IPsec.

Network protocols:

DNS, DHCP, HTTP, HTTPs, FTP, FTPs, POP3, SMTP, IMAP.

Network security cryptographic types:

Understand the types of cryptography, including symmetric encryption, asymmetric encryption and hashing.

Different types of public and private key cryptography such as Vigenère, Hash, Triple Data Encryption (3DES) and Feistel cipher.

The Advanced Encryption Standard (AES known as Rijndael), Data Encryption Standard (DES), Message Authentication Code (MAC).

Key Encapsulation Mechanisms (KEMs), Data Encapsulation Mechanisms (DEMs) and hybrid Public Key Encryption (PKE).

LO2 Design a secure network for a corporate environment

Planning a network:

Considerations must be thought through on what the network will be used for (purpose).

Backup, recovery and business continuity requirements.

Compliance with legislative and regulatory requirements.

Hardware and software considerations:

What hardware and software will be used on the network.

Size considerations:

Consideration of the size and distance between nodes on the network, use of public, private or hybrid connections between sites, who has access to the network, how connections are secured.

LO3 **Configure network security measures for the corporate environment**

Configure network security:

Select the appropriate tools and comply with organisational policies and processes when configuring and upgrading systems.

Configure network security measures such as firewalls, routers, switches, gateways, SSL, IPSec, HTTPs, FTPs, passwords and back-up devices.

Cybersecurity:

Explain the different threats posed to networks, e.g. malware and phishing, ransomware.

Identify different types of attacks on computer systems, illustrate the potential impact of different attacks.

Discuss ways in which system users affect system vulnerability and potential physical vulnerabilities to systems, data and information.

LO4 **Undertake the testing of a network using a Test Plan**

Testing methods:

Different testing methods, e.g. network scanning, penetration testing, vulnerability scanning, ethical hacking.

Testing in terms of checks on network connection speed, testing for network vulnerabilities, network connections types, e.g. cabled and wireless.

Collection and interpretation of relevant data to identify potential issues, e.g. latency, traffic, packet data, system logs.

Create a Test Plan:

Development of a test plan to include testing data, expected results, actual results.

Application of key behaviours to develop an effective test plan and correct defects, including consideration of cause and effect to design appropriate tests and test data.

Critical thinking and application root cause analysis to interpret results and identify and correct defects, e.g. critical thinking, effective questioning and deconstruction.

Comprehensively test all devices and the whole environment:

Tests should be carried out on all devices including firewall, servers, domain controllers, email servers, routers, switches, gateways and passwords.

Make recommendations:

Recommendations for improving the network security.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Examine network security principles, protocols and standards		**LO1 and LO2** **D1** Evaluate the importance of network security to an organisation.
P1 Discuss the different types of network security devices. **P2** Examine network security protocols and the use of different cryptographic types in network security.	**M1** Compare and contrast at least two major network security protocols.	
LO2 Design a secure network for a corporate environment		
P3 Investigate the purpose and requirements of a secure network according to a given scenario. **P4** Determine which network hardware and software to use in a secure network.	**M2** Create a design of a secure network according to a given scenario.	
LO3 Configure network security measures for the corporate environment		**LO3 and LO4** **D2** Critically evaluate the design, planning, configuration and testing of the network.
P5 Configure network security for a network.	**M3** Justify the choices made in the implemented network security configuration.	
LO4 Undertake the testing of a network using a Test Plan		
P6 Comprehensively test the network using a devised Test Plan.	**M4** Analyse the results of testing to recommend improvements to the network.	

Recommended Resources

Textbooks

Burns, B., et al (2009) *Hacking: The Next Generation.* O'Reilly.

Cole, E., et al (2008) *Network Security Fundamentals*. John Wiley & Sons, Inc.

Forouzan, B.A. (2008) *Introduction to Cryptography and Network Security.* London: McGraw-Hill.

Gollmann, D. (2006) *Computer Security*. Chichester: John Wiley.

Harris, S., et al (2004) *Gray Hat Hacking: The Ethical Hacker's Handbook.* McGraw-Hill.

Lammle, T. and Graves, K. (2007) *CEH: Official Certified Ethical Hacker Review Guide*. Sybex.

Lockhart, A. (2007) *Network Security Hacks: Tips & Tools for Protecting your Privacy.* 2nd edn. O'Reilly.

Manzuik, S., Gold, A. and Gatford, C. (2007) *Network security Assessment: from vulnerability to patch*. Rockland, Ma: Syngress Publishing.

Mather, T., Kumaraswamy, S. and Latif, S. (2009) *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly.

Scambray, J. and McClure, S. (2008) *Hacking Exposed Windows: Windows Security, Secrets and Solutions.* London: McGraw-Hill.

Schneier, B. (2000*) Secrets and Lies: Digital Security in a Networked World.* Chichester: John Wiley.

Sobrier, J., Lynn, M., Markham, E., Iezzoni, C. and Biondi, P. (2007) *Security Power Tools*, O'Reilly.

Stallings, W. (2005) *Cryptography And Network Security*. Rockland, Ma: Syngress Publishing.

Journals

The Computer Journal – Oxford Academic

Links

This unit links to the following related units:

Unit 2: Networking

Unit 5: Security

Unit 9: Computer Systems Architecture

Unit 27: Transport Network Design

Unit 39: Network Management

Unit 40: Client/Server Computing Systems.