## Program Content

| | | | |
|---|---|---|---|
| **Semester** | VI | | |
| **Course Code:** | IT6406 | | |
| **Course Name:** | Network Security and Audit | | |
| **Credit Value:** | 3 (2L + 1P) | | |
| **Core/Optional** | Core | | |
| **Hourly Breakdown** | Theory | Practical | Independent Learning |
| | 30 Hrs | 30 Hrs | 90 Hrs |

**Course Aim/Intended Learning Outcomes:**

**Aim**

Develop network security and auditing skills such as explaining basic concepts behind network security protocols and services, network security applications and implementations, and conceptual and practical knowledge of discovering, reporting and solving network compliance/security issues.

**Intended Learning Outcomes**

After following this course, students should be able to

- Describe examples of the types of threats and attacks that apply to different categories of computer and network assets.
- Design remote user authentication solutions using symmetric and asymmetric encryption.
- Discuss the principle concepts of a network access control system and access enforcement methods.
- Analyze different transport layer security protocols and integrate them into network solutions.
- Describe the technical details of email security implementations.
- Analyzing the security concepts of network protocols (DNSSEC, HTTPS, SSH).
- Analyze security requirements and apply Secure Virtual Private Networking (IP Security) solutions.
- Analyze computer networks and compile audit reports.
- Apply network auditing tools on both wired and wireless networks.
- Describe security concepts in cloud computing.
- Analyze perimeter security requirements and design solutions to minimize risks.

**Course Content: (Main Topics, Sub topics)**

| Topic | Theory (Hrs) | Practical (Hrs.) |
|---|---|---|
| 1. Computer and Network Security Concepts | 1 | 0 |
| 2. Transport Layer Security | 2 | 3 |
| 3. User authentication and Network Access Control | 5 | 5 |
| 4. Virtual Private Networks | 3 | 5 |
| 5. Network Perimeter Security | 4 | 5 |
| 6. Email security and Domain Name System Security | 2 | 4 |
| 7. Wireless Network Security | 2 | 4 |
| 8. Cloud Security | 2 | 0 |
| 9. IT Infrastructure Auditing Concepts | 5 | 0 |
| 10. IT Infrastructure Auditing and Remediation | 4 | 4 |
| **Total** | **30** | **30** |

**1. Computer and Network Security Concept (1 hours)**

1.1. Computer Security Concepts [Ref 1: Pg. (21-25)]
1.2. The OSI Security Architecture [Ref 1: Pg. (26)]
1.3. Security Attacks [Ref 1: Pg. (27-28)]
1.4. Security Services [Ref 1: Pg. (29-31)]
1.5. Security Mechanisms [Ref 1: Pg. (32-33)]
1.6. Fundamental Security Design Principles [Ref 1: Pg. (34-36)]
1.7. Attack Surfaces and Attack Trees [Ref 1: Pg. (37-40)]
1.8. A Model for Network Security [Ref 1: Pg. (41-42)]
1.9. Standards [Ref 1: Pg. (43)]

**2. Transport Layer Security (2 hours)**

2.1. Web Security Considerations [Ref 1: Pg. (547-548)]
  2.1.1.Web Security Threats
  2.1.2.Web Traffic Security Approaches
2.2. Transport Layer Security [Ref 1: Pg. (549-565)]
  2.2.1.TLS Architecture
  2.2.2.TLS Record Protocol Change Cipher Spec Protocol Alert Protocol
  2.2.3.Handshake Protocol Cryptographic Computations Heartbeat Protocol
  2.2.4.SSL/TLS Attacks
  2.2.5.TLSv1.3
2.3. HTTPS [Ref 1: Pg. (566)]
  2.3.1.Connection Initiation
  2.3.2.Connection Closure
2.4. Secure Shell (SSH) [Ref 1: Pg. (567-577)]
  2.4.1.Transport Layer Protocol
  2.4.2.User Authentication Protocol
  2.4.3.Connection Protocol

**3. User Authentication and Network Access Control (5 hours)**

- 3.1. Remote User-Authentication Principles [Ref 1: Pg. (474-477)]
- 3.2. Remote User-Authentication Using Symmetric Encryption [Ref 1: Pg. (478-481)]
- 3.3. Kerberos [Ref 1: Pg. (482-499)]
- 3.4. Remote User-Authentication Using Asymmetric Encryption [Ref 1: Pg. (500-501)]
- 3.5. Federated Identity Management [Ref 1: Pg. (502-507)]
- 3.6. Network Access Control [Ref 1: Pg. (520-522)]
- 3.7. Extensible Authentication Protocol [Ref 1: Pg. (523-526)]
- 3.8. IEEE 802.1X Port-Based Network Access Control [Ref 1: Pg. (527-528)]

**4. Virtual Private Networks (3 hours)**

- 4.1. Introduction to Virtual Private Networks
  - 4.1.1.Requirement of Remote Access and Private Communication
  - 4.1.2.Private Communication Technologies and Evolution
  - 4.1.3.VPN vs Secure VPN
- 4.2. IP Security Overview [Ref 1: Pg. (75-77)]
- 4.3. IP Security Policy [Ref 1: Pg. (668-672)]
- 4.4. Encapsulating Security Payload [Ref 1: Pg. (673-680)]
- 4.5. Internet Key Exchange [Ref 1: Pg. (684)]
- 4.6. Cryptographic Suites [Ref 1: Pg. (692)]

**5. Network Perimeter Security (4 hours)**

- 5.1. Intruders [Ref 1: Online Chapter 22.1]
- 5.2. Intrusion Detection [Ref 1: Online Chapter 22.2]
  - 5.2.1.Audit Records
  - 5.2.2.Statistical Anomaly Detection Rule-Based Intrusion Detection
  - 5.2.3.The Base-Rate Fallacy
  - 5.2.4.Distributed Intrusion Detection Honeypots
  - 5.2.5.Honeypots
- 5.3. Intrusion Prevention [Teachers Note]
- 5.4. Need for Firewalls [Ref 1: Online Chapter 23.1]
- 5.5. Firewall Characteristics and Access Policy [Ref 1: Online Chapter 23.2]
- 5.6. Types of Firewalls [Ref 1: Online Chapter 23.3]
- 5.7. Firewall Basing [Ref 1: Online Chapter 23.4]
- 5.8. Firewall Location and Configurations [Ref 1: Online Chapter 23.5]
- 5.9. Unified Threat Management [Teachers Note]
  - 5.9.1.Data Leakage Prevention (DLP)
  - 5.9.2.Deep Packet Inspection (DPI)

**6. Email Security and Domain Name System Security (2 hours)**

- 6.1. Email Security [Ref 1: Pg. (613-639)]
  - 6.1.1.Internet Mail Architecture [Ref 1: Pg. (613-616)]
  - 6.1.2.Email Formats [Ref 1: Pg. (617-624)]

6.1.3.Email Threats and Comprehensive Email Security [Ref 1: Pg. (625-626)]
6.1.4.S/MIME [Ref 1: Pg. (627-638)]
6.1.5.Pretty Good Privacy (PGP) [Ref 1: Pg. (638-639)]
6.2. Domain Name System Security [Ref 1: Pg. (639-658)]
6.2.1.DNSSEC [Ref 1: Pg. (639-642)]
6.2.2.DNS-Based Authentication of Named Entities [Ref 1: Pg. (643-644)]
6.2.3.Sender Policy Framework [Ref 1: Pg. (645-647)]
6.2.4.DomainKeys Identified Mail [Ref 1: Pg. (648-653)]
6.2.5.Domain-Based Message Authentication, Reporting, and Conformance [Ref 1: Pg. (654-658)]

**7. Wireless Network Security (2 hours)**
7.1. Wireless Security [Ref 1: Pg. (582-584)]
7.2. Mobile Device Security [Ref 1: Pg. (585-588)]
7.3. IEEE 802.11 Wireless LAN Overview [Ref 1: Pg. (589-594)]
7.4. IEEE 802.11i Wireless LAN Security [Ref 1: Pg. (595-609)]

**8. Cloud Security (2 hours)**
8.1. Cloud computing [Ref 1: Pg. (529-535)]
8.1.1.Cloud Computing Elements
8.1.2.Cloud Computing Reference Architecture
8.2. Cloud Security Risks and Countermeasures [Ref 1: Pg. (535-537)]
8.3. Data Protection in the Cloud [Ref 1: Pg. (537-541)]
8.4. Cloud Security as a Service [Ref 1: Pg. (541-544)]
8.5. Addressing Cloud Computing Security Concerns [Ref 1: Pg. (544)]

**9. IT Infrastructure Auditing Concepts (5 hours)**
9.1. The Need for Information Systems Security Compliance [Ref 2: Pg. (19-32)]
9.2. Auditing Standards and Frameworks [Ref 2: Pg. (83-106)]
9.3. Planning an IT Infrastructure Audit[Ref 2: Pg. (109-127)]
9.4. Conducting and IT Infrastructure Audit [Ref 2: Pg. (130-151)]
9.5. Writing IT infrastructure audit report [Ref 2: Pg. (155-165)]

**10. IT Infrastructure Auditing and Remediation (4 hours)**
10.1. Scope of an IT compliance audit
10.1.1. Compliance basics[Ref 2: Pg. (63-70)]
10.1.2. Introduction to IT Infrastructure auditing [Ref 2: Pg. (70-75)]
10.1.3. Maintaining IT compliance [Ref 2: Pg. (75-79)]
10.1.4. Compliance within user domain [Ref 2: Pg. (168-184)]
10.1.5. Compliance within workstation domain [Ref 2: Pg. (187-205)]
10.1.6. Compliance within LAN domain [Ref 2: Pg. (208-225)]
10.1.7. Compliance within LAN-to-WAN domain [Ref 2: Pg. (228-251)]
10.1.8. Compliance within the WAN domain [Ref 2: Pg. (255-271)]
10.1.9. Compliance within the remote access domain [Ref 2: Pg. (274-291)]
10.2. Network Auditing and Assessment Tools [Ref 3, Ref 4]
10.3. Network Security Issue Remediation and Infrastructure Hardening [Teachers Note]

**Teaching /Learning Methods:**
You can access all learning materials and this syllabus in the VLE: http://vle.bit.lk/, if you are a registered student of the BIT degree program.

**Assessment Strategy:**

**Continuous Assessments/Assignments:**
In the course, case studies/Lab sheets will be introduced, and students have to participate in the learning activities.

**Final Exam:**
Final examination of the course will be held at the end of the semester. The course is evaluated using a two hour question paper which consists of 4 structured questions.

**References/ Reading Materials:**


- **Ref 1.** Cryptography and Network Security, Principles and Practice, 7th Edition, William Stallings.
- **Ref 2.** Auditing It Infrastructures for Compliance, 2nd Edition, Martin Weiss; Michael G. Solomon
- **Ref 3.** https://nmap.org/docs.html
- **Ref 4.** https://www.wireshark.org/docs/