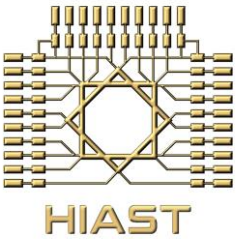
Syrian Arab Republic

Higher Institute for Applied Sciences and Technology



Course Specification Document

Title	Networks Security

Credits	3.5 ECTS

Aims	This course aims to provide the student with knowledge related to the security of data networks in various forms and configurations (including the threats and risks faced by these networks and setups) and the essential methods for protecting networks and information systems. It enables the student to use standards and procedures, including network security protocols and their applications, as well as software or hardware systems, to safeguard network security and detect intrusions.

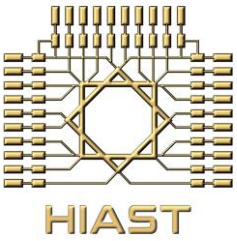
Intended learning outcomes

On successful completion of this course, the student will be able to:

- Recognize the most common types of threats faced by data networks, such as network attacks and malware, and understand the mechanisms behind these threats.
- Grasp the functioning of network security tools like firewalls and intrusion detection systems: their types, operational principles, and methods of utilization.
- Familiarize himself with standardized network security protocols and their applications, such as TLS, SSL, and IPSec.
- Recognize the risks and threats posed to operating systems and information centers and explore protective measures.
- Recognize the threats and risks associated with wireless networks and standard methods of safeguarding them.
- Recognize the threats and risks related to specific systems, such as the Internet of Things (IoT) and cloud computing.
- Avoid security vulnerabilities when designing a software.

Syllabus

- **Known network attacks and prevention methods:** DOS attacks, Spoofing, Flooding, Distributed DOS, Reflector and Amplifier, Responding to DOS attacks.
- **Malware:** Advanced Persistent Threat, Viruses, Worms, Social Engineering – Spam, Trojans, Information theft: Keylogger, phishing, spyware, Information theft: backdoors, rootkits, antivirus systems.
- **Physical network security:** Physical threats to infrastructure and equipment (cables, switches, routers), tools to prevent and mitigate physical threats, system recovery after a physical breach, integration of physical and logical security.



- **Intrusion detection systems:** Intrusion detection, analysis methods, host-based intrusion detection (HIDS), network-based intrusion detection (NIDS), distributed intrusion detection (DIDS), honeypots, example: Snort.
- **Firewall:** Firewall operation principles, access policies, types of firewalls, positioning and configurations of firewalls.
- **Network security standards and protocols and their applications:** SSL, TLS, SSH, IPSec, VPN, TOR.
- **Information centers and enterprise networks security:** Security at the MAC layer, Ethernet, Learning Bridging, VLAN, VLAN attacks, Spanning tree protocol, Attack on spanning tree, Switch Learning attacks, DHCP attacks.
- **Operating system security:** Windows Operating System Security, Linux Operating System Security.
- **Routing protocols security:** Threats to routing protocols, security techniques applied to RIP, OSPF, BGP attacks, SBGP, SOBGP protocols.
- **Wireless network security:** Threats to wireless networks, Wireless network security according to the 802.11 standard, 802.11i, Cloud Computing Security, Types of Cloud Computing, Threats, Risks, and Weaknesses in Cloud Computing, Security Considerations in Cloud Computing, Preferred Security Measures in Cloud Computing.
- **Internet of things (IoT) security:** Current state and applications of IoT, Importance of IoT Security, Confidentiality and Privacy of IoT according to ITU-T, Threats to IoT Networks, IoT Protection.