**Lecture topics and subtopics**

# Computer Network Fundamentals

## Network Architecture

## Protocols

## OSI Model and Layers

## TCP/IP Model

## Network Addressing and Subnetting

# Information System Security

## Security Goals (CIA)

## Risk, Threat, Vulnerability

## 7 IT Infrastructure Domains with Common Threats

## Security Policy Framework

## Data Classification Standards

## Security Principles

# Penetration Testing and Hackers

## Attack Phases/Stages

## Attack Motivations

## Intruder Types

## Social Engineering

## Information Gathering Sources

## Elicitation, Pretexting and Influence

# Attacks

## Threat Types (Fabrication, Interception, Interruption, Modification)

## HTTP and HTTPS

## TCP and UDP

## Passive and Active Attacks

## Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) Attacks

## Man-in-the-Middle (MITM) Attacks

## Session Hijacking and Countermeasures

# Malicious software

## Types of Malware and Explanation

## Business Threats

## Unsafe Employee Practices

## Security Countermeasures

# Access Control and Privilege Escalation

## Authentication Methods

## Access Control for Network Architectures

## Access Control Threats and Breaches

# IDS, IPS and Firewalls

## Firewall Types

## Intrusions

## IDS

# Auditing, Testing and Monitoring

## Auditing Planning

## Monitoring

## Log Information Types

## Network Mapping

## Testing Methods

## Honeypots

# Intro to Digital Forensics

## Evidence Gathering

## Mathematically Data Authentication

## Evidence Handling

# Network Forensics

## TAARA Methodology

## Network Evidence Sources

## Challenges of Network Evidence