ZÁKLADY BEZPEČNOSTI ICT

1. **Zabezpečení sítě pomocí síťových prvků**
   Základní pojmy (aktiva, hrozba, ochrana, bezpečnost, zranitelnost, riziko, incident a dopad), bezpečná konfigurace přepínače (obecně platný postup, útoky, bezpečnostní funkce, port security, port fast atd.), bezpečná konfigurace směrovače (obecně platný postup, útoky, bezpečnostní funkce, hardening, AAA (authentication, authorization and accounting) protokoly, testování nastavení atd.), firewally (základní pojmy, dělení, zástupci, vlastnosti a umístění v síti), zabezpečení 802.11 (WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2, používaná kryptografická primitiva, klíčové hospodářství, slabiny PSK (Pre-Shared Key), WPS (Wi-Fi Protected Setup)).

2. **IDS/IPS systémy a testování síťové infrastruktury**
   Problematika logování (log, kategorie, formát, obsah logu), hlavní cíle analýzy logů (rozdělení analýzy logů), operace nutné k automatické analýze záznamů, agregace, korelace, detekce na základě signatur, detekce na základě anomálií, IDS/IPS (Intrusion Detection System, Intrusion Protection System) (vzájemný vztah, efektivita, umístění, základní architektura, zástupci), útoky na odepření služeb - (D)DoS (Distributed Denial of Service) útoky (princip, rozdělení, popis základních útoků SYN Flood, HTTP Flood, Ping of Death), princip detekce a mitigace DoS, zátěžové testování (metodologie, typy testů, nástroje, report).

3. **Penetrační testování**
   Základní pojmy a definice, dělení penetračních testů (dle znalosti, způsobu realizace a cíle), metodologie testování, základních pět kroků testování, příklady nástrojů a výstupy pro jednotlivé fáze, penetrační testování síťové infrastruktury a webových aplikací (vzájemný vztah), OWASP (Open Web Application Security Project) (průzkum prostředí, mapování aplikace, testování vstupů, závěrečný report), OWASP Top 10, vysvětlení SQL-i a XSS (používané nástroje).

4. **Bezpečnostní protokoly a netechnické útoky**
   Protokoly IPsec a TLS (princip, umístění TCP/IP, průběh komunikace, autentizace, utajení a integrita dat), VPN použití, základy nastavení ve firemní síti, škodlivý software (rozdělení, definice), netechnické typy útoků, sociální inženýrství, phising (používané techniky), útoky MitM (ARP spoofing, DNS spoofing).