



Školní rok 2026/2027, pro studijní obor 79-41-K/41 Gymnázium

1. Úvod do kybernetické bezpečnosti

- základní pojmy (asset, hrozba, zranitelnost, riziko)
- cíle kybernetické bezpečnosti
- typy útočníků

2. Kybernetické útoky a jejich dopady

- charakteristika kybernetických útoků
- příklady kybernetických incidentů na úrovni uživatelů, firem a států
- dopady kybernetických útoků na organizace a uživatele

3. Security Operations Center (SOC)

- účel a fungování SOC
- činnosti vykonávané v SOC
- monitoring a analýza bezpečnostních událostí

4. Operační systém Windows

- charakteristika OS Windows – historie OS Windows, popis grafického rozhraní (GUI) a textového rozhraní (CLI)
- nástroje pro konfiguraci OS Windows v grafickém rozhraní a v příkazovém řádku
- nástroje pro sledování činnosti OS Windows v grafickém rozhraní a v příkazovém řádku

5. Architektura a princíp činnosti operačného systému Windows

- architektura systému Windows
- proces zavádění OS Windows
- procesy, vlákna, služby, správa paměti ve Windows, registr Windows

6. Zabezpečení operačního systému Windows

- nástroje pro sledování zabezpečení OS Windows
- správa aktualizací, místní zásady zabezpečení
- Windows Defender a firewall v OS Windows
- zásady pro bezpečné nastavení OS Windows

7. Linux v kybernetické bezpečnosti

- charakteristika a licencování Linuxu, pojem distribuce
- možnosti využití Linuxu v kybernetické bezpečnosti a v centru SOC
- možnosti zabezpečení počítače s Linuxem

8. Linuxové nástroje pro správu a zabezpečení

- základní příkazy Linuxu pro práci v shellu
- základní principy správy a zabezpečení linuxového serveru
- správa souborových systémů a oprávnění v Linuxu

9. Počítačové sítě – základní charakteristika, protokoly a modely

- účel počítačové sítě, rozdělení sítí podle velikosti
- síťové protokoly, sada protokolů TCP/IP
- referenční modely OSI a TCP/IP, zapouzdření dat

10. Počítačové sítě – Ethernet, IP, ICMP, ARP

- základní charakteristika protokolu Ethernet a protokolu IP
- základní principy adresování pomocí IP adres
- základní charakteristika protokolů ICMP a ARP

11. Počítačové sítě – protokoly transportní a aplikační vrstvy, síťové prvky

- základní charakteristika protokolů transportní vrstvy
- základní služby poskytované v síti – DHCP, DNS, NAT, FTP, TFTP, SMB, POP, IMAP, SMTP, HTTP
- zařízení pro komunikaci v drátové a bezdrátové síti

12. Technologie pro zabezpečení a sledování sítí

- architektury používané pro zabezpečení sítí
- zařízení a služby používané pro zabezpečení počítačových sítí
- základní způsoby a nástroje pro sledování sítí

13. Typy útočníků, ukazatele přítomnosti útočníka

- jednotlivci a organizované skupiny
- hacktivisté a státem podporované skupiny
- ukazatele přítomnosti útočníka – IoC, IoA

14. Nástroje používané útočníky, druhy útoků

- etický hacking versus penetrační testing
- charakteristika jednotlivých skupin nástrojů pro kyberútoky
- základní typy kyberútoků a jejich princip

15. Malware

- základní charakteristika malwaru
- viry, červi a trojské koně
- ransomware, spyware, rootkity a další druhy malwaru
- nejběžnější projevy malwaru a ochrana proti m alwaru

16. Útoky na protokoly IP, TCP a UDP

- struktura hlavičky paketu IPv4 a IPv6
- útoky využívající zranitelnosti protokolu IP
- útoky zneužívající protokol TCP
- útoky zneužívající protokol UDP

17. Útoky na protokoly ARP, DNS a DHCP

- funkce protokolů ARP, DNS a DHCP
- typické útoky na jednotlivé protokoly
- důsledky jednotlivých útoků na komunikaci v síti

18. Útoky na služby ve firemní infrastruktuře

- možnosti zneužití protokolů HTTP a HTTPS a obrana proti webovým útokům
- útoky využívající elektronickou poštu
- útoky na databáze

19. Základní principy ochrany před kybernetickými útoky

- použití principu Defense-in-Depth pro zajištění kybernetické bezpečnosti
- význam pravidel firem a zásad zabezpečení pro zajištění kybernetické bezpečnosti ve firmách
- nasazení zásad pro trend BYOD
- zajištění souladu s normami a standardy v oblasti zabezpečení

20. Řízení přístupu a Threat Intelligence

- základní principy řízení přístupu – modely CIA a ZeroTrust, způsoby řízení přístupu
- zabezpečení přístupu podle modelu AAA
- Threat Intelligence a zdroje informací o hrozbách

V Praze dne 1. 9. 2026

PhDr. Ing. Lukáš Hons v. r.
ředitel školy