Ainevaldkond	Informaatika ja küberturvalisus
Kursuse nimetus	Praktiline küberkaitse
Eelduskursused	Puuduvad. Eeldatakse tavapärast arvutikasutuse oskust ja huvi teema vastu.
Lõimumine	• informaatika – arvuti, operatsioonisüsteemid, virtualiseerimine, võrgud ja programmeerimine; • matemaatika ja loogika – probleemide lahendamine ning samm-sammuline mõtlemine; • inglise keel – IT- ja küberturbealane sõnavara; • ühiskonnaõpetus – digiturvalisus, vastutus, eetika ja seaduslik käitumine.
Kursuse maht ja õppekorraldus	1 kursus: 21 × 75 min. Kursus toimub intensiivõppena valikainete nädala jooksul. Kontakttunnid toimuvad arvutiklassis ning teooria seotakse võimalikult kiiresti praktiliste harjutustega. Igal õpilasel peab olema kasutada arvuti, millel on võimalik käivitada virtuaalset Linuxi masinat. Virtualiseerimise toimimine tuleb enne kursuse algust koos kooli IT-toega üle kontrollida.
Õpetamise aeg	I perioodi valikainete nädal (23.–27. november 2026)
Kursuse läbiviija(-d)	Henri Paas
Kursuse eesmärgid	• anda õpilasele arusaam küberhügieenist ning igapäevastest turvalistest digiharjumustest; • selgitada, kuidas arvuti, operatsioonisüsteem, virtualiseerimine ja internet „kapoti all“ töötavad; • õpetada Linuxi käsurea, lihtsa skriptimise ja programmeerimise põhitõdesid; • tutvustada arvutivõrkude, veebirakenduste ja turvalise programmeerimise põhimõtteid; • õpetada märkama turvariske ning mõistma, kuidas neid vähendada; • anda turvaline ja seaduslik võimalus proovida praktilist turvatestimist selleks loodud harjutuskeskkondades; • arendada probleemilahendust, iseseisvat uurimist, tehnilist mõtlemist ja oskust ise edasi õppida.
Kursuse lühikirjeldus	Kursus annab praktilise sissejuhatuse arvutite ja küberturbe maailma. Õpilased proovivad uusi teemasid võimalusel ise arvutis läbi; kursus ei ole üles ehitatud ainult loengutele. 1. Küberhügieen: paroolid ja paroolihaldurid, MFA, phishing, sotsiaalne manipuleerimine, uuendused, varukoopiad ning tundmatute USB-seadmete ja kaablitega seotud riskid. 2. Virtualiseerimine: virtuaalmasin, host, guest ja hypervisor ning virtuaalmasinate kasutamine eraldatud harjutuskeskkondade loomiseks. Tutvume ka Dockeri, image’ide ja container’ite põhimõtetega. 3. Linux: UNIXi ja Linuxi põhimõisted, kernel, shell, terminal, failisüsteem, kasutajad, protsessid, käsurida ja lihtne skriptimine. 4. Võrgundus: IP- ja MAC-aadressid, pordid, TCP/UDP, DNS, DHCP,

	NAT, Wi-Fi, HTTP/HTTPS, VPN ning võrgu uurimine tööriistadega nagu Nmap, Wireshark ja Burp Suite. 5. Programmeerimine: programmeerimise põhimõtted, lihtsad skriptid ja veebiserverid, HTTP suhtlus ning turvalise programmeerimise ja veebirakenduste turvalisuse põhialused. 6. Eetiline häkkimine ja turvatestimine: levinud turvanõrkused ja ründemeetodid, süsteemide ja veebirakenduste uurimine ning praktilised ülesanded spetsiaalsetes harjutuskeskkondades. 7. Lõppülesanne: õpilane tõendab enda valitud viisil, et on omandanud kursuse põhiteadmised ja oskab neid selgitada, seostada või praktiliselt rakendada. Turvatestimist tehakse ainult õpetaja määratud, selleks loodud või isoleeritud keskkondades. Kursuse osaks on küberturbe eetika ja seaduslikkuse põhimõtted.
Kursuse õpitulemused	• rakendab põhilisi küberhügieeni võtteid enda kontode, seadmete ja andmete kaitsmiseks; • selgitab virtualiseerimise põhimõtet ning virtuaalmasina ja container'i peamist erinevust; • selgitab lihtsas keeles Linuxi, operatsioonisüsteemi ja võrgu peamisi tööpõhimõtteid; • kasutab Linuxi käsurida tavapäraste ülesannete lahendamiseks ja koostab lihtsa skripti; • selgitab põhilisi interneti ja arvutivõrgu mõisteid ning kasutab lihtsaid vahendeid võrguühenduse uurimiseks; • koostab või muudab lihtsat programmi ning mõistab turvalise programmeerimise põhimõtteid; • tunneb ära levinumaid turvariske ja turvanõrkusi ning oskab kirjeldada, kuidas neid vähendada; • kasutab juhendamisel põhilisi turvatestimise tööriistu ainult selleks ette nähtud harjutuskeskkonnas; • mõistab, miks turvatestimiseks on vaja luba ning millised on eetilise ja seadusliku tegutsemise piirid.
Hindamine	Mitteeristav hindamine: AR (arvestatud) MA (mittearvestatud). Arvestuse saamiseks peab õpilane enda valitud viisil tõendama, et on omandanud kursuse põhiteadmised ja oskab neid oma sõnadega selgitada või praktiliselt rakendada. Praktilistes tegevustes tuleb järgida turvalise, eetilise ja seadusliku tegutsemise reegleid.
Õppematerjalid	• arvutiklass, kus igal õpilasel on oma arvuti; • virtualiseerimistarkvara ja ettevalmistatud Linuxi virtuaalmasin (nt Kali Linux); • veebibrauser, tekstiredaktor/programmeerimiskeskkond ning kursusel kasutatavad tasuta tööriistad; • õpetaja koostatud õppematerjalid, PowerPointi esitlused, juhendid, ülesanded ja spetsiaalselt õppetööks loodud harjutuskeskkonnad.

Kirjandus (soovituslik kirjandus)	• Kursuse põhiõppematerjal ja praktilised ülesanded: Google Drive õppematerjalid • õppematerjali „Lisad“ osades on iga teema kohta täiendavad videod, tasuta kursused, harjutuskeskkonnad, dokumentatsioon ja muud materjalid iseseisvaks edasiõppimiseks; • Riigi Infosüsteemi Ameti (RIA), OWASP-i, PortSwigger Web Security Academy ning kasutatavate tehnoloogiate ametlikud õppematerjalid ja dokumentatsioon.
Kursuse väljund	Kursuse väljund on lõppülesanne, mille vormi saab õpilane ise valida. Teadmisi võib tõendada näiteks suulise vestluse, esitluse, praktilise demonstratsiooni, testi või küsimustiku, oma projekti või õpimapi kaudu. Lõppülesande eesmärk on näidata, et õpilane mõistab kursuse põhiteemasid, oskab olulisemaid mõisteid oma sõnadega selgitada ning seostada küberhügieeni, virtualiseerimise, Linuxi, võrgunduse, programmeerimise ja turvatestimise teadmisi. Kõiki käske, porte või definitsioone ei pea pähe teadma.