HÖGSKOLAN I BORÅS

Taktisk cybersäkerhet
Tactical cyber security
7,5 högskolepoäng
7,5 credits

Ladokkod: A344TG
Revision: 1.0
Fastställd av: Utskottet för utbildningar inom teknik 2024-11-08
Gäller från: VT 2025

Nivå: Grundnivå
Huvudområde (successiv fördjupning): Datateknik (G1F)
Utbildningsområde: Teknik
Ämnesgrupp: Datateknik
Förkunskapskrav: Minst 3 hp från kursen “Cybersäkerhet för uppkopplade enheter”.
Betygsskala: U, 3, 4 eller 5

Innehåll
Denna kurs i taktisk cybersäkerhet ger en omfattande introduktion till de grundläggande principerna för kryptografi och hotbildsanalys. Kursen täcker centrala hotaktörer, hot mot informationssäkerhet, samt strategier för att identifiera och hantera dessa risker. Kursen kommer ge en fördjupad inblick i IT-säkerhet, inklusive övervakning och analys av nätverkstrafik. I kursen ingår även en genomgång av relevanta juridiska och etiska aspekter inom cybersäkerhet, såsom dataskyddslagar och etiska dilemman vid penetrationstestning. Praktiska moment inkluderar konfiguration av virtuella system och verktyg, grundläggande penetrationstestning samt incidenthantering.

Mål
Efter avklarad kurs ska studenten kunna, med avseende på,

Kunskap och förståelse
1.1 Redogöra för de teoretiska grunderna i kryptografi och steganografi,
1.2 Förklara hur moderna kryptografiska system används och vilka säkerhetsutmaningar de kan möta,
1.3 Beskriva de vanligaste cyberhoten samt olika typer av hotaktörer och deras motiv,
1.4 Redogöra för hur sårbarheter upptäcks, klassificeras samt hur risker bedöms och prioriteras för åtgärd,
1.5 Beskriva nätverksarkitekturer, metoder och tekniker för att nätverkssäkerhet skall upprätthållas,
1.6 Redogöra för tillämpliga lagar och regler inom cybersäkerhet, inklusive data- och EU-förordningar,
1.7 Beskriva komponenterna i en säkerhetsarkitektur och förklara hur de används för att skydda informationssystem och nätverk mot attacker och obehörig åtkomst.

Färdigheter och förmåga
2.1 Praktiskt övervaka och analysera nätverkstrafik för att identifiera avvikelser och potentiella säkerhetshot,
2.2 Konfigurera och använda system och tjänster i en virtualiserad miljö för att simulera och testa olika säkerhetsstrategier och metoder,
2.3 Bedöma, identifiera och analysera olika typer av cyberattacker samt föreslå lämpliga åtgärder för att minimera risken och skadan,
2.4 Tolka säkerhetsrisker för att utvärdera informationssystemens säkerhetsnivå och förmåga att motstå attacker,
2.5 Genomföra en strukturerad incidenthantering, från detektering till åtgärder som isolering och återställning efter säkerhetsincidenter,
2.6 Praktiskt använda grundläggande tekniker och metoder inom kryptografi.

Värderingsförmåga och förhållningssätt
3.1 Kritiskt granska och implementera tekniker och metoder för säkerhetstestande och säkerhetsåtgärder i enlighet med etiska riktlinjer och rådande lagverk,

3.2 Reflektera över och diskutera etiska dilemman som uppstår inom cybersäkerhetsarbete, såsom gränsdragningen mellan legala och illegala åtgärder vid säkerhetstestning och incidenthantering.

Undervisningsformer

Undervisningen i kursen består huvudsakligen av föreläsningar, övningar och laborationer.

Undervisningen bedrivs på svenska, men undervisning på engelska kan förekomma.

Examinationsformer

Kursen examineras genom följande examinationsmoment:

Tentamen
Lärandemål: 1.1–1.7
Högskolepoäng: 3
Betygsskala: U, 3, 4 eller 5

Laboration Malware
Lärandemål: 2.2, 2.3, 2.5 och 3.1 – 3.2
Högskolepoäng: 1
Betygsskala: Underkänd eller Godkänd

Laboration Kryptering
Lärandemål: 2.6
Högskolepoäng: 2
Betygsskala: Underkänd eller Godkänd

Laboration Analys & Åtgärd
Lärandemål: 2.1, 2.4
Högskolepoäng: 1,5
Betygsskala: Underkänd eller Godkänd

Omexamination av laboration begränsas till ett extra insatt laborationstillfälle under läsåret. Nästa tillfälle till omexamination av laboration sker då kursen ges reguljärt nästa gång.

Tentamen bestämmer kursens slutbetyg, vilket utfärdas först när samtliga moment är godkända.

Om studenten har ett beslut/rekommendation om särskilt pedagogiskt stöd från Högskolan i Borås på grund av funktionsnedsättning, har examinator rätt att anpassa examinationen. Examinator har att utifrån kursplanens mål avgöra om examinationen kan anpassas i enlighet med beslutet/rekommendationen.

Studentens rättigheter och skyldigheter vid examination är enligt riktlinjer och regelverk vid Högskolan i Borås.

Kurslitteratur och övriga läromedel

Diehl, Eric (2016). Ten Laws for Security (1st edition). Springer International Publishing.

Cisco, Cyberops Associate (online-material)

Ytterligare material som finns tillgängligt på kurssidan via HB:s lärplattform.

Studentinflytande och utvärdering

Kursen utvärderas i enlighet med gällande riktlinjer för kursvärderingar vid Högskolan i Borås, där studenternas synpunkter ska inhämtas. Kursutvärderingsrapporten publiceras och återkopplas till deltagande och blivande studenter i enlighet med ovan nämnda riktlinjer, och ligger till grund för framtida utveckling av kurser och utbildningsprogram. Kursansvarig lärare ansvarar för att utvärdering enligt ovan genomförs.

Övrigt

Obligatorisk närvaro gäller vid alla laborationer. Kursen ingår i IT-ingenjörsprogrammet