EN2720 Etisk hackning 7,5 hp

Ethical Hacking

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Fastställande

Kursplanen gäller från och med HT 2023 enligt skolchefsbeslut: J-2023-0148.Beslutsdatum: 2023-01-23

Betygsskala

A, B, C, D, E, FX, F

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik,Elektroteknik

Särskild behörighet

Kunskaper och färdigheter i grundläggande programmering, 6 hp, motsvarande slutförd kurs DD1310/DD1311/DD1312/DD1314/DD1315/DD1316/DD1318/DD1331/DD100N/ID1018.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten på en grundläggande nivå kunna

- upprätta resurser för att stödja offensiva säkerhetsoperationer
- utföra spaning och inhämtning för att planera operationer
- tillägna sig tillträdesuppgifter, t.ex. kontonamn, lösenord och åtkomsttoken
- etablera initialt fotfäste i nätverk och system
- exekvera skadlig kod på fjärrenheter
- upprätta kanaler för kommunikation med infekterade system
- eskalera rättigheter i system för att erhålla högre behörigheter
- bibehålla närvaro i nätverk efter avbrott
- förflytta sig lateralt i datornätverk
- undvika att upptäckas av nätverksförsvarare
- samla in och exfiltrera data från datornätverk
- bedöma säkerheten av datorsystem, tillämpningar och it-tjänster
- utföra lagliga och etiska säkerhetstester.

Detta kommer att ge studenterna en praktisk förståelse för angriparens möjligheter och förmågor, i syfte att utvärdera cybersäkerheten i datornätverk.

Kursinnehåll

Kursens huvudaktivitet utgörs av ett projekt där studenten självständigt angriper ett företags datornätverk i syfte att exfiltrera specifik information. Det angripna nätverket är riggat av kursledningen i en virtuell miljö. För att utföra angreppet är studenterna fria att använda sin fantasi och verktyg tillgängliga på Internet. Verktyg för nätverksskanning och sårbarhetsskanning, plattformar för utveckling av exploits, fjärrstyrning av datorer, lösenordsknäckning, m.m. presenteras under kursens gång, men det står kursdeltagare fritt att välja metoder och verktyg efter eget huvud.

Examination

- INL2 - Inlämningsuppgift, 0,5 hp, betygsskala: P, F
- PROA - Projekt, 7,0 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

Övergångsbestämmelser

Den tidigare inlämningsuppgiften INL1 har ersatts av INL2.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.