FEP3370 Avancerad etisk hackning 8,0 hp

Advanced Ethical Hacking

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

Fastställande

Skolchef vid EECS-skolan har 2023-01-18 beslutat att fastställa denna kursplan att gälla från och med VT 2023, diarienummer: J-2023-0093

Betygsskala

P, F

Utbildningsnivå

Forskarnivå

Särskild behörighet

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter genomförd kurs ska studenten 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.

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.

Dessutom förväntas studenten utveckla och testa ny skadlig kod för att utnyttja sårbarheter.

Examination

• EXA1 - Examination, 8,0 hp, betygsskala: P, 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.

Övriga krav för slutbetyg

- Inlämning av de datafiler som ska exfiltreras från det angripna nätverket
- Inlämning och godkännande av den egenutvecklade skadliga koden liksom testresultat
- Deltagande i alla seminarier

- Inlämning av veckovisa progressrapporter

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.