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

Kursplan för FEP3370 gäller från och med HT17

Betygsskala

Utbildningsnivå

Forskarnivå

Särskild behörighet

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter fullgjord kurs förväntas studenten därför kunna

- rekognoscera, identifiera och välja mål för angrepp, bland annat genom nätverksscanning,
- identifiera sårbarheter i nätverksutrustning och applikationer,

- förmedla och exekvera kod (exploits) på sårbara system,
- installera och använda programvara för fjärrstyrning av system,
- identifiera lösenordsfiler och utvinna löserord,
- exfiltrera data,
- vidta åtgärder för att stärka informationssäkerheten i ett nätverk.

Dessutom förväntas studenten kunna

- utveckla och testa skadlig kod för att utnyttja sårbarheter.

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.

Kursupplägg

Kursen är baserad i ett penetrationstestningsprojekt där studenterna förväntas exfiltrera ett antal datafiler från det angripna nätverket. Dessutom förväntas studenterna utveckla ny skadlig kod, vilken också testas under kursens gång. Utöver dessa praktiska moment erbjuds ett antal seminarier på relaterade tema, inklusive den etiska dimensionen av hackning.

Kurslitteratur

Rafay Balochs Ethical Hacking and Penetration Testing Guide, 2014 rekommenderas men är inte obligatorisk

Utrustning

Studenter förväntas använda sin egen dator, exempelvis genom att installera en penetrationstestningsdistribution som en virtuell maskin, i syfte att interagera med träningsnätverket.

Examination

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.