



HI2009 IT-säkerhet III: Laborationer 7,5 hp

IT-Security III: Computer Forensics Lab

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

Fastställande

Kursplan för HI2009 gäller från och med HT11

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Elektroteknik

Särskild behörighet

Genomgången kurs IT-säkerhet II, HI119V (tidigare 6H4082), eller motsvarande kunskapsnivå. Kunskaper i engelska motsvarande Engelska A/Engelska 5

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Denna högre kurs är avsedd som en direkt fortsättningskurs på IT-Säkerhet II, HI119V (tidigare 6H4082), 7,5p. Efter genomgången kurs skall deltagarna ha god praktisk kunskap om moderna undersökningsverktyg inom IT-Forensik. I kursen ingår bl.a. hur man undersöker och dokumenterar bl.a. datorer och mobiltelefoner. Kursen inkluderar ett flertal mjukvaruverktyg

Kursinnehåll

How to use typical Computer Forensics tools and techniques. Hard disk analysis, Mobile phone analysis, Sniffers, Network Monitoring. Wireless Surveillance.

Kursupplägg

Kursen är en distanskurs som ges på ca halvtid (beroende på studentens förkunskaper). Allt kursmaterial är på engelska. Det är fullt möjligt att genomföra hela kursen på distans. En kursdeltagare bör reservera ca 20-35 timmar/vecka för denna kurs, inkl. projektuppgifter och laborationer, lite beroende på tidigare utbildning och yrkeserfarenhet.

Kurslitteratur

Kursmaterial kan rekvireras från Högskolans Bokservice på Campus Haninge, telefon: 08-790 4885; e-post: bokservice@sth.kth.se.

Kurslitteratur: **Real Digital Forensics**, Jones, Bejtlich & Rose, Addison-Wesley, ISBN-10: 0321240693, ISBN-13:9780321240699.

Forensic Tools & Technology, Eoghan Casey, 2001, 448 pp, Academic Press, ISBN-10: 0121631036, ISBN-13: 9780121631031

Kurskompendium HI2009 på CD-ROM med laborationsmaterial, studieranvisningar och övningsuppgifter, programvara och referensmaterial. Förf. L.O. Strömberg.

Vi utgår från att studenterna redan har kursmaterialet från HI119V, och vi kommer i kursen att använda mjukvara och annat material som återfinnes i HI119V:s digitala kurskompendium och lab-kit (HI119V är

förkunskapskrav till denna kurs).

Utrustning

Tillgång till dator (PC med Windows XP, Vista 7 eller 8), browser och Internetanslutning krävs. Två fungerande e-postadresser är obligatoriska och måste anges i ansökan. Kursinformation utsändes endast per e-post. Inlämning av projektuppgifter kan endast ske via e-post. Vi använder SSS - Student Support System - i denna kurs. Detta Internetbaserade kurssupportsystem är skraddarsytt för yrkesverksamma studenter, som på ett säkrat sätt behöver kunna komma åt kursmaterial inifrån företag, myndigheter och länder med restriktiva

brandväggar, vilka oftast omöjliggör användning av traditionella utbildningsprogram, som kräver specifika öppna portar i organisationens brandvägg. I SSS erhålles normalt kvittens på alla insända kursuppgifter inom ca 5-10 minuter, dygnet runt. I vissa kurser ingår även en av textböckerna som e-bok i Kurskompendiet. Kurskompendiet distribueras därför på 3 CD-skivor ca 1,5 GB, och ej som nedladdningsbara filer på Internet.

Examination

- LAB1 - Laboration, 1,5 hp, betygsskala: P, F
- LAB2 - Laboration, 1,5 hp, betygsskala: P, F
- LAB3 - Laboration, 1,5 hp, betygsskala: P, F
- TEN1 - Tentamen, 3,0 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.

Tentamen ges i slutet på kursen, med möjlighet till omtenta i december och i maj. Tentamen, som är datorbaserad och på engelska, består av ca 60 flervalsfrågor och ca 8 beräknings/textfrågor. Tentamen kan avläggas på KTH eller, på begäran minst 30 dagar i förväg, på annat svenskt eller internationellt universitet eller svensk ambassad. Tentamen är på 3 poäng med betygsskala A-F. Resterande poäng är för laborationsuppgifter.

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.