



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 HT09

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 B.

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 Computer Forensics. 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 heltid. Under kursen erbjuds frivilliga kursmöten i form av heldagslaborationer i Haninge fem lördagar under augusti och september. Laborationerna går även att genomföra helt på distans. De frivilliga laborationerna på Campus Haninge ges på engelska. Allt kursmaterial är också på engelska. Det är fullt möjligt att genomföra hela kursen på distans. En kursdeltagare bör reservera ca 30-40 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.

Investigation;

Forensic Tools & Technology,

Eoghan Casey, 2001, 448 pp

Academic Press,

ISBN-10: 0121631036

ISBN-13: 9780121631031

Real Digital Forensics,

Jones, Bejtlich & Rose,

Addison-Wesley, 2005, 650 pp

ISBN-10: 0321240693

ISBN-13: 9780321240699

Digital Course Notes

IT-Sec III, 3 CDs, 1.5 GB, L.O.Stromberg

Vi utgår från att studenterna redan har kursmaterialet från HI119V (tidigare 6H4082), 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

- * A personal computer (PC) running Windows XP / Vista / 7
- * Internet access
- * two working email addresses (do not use free webmail clients, use POP3)
- * A scientific pocket calculator

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, 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.