Blekinge Tekniska Högskola
Institutionen för datavetenskap

Revision: 4
Dnr: BTH-4.1.1–0219-2018

KURSPLAN

Analys av illasinnad programvara (malware)

Malware Analysis

7,5 högskolepoäng (7.5 credits)

Kurskod: DV2582
Huvudområde: Datavetenskap
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Ämnesgrupp: Datateknik
Undervisningsspråk: Svenska men undervisning på engelska kan förekomma.
Gäller från: 2018-03-01
Fastställd: 2018-03-01

1. **Beslut**
   Denna kurs är inrättad av dekan 2017-12-20. Kursplanen är fastställd av prefekten vid institutionen för datalogi och datorsystemteknik 2018-03-01 och gäller från 2018-03-01.

2. **Förkunskapskrav**
   För tillträde till kursen krävs avklarade kurser i Programmering 12 hp, Realtids- och operativsystem 6 hp, Datakommunikation 6 hp samt genomgången kurs i Datorsystemsäkerhet 7,5 hp eller Nätverkssäkerhet 8 hp.

3. **Syfte och innehåll**

   3.1 Syfte
   Syftet med kursen är att studenten skall lära sig hur skadlig och illasinnad programvara (Malicous Software) kan analyseras på ett säkert sätt. En sådan analys är första steget i ett systematiskt angreppsätt för att förhindra eller neutralisera den skadliga programvaran. Fokus ligger på analys av avancerade metoder som används vid tillverkning av s.k. "cybervapen" och på praktiska motåtgärder för att detektera och oskadliggöra dessa.

   3.2 Innehåll
   - Olika tekniker för att attackera och smitta system med skadlig programvara
   - Utpressningsprogram (ransomware/scareware)
   - Botnets
   - Mobila hot under Android och iOS
   - Sårbarheter på web och i sociala nätverk
   - Rootkits and bootkits
   - Antivirustekniker
   - Data-mining för detektering och analys av skadlig programvara

4. **Lärandemål**
   Följande lärandemål examineras i kursen:

   4.1 Kunskap och förståelse
   Efter genomförd kurs ska studenten:
   - Kunna redogöra för klassificering av olika typer av skadlig programvara och känna till deras historik
   - Kunna förklara och exemplifiera beteendet för illasinnade programvaror, antivirustekniker och säkerhetsarkitekturer i Windows, Android och iOS

   4.2 Färdighet och förmåga
   Efter genomförd kurs ska studenten:
   - Kunna utföra rekonstruktion (reverse engineering) av programvara för ARM- och x86-processor arkitekturer
   - Kunna utföra statisk och dynamisk analys av skadlig kod under Windows, Android och iOS
   - Kunna sammanställa och dokumentera analys av skadlig kod på ett vedertaget sätt

   4.3 Värderingsförmåga och förhållningssätt
   Efter genomförd kurs ska studenten:

- Kunna värdera hotbilden baserad på utförd analys
- Kunna identifiera och verkställa lämpliga motmedel

5. Läraktiviteter

Kursen genomförs på campus och innehåller föreläsningar och laborationer (inklusive laborationsrapporter). Under föreläsningar presenteras de teoretiska aspekterna i kursen. Studenterna tillämpar innehållet från föreläsningarna i laborationerna.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
1810	Laboration 1	2,5 hp	GU
1820	Laboration 2	1,5 hp	GU
1830	Laboration 3	1 hp	GU
1840	Tentamen	2,5 hp	AF

Kursen bedöms med betygen A Utmärkt, B Mycket bra, C Bra, D Tillfredsställande, E Tillräckligt, FX Underkänd, något mer arbete krävs, F Underkänd.

I kurstillfällets kurs-PM framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

Kurslitteratur

Material från institutionen

10. Övrigt

Denna kurs ersätter kursen DV2567