**Blekinge Tekniska Högskola**
Institutionen för datavetenskap

**Revision:** 1
**Dnr:** BTH-4.1.14-0663-2021

# KURSPLAN

## Analys av skadlig programvara

### Malware Analysis

### 7,5 högskolepoäng (7.5 credits)

**Kurskod:** DV2613
**Huvudområde:** Datavetenskap, Programvaruteknik
**Utbildningsområde:** Teknik
**Utbildningsnivå:** Avancerad nivå
**Fördjupning:** A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

**Undervisningsspråk:** Engelska
**Gäller från:** 2022-01-17
**Fastställd:** 2021-09-01

1. **Beslut**
   Denna kurs är inrättad av dekan 2021-04-29. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2021-09-01 och gäller från 2022-01-17.

2. **Förkunskapskrav**
   För tillträde till kursen krävs minst 120 hp varav 90 hp inom ett tekniskt område och minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare.)

3. **Syfte och innehåll**

   **3.1 Syfte**
   Denna kurs syftar till att ge studenterna färdigheter för att analysera varierande typer av hot såsom nätfiske, avancerade långvariga hot (APTs), attacker mot sårbarheter (exploits), attacker mot leverantörskedjor, cybervapen och utpressningsattacker som har blivit populära.

   **3.2 Innehåll**
   Kursen ger en översikt av moderna säkerhetshot och nätfiske, attacker mot sårbarheter, skadliga implantat i office dokument, attacker mot leverantörskedjor, cyberspionage och utpressningskampanjer. Studenterna kommer att lära sig reverse engineering, statisk och dynamisk analys av skadlig programvara baserat på verkliga exempel för Windows och Android plattformar (IA-32/Intel® 64, ARM arkitekturer).

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

   **4.1 Kunskap och förståelse**
   Efter genomförd kurs ska studenten kunna:
   • Redogöra för moderna säkerhetshot som inkluderar nätfiske attacker, avancerade långvariga hot (APTs), attacker mot sårbarheter, attacker mot leverantörskedjor, cybervapen och utpressningsmjukvara)
   • Nå en god förståelse för reverse engineering, statiska och dynamiska tekniker för analys av skadlig programvara

   **4.2 Färdighet och förmåga**
   Efter genomförd kurs ska studenten kunna:
   • Identifiera skadlig programvara och nätfiske attacker
   • Analysera skadlig programvara för Windows och Androids plattformar

   **4.3 Värderingsförmåga och förhållningssätt**
   Efter genomförd kurs ska studenten kunna:
   • Utvärdera ett cyberhot
   • Välja lämpliga tekniker för upptäckt och analys av skadlig programvara

**5. Läraktiviteter**

Undervisningen sker i form av online föreläsningar, inspelat videomaterial, tillsammans med skrivet material, litteratur och forskningslitteratur. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare att ske via e-post, kursens lärplattform och via online möten.

**6. Bedömning och examination**

Examinationsmoment för kursen

| Kod | Benämning | Omfattning | Betyg |
|---|---|---|---|
| 2205 | Inlämningsuppgift 1 | 2,5 hp | GU |
| 2215 | Inlämningsuppgift 2 | 2,5 hp | GU |
| 2225 | Inlämningsuppgift 3 | 2,5 hp | GU |

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

**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**

Obligatorisk kurslitteratur:
Malware Reverse Engineering Handbook,
https://ccdcoe.org/library/publications/malware-reverse-engineering-handbook/
Referenslitteratur för vidare fördjupning:

- Reverse Engineering for Beginners, https://beginners.re/main.html
- Michael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition, 2012.
- Joshua J. Drake , Zach Lanier , et al. Android Hacker's Handbook, 2014.
- J. Saxe, H. Sanders. Malware Data Science. Attack detection and Attribution, 2018.