

KURSPLAN

Cybersäkerhet, 7,5 högskolepoäng

Cyber Security, 7,5 credits

Kurskod:	TCYK14	Utbildningsnivå:	Grundnivå
Fastställd:	2023-09-15	Utbildningsområde:	Tekniska området
Gäller fr.o.m.:	2026-08-31	Ämnesgrupp:	Övriga tekniska ämnen
		Fördjupning:	G1F Grundnivå, har mindre än 60 hp kurs/er på grundnivå som förkunskapskrav
		Huvudområde:	Informatik

Lärandemål

Efter genomgången kurs ska studenten:

Kunskap och förståelse

- visa kunskap om centrala begrepp och standarder inom cybersäkerhet
- visa förståelse för en SOC (Security Operations Center) och de roller som ingår i arbetet med en SOC
- ha kännedom om grundläggande begrepp inom IT-forensik

Färdighet och förmåga

- visa färdighet i penetrationstestning (etisk hackning) av IT-system
- visa förmåga att hantera incidenter i en IT-miljö
- visa färdighet i enklare IT-forensiska undersökningar
- visa förmåga att söka upp relevant forskning inom kursens område och presentera i ett kondenserat format.

Innehåll

Kursen går igenom cybersäkerhet och tekniska aspekter kopplat till informationssäkerhet. I kursen diskuteras begreppet SOC (Security Operations Center) och de rollerna som ingår i det arbetssättet. För att kunna hantera incidenter presenteras arbete med loggar, logghantering och forensik. Enklare penetrationstestning (etisk hackning) genomförs för att testa säkerheten hos system. Kursen innehåller också en fördjupning inom den senaste forskningen inom cybersäkerhet.

Kursen innehåller följande moment:

- Introduktion till cybersäkerhet, begrepp, standarder, etc.
- Arbete och olika roller i en SOC (Security Operations Center)
- Loggar och logghantering
- IT-forensik
- Penetrationstestning (etisk hackning)
- Incidenthantering
- Forskning inom cybersäkerhet

Undervisningsformer

Föreläsningar, seminarier och laborationer.

Undervisningen bedrivs på svenska men engelska kan förekomma.

Behörighetskrav

Grundläggande behörighet samt genomgången kurs i Nätverkssäkerhet, 7,5 hp (eller motsvarande kunskaper).

Examination och betyg

Kursen bedöms med betygen 5, 4, 3 eller U.

Poängregistrering av examinationen för kursen sker enligt följande system:

Examinationsmoment	Omfattning	Betyg
Tentamen ¹	3,5 hp	5/4/3/U
Laboration	3 hp	G/U
Seminarium	1 hp	G/U

¹Bestämmer kursens slutbetyg vilket utfärdas först när samtliga moment godkänts

Kurslitteratur

Observera att kurslitteraturen kan komma att ändras fram till åtta veckor före kursstart.

Debar, H. (2021). *The Cyber Security Body of Knowledge v1.1.0, 2021—Security Operations & Incident Management*. University of Bristol. www.cybok.org

Roussev, V. (2021). *The Cyber Security Body of Knowledge v1.1.0, 2021—Forensics*. University of Bristol. www.cybok.org

Stringhini, G. (2021). *The Cyber Security Body of Knowledge v1.1.0, 2021—Adversarial Behaviours*. University of Bristol. www.cybok.org

Lee, W. (2019). *The Cyber Security Body of Knowledge v1.0, 2019—Malware & Attack Technology*. University of Bristol. www.cybok.org

Referenslitteratur:

Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing.