KURSPLAN

Etisk hackning och penetrationstestning, 7,5 högskolepoäng

Ethical Hacking and Penetration Testing, 7.5 credits

Kurskod:	TEHS24	**Utbildningsnivå:**	Avancerad nivå
Fastställd av:	VD 2024-03-01	**Utbildningsområde:**	Tekniska området
Reviderad av:	Utbildningschef 2024-04-10	**Ämnesgrupp:**	DT1
Gäller fr.o.m.:	2024-08-01	**Fördjupning:**	A1F
Version:	2	**Huvudområde:**	Datavetenskap

Lärandemål

Efter genomgången kurs skall studenten:

Kunskap och förståelse
- ha kännedom om konceptet red team/blue team i cybersecurity operations
- ha kännedom om centrala standarder och ramverk för revisioner, sårbarhetsbedömningar och penetrationstester och deras del i den övergripande riskhanteringsprocessen
- visa kunskap om de olika stegen som ingår i metoder för penetrationstestning

Färdighet och förmåga
- visa färdighet i att använda vanliga verktyg för cybersäkerhetsbedömning och penetrationstestning
- visa förmåga att genomföra ett penetrationstest baserad på en fördefinierad metodik
- visa färdighet i att dokumentera och rapportera resultaten av ett penetrationstest

Värderingsförmåga och förhållningssätt
- visa insikt i de etiska och juridiska aspekterna av att genomföra ett penetrationstest

Innehåll

Etisk hacking är en avgörande del av att bedöma säkerhetsnivån i en organisation och är en viktig del av den övergripande riskhanteringsprocessen. Kursen fokuserar på penetrationstestning som ett verktyg för att testa cybersäkerheten i en organisations nätverk, system och processer. Kursen omfattar centrala standarder, ramverk och metoder för penetrationstestning. Under kursen kommer studenterna att få praktisk erfarenhet av vanliga verktyg som används för penetrationstestning.

Kursen innehåller följande moment:
- Begreppen etisk hacking och offensiv säkerhet
- Konceptet red team/blue team i cybersecurity operations
- Penetrationstestning som en del av riskhanteringsprocessen
- Standarder och ramverk för revisioner, sårbarhetsbedömningar och penetrationstester
- Metoder för penetrationstestning

- Verktyg för penetrationstestning
- Genomföra ett penetrationstest
- Dokumentation och rapportering av ett penetrationstest
- Etiska och juridiska aspekter av penetrationstestning

Undervisningsformer

Föreläsningar, laborationer och seminarium.

Undervisningen bedrivs på engelska.

Förkunskapskrav

Godkända kurser med lägst 90 hp i huvudområdet Datavetenskap, Informatik, Informationssystem, Datateknik eller motsvarande, samt genomgången kurs Översiktskurs cybersäkerhet, 7,5 hp eller motsvarande. Dessutom krävs kunskaper i Engelska 6 eller motsvarande.

Examination och betyg

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

Poängregistrering av examinationen för kursen sker enligt följande system:

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

[I] Bestämmer kursens slutbetyg vilket utfärdas först när samtliga moment godkänts.

Kurslitteratur

Kurslitteraturen fastställs åtta veckor före kursstart.

• Debar, H. (2021). The Cyber Security Body of Knowledge v1.1.0, 2021—Security Operations & Incident Management. University of Bristol. http://www.cybok.org Links to an external site.

• Stringhini, G. (2021). The Cyber Security Body of Knowledge v1.1.0, 2021—Adversarial Behaviours. University of Bristol. http://www.cybok.org Links to an external site.

• Lee, W. (2019). The Cyber Security Body of Knowledge v1.0, 2019—Malware & Attack Technology. University of Bristol. http://www.cybok.org Links to an external site.

• Forskningsartiklar enligt lärarens anvisningar