Kursplan

Fakulteten för teknik
Institutionen för datavetenskap och medieteknik

1DV704 Etisk hackning och penetrationstest, 7,5 högskolepoäng
Ethical Hacking and Penetration Testing, 7.5 credits

Huvudområde
Datavetenskap

Ämnesgrupp
Informatik/data- och systemvetenskap

Nivå
Grundnivå

Fördjupning
G1F

Fastställande
Fastställd 2025-06-25.
Kursplanen gäller från och med vårtermin 2026.

Förkunskaper
Inledande programmering 7,5 hp (1DV501), Datorsäkerhet 7,5 hp (1DV700), Systemadministration 7,5 hp (1DV721) samt Datornät – introduktion 7,5 hp (1DV701) eller motsvarande.

Mål

Efter avslutad kurs förväntas studenten kunna:
Kunskap och förståelse

- A.1 förklara etiska, juridiska och regulatoriska överväganden inom penetrationstestning och offensiv säkerhet,
- A.2 analysera samtida cybersäkerhetshot, angripares taktiker och försvarsmekanismer baserat på aktuell akademisk och industriell forskning, samt
- A.3 bedöma rollen av AI-drivna säkerhetsverktyg inom etisk hacking, inklusive

deras möjligheter, begränsningar och framväxande trender.

Färdighet och förmåga

- B.1 genomföra systematisk rekognoscering, sårbarhetsanalys och penetrationstestning med etablerade metoder,
- B.2 utnyttja sårbarheter i nätverk, webbapplikationer, molntjänster och operativsystem i kontrollerade miljöer med strikt efterlevnad av etiska riktlinjer, samt
- B.3 producera strukturerade penetrationstestningsrapporter och effektivt kommunicera resultat, exploateringssteg och evidensbaserade åtgärdsstrategier.

Värderingsförmåga och förhållningssätt

- C.1 kritiskt bedöma IT-säkerhetsrisker genom att syntetisera resultat från tekniska analyser och akademisk forskning,
- C.2 utvärdera de etiska, juridiska och samhälleliga implikationerna av offensiva säkerhetsmetoder, inklusive ansvarsfull rapportering, samt
- C.3 uppvisa professionell integritet och ett forskningsdrivet förhållningssätt vid tillämpning av penetrationstestningstekniker.

Innehåll

Denna kurs ger en djupgående utforskning av etisk hacking och penetrationstestning, och förser studenter med teoretisk kunskap, praktiska färdigheter och en kritisk förståelse av cybersäkerhetshot och försvarsmekanismer.

Grundläggande principer inom etisk hacking

- Juridiska, etiska och regulatoriska aspekter av penetrationstestning
- Ansvarsfull rapportering av sårbarheter och efterlevnad av regelverk
- AI:s roll inom cybersäkerhet och etisk hacking

Metodiker för penetrationstestning

- Rekognoscering, informationsinsamling och sårbarhetsanalys
- Exploateringstekniker för nätverk, webbapplikationer, molntjänster och operativsystem
- Strategier för post-exploatering: rättighetshöjning, persistens och lateral förflyttning

Offensiva säkerhetsverktyg och tekniker

- Branschstandardiserade verktyg: Metasploit, Burp Suite, Nmap, Wireshark
- AI-assisterade säkerhetsverktyg och automatiserad sårbarhetsbedömning
- Tekniker för att kringgå säkerhetsförsvar

Säkerhetsbedömning och rapportering

- Metodiker för riskbedömning och säkerhetsgranskning
- Strukturerad rapportering av penetrationstest och åtgärdsstrategier
- Kommunikation av resultat till både tekniska och icke-tekniska målgrupper

Forskning och framväxande trender inom etisk hacking

- AI-drivna offensiva säkerhetstekniker och angreppsinriktad machine learning
- Aktuell akademisk och industriell forskning inom penetrationstestning
- Etiska överväganden och den föränderliga hotbilden inom cybersäkerhet

Undervisningsformer

Undervisningen består av föreläsningar, seminarier och lärarledda laborationer. Laborativa moment genomförs självständigt eller i grupp. Deltagande i seminarier och laborationer är obligatoriska.

Examination

Kursen bedöms med betygen A, B, C, D, E eller F.

Betyget A utgör det högsta betygssteget, resterande betyg följer i fallande ordning där betyget E utgör det lägsta betygssteget för att vara godkänd. Betyget F innebär att studentens prestationer bedömts som underkända.

Bedömning av de studerandes prestationer sker genom individuell skriflig tentamen och praktiska uppgifter. De praktiska uppgifterna examineras genom inlämning av rapporter. För godkänt betyg på kursen krävs godkänt på alla moment. Slutbetyget bestäms från: skriftlig tentamen (40%) och laboration (60%).

Omexamination ges i enlighet med Lokala regler för kurs och examination på grundnivå och avancerad nivå vid Linnéuniversitetet.
I det fall student med funktionsnedsättning har rätt till särskilt pedagogiskt stöd beslutar examinator om anpassad eller alternativ examination.

Måluppfyllelse

Examinationen av kursen delas in i följande moment:
Modul 2601 Etisk hackning, laboration 4,5 hp med betygsskalan AF
Modul 2602 Etisk hackning, tentamen 3,0 hp med betygsskalan AF

Examinationsmomenten kopplas till lärandemålen enligt följande:
Modul 2601 kopplar till lärandemål: B.1, B.2, B.3, C.3
Modul 2602 kopplar till lärandemål: A.1, A.2, A.3, C.1, C.2, C.3

Kursvärdering

Kursvärdering genomförs under kursen eller i nära anslutning till kursens avslutning. Resultat och analys av genomförd kursvärdering ska skyndsamt återkopplas till de studenter som genomfört kursen. Studenter som deltar vid nästa kurstillfälle ska senast vid kursstart informeras om föregående kursvärderingsresultat och genomförda förändringar i kursen.

Kurslitteratur och övriga läromedel

Obligatorisk litteratur
Harper Allen et. al., *Gray Hat Hacking: The Ethical Hacker's Handbook*, senaste upplagan, McGraw Hill. Sidor 500 (700).

Material tillhandahålls av institutionen. Sidor 200.