



KURSPLAN

Penetrationstestning och etisk hackning

PEN testing and Ethical Hacking

7,5 högskolepoäng (7.5 credits)

Kurskod: DV2630

Huvudområde: Datavetenskap, Programvaruteknik

Utbildningsområde: Teknik

Utbildningsnivå: Avancerad nivå

Fördjupning: AIN - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Engelska

Gäller från: 2023-01-16

Fastställd: 2022-09-01

1. Beslut

Denna kurs är inrättad av dekan 2022-06-08. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2022-09-01 och gäller från 2023-01-16.

2. Förkunskapskrav

För tillträde till kursen krävs minst 120 hp varav minst 90 hp inom det tekniska området 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

Kursen ger en fördjupad förståelse av faserna i penetrationstestning, olika attackvektorer och förebyggande motåtgärder. Studenten lär sig att förstå och upptäcka svagheter och sårbarheter i informationssystem, utföra attacker samt kontrollera styrkan i befintliga säkerhetskontroller m.m.

3.2 Innehåll

- Introduktion och processer
- Footprinting och spaning
- Nätverksskanning, tunneling och firewall evasion
- Enumeration
- Sårbarhetsanalys
- Access attacks
- Sessionspoofing och kapning
- Trådlösa attacker
- Exploatering med Metasploit
- Efter exploatering och privilege escalation

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten kunna:

- Redogöra för nyckelfrågorna, inklusive att plåga informationssäkerhet världen, etisk hacking, informationssäkerhet lagar och standarder
- Visa förståelse för processerna inom informationssäkring samt neds inom penetrationstestning

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:

- Utföra rekognosering med de senaste teknikerna och verktygen.
- Utföra nätverks- och sårbarhetsskanning
- Utföra uppräknig
- Bryta säkerhetskontrollerna och utföra åtkomstattacker

- Utföra skript efter exploatering
- Öka privilegierna och kapa befintliga användarsessioner
- Utföra trådlösa nätverksattacker

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:

- Penetrationsprovning
- Analysera penetrationstestresultat

5. Läraktiviteter

Undervisningen sker i form av online-föreläsningar, inspelat videomaterial, nätlabbuppgifter och presentationer samt litteraturstudier. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare att ske via kursens lärplattform.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2305	Laboration 1	1,5 hp	GU
2315	Laboration 2	1,5 hp	GU
2325	Laboration 3	1,5 hp	GU
2335	Laboration 4	1,5 hp	GU
2345	Inlämningsuppgift	1,5 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

THE HACKER PLAYBOOK 3. Practical Guide to Penetration Testing Red Team Edition. Peter Kim. 2018. ISBN-13: 978-1980901754