Bedömningskriterier TDDE62

Modul **TEN1**

Lärandemål		Kriterier för betyg 3	Kriterier för betyg 5
1. förklara och använda säkerhetsterminologin och säkerhetsprinciperna som presenteras i kursen		- Känna till namn på och översiktligt kunna beskriva angreppsmetoder och skyddsmekanismer inom system- och nätverkssäkerhet. - Känna till och kunna redogöra för viktiga principer för design av säkra datorsystem och datornätverk	- I detalj kunna beskriva angreppsmetoder och skyddsmekanismer inom system- och nätverkssäkerhet. - Kunna relatera säkerhetsprinciper inom system- och nätverkssäkerhet till praktiska användningsfall och tekniker.
2. i ett givet sammanhang, a. identifiera säkerhetssvagheter hos ett givet system/nätverk, b. i detalj identifiera och förklara säkerhetshoten mot systemet/nätverket, c. föreslå lämpliga tekniker/metoder/designval för att mitigera säkerhetshoten mot systemet/nätverket	Nätverkssäkerhet	- Översiktligt kunna redogöra för säkerhetssvagheter i vanliga nätverksprotokoll och kommunikationstekniker. - Översiktligt kunna redogöra för protokoll och tekniker för säker kommunikation. - Kunna redogöra för funktionssätt hos vanliga skyddsmekanismer och skyddstekniker för nätverk (t.ex. brandväggar, IDS) och vilka typer av hot de kan mitigera.	- I detalj kunna redogöra för säkerhetssvagheter i vanliga nätverksprotokoll och kommunikationstekniker. - I detalj kunna redogöra för protokoll och tekniker för säker kommunikation.
	Systemsäkerhet	- Kunna redogöra för klassisk säkerhetsarkitektur och metoder för åtkomstkontroll i hårdvara och systemprogramvara, samt dess begränsningar. - Översiktligt kunna redogöra för moderna tekniker för utökad säkerhet i hårdvara och systemprogramvara (t.ex. trusted computing, isolering, skydd mot specifika attackmetoder). - Kunna redogöra för de vanligaste typerna av skadlig kod, och de hot de utgör för ett datorsystem. - Översiktligt kunna beskriva vanliga metoder för detektering och skydd mot skadlig kod på olika typer av enheter.	- Mer i detalj kunna redogöra för moderna tekniker för utökad säkerhet i hårdvara och systemprogramvara. - Mer i detalj kunna beskriva vanliga metoder för detektering och skydd mot skadlig kod. - I detalj resonera om samspelet mellan angripare och försvarare när det gäller skadlig kod, och hur detta påverkat den tekniska utvecklingen av både angrepps- och försvarstekniker. - Kunna resonera om svårigheter och fallgropar vid användning av maskininlärning/AI för detektering av skadlig kod.
		- Kunna redogöra för konsekvenserna av ett lyckat angrepp mot ett givet system/nätverk.	- Kunna kontrastera olika tekniker för skydd mot en viss typ av hot, och resonera om dess för- och nackdelar när det gäller, t.ex. prestanda, användarvänlighet, resursanvändning och kostnad.
3. förklara och tillämpa teknikerna och metoderna för upprätthållande av *privacy* som presenteras i kursen		- Kunna redogöra för viktiga begrepp inom *privacy* (t.ex., *anonymity*, *unlinkability*, *hard vs soft privacy*) - Känna till de viktigaste typerna av risker/hot inom *privacy*. - Översiktligt kunna redogöra för välkända tekniker för säkerställande av *privacy* i digital kommunikation. - Översiktligt kunna redogöra för, samt på mindre problem kunna tillämpa, viktiga metoder för upprätthållande av *privacy* vid databehandling i databaser.	- I detalj kunna redogöra för viktiga metoder för upprätthållande av *privacy* vid databehandling i databaser, samt resonera om graden av skydd de erbjuder i en given situation.

För betyg 4: samtliga kriterier för betyg 3 uppfyllda, samt huvuddelen av kriterierna för betyg 5.

Modul **LAB1**

Lärandemål	Kriterier för betyg G
4. för några utvalda tekniker, implementera säkerhetslösningar utifrån givna säkerhetskrav	Utifrån en given kravspecifikation för respektive uppgift, kunna: (1) implementera en brandvägg samt intrångsdetekteringspolicy för ett typiskt mindre företagsnätverk och (2) designa och implementera en autentiseringslösning med hjälp av en etablerad teknik för *trusted computing,* samt dokumentera respektive lösning i en skriftlig laborationsrapport.

Examinering

Tentamen omfattar 4 delar, motsvarande de 4 delområdena *nätverkssäkerhet*, *systemsäkerhet (hårdvara och systemprogramvara)*, *systemsäkerhet (skadlig kod)*, samt *privacy*.

För betyg 3 krävs minst 40% av maxpoäng på var och en av de 4 delarna, samt 55% av totalpoäng.

För betyg 5 krävs minst 70% av maxpoäng på var och en av de 4 delarna, samt 85% av totalpoäng.

För betyg 4 måste krav för betyg 3 vara uppfyllda, samt 75% av totalpoäng.

Preliminär totalpoäng är 32, med preliminär fördelning

	nätverkssäkerhet	systemsäkerhet	skadlig kod	privacy	**Totalpoäng**
Max	**10**	**10**	**6**	**6**	**32**
Krav betyg 3	4	4	2,5	2,5	18
Krav betyg 4	”	”	”	”	24
Krav betyg 5	7	7	4	4	27