Tentamen i Säkerhet (EDA625) för IT-programmen

060225 kl. 9.00 – 13.00

INGA HJÄLPMEDEL

Tentamen omfattar 2 stycken 15-poängsuppgifter som kräver ordentliga beskrivningar och förklaringar samt 10 stycken 3-poängsuppgifter som kan besvaras relativt kortfattat. Maxpoängen totalt är alltså 60. För betyget 3 krävs minst 30 poäng som får vara fördelade hur som helst mellan uppgifterna. Lycka till !

1. Ett mindre postorderföretag (10 anställda) i skiv- och bokbranschen har ett litet internt nätverk för administration och bokföring. Man skall nu skaffa en server för att lägga ut katalog/beställningstjänst på internet. Samtidigt vill man öppna en kontakt via internet med en filial (butik) på en annan ort. Konkurrensen är stor och satsningen bedöms som en överlevnadsfråga för att skaffa/behålla kunder och ekonomi. Man har en dataintresserad bland de anställda och tänker implementera det själv.

   Redogör utifrån de tre huvudkriterierna vilka hot och risker som kan finnas i samband med satsningen. Föreslå motiverade åtgärder. (15p)

2. Vid kommunikation över öppna datanät är kryptering ett viktigt hjälpmedel dels för att verifiera identiteten hos varje användare och dels för att hindra obehöriga från att läsa eller ändra data som skickas över nätet.

   Antag att du skall skicka en stor datamängd över ett öppet datanät, till en person som du inte känner sedan tidigare och inte heller planerar att ha kontakt med i fortsättningen. Antag också att du och mottagaren har kommit överens om att de data som skickas bör hållas hemliga för utomstående och därför behöver krypteras på lämpligt sätt.

   Beskriv hur krypteringen bör hanteras i den beskrivna situationen. Vilka krypteringsverktyg behövs för att lösa de olika delproblem som finns ? Motivera !
   (15p)

VÄND!

3. Säkerhetskopiering anses vara en viktig säkerhetsåtgärd eftersom fördelarna överväger dom nackdelar som trots allt finns. Ange en fördel och en säkerhetsmässig nackdel med säkerhetskopiering. (3p)

4. Ange eller beskriv viktiga punkter/rutiner/principer/åtgärder som du som systemansvarig administratör bör tillämpa för att upprätthålla en god förebyggande säkerhet. För full poäng skall minst sex olika punkter nämnas. (3p)

5. Beskriv den svaghet som finns hos alla överlagringskrypton (2p). Vilken är dess fördel?(1p) (3p)

6. Vad innebär begreppen Reference Monitor, Security Kernel och TCB (Trusted Computing Base) (3p)

7. Vilka är de tre huvudsatserna i säkerhetsmodellen BLP (Bell LaPadula). Vad är svagheterna hos modellen? (3p)

8. Förklara vad som menas med en envägsfunktion och ge två exempel på situationer då envägsfunktioner används. (3p)

9. Förklara vad som menas med stark autentisering. (3p)

10. En lösenordstestare kan prova en dictionary attack, en brute force attack eller replay. Vilka skyddsmekanismer kan användas mot respektive teknik? (3p)

11. Brandväggar kan vara av typen paketfilter eller applikations-gateway (proxy). Förklara kort vad resp. typ kan göra (2p). Vad är en DMZ (demilitariserad zon) (1p) (3p)

12. Hur fungerar (i princip) en 1) DoS-attack, 2) Buffer overflow och 3) IP-spoofing (3p)