EKSAMEN
TK2100 Informasjonssikkerhet
Tillatte hjelpemidler: Ingen **Varighet:** 3 timer **Dato:** 2019-xx-xx
I alle oppgavene teller deloppgavene a), b) og c) 5 % hver, mens deloppgave d) teller 10 %

Det anbefales å svare kort og konsist på alle oppgavene, men på alle deloppgave d) på hver av oppgavene forventes det et mer omfattende svar.

Oppgave 1. Generelt (25 %)
a) Definer «informasjonssikkerhet». Ta utgangspunkt i CIA-modellen.

b) Hva er GDPR? Hva har GDPR til hensikt å beskytte?

c) Hva innebærer begrepet «penetrasjonstesting»? Hvorfor utfører man dette?

d) Drøft hva som er de største truslene mot din egen informasjonssikkerhet. Beskriv de viktigste tiltakene for å redusere risiko.

Oppgave 2. Kryptering (25 %)
a) Forklar hvordan et Substitution Cipher fungerer? Dekrypter den krypterte teksten «JVA» som er kryptert med ROT-13 krypteringen.

b) Hva er krypteringsmetoden AES? Nevn minimum 1 modus som kan brukes i AES kryptering og hva som gjøres med krypteringsnøkkelen for hver blokk i denne modusen.

c) Hva er TLS? Hvilken av de følgende TLS oppsettene er mest sikre, og hvorfor:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA

d) Forklar hva som menes med «public key» (asymmetrisk) kryptering. Forklar forskjellen på public key kryptering og public key nøkkelutveksling. Gi ett eksempel på hver av disse og forklar hvordan de fungerer.

Oppgave 3. Operativsystemet og Malware (25 %)

a) Forklar hvordan et anti-virus program fungerer og hvordan et anti-virus program oppdager malware.

b) Forklar hvordan adgangsrettigheter på filer fungerer i operativsystemet Unix/Linux.

c) Forklar hvordan Buffer Overflow fungerer, ta utgangspunkt i et lavnivå programmeringsspråk som C/C++?

d) Hva er et rootkit? Beskriv hva formålet med et rootkit er, og forskjellige teknikker et rootkit kan bruke for å oppnå dette. Tegn og forklar hvordan et rootkit kan skjule en fil i operativsystemet ved å endre funksjonen NtQueryDirectoryFile.

Oppgave 4. Nettverk (25 %)

a) Forklar hvordan et SMURF angrep fungerer? Hva slags type angrep er dette?

b) Forklar hvordan ARP spoofing / poisoning gjennomføres.

c) Hva er en phishing epost? Drøft truslene ved at dette kan brukes som en del av et målrettet hacker angrep mot et selskap.

d) En web server håndterer login av brukere, brukernavn og passord skrives inn i to input felter på en web side, og koden som sjekker om brukerens passord er riktig slår opp i en SQL database på denne måten:

```
Set rst = Conn.Execute( " SELECT * FROM Users WHERE
Username = ' " + txtUser.Text + " ' AND Password = ' "
+ txtPassword.Text + " ' ");
```

Hvilken input verdier kan en hacker oppgi i input feltene for å få tilgang til brukeren 'Bengt' sin konto, uten å kunne passordet, ved å bruke sårbarheten SQL Injection? Hvorfor kan websiden utnyttes på denne måten? Beskriv andre angrep som kan utføres mot denne serveren ved å bruke SQL Injection.

Slutt på oppgavesettet.