Fasit til eksamensoppgaver – nettverk og sikkerhet (uke 45)

Oppgave 1:

Sikkerhetstiltak - konfidensialitet

Hvilke av følgende er sikkerhetstiltak som kan bidra til å oppnå sikkerhetsmålet konfidensialitet?

Velg ett eller flere alternativer:

- [ ] Benytte sjekksumalgoritmer for data som skal overføres i nettverk.
- [ ] Bruk av tofaktor-autentisering for systemer som behandler konfidensielle (✔ a.
- [ ] Benytte diskkryptering ved lagring av data. ✔
- [ ] Benytte HTTPS framfor HTTP som protokoll i nettverkskommunikasjon. ✔
- [ ] Bevissthetstrening for alle som behandler data. ✔

Oppgave 2:

Digital signatur

Et konsulentfirma har kunder over hele landet. De ønsker å erstatte den tungvinte prosessen med å signere kontrakter med med penn på papir med en digital variant av signatur som kan garantere at det er kunden og ikke en svindler som signerer avtalen. De har hørt om en metode som kalles *digital signatur*, som kanskje kan gi dem nødvendig bekreftelse på identiteten til den som signerer en kontrakt digitalt.

a) Hva kjennetegner det som i informasjonssikkerhet kalles en *digital signatur*:
Velg ett eller flere alternativer:

- [ ] Kan bekrefte avsenders identitet ovenfor mottager. ✔
- [ ] Baserer seg på symmetrisk kryptering.
- [ ] Kan bekrefte avsenders identitet ovenfor en tredjepart (uavviselighet). ✔
- [ ] Sikrer konfidensialitet for meldingen som signeres.

b) Hvilke *kryptografiske nøkler* er involvert når *digital signatur* benyttes :
Velg ett eller flere alternativer

- [ ] Mottagers private nøkkel.
- [ ] Senderens offentlige nøkkel. ✔
- [ ] Mottagers offentlige nøkkel.
- [ ] Symmetrisk nøkkel generert av sender.
- [ ] Symmetrisk nøkkel generert av mottager.
- [ ] Senderens private nøkkel. ✔

Oppgave 3:

Peer-to-peer

Hvilke utsagn er sanne?
En peer-to-peer aksessmodell...
Velg et eller flere alternativer

- har én sentral tjener som mottar forespørsler fra mange klienter.
- har likeverdige vertsmaskiner som samarbeider om å levere en tjeneste. ✔
- brukes kun til ulovlige tjenester.
- har et distribuert eierskap. ✔
- kan bidra til å unngå at et selskap eller en statsmakt har kontroll over tjenesten. ✔

Oppgave 4:

HTTP - Del 1

Hvilket av disse utsagnene er korrekt for en persistent forbindelse i HTTP?
Velg et eller flere alternativer

- Nyttelasten sendes mange ganger uavhengig av nettverksforhold for å være sikker på at de kommer frem.
- TCP-forbindelsen fortsetter å forsøke å koble seg opp, selv om den blir avsluttet eller brutt.
- HTTP-forespørsler kan ikke multiplekses over denne forbindelsen.
- Den samme TCP-forbindelsen blir gjenbrukt til flere runder med nye HTTP-forespørsler. ✔

Oppgave 5:

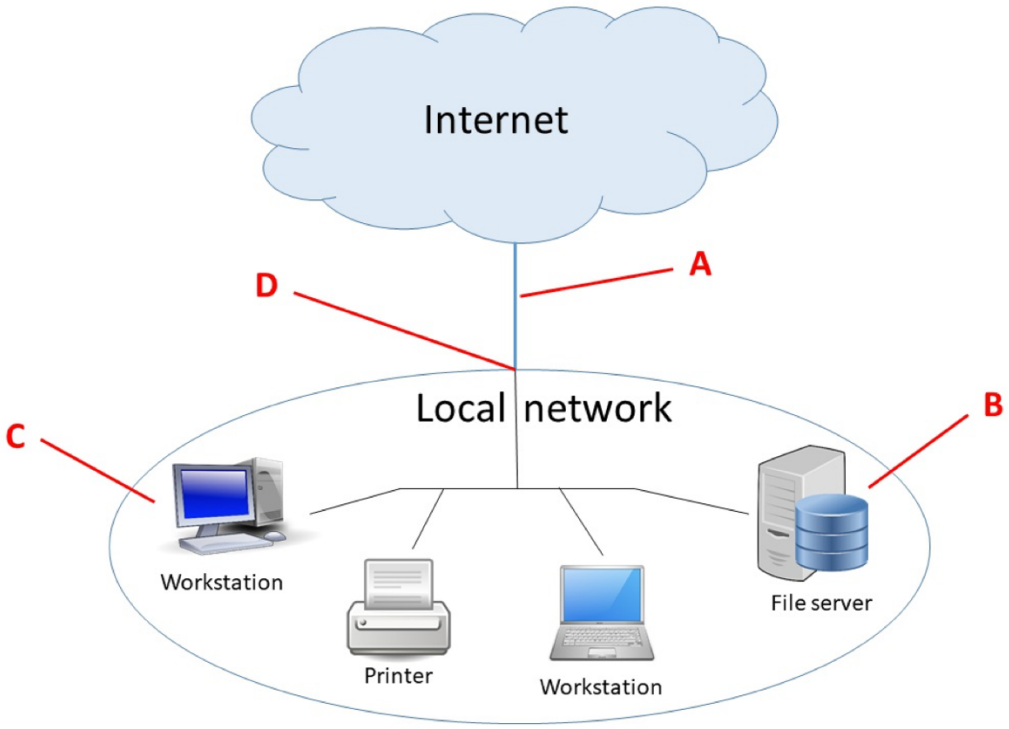
HTTP - Del 2

Hvilke utsagn er sanne?
Multipleksing av HTTP-forespørsler...
Velg et eller flere alternativer

- ...betyr at klienten sender flere forespørsler, og tjeneren kan sende svar på alle i samme rekkefølge som forespørslene kom inn.
- ...betyr at tjeneren kan "gjette" hvilke forespørsler som kommer og sende svar før den har mottatt forespørselen.
- ...innebærer at for hver forespørsel som sendes, må man vente på svar før neste forespørsel sendes.
- ...betyr at klienten sender flere forespørsler, og tjeneren kan sende svar på alle i en rekkefølge bestemt av tjeneren selv. ✔

Oppgave 6:

Sikkerhetstiltak 2



Figuren over illustrerer et lokalt nettverk knyttet til internett.

Hvilke sikkerhetstiltak passer inn på hvilke sted i figuren? Knytt sammen bokstav med tiltaket du mener passer.

	A	C	B	D
Kryptert trafikk	✔			
Innbruddsdeteksjon				✔
Brannmur				✔
Sikkerhetskopiering			✔	
Brukeropplæring		✔		

Oppgave 7:

Trusselmodellering 1

Et helseforetak behandler og lagrer en rekke opplysninger om pasienter, til dels av sensitiv karakter. Systemet er lukket, og ikke tilkoblet andre nettverk enn det interne nettverket for akkurat dette systemet.

Hvilke av følgende utsagn vil du betegne som sanne på bakgrunn av disse opplysningene:
Velg et eller flere alternativer

- [x] Fysisk sikring av systemets endenoder (f.eks. de ansattes arbeidsplassmaskiner) er spesielt viktig
- [x] Helseforetaket bør ha en nøye utarbeidet policy for hvilke ansatte som har tilgang til å lese, endre og slette opplysninger om hvilke pasientene.
- [ ] Å sikre sporbarhet er ikke viktig hvis man har gode mekanismer for autentisering på plass, for eksempel tofaktor-autentisering.
- [ ] Siden systemet er lukket er det ingen risiko for angrep utenfra, og det er derfor ikke nødvendig å prioritere sikring av informasjon høyt.

Oppgave 8:

Skadevare

Skadevare er en samlebetegnelse på programvare som med hensikt gjør skade på et datasystem.

Knytt sammen riktig funksjon og benevnelse på skadevaren:

	Orm	Bakdør	Tastelogger	Logisk bombe	Virus
Sprer seg på egenhånd til andre datasystemer	✓				
Gir tilgang til et system via ukjent inngang		✓			
Kjøres når spesielle forhold inntreffer eller oppfylles				✓	
Sprer seg når det kjøres					✓
Overvåker all tastatur-input fra brukeren			✓		

Oppgave 9:

Brukerautentisering og passord

Stortingets IT-organisasjon skal utarbeide et nytt, felles system for brukerautentisering til alle IT-systemene på Stortinget. De har besluttet at det skal benyttes passord som autentiseringsfaktor.

Det å utarbeide et trygt system og gode rutiner for å håndtere og lagre passord er viktig i ethvert system som involverer brukerautentisering med passord. Nedenfor er det listet fire krav som Stortinget har satt til passordhåndtering i sitt system.

For hvert krav, velg det mest relevante sikkerhetstiltaket for å sørge for å oppfylle kravet:

	Tilgangskontroll	Komplekse passord	Bruke salting	Bruke hash-algoritme
Forhåndsutregnede hash-tabeller skal ikke kunne benyttes for enkel passordknekking.	○	○	✓	○
Det skal være vanskelig for angripere å knekke passord lagret i databasen, også når passord er både saltet og hashet.	○	✓	○	○
Det skal ikke være mulig å lese passord i klartekstform i databasen.	○	○	○	✓
Kun autoriserte enheter/personer skal kunne lese passord-databasen.	✓	○	○	○

Oppgave 10:

Risikoanalyse

Hvilke **to hovedelementer** er sentrale når det skal gjennomføres en risikoanalyse av et IT-system?
Velg to alternativer:

- [x] Konsekvens av en hendelse
- [x] Sannsynlighet for en hendelse
- [ ] Mulige rootkit
- [ ] Verdibasert trusselidentifikasjon
- [ ] Angrepsvektor som benyttes

Oppgave 11:

Trusselmodellering

For enkelhets skyld benytter en liten gruppe ansatte i en underavdeling i Forsvarsdepartementet en og samme brukeridentitet og passord for å autentisere seg i et saksbehandlingssystem.

Denne gruppen ansatte har en superbrukerrolle i saksbehendlingssystemet, som medfører utvidede privilegier sammenlignet med en ordinær ansatt i departementet. Blant annet har de privilegier til å både endre og slette *alle* lagrede dokumenter og saker.
Velg de utsagnene som er korrekte med bakgrunn i dette scenariet.

- [ ] Så lenge de ansatte har de samme privilegiene har det ingen hensikt å utstyre hver enkelt ansatt med en egen brukeridentitet.
- [ ] Det er mindre sannsynlig at passord kommer på avveie når det kun er ett felles passord å håndtere.
- [x] Selv om de ansatte har de samme privilegiene er det nødvendig å kunne knytte hendelser til enkeltpersoner, og dermed enkeltbrukere, for å sikre sporbarhet.
- [x] Når hendelser i saksbehandlingssystemet ikke kan knyttes til en enkeltperson kan det være vanskelig å etterprøve endringer i systemet som skyldes for eksempel menneskelige feil.

Oppgave 12:

DNS

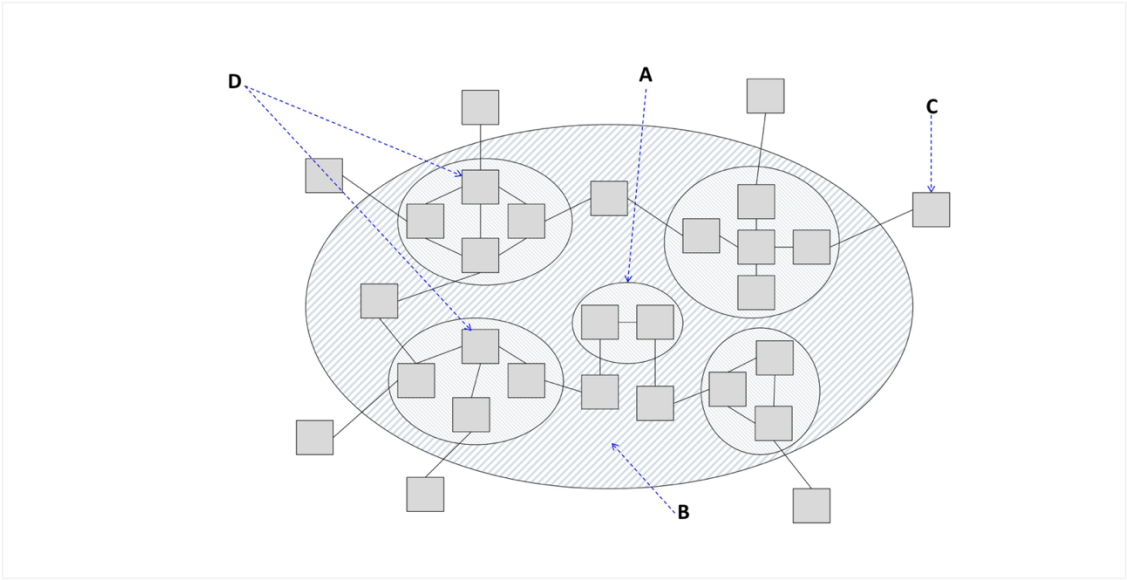
Hva er DNS-prefetching?

Velg et eller flere alternativer

- [ ] En tjeneste mellomlagrer MAC-adressen til webtjenere for raskt oppslag.
- [ ] En nettleser slår opp IP-adressen på alle domenenavn (URLer) den finner i et webdokument for å spare tid i tilfelle brukeren trykker på linken. ✔
- [ ] En hjemmerouter lagrer DNS-oppslag slik at brukeren ikke behøver å kontakte en rottjener.
- [ ] En tjener mellomlagrer hjemmesider, slik at forespørselen ikke trenger å gå helt til kilden.

Oppgave 13:

Topologi i Internett



Hva er riktig navn på etikettene?

Velg ett alternativ

- ○ A) Gateway, B) Intermedate system, C) Router, D) Endesystem
- ○ A) Server, B) Gateway, C) Intermediate system, D) Subnett
- ○ A) Subnett, B) Nettverk C) Endesystem D) Intermediate system ✔
- ○ A) Repeater, B) Bridge, C) Gateway, D) Gateway

Oppgave 14:

Behandling av personopplysninger

Institutt for informatikk ønsker å teste en nytt datasystem for gjennomføring av eksamen, som bl.a gjør det mulig for studentene å programmere Python under selve eksamenen.

Datasystemet instituttet vil benytte er en ren sky-tjeneste fra en ekstern leverandør, tilgjengelig gjennom en web-applikasjon. Både lagring av data og kjøring av applikasjonen skjer på leverandørens datautstyr som står fysisk plassert i et EU-land, mens selve eksamen gjennomføres/avlegges via en nettleser på UiOs datamaskiner i UiOs lokaler.

Den enkelte student får utdelt et unikt kandidatnummer og et unikt passord, som de bruker når de skal logge inn i systemet for å avlegge eksamen. En levert besvarelse knyttes til en student gjennom studentens kandidatnummer.

Vurder følgende utsagn, og velg de du mener er korrekte med utgangspunkt i opplysningene gitt over.

Velg ett eller flere alternativer:

- [ ] Institutt for informatikk er juridisk ansvarlig for at informasjon om studentene og deres eksamensbesvarelse behandles i samsvar med personvernregelverket. ✔
- [ ] Navn eller fødselsnummer lagres ikke i systemet, og det er dermed ikke nødvendig å forholde seg til personvernregelverket.
- [ ] Studentene har rett til å få vite hvilke opplysninger om dem som behandles i systemet. ✔
- [ ] Fordi tjenesten helt og holdent er levert av andre, er Institutt for informatikk er ikke juridisk ansvarlig for at informasjon om studentene og deres eksamensbesvarelse behandles i samsvar med personvernregelverket.

Oppgave 15:

Overføring

Du ønsker å laste ned en fil på 50 megabyte, og den maksimale nedlastingshastigheten på din Internettforbindelse er 20 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

Velg et eller flere alternativer

- 2,5 sekunder
- 50 sekunder
- 10 sekunder
- 20 sekunder ✔