NB! Dette er et forenklet løsningsforslag. Spesielt tekstoppgavene bør ha noe mer utdypende svar enn stikkordene

Del 1. Sant/usant – 25 % / 30-45 min

Du skal her svare på om påstanden er sann eller usann.

NB! Feil avkrysning vil telle negativt, slik at det ikke lønner seg å gjette.

1. VPN sikrer deg mot phishing. U
2. HTTPS sikrer deg mot XSS (Corss-site scripting). U
3. Backup kan være nyttig for integritetskontroll. S
4. Backup kan være nyttig for konfidensialitet. U
5. Backup kan være nyttig for tilgjengelighet. S
6. Dersom et antivirusverktøy klarer å fjerne en skadevare helt fra maskinen, vil også alle konsekvensene av nyttelasten bli tilbakestilt. U
7. Å sende data via POST-forespørsler er vesentlig sikrere mot avlytting enn å sende via GET-forespørsler. U
8. HTTPS sikrer konfidensialitet i overføring, samt autentisering av parten(e). S
9. Å lukke porter og/eller fjerne tjenester på en maskin øker sannsynligheten for at noen kan utnytte exploits mot deg. U
10. For å kunne utføre autentisering er det viktig og først ha utført autorisering. U
11. EXIF er en teknikk for å oppdage virus. U
12. Det vil kunne være mulig å benytte en mobils Wifi til å detektere en persons (mobils) tilstedeværelse, selv om man ikke er tilkoblet et trådløst nett. S
13. For å forfalske en basestasjon (lage et nett med samme SSID) må man først være påkoblet denne basestasjonen. U
14. Ved å benytte et utviklerpanel i nettleseren (typisk F12-tasten) kan vi endre kildekoden (HTML/CSS/JS) bak en nettside vi besøker, slik at fremtidige besøkende på denne nettsiden får se den manipulerte informasjonen. U
15. En av farene ved ukjente trådløse nett er automatisk tildeling av DNS-server. S
16. Om du kobler på et trådløst nett driftet av en hacker blir det svært enkelt for hackeren å lese av innholdet også i HTTPS-trafikk. U
17. Begrepet security passer bedre enn begrepet safety når vi snakker om

datasikkerhet i forbindelse med datakriminalitet. S

18. Dersom en hacker får tilgang til en brukers informasjonskapsler kan dette bl.a. medføre session hijacking. S
19. *Ciphertext* og *meldingen som skal krypteres* er to begreper som dekker det samme, og kan benyttes om hverandre. U
20. Trojanere kjennetegnes først og fremst ved at de svært effektivt, og nærmest "på egenhånd", spres rundt i nettverket. U
21. En web-trojaner (CSRF/XSRF) vil alltid være koblet mot en GET-forespørsel. U
22. Loggfiler er sentralt i forbindelse med non-repudiation. S
23. Inputvalidering kan også forhindre ulike denial of service-angrep. S
24. Ved å endre et offers innstillinger for DNS-server kan vi få webadresser (domenenavn) til å peke på phishingsider, uten at dette lar seg avsløre gjennom selve URLen i nettleseren. S
25. Det er per definisjon ikke mulig å oppdage/varsle noen former for *social engineering* angrep ved hjelp av tekniske løsninger. Det er kun brukerens fornuft som kan avdekke disse angrepene. U

Del 2. Flervalg – 20 % / 30-45 min

Det er kun ett alternativ som er riktig på hver oppgave. Dersom du svarer flere alternativer vil dette telle som feil svar. Merk deg at oppgavene etterspør det alternativet som er mest riktig eller best beskrivende.

NB! Feil avkrysninger vil telle negativt, slik at det ikke lønner seg å gjette.

1. Det beste sikkerhetstiltaket mot XSS (Cross-site scripting) er? B
   a) Skru av JavaScript hos brukeren.
   b) Inputvalidering.
   c) Detektere endringer i brukers IP-adresse.
   d) Oppgradere nettleser og operativsystem.
2. Hva menes med *mail spoofing*? C
   a) Å hindre at mail kan bli sendt (en form for *denial of service*).
   b) Å sende så mye mail til en bruker at all reel mail forsvinner i mengden.
   c) Å sende mail som ser ut til å komme fra en annen avsender.
   d) Å sende ut svindler via mail. Typisk phining-angrep.

3. Hva menes med begrepet *heuristikk* i forbindelse med virus? A

a) En metode for å oppdage virus.
b) En metode for å isolere virus.
c) En metode for å spre virus.
d) En metode for å fjerne virus.

4. Hvilken påstand passer best om lagring av verdier i cookies for en utvikler? D

a) Alle verdier i en nettside bør lagres i cookies, ettersom de da er sikrere hos brukeren i stedet for i serveren (som er et yndet mål for hacking).
b) Alle verdier i en nettside bør lagres i cookies, ettersom GDPR krever at brukeren har tilgang på sine data.
c) Alle verdier i en nettside bør lagres i cookies, ettersom man da slipper sesjoner og problemet med session hijacking.
d) Cookies bør unngås til kritiske verdier i en nettside ettersom de lagres hos brukeren.

5. Hvilken påstand beskriver et *botnet*? C

a) Et kriminelt nettverk som har satt hacking i system (ofte styrt av mafia).
b) Et nettverk som benytter kunstig intelligens til å avsløre svindler og skadevare.
c) Et nettverk av infiserte maskiner som styres av en eller flere hackere.
d) Et nettverk av servere (honeycombs) som ønsker å tiltrekke seg hackere, og som har spesiell programvare for å avsløre dem.

6. Følgende egenskap ved *private/public key*-kryptering gjør at man ofte foretrekker den fremfor *secret key*-kryptering? C

a) Algoritmen bak private/public key er mye sterkere fordi den utelukkende baserer seg på primtall som er umulige å knekke med dagens matematikk.
b) Vi trenger to nøkler (en til krypteringen og dekrypteringen). Dette er sikrere enn én enkelt nøkkel. Vi kan da også oppbevare de to nøklene på ulike steder for å forhindre at noen får tak i begge
c) Man slipper å utveksle en hemmelig nøkkel.
d) Secret key er alltid best.

7. Ved å besøke en (for oss ukjent) webserver som har *HTTPS* er vi sikre på at? A

a) Vi ikke blir utsatt for man-in-the-middle angrep/avlytting.
b) Vi ikke kan bli utsatt for webtrojanere og cross-site scripting, da dette er en sikker kommunikasjon mot serveren.
c) Vi ikke kan bli sporet i våre handlinger.
d) Alle de tre andre alternativene er korrekte.

8. Hvilket av følgende passord vil i snitt ta lengst tid å finne ved hjelp av de tre teknikkene bruteforce, ordliste og gjetting i kombinasjon? A

a) storebananerblomstrer
b) =a45
c) qazwsx
d) michael89

9. For å sikre at en fil blir permanent slettet er det viktig å? B

a) Tømme papirkurven (recyle bin) etter at man har slettet en fil.
b) Randomisere dataposisjonene der fila lå fila med 0-ere og 1-ere.
c) Overskrive filsystemtabellen der fila lå med 0-ere og 1-ere.
d) Randomisere filsystemtabellen der fila lå med 0-ere og 1-ere.

10. Sikkerhetsmessig bør man kun koble til en trådløs basestasjon som benytter følgende teknolgi i kommunikasjonen? A

a) WPA
b) WEP
c) VPN
d) DHCP

11. Hvilken teknologi er mest sentral i oppsett av en demilitarisert sone? B

a) ARP
b) Brannmur
c) VPN
d) DHCP

12. Innen datasikkerhet er en snubletråd? C

a) Noe hackere legger inn for å detektere bruk av systemet.
b) Noe hackere legger inn for å hindre bruk av systemet.
c) Noe systemeier legger inn for å detektere hacking.
d) Noe systemeier legger inn for å hindre hacking.

13. En logisk bombe er? D

a) En type/kategori av skadevare.
b) En hackerteknikk som hindrer at de logiske kretsene i en CPU kan utføre riktige beregninger.
c) En hackerteknikk som spiller på å forvirre de logiske slutningene en bruker tar (en variant av social engineering).
d) Noe som trigger utførelsen av et payload/nyttelast.

14. En hacker som tester bedriftens systemer, uten å fått beskjed om/tilatelse til å gjøre det, men som rapportere feil som finnes, kalles ofte for en? B

a) White hat hacker.
b) Gray hat hacker.

c) Black hat hacker.
d) Red hat hacker.

15. Begrepet *denial of service* kan best beskrives som? D

a) En teknikk som gjør at dersom et hackingforsøk blir oppdaget av systemet, blir systemet automatisk stengt (nektet tilgang til tjenesten).
b) En metode som skjuler tjenestene som kjører på serveren (maskinen nekter for at tjenesten finnes). Dette er spesielt nyttig i forbindelse med *portscanning*.
c) Noen krever at en tjeneste som blir eller kan bli misbrukt av hackere for videre angrep stenges ned.
d) En hacker gjør en tjeneste utilgjengelig.

16. For en krypteringsalgoritme slik som DES vil en dobling av nøkkelens lengde gjøre følgende endringer på tiden det tar å knekke en kryptert melding? D

a) Halvere tiden.
b) Ingen endring.
c) Doble tiden.
d) "Mangedoble" tiden.

17. GDPR gjelder følgende bedrifter (velg den som passer **best**)? D

a) Alle bedrifter med mer enn 20 milliarder euro i omsetning
b) Alle bedrifter i Norge
c) Alle bedrifter i Europa
d) Alle bedrifter med europeiske kunder

18. Beste sikkerhetstiltak mot web-trojanere (CSRF/XSRF) for en bruker er? B

a) Skru av JavaScript.
b) Logg ut av tjenester når man er ferdige med å bruke de.
c) Sørge for å ha oppdatert programvare.
d) Brukeren kan ikke gjøre noe fra eller til. Det er utvikleren som må legge til sikkerhetstiltakene.

19. I kurset og på labbene har dere fått demonstrert flere varianter av reverse shell. Hva er dette? A

a) Et angrep der man benytter skadevare som kjøres hos offeret.
b) En teknikk for å sikre maskiner mot angrep.
c) Et angrep som benytter et bestemt exploit mot tjenester og programvare hos offeret.
d) En teknikk for å detektere angrep.

20. Spear phishing er? A

a) Phishing som er målrettet mot et offer eller en gruppe offer gjennom å være basert på spesifikk informasjon om offeret.

b) Phishing som benytter skadevare for å komme gjennom filtre (for eksempel SPAM-filter).

c) Et av de få mottiltakene man har mot phishing der man gjennom heuristikk klarer å fange opp kjennetegn på phishing.

d) Ingen av punktene stemmer.

Del 3 – Faktaspørsmål - 40 % / 1,5 time

Husk at det ikke er mengden tekst, men hvor godt innholdet er, som teller. Enkelte oppgaver kan besvares som punktlister.

Oppgave 3.1 – 10 %

a) Forklar hva en hash-funksjon(sjekksum) er.

- Lager en liten "oppsummering" av fila/tekst.
- En liten/bevisst endring i fila/tekst vil gi en totalt annen sjekksum.
- Umulig å finne to filer/tekster som gir samme hash
- Umulig å finne tekst ut i fra hash

b) Hva kan en hash-funksjon benyttes til innen datasikkerhet. (Flere svar her)

- Signering av filer(man krypterer sjekksum med en privat nøkkel)
- Nedlastingav filer (en (((signert))) sjekksum forteller at fila er korrekt)
- Deteksjon av skadevare (signaturen kan være en sjekksum) – lite omtalt i pensum
- Lagring av passord (kun hash lagres)
- Ved overføring av data kan sjekksummen benyttes for integritetskontroll
- Sjekksummer av applikasjoner kan benyttes for å detektere endringer (tripwire - for eksempel rootkits og trojanere)

Oppgave 3.2 – 15 %

a) Forklar kort de ulike hovedmomentene/-stegene i å lage en risiko- og sårbarhetsanalyse (ROS-analyse). Dersom du ønsker å benytte deg av tabeller i forklaringen, og sliter med å få til dette i eksamensverktøyet, kan du sette de opp tekstlig og beskrive evt. farger med ord/fargenavn.

(må ikke svare i eksakt disse punktene bare hovedideen er med. Punkt 8-12 er ikke en direkte del av oppgaven.)

1. Planlegging og organisering
    1. Kategorier av sannsynlighet
    2. Kategorier av konsekvens
2. Hva er akseptabel risiko?
3. Identifisere sårbarheter/hendelser

4. "Gjette på" sannsynlighet og konsekvens for hver sårbarhet/hendelse
5. Beregne risiko (Risiko = sannsynlighet * konsekvens) for hver sårbarhet/hendelse
6. (Plotte i tabell for oversikt) – Tegne opp tabellen her…

	K1	K2	K3	K4
S1			H3	
S2				H2
S3		H1		
S4				

7. Hva er de viktigste truslene / Hvilke har en ikke-akseptabel risiko?
8. Hvordan sikre?
9. Utføre
10. Teste
11. Evaluere
12. Gå til start...

b) Forklar kort noen fordeler og ulemper med denne typen analyse

(Ingen absolutt liste)

- Fordeler:
  - Tvinges til å gjøre noe
  - Standardisert metode
  - Får oversikt
  - Får sortert farer
  - ((Fine farger og rapporter)))
  - Systematisk prosess
- Ulemper:
  - Metode blir i fokus => Mer viktig enn hva som kommer ut
  - Stort sett gjettinger
  - Gjettinger/unøyaktigheter leder til "fikses/ikke fikses"
  - Tar ikke med "kostnader for å fikses" i prioriteringen
  - Ledelsen synes de har gjort en god jobb og lagd en fin rapport
  - Metodikken sikrer "behandling" av det man kom på, men ikke at alt er husket på…
  - Ofte fokus på "fysisk sikring" når man involverer ansatte….

c) På hvilke måter kan innføringen av GDPR påvirke bedrifters arbeid med risikoanalyser og sikkerhetsarbeid?

- pålagt å gjøre det + mer fokus på sikkerhet

- pålagt å ha en plan for sikkerhet, samt varsling
- ansvar legges på bedriften dersom noe går galt
- bøter vil gjøre at konsekvens-delen av hendelser øker, og derfor vil flere hendelser havne innenfor "må fikses"-kategorien (så sant ikke grenser også endres)

Oppgave 3.3 – 5 %

a) Hvorfor er en tofaktorautentisering regnet å være sikrere enn et vanlig passord

Kommer passordet på avveie må hackerne ha noe mer for å få tilgang til din brukerkonto, noe som gjør det "usannsynlig" at de får missbrukt passordet. (Enkelte varianter vil også "varsle" kontoeier om hackingforsøk – typisk SMS-koder)

b) Hvilke tre faktorer er vanligst å omtale i en tofaktorautentisering (multi-faktor-autentisering)? Gi også eksempler på hva hver av disse faktorene kan være i praksis.

Noe man vet: passord, pin
Noe man er: retina, fingeravtrykk, stemme, ansikt
Nor man har: passordkort, kodebrikke

Oppgave 3.4 – 5 %

Forklar hvordan hackere kan få brukere til å uføre en nyttelast (payload) uten å benytte tradisjonell skadevare (virus, ormer osv) for å transportere skadevaren. (omtalt som "manuell skadevare" i forelesningen). Få med begrepene stridshode (warhead) og spredning (propagation) i en slik setting.

Typisk gjennom å lure offer til å gjøre endringer og handlinger på sin egen maskin. For eksempel slette systemfiler (denial of service) eller endre konfigurasjon (for eksempel DNS).

Warhead vil da være social engineering, altså det å lure offeret til å tro at det som gjøres er en fornuftig handling gjennom hoax osv.

Propagation kan for eksempel være annonser (malwaretising) eller forum. Også sosiale medier, der mange er med på å spre flaske oppskrifter nærmest som kjedebrev.

Oppgave 3.5 – 5 %

a) Hva menes med blacklisting og whitelisting i inputvalidering?

Blacklisting: Vi angir hvilken input som er ulovlig
Whitelisting: vi angir hvilken input som er lovlig

b) Hvilken fordel/ulempe er det ved de to metodene i spørsmål a?

Blacklisting: Vanskelig å huske på alt som kan være skadelig, men fjerner de største problemene. Kan bli en omfattende liste.
Whitelisting: Blir ofte "for streng" for "gyldig input" som vi ikke hadde tenkt på.. Sikkrere da vi må ta et bevisst valg til hvert tegn/input/regel.

c) Foruten validering på enkelttegn, hvilke andre typer/grupper/teknikker har vi?

lengde, domene (sett med gyldige ord / uttrykk), mønstre (typisk regexp)

Del 4 - Diskusjon – 15 % / 0,5 time

På denne delen har ikke oppgaven noen "fasitsvar", men du skal sette opp punkter du mener er viktige momenter. Det ønskes altså at du svarer som en punktliste.

Punktene må være såpass godt beskrevet at man forstår hva du mener, men du trenger ikke skrive mye. Typisk kun noen setninger på hvert punkt. Marker også veldig gjerne 1-3 viktige ord i hvert punkt med bold. Dette vil gjøre at det under sensur er lettere å sammenligne hele bredden av besvarelser, når sensor blar frem og tilbake.

Oppgave 4.1

Fra et sikkerhetsperspektiv, hva tenker du er viktige momenter innen internet of things (både hjemmeenheter og bedrifter). Det teller positivt om du får inn mange ulike aspekter fra pensum her.

Noen momenter (kun stikkordsform her):

- Utvikling går fort – sikkerhet henger etter
    - Lite fokus på sikkerhet (kostnad + utviklignstid)
    - Lages av bedrifter som ikke har tradisjon med "software"
- Bygges på ferdige systemer, men som ofte er utdaterte
- Firmware-oppdateringer (viktighet + falske)
- Passord / adminpanel
- Ønsket om lett installasjon og bruk
- Ønsket om "adminpanel"/apper som også er tilgjengelig på eksternnett
- Logging av data (ofte også på levrandørens servere)
- Utsatt for spesielt Denial of Service + Avlytting/Overvåkning
- Helse/Sikkerhet/Miljø (feilfunksjon/DoS)
- IoT-ting blir "insidere" i andre angrep
- IoT-ting benyttes for større distribuerte angrep
- Mye er bygget på "security by obscurity"