Informasjon om eksamen

EKSAMEN

Emnekode: ITF15019

Emnenavn: Innføring i datasikkerhet

Dato: 02/05-2023

Eksamenstid: 09.00-13.00, 4 timer + 15 minutter til klargjøring og innlevering av besvarelsen.

Hjelpemidler: Ingen

Faglærer: Ole-Edvard Ørebæk

Om eksamensoppgaven:
Oppgavesettet er inndelt i **3 deler** med forskjellige typer oppgaver. Det er på hver del angitt hvor mye denne teller av totalen. **Karakter fastsettes dog på basis av en helhetsvurdering av besvarelsen.**

Del 1 - Sant/usant - 30 %
Del 2 - Flervalg - 15 %
Del 3 - Skriftlig besvarelse - 55%

Merk at selv om Del 1 og 2 utgjør 45%, kan det lønne seg å sette av god tid til Del 3.

Takk for et hyggelig semester! - og beklager hvis jeg har gjort dere paranoide...

Lykke til!

Sensurfrist: 23/05-2023
Karakterene blir publisert i Studentweb.

Del 1 - Informasjon

Denne delen består av 30 påstander som du skal vurdere om er sanne eller usanne. Hver oppgave gir 1 poeng ved riktig svar og -0.5 poeng ved feil svar. Hver oppgave har i tillegg et valg for "Vet ikke", som alltid vil gi 0 poeng. Altså verken positiv eller negativ uttelling. Så hvis du er usikker, lønner det seg typisk å velge "Vet ikke" i stedet for å gjette. **Merk at dette er den eneste delen som gir minuspoeng for feil svar.**

Påstandene er ikke intensjonelt laget for å være utydelige eller flertydige, men det er jo alltids en mulighet for at dette blir tilfellet likevel. Det er derfor lagt til et tekstfelt slutten av denne delen, hvor du kan kommentere eventuelle forutsetninger du gjør for oppgaver du mener er utydelige.

1 Del 1 - Sant/Usant - 30%

OPPGAVER

1. Begrepet *ARP-spoofing* er forbundet med en type man-in-the-middle-angrep som kan utføres internt i et nettverk.
Velg ett alternativ:

- Sant
- Usant
- Vet ikke

2. Dersom en nettside benytter HTTPS er det nesten garantert at nettsiden IKKE er svindel.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

3. Begrepene *white hat*, *gray hat* og *black hat* benyttes til å klassifisere hackeres kompetansenivåer. Spesifikt betegner white hat en uerfaren og offentlig ukjent hacker, en gray hat har noe erfaring og er offentlig kjent for enkelte angrep, mens en black hat er en meget erfaren hacker som er godt kjent både innenfor hackermiljøer og utenfor.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

4. Å benytte POST som overføringsteknikk i HTTP forhindrer avlytting av dataene, selv uten kryptering.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

5. *Port scanning* handler om/innebærer å avsløre hvilke tjenester som kjører på en maskin.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

6. Kryptering kan benyttes for *signering* ved at avsender krypterer en melding med sin private nøkkel, og videre for *verifisering* ved at mottaker dekrypterer meldingen med avsenders offentlige nøkkel.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

7. Sikkerhetstjenestene *authentication* (autentisering) og *access control* (tilgangskontroll) omhandler det samme, men authentication er vinklet mer mot innlogging, og access control mot fysisk tilgang og dørlåser.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

8. *Simple Network Management Protocol* (SNMP) og er en protokoll for hvordan nettverk-kommunikasjon bør struktureres i henhold til nettverkspakker for å forhindre/redusere avlytting av innhold.
Velg ett alternativ

- Sant
- Usant
- Vet ikke

9. Trådløse nett har gjennom tidene hatt diverse protokoller for kryptering. Disse er hovedsakelig WEP, WPA, WPA 2 og WPA 3. Av disse er WPA 2 den som er mest benyttet i dag.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

10. En DMZ, eller *demilitarized zone* (demilitarisert sone), er et prinsipp som handler om å skille de offentlige delene av et system (slik som offentlige nettsteder) og de private delene (skal bare være tilgjengelig for systemeiere). Skillet gjøres ofte med brannmurer.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

11. Kryptering kan være en effektiv mekanisme for å oppnå sikkerhetstjenesten *tilgjengelighet*.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

12. DNS er en grunnleggende, men utdatert, funksjonalitet som inneholder sårbarheter for uautorisert fjernstyring av brukens datamaskin.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

13. Når vi snakker om “IT-sikkerhet” omhandler dette kun hackerangrep/-forsøk gjort av personer med onde hensikter.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

14. Et *makrovirus* er en spesifikk type datavirus som ofte har vært basert på å inkludere skadelig kode i makrodokumenter, altså tekstdokumenter som inneholder et script som kjøres når dokumentet åpnes.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

15. En *logic bomb* (logisk bombe) er en betegnelse som beskriver en skadevare som først ikke har (eller har få) skadelige effekter, men som aktiveres for full effekt på et senere tidspunkt. Dette kan for eksempel være basert på et definert tidspunkt eller en dynamisk hendelse.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

16. Smarttelefoner kan, på grunn av måten de er utviklet, ikke bli infisert av skadevare.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

17. Backups kan benyttes som en metode for å regelmessig kontrollere om et system er blitt infisert av skadevare.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

18. Samtidig som du besøker en nettside i nettleseren din kan du potensielt også gi fra deg informasjon, slik som type maskin/system du benytter og hvilken nettside du var på før dette besøket.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

19. For å innføre sikkerhet ved oversending av *cookies/informasjonskapsler* kan vi blant annet aktivere attributten HTTPOnly. Denne attributten forhindrer slikt som JavaScript-kode fra å hente ut informasjonen.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

20. *Botnet* er en betegnelse for et type hackerkontrollert trådløst nettverk med en rekke falske tilkoblede enheter (“bots”) som stjeler informasjon fra ekte enheter koblet til det samme nettverket.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

21. Når vi snakker om et *passivt angrep* i datasikkerhet, betyr det at angrepet ble utført med uhell. Et eksempel på dette kan være at en ansatt med uhell offentliggjør hemmelig informasjon fra bedriften sin.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

22. *Multi-faktor-autentisering* (MFA) fjerner fullstendig risikoen for *phishing*-angrep relatert til tjenester hvor MFA er innført.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

23. At en epost er pen i utseende, med farger, logoer, spesialtilpassede fonter og så videre, er en god indikasjon på at eposten er ekte og ikke svindel.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

24. Ved å benytte utviklerpanelet i nettleseren (typisk F12-tasten) kan man endre kildekoden (HTML/CSS/JS) bak en nettside vi besøker. Dette kan potensielt benyttes til å omgå eventuelle sikkerhetstiltak og begrensinger som er innført i nettsidens frontend, spesielt hvis det ikke er tilsvarende sikkerhetstiltak i backend.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

25. En av de store fordelene med å benytte VPN er at du alltid er fullstendig anonym.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

26. Ordet “hacker” hadde originalt ingen direkte kobling til kriminelle handlinger, men betegnet generelt en kompetent, dedikert og nysgjerrig person, oftest uten onde intensjoner.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

27. Begrepet *script kiddie* betegner en type script med skadelige effekter for maskinen som kjører det. Script av denne typen skiller seg fra andre script i at de er små i størrelse og generert med ferdiglagde verktøy.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

28. Metadata i bildefiler kan potensielt inneholde informasjon som kan benyttes til sporing, for eksempel den nøyaktige lokasjonen bildet ble tatt.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

29. *Salting* er en teknikk som kan benyttes ved passordhashing for å redusere farene for *rainbow table*-angrep.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

30. Å gjøre en ressurs vanskelig å finne (*security by obscurity*), for eksempel ved å gjøre en nettside kun tilgjengelig gjennom direktelenke, er et meget godt sikkerhetstiltak for å unngå uautorisert tilgang.

Velg ett alternativ

- Sant
- Usant
- Vet ikke

Maks poeng: 30

2 Kommentarer til Del 1

Hvis du gjør forutsetninger eller andre kommentarer for enkelte av oppgavene i Del 1, kan du skrive disse her. I så fall, merk at det er viktig at gjør det tydelig nøyaktig hvilke oppgaver du kommenterer på. Merk også at kommentarene her ikke gir noen uttelling i seg selv.

Skriv ditt svar her

Maks poeng: 0

Del 2 - Flervalg - 15%

Denne delen består av 15 flervalg-oppgaver som hver gir 1 poeng ved riktig svar. Merk at det det IKKE gis minuspoeng for feil svar, så hvis du er usikker, kan det lønne seg å gjette i denne delen.

Selv om alle oppgavene i denne delen er flervalg-oppgaver, er det i midlertid 2 varianter av disse. De første 12 oppgavene er av typen "Velg en" hvor du for hver oppgave skal velge nøyaktig ett alternativ.

De siste 3 oppgavene er av typen "Velg en eller flere" hvor hver oppgave kan ha alt fra 1 til 4 riktige alternativer. Merk at du kun får poeng på en gitt oppgave hvis du har valgt nøyaktig de riktige alternativene. Avhukninger som er delvis riktige gir altså ingen uttelling.

Merk at de siste 3 oppgavene også er skilt ut i forskjellige sider.

Som i Del 1, er det et tekstfelt på slutten av denne delen, hvor du kan kommentere eventuelle forutsetninger du gjør ved oppgaver du mener er utydelige eller flertydige.

3 Del 2 - Velg en

"VELG EN" OPPGAVER

Det er totalt 12 oppgaver av denne typen flervalg, hvor du skal for hver oppgave velge nøyaktig ett alternativ.

OPPGAVER

1. Hvilket alternativ beskriver best begrepet *innsider*?

Velg ett alternativ:

- En bit med kode eller ett program, som tillater en hacker å fjernstyre PC-en din.
- Dette er hva en hacker som med suksess har brutt seg inn i et system, og er nå på "innsiden", kalles.
- Et program som virker ekte og troverdig, men som inneholder skadelig kode.
- En person på innsiden av en bedrift, oftest en ansatt, som aktivt utfører skadelige handlinger mot bedriften.

2. Hvilket alternativ beskriver best begrepet *phishing* (nettfiske)?

Velg ett alternativ

- En søketeknikk hackere kan benytte for å samle informasjon på internettet om et potensielt angrepsmål.
- En teknikk som lokker/lurer brukere til å oppgi informasjon de ellers ville holdt hemmelig.
- En teknikk hackere kan benytte for å knekke krypterte meldinger over nett, som er basert på å "fiske" frem velkjente/typiske deler av meldingen.
- En teknikk hackere benytter under avlytting av informasjon til å filtrere akkurat det de er ute etter.

3. Hvilket av de følgende alternativene er IKKE en teknikk benyttet for håndtering av *risiko*?

Velg ett alternativ

- Risikoaksept
- Risikoreduserende tiltak
- Risikooverføring
- Risikoforhandling

4. Hvilket av de følgende alternativene beskriver best begrepet *hoax*?
Velg ett alternativ

- En type skadevare som sender brukeren falske advarsler med jevne mellomrom.
- En strategi svindlere/hackere kan benytte for å lure ofre til å selv ta kontakt.
- Dette er hva vi kaller en tidligere sikkerhetstrussel som har blitt avdekket å egentlig være harmløs.
- Navnet på et verktøy i kali som kan benyttes av svindlere/hackere for å kartlegge aktuelle mål.

5. Hvilket av de følgende alternativene passer best for å beskrive begrepet *personvernombud*?
Velg ett alternativ

- Et personvernombud betegner en type bot som kan utgis til organisasjoner som har brutt GDPR.
- Et personvernombud er en person fra Datatilsynet som regelmessig besøker en organisasjon for å kontrollere at personvernregler følges riktig.
- En rolle i en organisasjon hvor den ansatte med denne rollen er ansvarlig for å gi organisasjonen råd i henhold til personvern og GDPR.
- "Personvernombudet" er navnet på et lovverk som angir retningslinjer for personvern i en organisasjon, samt konsekvensene ved brudd.

6. Hvilket av de følgende alternativene er IKKE et aspekt som er dekket i GDPR?
Velg ett alternativ

- Brukere av en tjeneste skal alltid ha muligheten til å hente ut og slette alle personopplysninger lagret av tjenestens produsent/bedrift
- Bedrifter underlagt GDPR er pålagt å gjennomføre vurderinger av risiko og konsekvenser.
- Alle tjenester skal ha en personvernserklæring som er skrevet til å være forståelig for alle som leser den.
- Ved et hackerangrep er bedriften som er blitt angrepet ansvarlig for å spore opp hackeren(e) og legge frem bevis for politiet.

7. Gitt den følgende beskrivelsen, hvilket av alternativene under passer best? - "En type skadevare som er et selvstendig program og sprer seg helt på egenhånd, for eksempel ved å automatisk sende mail med seg selv som vedlegg".

Velg ett alternativ

- Orm
- Trojaner
- Virus
- Rootkit

8. Hvilket av de følgende alternativene beskriver best *signaturbaserte teknikker* i sammenheng med antivirusprogramvare?

Velg ett alternativ

- Skadevare oppdages ved å kjøre den undersøkte programvaren i et kontrollert og isolert miljø og analysere hvordan den oppfører seg, sammenlignet med hvordan skadevare typisk oppfører seg.
- Skadevare oppdages ved å gjenkjenne kodesekvenser, eller annet fil-innhold, som tidligere er dokumentert til å være skadevare.
- Skadevare oppdages/unngås hovedsakelig av brukeren ved at antivirusprogramvaren tilbyr brukeren innsikt og statistikk over slikt som forskjellige typer skadevare, kjente infiserte produkter og typiske infeksjonsmetoder.
- Skadevare oppdages ved å kontinuerlig sammenligne nåværende systemfiler med slik de var på et tidligere tidspunkt. Hvis uventede endringer har forekommet, flagges dette som potensiell skadevare.

9. Hvilket av alternativene under passer best til å beskrive begrepet *whitelist*?

Velg ett alternativ

- En liste over brukere som er ekstra sikkerhetskritiske og som derfor krever flere sikkerhetstiltak.
- En liste over programmer, nettsider, funksjoner eller lignende, som er tillatt å benytte. Alt annet er ikke tillatt som standard.
- En liste over tjenester/nettsider som aldri har blitt hacket.
- En liste over “farlige” tegn vi må oversette eller fjerne ved input-validering.

10. Hvilket av alternativene beskriver best begrepet *spoofing*?

Velg ett alternativ

- At noe (eller noen) utgir seg for å være noe annet enn hva som er tilfellet
- At pakker og informasjon som går over nettrafikk blir overvåket.
- At tilgangrettighetene for en eller flere brukere blir endret av hackere.
- At en sårbarhet eller et sikkerhetshull utnyttes for å utføre et angrep.

11. Hvilket av alternativene er generelt et godt sikkerhetstiltak brukere kan gjøre mot *Cross Site Request Forgery* (CSRF/Webtrojaner)?

Velg ett alternativ

- Avinstallere alle nettlesertillegg (plugins)
- Benytte Tor-browser for nettsurfing
- Logge ut av tjenester når man ikke benytter dem
- Jevnlig slette aktivitetslogger i nettleser og tjenester

12. Hvilket av alternativene passer best for å beskrive begrepet *denial of service* (DoS)?

Velg ett alternativ

- Et type angrep som gjør en tjeneste midlertidig eller permanent utilgjengelig.
- Et lovmessig brudd på systembrukeres rettigheter, hvor brukere ikke har fått eller har mistet tilgang til en tjeneste de har betalt for.
- En metode hackere benytter for å skjule seg selv etter angrep, ved å stenge ned alle maskiner som ble benyttet i angrepet.
- En teknikk tjenesteprodusenter kan benytte ved et oppdaget hackerangrep, hvor hackerene blir utestengt fra å benytte tjenesten videre.

Maks poeng: 12

4 Del 2 - Vel en eller flere (1/3)

"VELG EN ELLER FLERE" OPPGAVER

Det er totalt 3 oppgaver av denne typen hvor du skal for hver oppgave velge alle alternativer du anser som riktige/passende. De tre oppgavene er likevel delt opp i tre forskjellige sider, på grunn av begrensninger i eksamenssystemet...

OPPGAVER

13. Hvilke av alternativene under kan bli benyttet som faktorer i *multi-faktor-autentisering*? (For kontekst: De riktige alternativene er faglig etablerte faktorer og er ikke en tolkningssak.)

Velg ett eller flere alternativer

- [ ] Noe du GJØR
- [ ] Noe du HAR
- [ ] Noe du ER
- [ ] Noe du VET

Maks poeng: 1

5 Del 2 - Velg en eller flere (2/3)

14. Hvilke av alternativene under er aspekter/angrep en VPN kan beskytte mot?

Velg ett eller flere alternativer

- [ ] Svindelstrategier
- [ ] Drive-by-download
- [ ] Falske plugins (utvidelser) i nettleser
- [ ] Falske/usikrede nettverk

Maks poeng: 1

6 Del 2 - Velg en eller flere (3/3)

15. Hvilke av alternativene under er aspekter i den generelle oppbygningen av en skadevare?
Velg ett eller flere alternativer

- [ ] Stridshode (Warhead)
- [ ] Nyttelast (Payload)
- [ ] Integritet (Integrity)
- [ ] Spredning (Propagation)

Maks poeng: 1

7 Kommentarer til Del 2

Hvis du gjør forutsetninger eller andre kommentarer for enkelte av oppgavene i Del 2, kan du skrive disse her. I så fall, merk at det er viktig at du gjør det tydelig nøyaktig hvilke oppgaver du kommenterer på. Merk også at kommentarene her ikke gir noen uttelling i seg selv.
Skriv ditt svar her

Maks poeng: 0

Del 3 - Skriftlig besvarelse - 55%

Denne delen består av 5 oppgaver hvor du selv skal formulere skriftlige svar. Hver oppgave er vektlagt omtrendtlig like mye, men nøyaktig fordeling kan justeres noe under sensuren. Dermed lønner det seg generelt å fordele tiden for å svare noe på alle oppgaver, i stedet for å kun fokusere på et lite utvalg. Anbefaling: Les alle oppgaver før du begynner å svare og planlegg tiden.

Merk at helhetsinntrykket av svarene dine også er viktig. Følg strukturen oppgavene gir. (Hvis det er deloppgaver a), b) og c), del også opp svarene dine slik). Det lønner seg som regel å holde seg til hva oppgaven etterspør og utelatte annen urelatert informasjon. Det er typisk også en fordel jobbe med formuleringene dine. Du får ikke uttelling basert på lengden av hva du skriver, men hvor godt innholdet besvarer oppgaven. Anbefaling: Les over (og omformuler) besvarelsene dine flere ganger før du avslutter eksamen.

Merk også at noen oppgaver kan virke veldig enkle å besvare, men vit at det typisk er nødvendig å drøfte, forklare, begrunne osv. for å få noen uttelling. Å svare "Fordi det er farlig" (eller tilsvarende) gir ingen innsikt i kompetansenivå/forståelse, så vis hvordan du tenker.

Ved drøfting, kan noen av oppgavene ellers bli litt omfattende i antall eksempler og situasjoner som kan være relevante å skrive om. Merk likevel at det viktigste alltid er å vise at man forstår forskjellige sider av temaet, IKKE mengden eksempler/situasjoner man klarer å liste. Så det kan ofte være en god strategi å starte med å svare abstrakt/generelt, for deretter å skrive om mer konkrete aspekter.

8 Del 3 - Oppgave 1 - Sletting av data

a) Forklar hvorfor det er vanskelig å slette digital informasjon/data fra slikt som harddisker, SSD-er eller andre lagringsmedier.

b) Drøft hva har dette å si for slikt som gjenbruk/salg og kasting/avhending av brukte lagringsmedier (eller enheter som inneholder lagringsmedier).

c) Forklar hva som må til for at dataene faktisk skal bli "slettet" (eller praktisk oppnå samme effekt), og gi noen råd til hvordan man kan oppnå dette.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

9 Del 3 - Oppgave 2 - Cookies og Sessions

a) Forklar hva en *cookie/informasjonskapsel* er, og overordnet hvordan/hvorfor disse er relevante for sikkerhet.

b) Forklar videre hva en *session* er og den overordnede prosessen av hvordan disse blir opprettet og lukket.

c) Drøft ulike måter en *session* kan komme på avveie og hvilke negative konsenser dette kan medføre.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

10 Del 3 - Oppgave 3 - SQL-injection

a) Forklar hva *SQL-injection* er og overordnet hvordan dette fungerer. Du kan gjerne også vise et eksempel eller to på relevante angrepsteknikker, men dette er ikke nødvendig for å få full uttelling.

b) Hva kan konsekvensene av en suksessfull *SQL-injection* være? Her er det mulig å tenke både generelt og konkret. Det viktigste er imidlertid å vise forskjellige vinklinger/kategorier, ikke å liste absolutt alle konkrete muligheter.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

11 Del 3 - Oppgave 4 - Social Engineering

a) Forklar hva *social engineering* (sosial manipulasjon) er. Benytt gjerne eksempler og konkrete begreper for å demonstrere forskjellige former dette kan forekomme. Det er imidlertid ikke nødvendig å gå veldig dypt i hver form og du kan gjerne lage/vise kategorier.

b) Drøft forskjellige aspekter som ofte er inkludert i *social engineering* angrep og hvordan disse har en sammenheng med hvordan brukere kan beskytte seg selv mot slike angrep. Igjen; Det er ikke nødvendig å liste alt, men prøv å vise noen forskjellige kategorier.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

12 Del 3 - Oppgave 5 - Minnepenn og Fysisk Tilgang

a) Ta perspektivet av en hacker. Hvordan kan du benytte en minnepenn for å angripe en PC du har fysisk tilgang til. Her lønner det seg å tenke kreativt og diskutere forskjellige metoder. Det er også lov å gjøre forutsetninger, slik som hva for slags minnepenn dette er og hva brukeren/offeret gjør.

b) Drøft hva kan en bruker gjøre for å beskytte seg mot angrep som benytter minnepenner (kan også gjelde andre USB-enheter). Diskuter gjerne i forhold til noen tiltenkte situasjoner.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10