Informasjon om eksamen

EKSAMEN

Emnekode: ITF15015

Emnenavn: Innføring i datasikkerhet

Dato: 10/05-2019

Eksamenstid: 09.00-13.00, 4 timer

Hjelpemidler: Ingen

Faglærer: Tom Heine Nätt

Om eksamensoppgaven:
Oppgavesettet er inndelt i 4 deler. Det er på hver del, og deloppgavene i del 3, angitt hvor mye disse teller av totalen. Karakter fastsettes dog på basis av en helhetsvurdering av besvarelsen.

Gjør dine egne forutsetninger dersom du mener noe er uklart.

Takk for et hyggelig semester - beklager at jeg har gjort dere paranoide.

Lykke til!

Sensurfrist: 03/06-2019
Karakterene er tilgjengelige for studenter på Studentweb.

1 Del 1. Sant/usant

Del 1. Sant/usant – 25 %
Du skal her svare på om påstanden er sann eller usann.
NB! Feil avkrysning vil telle negativt, slik at det ikke skal lønne seg å gjette. Svar derfor kun på de oppgavene der du er så godt som sikker på svaret.

På neste "side" i eksamenssystemet er det en tekstboks du kan benytte for ytterligere kommentarer til del 1. MERK: Det skal ikke være nødvendig å benytte denne tekstboksen annen en til helt spesielle tilfeller.

NB! Pass på å lese teksten nøye så du ikke går glipp av vesentlige ord slik som *ikke*.

1. VPN sikrer deg mot phishing.

Velg ett alternativ

- Sant
- Usant

2. HTTPS sikrer deg mot XSS (Corss-site scripting).
Velg et alternativ

- Sant
- Usant

3. Backup kan være nyttig for integritetskontroll.
Velg et alternativ

- Sant
- Usant

4. Backup kan være nyttig for konfidensialitet.
Velg et alternativ

- Sant
- Usant

5. Backup kan være nyttig for tilgjengelighet.

Velg et alternativ

- Sant
- Usant

6. Dersom et antivirusverktøy klarer å fjerne en skadevare helt fra maskinen, vil også alle konsekvensene av nyttelasten bli tilbakestilt.
Velg et alternativ

- Sant
- Usant

7. Å sende data via POST-forespørsler er vesentlig sikrere mot avlytting enn å sende via GET-forespørsler.
Velg et alternativ

- Sant
- Usant

8. HTTPS sikrer konfidensialitet i overføring, samt autentisering av parten(e).
Velg et alternativ

- Sant
- Usant

9. Å lukke porter og/eller fjerne tjenester på en maskin øker sannsynligheten for at noen kan utnytte exploits mot deg.
Velg et alternativ

- Sant
- Usant

10. For å kunne utføre autentisering er det viktig og først ha utført autorisering.
Velg et alternativ

- Sant
- Usant

11. EXIF er en teknikk for å oppdage virus.

Velg et alternativ

- Sant
- Usant

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.
Velg et alternativ

- Sant
- Usant

13. For å forfalske en basestasjon (lage et nett med samme SSID) må man først være påkoblet denne basestasjonen.
Velg et alternativ

- Sant
- Usant

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.
Velg et alternativ

- Sant
- Usant

15. En av farene ved ukjente trådløse nett er automatisk tildeling av DNS-server.
Velg et alternativ

- Sant
- Usant

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.
Velg et alternativ

- Sant
- Usant

17. Begrepet security passer bedre enn begrepet safety når vi snakker om datasikkerhet i forbindelse med datakriminalitet.
Velg et alternativ

- Sant
- Usant

18. Dersom en hacker får tilgang til en brukers informasjonskapsler kan dette bl.a. medføre session hijacking.
Velg et alternativ

- Sant
- Usant

19. *Ciphertext* og *meldingen som skal krypteres* er to begreper som dekker det samme, og kan benyttes om hverandre.
Velg et alternativ

- Sant
- Usant

20. Trojanere kjennetegnes først og fremst ved at de svært effektivt, og nærmest "på egenhånd", spres rundt i nettverket.
Velg et alternativ

- Sant
- Usant

21. En web-trojaner (CSRF/XSRF) vil alltid være koblet mot en GET-forespørsel.
Velg et alternativ

- Sant
- Usant

22. Loggfiler er sentralt i forbindelse med non-repudiation.
Velg et alternativ

- Sant
- Usant

23. Inputvalidering kan også forhindre flere typer denial of service-angrep.
Velg et alternativ

- Sant
- Usant

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.
Velg et alternativ

- Sant
- Usant

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.
Velg et alternativ

- Sant
- Usant

2 Kommentarer - del 1

Her kan du gi kommentarer til del 1.
MERK: Det skal ikke være nødvendig å benytte denne tekstboksen annen en til helt spesielle tilfeller.
For å unngå at eksamenssystemet sier at oppgaver er ubesvart, kan du sette et punktum i boksen.

Skriv ditt svar her...

3 Del 2. Flervalg - 20 %

Del 2. Flervalg – 20 %
Det er kun ett alternativ som er riktig på hver oppgave. Dersom du svarer flere alternativer vil dette telle som feil svar (skal ikek være mulig å eksamenssystemet). Merk deg at oppgavene etterspør det alternativet som er mest riktig eller best beskrivende.

NB! Feil avkrysninger vil telle negativt, slik at det ikke skal lønne seg å gjette. Svar derfor kun på de oppgavene der du er temmelig sikker på svaret.

På neste "side" i eksamenssystemet er det en tekstboks du kan benytte for ytterligere kommentarer til del 2. MERK: Det skal ikke være nødvendig å benytte denne tekstboksen annen en til helt spesielle tilfeller.

1. Det beste sikkerhetstiltaket mot XSS (Cross-site scripting) er?
Velg ett alternativ

- Oppgradere nettleser og operativsystem
- Skru av JavaScript hos brukeren.
- Detektere endringer i brukers IP-adresse
- Inputvalidering

2. Hva menes med *mail spoofing*?
Velg ett alternativ

- Å hindre at mail kan bli sendt (en form for denial of service)
- Å sende så mye mail til en bruker at all reel mail forsvinner i mengden
- Å sende mail som ser ut til å komme fra en annen avsender
- Å sende ut svindler via mail. Typisk phining-angrep

3. Hva menes med begrepet *heuristikk* i forbindelse med virus?
Velg ett alternativ

- En metode for å oppdage virus
- En metode for å isolere virus
- En metode for å spre virus
- En metode for å fjerne virus

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

Velg ett alternativ

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

5. Hvilken påstand beskriver et botnet?
Velg ett alternativ

- Et kriminelt nettverk som har satt hacking i system (ofte styrt av mafia)
- Et nettverk som benytter kunstig intelligens til å avsløre svindler og skadevare
- Et nettverk av infiserte maskiner som styres av en eller flere hackere
- 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?
Velg ett alternativ

- Algoritmen bak private/public key er mye sterkere fordi den utelukkende baserer seg på primtall som er umulige å knekke med dagens matematikk
- 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
- Man slipper å utveksle en hemmelig nøkkel
- Secret key er alltid best

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

- Vi ikke blir utsatt for man-in-the-middle angrep/avlytting
- Vi ikke kan bli utsatt for webtrojanere og cross-site scripting, da dette er en sikker kommunikasjon mot serveren
- Vi ikke kan bli sporet i våre handlinger
- 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

Velg ett alternativ

- storebananerblomstrer
- =a45
- qazwsx
- michael89

9. For å sikre at en fil blir permanent slettet er det viktig å?
Velg ett alternativ

- Tømme papirkurven (recyle bin) etter at man har slettet en fil
- Randomisere dataposisjonene der fila lå fila med 0-ere og 1-ere
- Overskrive filsystemtabellen der fila lå med 0-ere og 1-ere
- 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?
Velg ett alternativ

- WPA
- WEP
- VPN
- DHCP

11. Hvilken teknologi er mest sentral i oppsett av en demilitarisert sone?
Velg ett alternativ

- ARP
- Brannmur
- VPN
- DHCP

12. Innen datasikkerhet er en snubletråd?
Velg ett alternativ

- Noe hackere legger inn for å detektere bruk av systemet
- Noe hackere legger inn for å hindre bruk av systemet
- Noe systemeier legger inn for å detektere hacking
- Noe systemeier legger inn for å hindre hacking

13. En logisk bombe er?

Velg ett alternativ

- En type/kategori av skadevare
- En hackerteknikk som hindrer at de logiske kretsene i en CPU kan utføre riktige beregninger
- En hackerteknikk som spiller på å forvirre de logiske slutningene en bruker tar (en variant av social engineering)
- 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?
Velg ett alternativ

- White hat hacker
- Gray hat hacker
- Black hat hacker
- Red hat hacker

15. Begrepet denial of service kan best beskrives som?
Velg ett alternativ

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

- Halvere tiden
- Ingen endring
- Doble tiden
- "Mangedoble" tiden

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

Velg ett alternativ

- Alle bedrifter med mer enn 20 milliarder euro i omsetning
- Alle bedrifter i Norge
- Alle bedrifter i Europa
- Alle bedrifter med europeiske kunder

18. Beste sikkerhetstiltak mot web-trojanere (CSRF/XSRF) for en bruker er å?
Velg ett alternativ

- Skru av JavaScript
- Logg ut av tjenester når man er ferdige med å bruke de
- Sørge for å ha oppdatert programvare
- 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?
Velg ett alternativ

- Et angrep der man benytter skadevare som kjøres hos offeret
- En teknikk for å sikre maskiner mot angrep
- Et angrep som benytter et bestemt exploit mot tjenester og programvare hos offeret
- En teknikk for å detektere angrep

20. Spear phishing er?
Velg ett alternativ

- Phishing som er målrettet mot et offer eller en gruppe offer gjennom å være basert på spesifikk informasjon om offeret
- Phishing som benytter skadevare for å komme gjennom filtre (for eksempel SPAM-filter)
- Et av de få mottiltakene man har mot phishing der man gjennom heuristikk klarer å fange opp kjennetegn på phishing
- Ingen av punktene stemmer

4 Kommentarer - del 2

Her kan du gi kommentarer til del 2.

MERK: Det skal ikke være nødvendig å benytte denne tekstboksen annen en til helt spesielle tilfeller.

For å unngå at eksamenssystemet sier at oppgaver er ubesvart, kan du sette et punktum i boksen.

Skriv ditt svar her...

i Del 3 - Faktaspørsmål

Del 3. Faktaspørsmål (40 %)

Alle disse oppgavene har et slags forventet svar, selv om det ikke er noen eksakt fasit.

Selv om det kan være mulig å svare på flere av deloppgavene samlet, ønskes det at du er nøye med å skille svarene på deloppgavene fra hverandre i din besvarelse.

Husk at det ikke er mengden tekst, men innholdet, som er viktig. Svar derfor gjerne som korte setninger og punktlister. Det viser god kompetanse i et tema at man klarer å svare kort og konsist. Pass imidlertid på at det ikke blir så kort at innholdet forsvinner eller at det blir utydelig for sensor om du kan temaet eller bare har pugget et begrep.

Mange av oppgavene vil også ha flere ulike momenter (for eksempel teknikker eller farer) som mulige svar. Å kun nevne ett moment vil da ikke gi full uttelling, selv om det i seg selv er riktig.

5 Oppgave 3.1

Oppgave 3.1 – Hash-funskjoner – 10 %

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

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

Skriv ditt svar her...

6 Oppgave 3.2

Oppgave 3.2 - Risiko- og sårbarhetsanalyse, bedrifters sikkerhetsarbeid - 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.
b) Forklar kort noen fordeler og ulemper med denne typen analyse.
c) På hvilke måter kan innføringen av GDPR påvirke bedrifters arbeid med risikoanalyser og sikkerhetsarbeid?

Skriv ditt svar her...

7 Oppgave 3.3

Oppgave 3.3 - Tofaktorautentisering - 5 %

a) Hvorfor er en tofaktorautentisering regnet å være sikrere enn et vanlig passord
b) Hvilke tre faktorer er vanligst å omtale i en tofaktorautentisering (multifaktorautentisering)? Gi også eksempler på hva hver av disse faktorene kan være i praksis.

Skriv ditt svar her...

8 Oppgave 3.4

Oppgave 3.4 - Manuell skadevare - 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. (Dette er omtalt som "manuell skadevare" i forelesningen). Få med begrepene stridshode (warhead) og spredning (propagation) i en slik setting.

Skriv ditt svar her...

Oppgave 3.5

Oppgave 3.5 - Inputvalidering - 5 %

a) Hva menes med blacklisting og whitelisting i inputvalidering?
b) Hvilken fordel/ulempe er det ved de to metodene i spørsmål a?
c) Foruten validering på enkelttegn, hvilke andre typer/grupper/teknikker har vi?

Skriv ditt svar her...

Del 4

Del 4. Åpne spørsmål (15 %)
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.

10 Oppgave 4.1

Oppgave 4.1 - Internet of Things - 15 %
Fra et datasikkerhetsperspektiv, hva tenker du er viktige momenter å påpeke innen temaet Internet of Things (både hjemme og for bedrifter)?

Det teller positivt om du får inn mange ulike aspekter fra pensum her. Prøv å ta for deg både overordnede problemstillinger og utfordringer, samt noen litt mer konkrete og "detaljertere" farer.

Selve begrepet Internet of Things kan være litt ullent å definere, men du kan ta som utgangspunkt fysiske enheter som lar seg monitorere og ofte også kontrollere over Internet. Gjerne gjennom standard webprotokoller og webgrensesnitt/apper.

Det vil ikke være mulig å dekke alt, men sørg for at svaret ditt viser bredden i kunnskapen din og reflekterer tiden som er til rådlighet på denne oppgaven.

Skriv ditt svar her...