Høgskolen i Østfold

EKSAMEN

Emnekode:	Emnenavn:
ITF15015	Innføring i datasikkerhet
Dato:	**Eksamenstid:**
24/5-2016	09.00-13.00
Hjelpemidler:	**Faglærer:**
Ingen	Tom Heine Nätt

Om eksamensoppgaven og poengberegning:

Oppgavesettet består av 7 sider inklusiv denne forsiden.

Kontroller at oppgaven er komplett før du begynner å besvare spørsmålene.

Eksamensoppgaven består av tre deler.

Del 1 inneholder påstander som du skal svare sant/usant på.

Del 2 inneholder flervalgsoppgaver der du skal velge ett alternativ på hver oppgave.

Del 3 inneholder oppgaver som krever tekstsvar.

Del 1 og 2 bør gjøres på godt under 1 time.

Del 3 får da minst 3 timer til rådighet, noe som betyr ca. 15 minutter på hver oppgave.

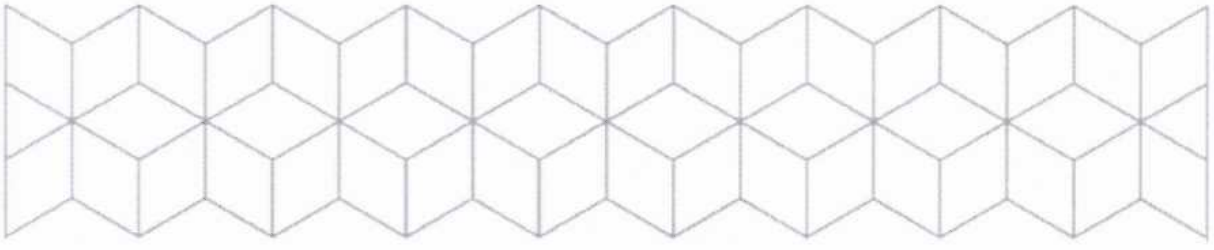
Gjør dine egne forutsetninger dersom du mener noe er uklart.

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

Ha en sikker og god sommer :-)

Sensurfrist: 15/6-2016

Karakterene er tilgjengelige for studenter på Studentweb senest 2 virkedager etter oppgitt sensurfrist. www.hiof.no/studentweb



Del 1 – Påstander – 15 %

(Sant eller usant)

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

1. En *private/public key*-kryptering er i seg selv (selve algoritmen/krypteringsmetoden) alltid sikrere enn en *secret key*-kryptering.
2. En *web-trojaner* (CSRF/XSRF) vil alltid være koblet mot en GET-forespørsel.
3. *HTTPS* beskytter mot avlytting (man-in-the-middle angrep).
4. *WPAv2* er sikrere enn *WEP*.
5. *DMZ* er et oppsett av nettverk der tjenester som må være åpne utad står mellom en ytre og en indre brannmur.
6. Det er teknisk sett helt umulig å lage et verktøy som kan gjenkjenne enkelte nye og ukjente svindler som baserer seg på social engineering.
7. *Reverse social engineering* betyr at man klarer å avsløre en svindel og benytter dette overtaket til å lure den som opprinnelig var angriperen.
8. Det er langt sikrere å lagre systemverdier for en nettside som er kritiske for sikkerhetsmekanismer (innlogging, validering osv.) i en *cookie* enn i en *session*. Dette fordi verdiene da ligger trygt lagret hos hver enkelt bruker, og dermed ikke er like utsatt for angrep mot selve webserveren.
9. *Spoofing* er en teknikk som vanligvis benyttes for å oppnå *denial of service*.
10. Ettersom *HTTPS* er basert på sertifikater får vi en ekstra trygghet ved at sertifikater kun utstedes til nettsider som følger strenge retningslinjer (bl.a. TEPAC4 som angir hvordan netthandel skal foregå).
11. *EXIF* er et verktøy/teknikk som benyttes for å hente ut *metadata* fra ulike filformater.
12. Backup er et effektivt tiltak for å redusere konsekvensene av *ransomware*.
13. *Heuristikk* er en metode (av flere mulige) som skadevare benytter for å holde seg skjult.

Del 2 – Flervalg – 15 %

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

Det er kun ett alternativ som er riktig på hver oppgave. Legg merke til at flere av oppgavene etterspør det alternativet som er mest riktig eller best beskrivende.

Oppgave 2.1

Tenk deg to ulike passord, ett satt sammen av tre helt tilfeldige tegn (a-z, A-Z og 0-9), og ett satt sammen av tre tilfeldige norske ord.

Hvis vi forsøker knekke det første med brute-force og det andre med et ordlisteangrep, hvilken påstand stemmer best:

a) De to passordene er omtrent like sikre.
b) Passordet med tre tilfeldige **tegn** er vesentlig sikrere.
c) Passordet med tre tilfeldige **ord** er vesentlig sikrere.
d) Siden et gjennomsnittsord er ca 4 tegn, er passordet med ord ca fire ganger sikrere enn det med tilsvarende antall tegn.

Oppgave 2.2

Hva er *ISO/IEC 27002*?

a) En standard for informasjonssikkerhet.
b) En internasjonal lov for informasjonssikkerhet.
c) Et produkt som hjelper til med å analysere informasjonssikkerhet.
d) En konferanse for informasjonssikkerhet.

Oppgave 2.3

En hacker som har fått et oppdrag av en bedrift om å teste bedriftens egne systemer kalles ofte for en:

a) White hat hacker.
b) Gray hat hacker.
c) Black hat hacker.
d) Red hat hacker.

Oppgave 2.4

Et *botnet* kan best beskrives som et nettverk av maskiner som

a) benyttes av kriminelle for å kommunisere.
b) benyttes til kriminelle handlinger.
c) analyserer nettrafikk og oppdager nye farer.
d) kan overføre data uten å legge igjen spor.

Oppgave 2.5

Begrepet *denial of service* kan best beskrives som:

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.

Oppgave 2.6

SQL-injection kan best beskrives som:

a) En hacker lurer webserveren til å vise den bakenforliggende SQL-koden.
b) En hacker utsetter brukerens/offerets maskin for SQL-kode.
c) En skadevare som har payload (nyttelast) basert på SQL-kode.
d) En hacker angir deler av SQL-kode som input til et system gjennom for eksempel et skjema på en nettside.

Oppgave 2.7

Portscanning kan best beskrives som:

a) En teknikk vi kan benytte for å se om hackere forsøker koble til maskinen vår.
b) En teknikk der vi analyserer trafikk på en bestemt port for å lete etter skadevare.
c) En teknikk hackere benytter for å finne ut hvilke tjenester som kjører på en maskin.
d) En teknikk hackere benytter for å lure et offer inn på en falsk tjeneste (bl.a. benyttet til *phishing*).

Oppgave 2.8

Phishing kan best beskrives som:

a) Forsøke å fralure offeret personlig informasjon (gjennom for eksempel sosiale medier, e-post eller nettsider)
b) Prosessen med å lage en falsk kopi av en nettside.
c) Misbruk av stjålet informasjon.
d) Svindlere hacker en tjeneste for å hente ut personlig informasjon om offeret.

Oppgave 2.9

XSS (*Cross-Site Scripting*) kan best beskrives som:

a) En svindler drifter to ulike nettsteder og du blir automatisk sendt fra den ene til den andre.
b) En svindler har hacket en nettside som så videresender deg til hackerens egen versjon.
c) En svindler har fått plassert kode (vanligvis JavaScript) i en nettjeneste. Denne koden utføres av nettleseren til alle de besøkende når nettsiden med koden vises.
d) En svindler drifter en nettside som inneholder programkode som infiserer din nettleser gjennom sikkerhetshull (en variant av *drive-by-download*)

Oppgave 2.10

Kali kan best beskrives som:

a) En hackerteknikk.
b) En samling verktøy som kan teste sikkerhet og motstand mot kjente angrep i et system (ikke nødvendigvis ditt eget).
c) Et av de største kjente kriminelle nettverkene (datakriminalitet).
d) Et verktøy som skal forhindre at du kommer inn på svindelnettsider.

Del 3 – Tekstsvar – 70 %

Husk at det ikke er mengden tekst, men hvor godt innholdet er, som teller. Enkelte oppgaver kan besvares som punktlister. Du har ca. 15 minutter på hver oppgave i snitt. Fordel tiden godt! Det er ikke gitt at alle oppgavene er helt identiske i omfang. Noen av oppgavene i denne delen vil kreve noe mer tid/besvarelse, og vil da også bli vektet noe høyere i totalbedømmingen.

Oppgave 3.1

Hvilke råd ville du gitt til en ordinær bruker om hva man bør gjøre og hva man bør unngå å gjøre når man skal lage et godt passord?

Oppgave 3.2

Du søker etter et produkt i Google og kommer deretter inn i en for deg ukjent nettbutikk. Hvilke sjekker/kontroller kan det være lurt å gjøre før du handler?

Oppgave 3.3

Nevn noen grunner til at det er viktig å ha en skjermlås på en mobil enhet (telefon/nettbrett).

Oppgave 3.4

Hvilke muligheter får en hacker, dersom han/hun får satt opp din maskin til å benytte en DNS-server som hackeren kontrollerer.

Oppgave 3.5

a) Forklar hvordan en hacker kan utføre et *APR-spoofing-angrep* uten å fysisk være *til stede på lokalnettverket. (Du behøver ikke forklare hvordan et ARP-spoofing-*angrep fungerer rent teknisk, men forklar hva det innebærer.)

b) Forklar hvordan/hvorfor VPN kan benyttes for å gjøre kommunikasjon over ukjente nettverkt sikrere. Du behøver ikke gå inn i tekniske detaljer eller oppsett av VPN.

Oppgave 3.6

To-faktor-autentisering (egentlig *multifaktor-autentisering*) baserer seg på faktorer tilhørende tre ulike generelle grupper.

a) Hvilke tre generelle faktorer/metoder er det snakk om?

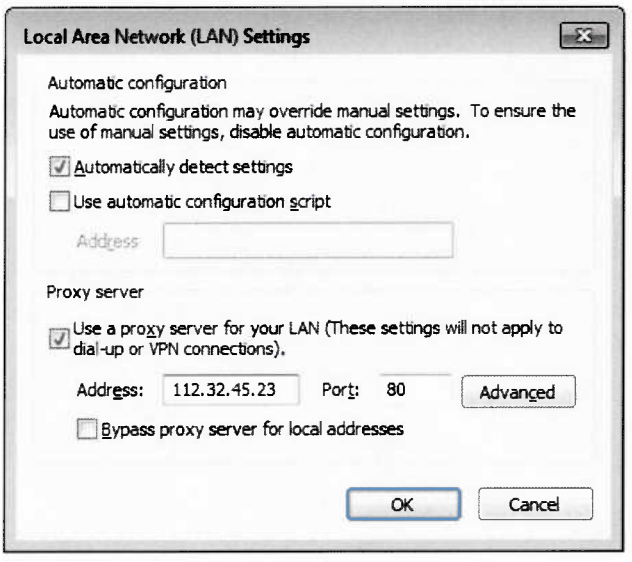
b) Nevn noen eksempler på hver faktor/metode

Oppgave 3.7

En venn av deg skal selge sin gamle Samsung Galaxy S5 på finn.no (ca. 2 år gammel smarttelefon). Hvilke råd vil du gi han for å sikre at det er trygt å gi fra seg telefonen til en ny eier? Du skal her altså IKKE si noe om sikkerhet i selve salgsprosessen.

Oppgave 3.8

Ved en tilfeldighet finner du plutselig følgende innstilling satt i maskinen til en bekjent. Et raskt søk viser at IP-adressen tilhører til en maskin i Indonesia.



Hva er det som har skjedd her? Forklar også hva eventuelle svindlere kan ha oppnådd, og hvordan innstillingen kan ha blitt satt.

Oppgave 3.9

Social Engineering benytter en rekke (enkle) prinsipper i psykologi for å gjøre svindlene mer troverdige (ett eksempel er *frykt*). Nevn noen psykologiske teknikker som benyttes, og gi et kort eksempel på angrep/farer/svindler knyttet til hver av dem.

Oppgave 3.10

a) Forklar hvordan sesjoner i nettsider benytter cookies (informasjonskapsler), og hvordan en slik cookie på "avveie" kan misbrukes.

b) List opp noen måter som en hacker/svindler kan få tak i brukerens cookie.