Høgskolen i Østfold

EKSAMEN

Emnekode:	**Emnenavn:**
ITF15015	Innføring i datasikkerhet
Dato:	**Eksamenstid:**
26/05-2017	09.00-13.00
Hjelpemidler:	**Faglærer:**
Ingen	Tom Heine Nätt

Om eksamensoppgaven og poengberegning:

Oppgavesettet består av **7** sider inklusiv denne forsiden. Kontroller at oppgavesettet komplett før du begynner å besvare spørsmålene.

Oppgavesettet 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 under 1 time.

Del 3 får da minst 3 timer til rådighet. Bruk tiden her godt.

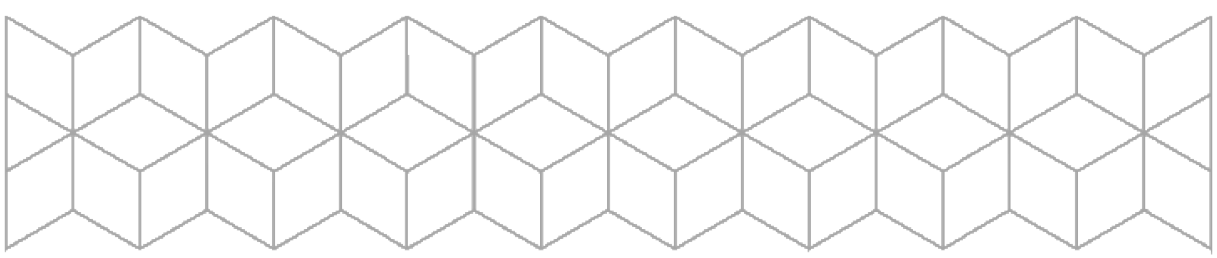
Gjør dine egne forutsetninger dersom du mener noe er uklart.

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

Ha en god og sikker sommer :-)

Sensurfrist: 17/6-2017

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



Del 1 – Påstander – 25 %

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. Begrepet **security** passer bedre enn begrepet **safety** når vi snakker om datasikkerhet i forbindelse med datakriminalitet.
2. Å benytte **POST** som overføringsteknikk i **HTTP** hindrer ikke at data kan avlyttes.
3. **BASE64** og **quoted-printable** er eksempler på krypteringsalgoritmer.
4. **Drive-by-download** vil si at noen klarer å hente ut informasjon fra dine servere/maskiner ved å koble seg på det trådløse nettet fra utsiden.
5. **Skadevare** og **virus** er to begreper som dekker eksakt det samme, og kan benyttes om hverandre.
6. Dersom en hacker får tilgang til en brukers **informasjonskapsler** kan dette bl.a. medføre **session hijacking**.
7. **HTTPS**-protokollen gir beskyttelse mot **XSS** (cross-site scripting).
8. 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.
9. Loggfiler er sentralt i forbindelse med **non-repudiation**.
10. **Authentication** og **access control** er to begreper som dekker eksakt det samme, og kan benyttes om hverandre.
11. **Ciphertext** og **kryptert melding** er to begreper som dekker eksakt det samme, og kan benyttes om hverandre.
12. **SHA1**, **MD5** og flere lignende algoritmer kan benyttes til å avsløre endringer/integritetsproblemer som er gjort både bevisst og ubevisst i programvare du laster ned.
13. **Phishing-angrep** innebærer at du lures til å oppgi sensitiv informasjon (passord, bankkortnummer osv).
14. **ARP-spoofing** er en form for **man-in-the-middle**-angrep.
15. All data som er slettet på en disk kan gjenskapes, så lenge ikke referansene til filene i selve ”filsystem-tabellen” er slettet.
16. **Whois-tjenester** kan være nyttige for å avsløre svindel-nettsider.
17. **Ormer** kan spille på **social engineering** for å spre seg selv.
18. En **trojaner** vil spres til alle filer på maskinen om den får være aktiv lenge nok.
19. Det at et **antivirusverktøy** oppdager en infeksjon betyr ikke nødvendigvis at det er i stand til å fjerne infeksjonen.
20. **VPN** er en kjekk måte å beskytte seg mot angrep der man ufrivillig blir lurt til å benytte en **proxyserver**.

Del 2 – Flervalg – 15 %

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.

Oppgave 2.1

Innen datasikkerhet er **snubletråd**:

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.

Oppgave 2.2

I forbindelse med passordlagring er **salt**:

a) En teknikk for å enkelt kunne knekke passord ut i fra mønstre på den hashede versjonen.
b) En av flere ulike varianter hash-algoritmer (Salt-SA1 og Salt-SA2 er de variantene vi vanligvis benytter i dag) som anses ekstra sikre ettersom de gjør hashingen to-veis.
c) En metode som gjør at brukerens passord får en ekstra sikkerhet når de hashes ved at de blir forlenget med noen ekstra forutbestemte tegn før hashing.
d) En teknikk for å lagre hashede passord.

Oppgave 2.3

En **logisk bombe** er:

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.

Oppgave 2.4

I forbindelse med validering av input fra brukere, hva menes med **whitelist**?

a) Liste med brukere som er "klarert" og som vi ikke trenger å validere input for.
b) Liste med gyldige tegn/input.
c) Liste med operasjoner vi kan gjøre for å endre ugyldige input til å bli gyldige.
d) Liste med datafelter som ikke trenger noen validering, da de allerede er validert tidligere i prosessen.

Oppgave 2.5

Ved å besøke en (for oss ukjent) webserver som har **HTTPS** er vi sikre på at:

a) Webserveren er godkjent av en tredjepart.
b) Det er vanskelig å utføre man-in-the-middle angrep på kommunikasjonen.
c) Webserveren følger standarden ISO-55-231 som bl.a. forteller hvordan tjenester skal håndtere overføring og lagring av data.
d) Vi slipper innlogging og dermed også faren for phishing-angrep.

Oppgave 2.6

Det begrepet som passer best i følgende utsagn er:
"…… skal sikre mot at uvedkommende får kjennskap til sensitive data".

a) Konfidensialitet.
b) Integritet.
c) Tilgjengelighet.
d) Autentisering.

Oppgave 2.7

Begrepet **spoofing** vil innen datasikkerhet si:

a) Hindre at man får sendt en melding (en form for *Denial of Service*).
b) Sende en melding som ser ut til å komme fra en annen avsender.
c) Sende så mange meldinger til en bruker at alle reelle meldinger forsvinner i mengden.
d) Endre innholdet i en melding som noen sender til en mottaker (en form for *man-in-the-middle*).

Oppgave 2.8

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

a) Noe du gjør, noe du får, noe du vet.
b) Noe du vet, noe du gjør, noe du er.
c) Noe du vet, noe du er, noe du har.
d) Noe du gjør, noe du har, noe du vet.

Oppgave 2.9

Hvilket av følgende begreper beskriver **IKKE** en av hovedkomponentene i skadevare:

a) Stridshode (warhead).
b) Omformer (reprogrammer).
c) Spredning (propagation).
d) Nyttelast (payload).

Oppgave 2.10

En **demilitarisert sone** (DMZ) kan beskrives som:

a) En del av organisasjonens nettverk som er delvis åpent ut mot Internett og som har lavere sikkerhetsnivå enn resten av nettverket.
b) En ekstern del av organisasjonens nettverk der man samler alle brannmurene bedriften har.
c) En del av organisasjonens nettverk hvor kun eksterne har tilgang.
d) En del av organisasjonens nettverk hvor kun interne har tilgang.

Del 3 – Tekstsvar – 60 %

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

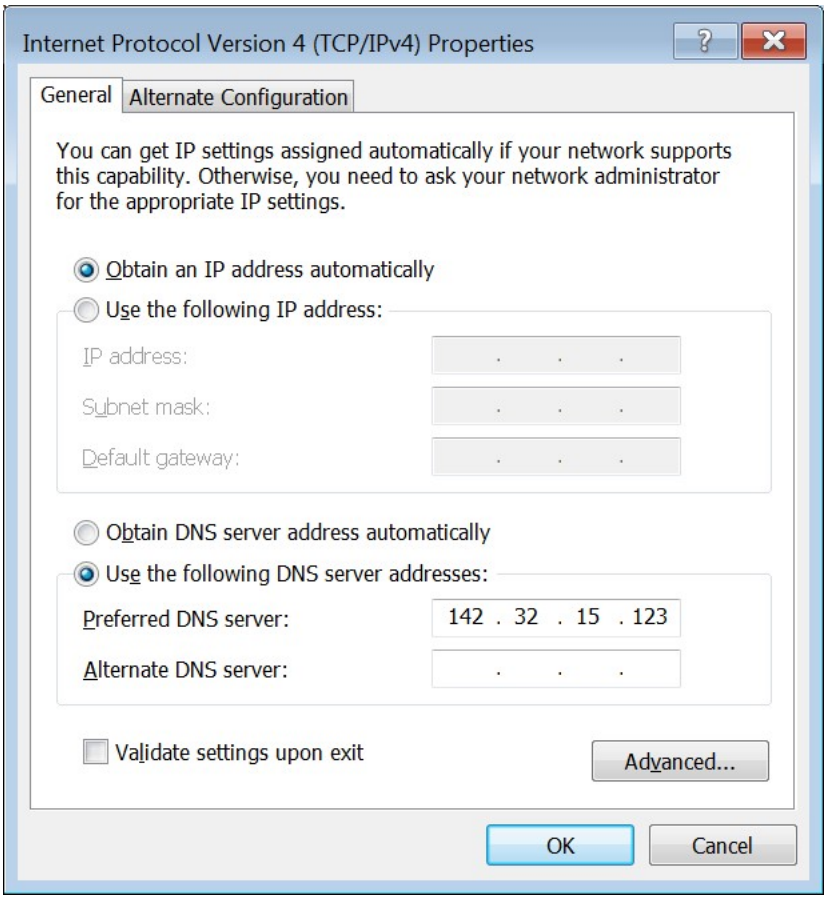
Fordel tiden godt! Oppgavene er ikke identiske i omfang. Noen av oppgavene i denne delen vil kreve noe mer tid/besvarelse, og vil da også bli vektet noe høyere i totalbedømmingen.

Mange av oppgavene etterspør ulike metoder/varianter/fremgangsmåter/ fordeler/ulemper osv. Husk at du forsøker vise bredden i din kunnskap. Ikke bare svar det mest opplagte, og gå videre.

Oppgave 3.1

Ved en tilfeldighet finner du plutselig følgende innstilling satt i maskinen til en bekjent av deg. IP-adressen er ikke til noen maskin i nettverket, og mye tyder på at maskinen med denne IP-adressen er lokalisert i Asia.

(fortsetter på neste side)



a) Hva kan svindlere kan ha oppnådd ved å få satt denne innstillingen på maskinen?

b) Skisser ulike metoder for hvordan innstillingen kan ha blitt satt.

c) Skisser noen scenarioer der du kunne blitt utsatt for DNS-svindel selv om innstillingen stod på ”Obtain DNS server address automatically”

Oppgave 3.2

Du kommer over en nettside for å organisere informasjon om, og påmelding til, ulike arrangementer. Nettsiden krever registrering og pålogging. Etter at man er logget på får man listet opp alle arrangementer fremover i tid. Sammen med informasjonen om hvert av arrangementene er det en unik link til påmelding for hvert arrangement. Linkene ser typisk slik ut:

```
<a href="http://www.hvaskjerherdatro.no/attend.php?happening=34524">Meld deg på</a>
```

Tallkoden som settes i *happening*-parameteret er en unik ID for det aktuelle arrangementet. Selve nettsiden linken fører deg til (attend.php) utfører påmeldingen og viser en bekreftelsesside.

a) Forklar hvordan en svindler kan benytte teknikken CSRF (Cross-site request forgery) til å melde på et offer til arrangementet 42434

b) Hva kan offeret gjøre for å beskytte seg mot slike CSRF-angrep?

c) Hva kan utviklerne gjøre for å (forsøke) forhindre CSRF-angrep?

Oppgave 3.3

a) Forklar hva SQL injection er.

b) Hva innebærer det at et SQL injection angrep omtales som blind og/eller som time based?

c) Hvordan kan SQL injection hindres?

Oppgave 3.4

a) Forklar forskjellen på kryptering med *delt nøkkel* (pre shared key / secret key) og *privat/offentlig nøkkel* (private/public-key).

b) Hvilke ulemper og fordeler er det med hver av de to metodene?

c) Hvorfor kan det være hensiktsmessig å benytte de to metodene sammen?

Oppgave 3.5

Du har tatt et litt pinlig bilde på en fest, og velger så å dele dette med dine Facebook-venner. Du er nøye med å sette ”friends only” som tilgang til bildet, da det ikke er helt heldig om det kommer ut til andre. To dager senere blir du tipset om at bildet ligger åpent på et nettsted. Forklar ulike scenarier for hvordan bildet kan ha havnet der.

Oppgave 3.6

Du finner en ukjent USB-minnepenn i gangen på skolen. Nevn ulike grunner til at du ikke bør sette denne inn i din egen maskin. Forsøk å fokusere på tekniske farer.

Oppgave 3.7

a) Forklar hvordan en hacker kan få deg til å koble på sin trådløse basestasjon/aksesspunkt. Husk at det er flere metoder som kan nevnes her (både at brukeren gjør noe dumt og at maskinen "blir lurt"). For de tekniske variantene så er det nok å forklare overordnet hvordan det gjøres.

b) Nevn noen muligheter som en hacker kan få dersom din trafikk går gjennom hackerens basestasjon/aksesspunkt. Fokuser på å få med mer enn kun "det opplagte" svaret.

c) Hvilke forhåndsregler kan du ta for å minimere sikkerhetsrisikoen ved ukjente og falske basestasjoner. Fokuser både på å forhindre bruk, og å gjøre bruk tryggere.