Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

Teori 5 (Del 5): Angrepsvektorer og skadevare

Oppgave 1: Angrepsvektorer

a. Hva er den vanligste angrepsvektoren for cyberangrep?
b. Hvordan kan deepfake-stemme og video brukes i cyberangrep?
c. Hvordan kan USB-enheter som f.eks. (ligner på) en minnepinne brukes for å angripe en datamaskin?

Oppgave 2: Leveransekjedeangrep

a. Forklar hva som menes med leveransekjedesårbarheter.
b. Beskriv eksempler på leveransekjedeangrep som har skjedd i de siste årene.
c. Hvilke tiltak kan en virksomhet benytte for å redusere leveransekjederisiko (eng. Cyber Supply Chain Risk Management, C-SCRM)?

Oppgave 3: Bottnett

a. Hva er et bottnett?
b. Hva er et DDoS, og hvordan kan et bottnett brukes til å gjøre et DDoS-angrep?
c. Mirai er en skadevare som ble brukt til å «ta ned» internett i store deler av USA gjennom et angrep på en Dyn DNS en dag i oktober 2016. Beskriv kort Mirai og hvordan dette angrepet ble utført

Oppgave 4: XSS

Du er medlem av en ny sosial plattform kalt FAGSNAKK utviklet av og for studenter ved universitetet hvor dere kan ha faglige diskusjoner, organisert med én side for hvert fag. En dag er FAGSNAKK-siden full av det samme hundebildet som (det ser ut som) har blitt postet av ulike brukere (inkludert deg), uten at noen kan huske at de har gjort. En medelev mener at dette kan skyldes en XSS-sårbarhet i FAGSNAKK og at bildene er et resultat av et XSS-angrep.

a. Hva et XSS-angrep?
b. Hvordan kan XSS-angrepet beskrevet ovenfor vært gjennomført?
c. Hvordan kunne angrepet på FAGSNAKK ha vært forhindret?

Oppgave 5 Tilgang for skadevare (eksamensoppgave 2023):

3.1 Tilgang for skadevare

Du kjører uheldigvis skadevare på maskinen din med din administratorbruker. Du har slått av UAC (User Account Control) på maskinen din – Hvilke rettigheter får skadevaren da?

Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Bruker
- Gjest
- Administrator
- Power user

Maks poeng: 1

Oppgave 6 Skadevare (eksamensoppgave høsten 2023)

3.4 Skadevare

Velg den kolonnen som passer best med hver rad. Det gis ett poeng for hvert svar, 0 for blanke og minus ett for hvert gale.

Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

Finn de som passer sammen:

	Bakdør	Dataorm	Virus	Løsepengevirus	Trojaner
En skjult metode for å omgå normal autentisering og tilgangskontroll					
Maskerer seg som legitime programmer som faktisk (eller tilsynelatende) har nyttige funksjoner.					
Infiserer andre programmer ved at skadelig kode legges til og flettes inn i andre programmer.					
SQL-slammer er en					

Maks poeng: 4

Oppgave 7 Løsepengevirus (eksamen høsten 2022)

(true/false – 0,5 poeng for riktig svar, -0,5 for galt – minimum 0 poeng)

a) Mange løsepengevirus krypterer offerets systemer ved hjelp av av SHA-256

b) Et viktig sikkerhetstiltak mot løsepengevirus i virksomheter er å ikke gi brukerne administratorrettigheter