IN1020: Øvingsoppgaver uke 47 (18.-22. november 2019)

Oppgave 1:

Kom med forslag til hvordan en angriper kan bruke sosial manipulering til å:

a) få uautorisert tilgang til en virksomhets/en bedrifts lokaler/bygg

b) installert skadevare på de personlige datamaskinen til selskapets direktør

Oppgave 2:

a) Hvilke sårbarheter er det vanlig å utnytte i det vi kaller phishing attacks?

b) Foreslå sikkerhetstiltak for å forebygge slike angrep (phishing attacks).

Oppgave 3:

På semestersiden til IN1020 finner dere et bilde:

https://www.uio.no/studier/emner/matnat/ifi/IN1020/h19/ukeoppgaver/vinterblomst.jpg

a) Finn ut hvor bildet er tatt ved å se på *metadataene* som følger med i bildefilen.

b) Finner du annen interessant informasjon i bildets *metadata*?

Oppgave 4: Kryptografi

a) I hvilke situasjoner og til hvilke formål kan kryptografi benyttes til å beskytte informasjon?

b) Hvorfor er riktig *administrasjon* av kryptografiske nøkler så viktig?

c) Beskriv kort hovedformålet med PKI

Oppgave 5: Kryptering

Anne skal sende en melding til Per, uten at Tom kan få tak i den. Anne og Per har avtalt å bruke symmetrisk kryptering og de har allerede utvekslet nøkler. Beskriv fremgangsmåten (stegene) de må følge for å kryptere, sende og dekryptere meldingen.

Oppgave 6: Kryptering

Assymetrisk kryptering med nøkkelpar bestående av privat og offentig nøkkel, benyttes til både digital signatur og kryptering av innhold av en melding. Hvordan må nøkkelparet benyttes (dvs. skal avsender eller mottagers nøkkelpar benyttes? Hvem skal benytte offentlig og hvem skal benytte privat nøkkel?) ved

a) digital signatur (uavviselighet/autentisere opphav til en melding, altså at avsender er korrekt)?

b) kryptering av innhold i en melding?

Oppgave 7: Case-oppgave

Til tross for at en webtjeneste for en nettbank er svært sikkert konfigurert, kan ting gå galt f.eks. når en bruker skal bruke (logge seg inn til) banken for å betale en regning. Diskuter mulige feil som kan oppstå (hint: brukerfeil, trådløst nett, etc).

Oppgave 8: Case-oppgave

I oppkobling mot en online webtjeneste autentiseres brukeren i starten av sesjonen. Data utveksles så med webtjeneren til og fra vedkommendes lokale maskin (endenode). Kan tjenestetilbyder på bakgrunn av brukerautentiseringen anta at data som mottas gjennom den etablerte forbindelsen er autentiske?

Oppgave 9: Sjekksumalgoritme (hash-funksjon)

Gjennomføres på Ifis linux-maskiner.

a) Programmet sha256sum genererer en sjekksum av en fil basert på algoritmen SHA256:

```
[kritisk@vestur]>sha256sum abc.txt
[6ee0c32c675ce6d3bd3f6e326c81e45b3d6675c29c0c9ced1398684a667804e9  abc.txt
```

Gjør endringer i fila abc.txt, og kjør programmet en gang til. Er nøkkelen den samme?

b) Hvordan kan sjekksumalgoritmer bidra til å sikre dataintegritet?

c) Finn og diskuter situasjoner/eksempler hvor bruk av sjekksumalgoritme kan være nyttig for deg.

Oppgave 10: SSL

SSL Labs er et forskningssamarbeid som jobber for økt bevissthet rundt bruk av SSL. De tilbyr også en online-tjeneste for å teste nettlesere og web-tjenere med tanke på hvor godt (sikkert) SSL er implementer og konfigurert i den enkelte nettleser/tjener.

a) Bruk https://www.ssllabs.com/ for å sjekke nettleseren din. Nettleser på Ifi, laptop, mobil, nettbrett, etc. Er den sårbar? Hvilke protokoller støtter den?

b) Bruk https://www.ssllabs.com/ for å sjekke kjente web-tjeneres sertifikat og konfigurasjon. Finner du sårbarheter? Kan du si noe om sertifikat, nøkkel samt protokoll(er) den enkelte tjener støtter?

c) Ta også en kikk på https://www.ssllabs.com/ssl-pulse/

Oppgave 11: Tilgangskontroll i Unix

Tilgangskontroll er et av mange sikkerhetstiltak innen informasjonssikring. I denne oppgaven skal du anvende det du har lært om beskyttelser av filer i Unix, samt tilgangsstyring, til å utforske enkel tilgangskontroll i praksis.

Oppgaven utføres på Ifis linux-maskiner. Bruk de to siste sidene i presentasjon fra forelesning 13.11.19 ("Tilgangskontroll i Unix"), samt avsnittet om "Filer" i forelesning 25.09.19 som hjelp.

Opprett en mappe på hjemmeområdet ditt, og legg en fil med litt tekst i denne mappen (abc.txt). Endre rettighetene på mappen slik at eieren kun har tilgang 'execute'. Prøv deretter å

a) Liste innholdet i mappen, se på innholdet i fila abc.txt, lage en kopi av abc.txt i samme mappe, samt flytte deg inn til mappen med kommandoen 'cd'.

b) Gjenta det samme eksperimentet, men med å først sette readrettighet og deretter "writerrettighet på mappen. Forsøk å forstå det du observerer.

c) Hvordan bidrar denne enkle tilgangskontrollen til å oppnå sikkerhetsmål som konfidensialitet og dataintegritet?