IN1020 - Datasikkerhet og nettverkskommunikasjon: Øvingsoppgaver gruppetime 9 (uke 43)

1 Teori- og diskusjonsoppgaver

1. DNS
   (a) a) Hva er en DNS-adresse, og hvorfor benytter man dette i tillegg til IP-adresser?
   (b) b) Hvilken tjeneste utfører en DNS-rottjener?
2. Forbindelsesstrategier Push, Pull og Publish-subscribe er noen paradigmer for initiering og gjennomføring av kommunikasjon over Internett. Hva er forskjellen mellom disse paradigmene? Nevn eksempler på applikasjoner som benytter paradigmene.
3. Aksessmodeller Hva er forskjellene mellom klient/tjener og peer-to-peer topologiene? Nevn eksempler på begge modeller.
4. CDN
   (a) Hva er et "Content Delivery Network (CDN)"?
   (b) Nevn 3 grunner til at man velger å bruke et CDN for distribusjon av data:
5. Streaming Hva er Dynamisk, Adaptiv Streaming over HTTP (DASH)?
6. HTTP
   (a) Forklar kort kommunikasjonen mellom en nettleser og en HTTP-tjener når du spør etter en hjemmeside over nettverket.
   (b) Hvilken transportprotokoll bruker HTTP, og hvilken port er standard for tilkobling for denne tjenesten?
   (c) Hva er forskjellen på persistente og ikke-persistente TCP-forbindelser?
   (d) I hvilken grad beskytter bruk av https og digitale sertifikater i internettrafikk oss mot svindel og utnyttelse, og hva beskytter det evt. ikke mot?
   (e) Bonusoppgave: Hvilken port er standard for tilkobling med HTTPS?
7. Sosial manipulasjon
   (a) Hvilke sårbarheter er det vanlig å utnytte i det vi kaller phishing attacks?
   (b) Foreslå sikkerhetstiltak for å forebygge slike angrep (phishing attacks).
   (c) Kom med forslag til hvordan en angriper kan bruke sosial manipulering til å:
      i. få uautorisert tilgang til en virksomhets/en bedrifts lokaler/bygg
      ii. installert skadevare på de personlige datamaskinene til selskapets direktør
8. Innsamling av fritt tilgjengelige data benyttes ofte av hackere for mer rettet phishing. Her er noen oppgaver du kan forsøke deg på.

(a) Hvor spiste Erna Solberg middag 26. februar 2021?

(b) På semestersiden til IN1020 finner dere et bilde:
https://www.uio.no/studier/emner/matnat/ifi/IN1020/h23/ukeoppgaver/vinterblomst.jpg

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

ii. Finner du annen interessant informasjon i bildets metadata?

(c) Hva er brukernavnet til Universitetsdirektøren til UiO? (Og hvordan fant du det?) Hvordan kan kjennskap til noens brukernavn potensielt misbrukes?

9. Dataangrep:

Året er 2017. På jobben din er bruk av datamaskiner en essensiell del av arbeidet. Hver av de ansatte sitter på harddisker fulle av halvferdig arbeid og businesshemmeligheter som til sammen er verdt milliarder! En dag blir du møtt med denne meldingen på desktoppen din:

```
"Ops, your important files are encrypted"
```

Videre ber meldingen deg å kjøre en dekrypterings-programvare, som allerede har poppet opp. I dekrypterings-programvaren ser du en klokke som teller ned, og en melding som ber om 300 bitcoin (som var mye penger i 2017). Du ser rundt deg og flere og flere av kollegaene dine ser ut til å bli rammet. Full panikk! Hva nå?

(a) Hvordan tror dere hovedpersonen ble rammet av denne skadevaren? Har de gjort noe dumt eller kan dette skje uansett om man er flink selv?

(b) Diskuter hva slags skadevare det er snakk om her.

(c) Hvordan kunne arbeidsplassen forhindret angrepet? (Kunne de det i det hele tatt?) Hva er lurt å gjøre når angrepet først har begynt?

(d) Hvilke sikkerhetsmål er svekket av angrepet?

(e) Denne oppgaven er basert på ekte hendelser. Kjenner dere til dette angrepet?

10. Tjenestenektangrep er en form for angrep som gjerne forbindes med herverk og sabotasje, eller økonimisk kriminalitet i form av utpressing.

(a) Hvilke sikkerhetsmål påvirkes av denne type angrep?

(b) Hvilke ulike former for tjenestenektangrep benyttes ofte av hackere i dag?

(c) Hva kan virksomheter gjøre for å sikre seg mot denne typen angrep?

11. EUs *"The cookie law"*, eller *ePrivacy Directive* trådde for alvor i kraft i 2011, og regulerer bruk av informasjonskapsler (cookies) på nettsider. Dette har du nok lagt merke til ettersom nesten alle nettsiden i dag spør om lov til å bruke cookies. Hvorfor ønsker/ønsker vi ikke at nettsider skal lage cookier for oss?

12. 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).

13. 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?

2 Praktiske oppgaver for å bli kjent med nyttige nettverksverktøy

- **P1)**

  Programmene på din datamaskin kan bare sende beskjeder til andre maskiner hvis den kjenner IP adressen til maskinen den skal snakke med. Vi foretrekker å bruke navn i stedet for en IP-adresse. Maskinen guanin.uio.no har for eksempel adressen 129.240.65.61

  Åpne opp en terminal i Linux og bruk kommandoen "dig" for å finne adresse for navnene.

  Hva finner du ut hvis du for eksempel kjører "dig ifi.uio.no" og dig "login.ifi.uio.no". Hva med "dig www.microsoft.com".

- **P2)**

  "whois" er et verktøy som kan brukes til å slå opp informasjon om hvem som administrerer en IP-adresse eller et domenenavn.

  Hvem administrerer IP-adressen som ble returnert da du kjørte "dig www.microsoft.com"? Hvem administrerer domenet "microsoft.com"?

- **P3)**

  Når du programmerer på applikasjonslaget bruker vanligvis programmet transportlaget, som igjen bruker lagene under. Kommandoen "traceroute" bruker for å vise stien som pakken bruker fra din datamaskin til destinasjonen.

  Hvor mange routere er brukt for å sende en pakke til www.ifi.uio.no, www.uio.no, www.ntnu.no, www.kth.se, www.cmu.edu

  Hvis ikke programmet "traceroute" er installert på din maskin kan du bruke et online verktøy:

  http://networktools.nl/traceroute/

  Finn en maskin på hvert kontinent, og kjør traceroute til dem. Tips: For å finne en maskin på et bestemt sted, kan du forsøke å søke etter et universitet eller en bedrift som hører til på stedet og prøve traceroute til hjemmesidens domenenavn.

  Bruk verktøyet Traceroute Mapper til å analysere rutene dere har funnet

  https://stefansundin.github.io/traceroute-mapper/

- **P4)**

  Hvor mange aktive TCP-forbindelser har maskinen? (for å telle, kan du kjøre "netstat -t | grep ESTABLISHED | wc -l")