T-02
MALWARE

1) Hva står «malware» for? Hva betyr «malware»?
Malware står for «Malicious Software».
Malware er en fellesbetegnelse på «ondsinnet programmvare» som utfører uautoriserte og (oftest) skadelige handlinger.

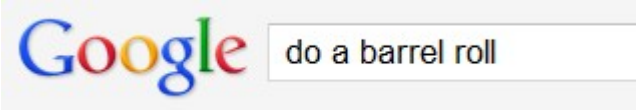
2) Hvilke ulike klassifikasjoner av malware har vi?
Vi kan dele malware opp i ulike typer etter hvordan den spres og skjules.

- Spredning
  - Virus
    - Menneskeassistert spredning (Spres ikke automatisk). Denne typer krever for eksempel at en bruker åpner et vedleg i epost.
  - Orm
    - Spres automatisk og krever dermed ikke at noen menneskeassistering. Denne typen kan spres mellom maskiner over nett.
- Skjuler seg
  - Rootkit
    - Endrer OS for å skjuler sitt nærvær.
  - Trojaner
    - Nytteprogram som skjuler ondsinnede operasjoner. Dette vil si at det er et program som en bruker ser på som «vanlig» og ikke farlig, men inneholder onsinnede operasjoner. Eksempler her er keylogger
- «Nyttelast» (Payload)
  - Alt fra humor/irritasjon til ran av maskinkraft og identitetstyveri

3) Hva menes med «innside-angrep»?
Insider-angrep betyr at det er noen som er en del av orginisasjonen som er med å kontrollere eller bygge tjenesten som legger inn for eksempel «backdoor» (sikkerhetshull som er lagt inn med vilje av en programmerer)

4) Hva menes med «backdoor»?
En skjult metode/kommando i et program som tilater en bruker å utføre handlinger man normalt ikke har tillatelse til.

5) Hva er «Easter Egg» i forhold til Malware?
Easter egg er en type backdoor som ofte er lagt inn med vilje, men ikke er skadelig.
Eksempel på dette kan være å gå på «www.google.com» og søke på «do a barel roll»



6) Hva menes med Logikkbomber
Logikkbomber utfører en handling først når en bestemt betingelse inntreffer

Eksempel på Logikkbombe kan være at en person er med å lage software til mini-bank. Enten legger personen inn en «bug» i koden med vilje eller ikke og i dette eksempelet kan dette føre til at visst man utfører en kommando klokken 15:02 så vil maskinen «spytte» ut penger.

7) Hva er et virus?
Ett virus er et program som kan replisere seg selv ved å enten endre andre filer/program, infisere dem med kode eller formere seg viere. Virus krever vanligvis brukerassistering for å formere seg.

8) Hvordan spredde «Brain»-viruset seg?
Viruset spredde seg rundt i verden via diskett

9) Hva er en orm («Worm»)?
Dette er malware som sprer kopier av seg selv uten å infisere andre program, og vanligvis kreves det ingen menneskelig medvirkning(brukerassistering). I de fleste tilfeller vil ormen ha en ondsinnet nyttelast (payload) der den for eksempel kan installerere en bakdør(backdoor) eller slette filer

10) Skriv en kort sammendrag av hva «ILOVEYOU»-ormen var
ILOVEYOU-ormen var den aller første ormen som spredde seg gjennom epost og kom 4. mars 2000. Brukeren måtte manuelt åpne en fil i eposten. Den gjorde egentlig ikke noen skade, men bare spredde seg. I løpet av 9 dager så hadde 50 millioner Pcer blitt infisert

11) Hva er en «Trojaner»
Dette er malware som ser ut til å utføre en nyttig jobb, men i tillegg gjør noe ondsinnet. Eksempler på dette kan være at man laster ned en musikkspiller, men uten at du vet det så eksekverer dette programmet kode som logger alle tastetrykk og sender det til en «ond» person.

12) Hva er et Rootkit?
Rootkits er en samling av software som brukes til å få tilgang til områder personen ikke er autorisert til. Rootkits kan manipulere data på root-nivå og dermed endre/fjerne filer. Siden rootkit kan endre filer så kan den også skjule seg for antivirus programmer.

13) Hva er «botnet»?
Malware kan gjøre maskinen om til en «zombie», som er en eksternt kontrollert maskin som benyttes i ondsinnede angrep, vanligvis som en del av et botnet

14) Hvordan bruker antivirusprogrammer signaturen til å flagge programmer?
Signaturen til et malware er selve «fingeravtrykket» og antivirusprogrammer har en malware database med alle kjente signaturer. Så fort antivirusprogrammer klarer å finne en kjent signatur så vil den flagges.

15) Hva er en Heuristisk analyse?
Dette er en analyse som brukes til å identifisere nye og «zero-day-malware». Basert på instruksjonene forsøker antiviruset å bestemme om det er malware ut fra om det for eksempel forsøker å ende/slette system-filer. Også Emulering av eksekvering hvor man kan kjøre koden i et isolert miljø og overvåke atferden, dersom det finnes mistenkelig atferd så markeres det som malware.