Week-03 Logging and monitoring

- **Explain the difference between prevention, detection and recovery for systems you develop.**

  Prevention/forebyggelse, er hvor man "ruster" systemet, så det er modstandsdygtigt over for eventuelle angreb på systemet. Ifølge OWASP er *insufficient logging and monitoring* et grundlag for størstedelen af store hændelser.

  Detection, hvor man benytter sig af monitoring og logs til at finde ud af, om der er sket et brud, og i så fald hvem der har forårsaget bruddet.

  Recovery, hvor der skal rettes op på skaderne ved bruddet.

- **Discuss how a firewall can produce log files.**
  For hver request der bliver lavet, skal denne 'forbi' firewallen. Alt efter hvordan man har konfigureret sin firewall vil dette request blive godkendt og klienten vil blive sendt videre eller denne vil blive blokeret.

  Firewallen kan konfigureres med en whitelist og en blacklist.
  - Blacklist er 'threat-centric', så denne vil blokere suspekte requests eller ondsindede entiteter(default er at give adgang).
  - Whitelist er 'trust-centric', så denne involvere kun at give adgang til troværdige entiteter (Default er at nægte adgang).

  En log kan tilkobles en firewall, så f.eks. IP-adresse og tid kan noteres og gemmes i en logfil, man kan tilgå efter ønske.

- **Explain how to set up a remote logging server, and use that to register logins to an ubuntu server.**
  I tilfælde af at man bliver hacket vil det ikke værte muligt at se i log-filerne hvad der skete, derfor er det en god idé at logge til en anden maskine.
  Konceptuelt sætter man en server op hvori man laver en context path til sin(e) log-fil(er). På en anden server opsætter man en firewall, som sender et POST request til log-fil serveren, hvor de ønskede informationer skrives ind i filen.

- **Explain how to use a cloud-based logging service to enable anomaly detection.**
  Flere firmaer tilbyder ovenstående som service. Tag et eksempel som Logentries, et firma som tilbyder cloud-based logging og anomaly detection.
  Som bruger vil man f.eks. kunne opsætte real-time alerting baseret på afvigelser fra vigtige mønstre og log begivenheder. Så antag at en server responstid skifter fra et sekund til fem sekunder, men at der ikke bliver genereret nogle standardfejl, dette vil let kunne blive overset, men Logentries kan lave en query, som henter specifik log-data som kan monitoreres.