**Week-03 Continued A10 - Logging and monitoring**

**Agenda**

1. Prevention, Detection og Recovery
2. Forklar hvordan en firewall kan logge
3. Praktisk eksempel: Remote logging server
4. Forklar hvad cloud-based logging service er

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

**Prevention**: Fokuserer på at holde ondsindet software ude af systemet og inkluderer antivirus-, firewall- og e-mail-filtreringsløsninger. Prevention dækker bl.a. over authentication, access control, identification og authorization.

**Detection**: Fokuserer på at skabe opmærksomhed på sikkerhedsbrud så hurtigt som muligt, og inkluderer logging og monitoring, samt anvendelse af netværks overvågningsværktøjer.

**Recovery**: Fokuserer på at rydde op efter et angreb så hurtigt som muligt og inkluderer sikkerhedskopiering/backups.

Hvis vi er blevet hacket har vi forhåbentlig en backup af vores server så vi kan nulstille systemet og derudover har vi forhåbentligt detekteret hvem der har hacket os, og logget dette på en separat urørt server.

Hvis vi har anvendt **Detection** rigtigt, ved vi hvordan hackeren er kommet ind og kan anvende dette til **Prevention** så det ikke sker igen.

**Discuss how a firewall can produce log files.**

Ved at sætte en firewall op på sin server, har man mulighed for at styre den indadgående og udadgående trafik. Dette kan gøres ved at ‘DENY’ eller ‘ALLOW’ specifikke porte, IP-adresser eller kombinationer af disse. Ved at aktivere logging på sin server, kan man således monitorere den indgående trafik, som bliver gemt i logfilerne. Her kan man bl.a. se:

**SPT (source port) =** som er den port den besøgende sender fra

**DPT (destination port) =** som er den port den besøgende forsøger at komme igennem til serveren.

**SYN URGP (urgent pointer) = 0**, som indikere at den besøgende har forsøgt at tilgå serveren flere gange, men fra en ny forbindelse.

Alle disse informationer findes i transport laget på de pakker, som sendes med requestet til serveren. En firewall kan kigge på det lag, trække informationerne ud og gemme dem i en logfil.

Logging kommando: sudo ufw **logging** on|off|LEVEL

**Explain how to set up a remote logging server, and use that to register logins to an ubuntu server.**

Først lægger vi et logger program op på vores server. Dette program har kun en funktion. Den lytter på en port og gemmer den information der bliver sendt til den port, i en logfil angivet af environment variablen LOG\_PATH



Herefter sættes en firewall til, og tillader adgang gennem port 22 (SSH) og 8765 (porten på log-serveren). Det er vigtigt at denne server er sikret mod hackere så på den måde øger vi sikkerheden.

På den server vi ønsker at logge logins fra tilføjer vi et script som sender et request til logger serveren ved hvert login forsøg:

nano /etc/profile.d/logger.sh

I denne fil skriver vi scriptet:

Et billede, der indeholder skærmbillede, monitor, skærm, tv

Automatisk genereret beskrivelse

Når nogen forsøger at logge ind på serveren, vil der oprettes en log inde på log-serveren, som fortæller hvem der er logget ind. Det kan ses på nedenstående billede:

**Et billede, der indeholder skærmbillede, monitor, skærm, sort

Automatisk genereret beskrivelse**

**Explain how to use a cloud-based logging service to enable anomaly detection.**

laas = logging as a service

<https://docs.datadoghq.com/logs/>

I stedet for selv at skulle lave et program der kan tage imod informationer, logge dem og analysere dataen kan vi ved at anvende **cloud-based logging** overgive den opgave til en laas (logging as a service) virksomhed. Disse virksomheder har langt bedre værktøjer til at analysere trafikken på din server og kan hurtigt advare dig hvis der er anormal adfærd.

Ved at anvende Cloud based logging, er monitorering uafhængig af dit netværk, som således ikke bliver langsommere grundet errors.

Disse laas virksomheder anvender avancerede algoritmer og Machine Learning til at analysere din data og lære at identificere adfærd som er mistænksom, samt relevante mønstre.