

□ Uge 10 – Fysisk sikkerhed og host-based firewall

I denne uge arbejder vi med **klassiske sikkerhedsmekanismer på host-niveau**, med fokus på både den **fysiske kontekst omkring systemer** og **teknisk netværksbeskyttelse via host-based firewalls**.

Ugen fungerer samtidig som **forberedelse til senere arbejde med Wazuh, logning og detektion**.

□ Forberedelse

- Se kolonen *Forberedelse og pædagogisk tilrettelæggelse* i planen på It's learning

□ ♂ Øvelser

- [Installation af iptables](#)
 - [Bloker alt indgående trafik](#)
 - [Tillad indgående trafik fra etablerede forbindelser](#)
 - [Tillad indgående trafik fra specifikke ICMP-beskeder](#)
 - [Opsætning af Wazuh server](#)
(*Eftermiddagsøvelse – selvstændigt gruppearbejde*)
-

□ Læringsmål der arbejdes med i faget denne uge

Overordnede læringsmål fra studieordningen

□ Viden

Den studerende har viden om:

- Relevante it-trusler

▮ Færdigheder

Den studerende kan:

- Udnytte modforanstaltninger til sikring af systemer

▮ Kompetencer

Den studerende kan:

- Håndtere værktøjer til at reducere endpoint-trusler
- Udvalge og anvende praktiske mekanismer til at forhindre it-sikkerhedsmæssige hændelser

▮ Praktiske mål for ugen

- Den studerende forstår, at hændelser i den fysiske verden også udgør it-sikkerhedstrusler
- Den studerende kan lave en grundlæggende firewall-opsætning på en Linux-host
- Den studerende forstår firewallens rolle i host-baseret sikkerhed
- Den studerende kan forklare forskellen på *block list* og *allow list*-tilgange

▮ Afleveringer

- Ingen formel aflevering
- Eftermiddagsøvelsen danner grundlag for senere arbejde med Wazuh og semesterprojektet

▮ Skema

Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen
08:30	Oplæg og gruppeøvelser: Fysisk sikkerhed

Tid	Aktivitet
09:30	Oplæg: Firewalls og host-based firewall
09:45	Pause
10:00	Individuelle øvelser: iptables firewall
11:20	Opsamling på dagen
11:30	Eftermiddagsøvelse: Opsætning af Wazuh på Proxmox Ubuntu-server

□ Kommentarer

- Fokus i denne uge er **beskyttelse på host-niveau**, ikke netværksperimeter.
- Firewall-øvelserne anvender en *allow list*-tilgang, som er central i moderne systemsikkerhed.
- Wazuh-opsætningen er **forberedende** og skal ikke færdiggøres – formålet er overblik, forståelse og dokumentation.
- Erfaringerne fra ugen bruges direkte i senere undervisning om logning, detektion og SIEM/XDR.

Last update: 2026-03-20 13:58:28