# IDS – Järjestelmät

Noa Julkunen

Esitelty vain murto-osa IDS-järjestelmistä. Hyökkäysten torjuntajärjestelmiä (IPS) on jo integroitu uusimpiin palomuureihin.

## Snort

Snort on avoimen lähdekoodin IDS- ja IPS-ohjelmisto Linuxille. Se on kehitetty vuonna 1998 Martin Roeschin toimesta. Ohjelmisto tarkkailee liikkuvien pakettien sisältöä, protokollia, porttien käyttöä ja skannausta. Sovellusta voidaan käyttää kolmessa eri tilassa, sniffer mode, packet locker mode ja network intrusion detection system mode. **Sniffer** mode lukee internetissä liikkuvia paketteja ja näyttää niitä consolessa. **Packet Logger** mode pitää tallentaa tietoja paketeista tietokoneelle. **Network Intrusion Detection System** modessa ohjelma tarkkailee liikennettä verkossa ja tarkistaa niitä määritellyn säännön mukaan, suorittaen tarkistuksen tuloksen mukaan tarpeellisia toimintoja. Snort-ohjelmisto on ilmainen ja sen voi ladata osoitteesta https://www.snort.org/downloads#snort-downloads.

## Smoothwall Express

Smoothwall on avoimen lähdekoodin palomuuri Linuxille. Ilmaisversio julkaistiin vuonna 2000, maksullinen puolestaan 2001. Ohjelmisto tarjoaa monia ominaisuuksia, joka tekee palomuurista kattavamman. **Portforwarding**, **outbound rules**, **QoS (**Quality-of-Service) sekä verkon statistiikan seuraaminen on muutamia lukuisista ominaisuuksista. Ohjelmiston voi ladata osoitteesta https://smoothwall.org/download.html

## Security Onion

Security Onion avoimen lähdekoodin IDS-ohjelmisto. Se tarjoaa ominaisuuksia kuten verkossa liikkuvien pakettien kiinniottaminen (haitallisten pakettien), pakettien hakemista ja indeksointia sekä datan esittämistä visuaalisessa muodossa. Ensimmäinen versio on julkaistu vuonna 2009. Ohjelmiston voi ladata osoitteesta https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md.

## TippingPoint

TippingPoint on IPS-ohjelmisto joka suojaa tietokonetta monimutkaisilta hyökkäyksiltä. Ohjelmisto voi näyttää ja estää inbound ja outbound network liikennettä reaaliajassa. Ohjelmisto ei ole avoimen lähdekoodin sovellus, vaan se on maksullinen.

## Lähteet


https://talosintelligence.com/snort

https://en.wikipedia.org/wiki/Snort_(software)

https://www.linuxlinks.com/smoothwallexpress/

https://www.csoonline.com/article/3453199/what-is-security-onion-and-is-it-better-than-a-commercial-ids.html

https://docs.securityonion.net/en/2.3/about.html#security-onion

https://www.trendmicro.com/en_us/business/products/network/intrusion-prevention/tipping-point-threat-protection-system.html