# Snort

Fix Me!

Является свободной сетевой системой предотвращения вторжений (IPS) и сетевой системой обнаружения вторжений (IDS) с открытым исходным кодом, способной выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP сетях. Snort была написана Мартином Роешом и в настоящее время разрабатывается компанией Sourcefire, основателем и техническим директором которой является Роеш. Snort выполняет протоколирование, анализ, поиск по содержимому, а также широко используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как переполнение буфера, стелс-сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения ОС. Программное обеспечение в основном используется для предотвращения проникновения, блокирования атак, если они имеют место.

Snort может работать совместно с другим программным обеспечением, например, SnortSnarf, sguil, OSSIM и Базовый Механизм Анализа и Безопасности (BASE) обеспечивающий визуальное представление данных вторжения. С дополнениями для исходников Snort от Bleeding Edge Threats, поддерживает антивирусное сканирование потоков пакетов ClamAV и анализ сетевых аномалий SPADE в 3 и 4 слое сети, возможно с учётом истории изменений.

http://ru.wikipedia.org/wiki/Snort

http://sysadminmosaic.ru/snort/snort

2015-11-30 17:21