SNORT v3

Cisco Partner
https://cs.co/1page

Snort is an open-source network intrusion prevention system (IPS), capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks such as buffer overflows, stealth port scans, CGI attack and much more.

v3 Benefits:

- Updated from Snort v2 for better efficacy, performance, scalability, usability and extensibility
- Multi-Threaded Architecture - frees up more memory for packet processing
- Improved shared object rules, including the ability to add rules for zero-day vulnerabilities
- Next-Gen Cisco Talos Rules – (e.g., REGEX/Rule Options/Sticky Buffers)
- New and Improved HTTP Inspector (e.g., HTTP/2 support)
- Lightweight content updates from Talos
- Access to more than 200 plugins
- Distribution through GitHub repo with updates every 2 weeks
- Fully configurable Port scan detection thresholds

Features:

Real-Time Traffic Monitor: Monitor traffic in real-time and issue alerts when potentially malicious packets or threats are discovered on the network.

Packet Logging: Log packets and collect every packet in a hierarchical directory based on the host network's IP address.

Content Matching: Collate rules by protocol (ip, tcp, udp, icmp), by ports, then by those with/without content. For rules with content, a multi-pattern matcher is used to select rules that have a chance at matching based on a single content.

OS Fingerprinting: Snort can be used to passively determine the Operating System (OS) used by a computer accessing the monitored network.

Oinkcode: Unique key(s) associated to a user account. The oinkcode acts as an API key for downloading rule packages with specific URLs.

FAQs:

What is Snort?

Snort is an open-source intrusion prevention system (IPS) capable of real-time traffic analysis and packet logging.

How can Snort help with network intrusion detection?

Snort operates as a packet sniffer. It can then apply detection rules to look for signs of intrusion. The tool can examine traffic as it travels into the network and packets that are leaving the network.

Can Snort detect zero-day network attacks?

Snort can identify zero-day attacks by looking for types of action against specific types of targets. This generalization and behavior scanning means that the Snort detection rules don't need to rely on previously reported attacks for guidelines.

What are the three modes of Snort?

Packet Sniffer: Reads packets from network and displays in the Snort console.

Packet Logger: Reads packets from the network and writes them to a file.

NIDS (Network Intrusion Detection System): Snort can log and alert on malicious packets using the characteristics of malicious packets defined in its rules.

Solutions:

Open Source: Snort is available for anyone who wants to use an IDS or IPS to monitor and protect their network at no cost.

Rule Subscriptions:

Unregistered Users: Access to the Community Ruleset (GPLv2 Talos certified).

Registered Users: Receive Talos validated rulesets 30 days after Subscribers.

Personal Subscription: Talos validated Snort ruleset available immediately upon release for home use or Educational purposes.

Business Subscription: The same Talos validated ruleset developed for NGIPS customers, available immediately upon release.

Integrators: Program enables 3rd parties to distribute the Snort Subscriber Rule Set as part of a commercial product or service.

Rule Anatomy:

Resources:

Snort v3
Snort Docs
Snort 3 Rules
Snort Documents
Snort FAQ
Snort Downloads
Snort Training
Snort Blog
Snort Rule Search

3rd party tools:

BASE
Barnyard2
Security Onion
Squil (squeal)

Public pages:

Talos Intelligence
Wikipedia
Snort.org