



Explore

**Snort** is an **open-source network intrusion prevention system** that can detect and prevent various attacks and probes on IP networks. [It performs protocol analysis, content searching/matching, and real-time traffic logging](https://www.snort.org/faq/what-is-snort) [1](https://www.snort.org/faq/what-is-snort).

Here are **five reference links** where you can learn more about Snort for free:

1. [**Snort Official Website**](https://www.snort.org/): Explore detailed information about Snort, including installation instructions, features, and usage [2](https://www.snort.org/).
2. [**Snort (software) - Wikipedia**](https://en.wikipedia.org/wiki/Snort_%28software%29): Learn about the history, development, and features of Snort as an open-source network intrusion detection system [3](https://en.wikipedia.org/wiki/Snort_%28software%29).
3. [**Snort IDS/IPS Explained: What - Why you need - How it works**](https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort): Understand how Snort works, its importance in cybersecurity, and its role in detecting and preventing intrusions [4](https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort).
4. [**Snort Tutorial and Practical Examples**](https://hackertarget.com/snort-tutorial-practical-examples/): Dive into practical examples and use cases for deploying Snort to protect networks from cyber threats [5](https://hackertarget.com/snort-tutorial-practical-examples/).
5. [**Snort 3 Rule Writing Guide**](https://docs.snort.org/start/installation): Get started with Snort 3 by exploring installation instructions, rule writing, and foundational concepts [6](https://docs.snort.org/start/).

Feel free to explore these resources to enhance your understanding of Snort! 🚀🔍