Paper 3 Summary

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

All Sections

No unread replies.1212 replies.

Search entries or author Filter replies by unreadUnread     Collapse replies Expand replies

[Subscribe](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

[Alexander Bladow](https://unomaha.instructure.com/courses/43633/users/37067)

[**Alexander Bladow**](https://unomaha.instructure.com/courses/43633/users/37067)

Apr 10, 2021Apr 10 at 3:09pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Alexander Bladow

CSCI 8410

Paper summary 3

In this paper over snort, they describe what Snort is, how it compares to other sniffers and NDIS (Network intrusion detection System) program, and some options on how to use it. Snort is a “libcap based packet sniffer and logger” which can be used as a lightweight NIDS. Two other programs that are similar in nature to Snort are tcpdump and network fight record(NFR), which difference, pros, and cons vs Snort. Tcpdump is a generalized packet sniffer compared to Snort which is more focused on packet sniffing in regards to its security applications, which primarily due to Snort’s ability for packet inspection, this is aided by Snort’s more user-friendly output. NFR on the other hand is a more flexible and complete network analysis tool, but it is larger and more cumbersome when compared to Snort which has simpler one-dimensional rules and can detect a new attack in minutes once the signature has been determined. Each of these tools has its own niche in the security life cycle no one is better than another. Snort has three main sub-systems it uses to run these are a Packet decoder, a detection engine, and the logging/Alerting subsystem. These three systems break down analyses and record the results of packets for malicious software, keeping it limited to three specialized systems keeps it more streamlined and easier to understand/operate compared to others. The next sections go over how to operate Snort along with how to write rules for it and do some more advanced features. In the Rule development section, they go over the basics of how to develop rules for snort along with an example signature that is commonly looked for. Another thing that I found helpful was the fact that they gave guidance on how High-performance rules are written, align with advanced Snort features and techniques such as Shoring up commercial IDS’s, installing passive traps, giving info involving SHADOW which can augment your system, and finally more focused monitoring. Overall this paper was not a technical guide but more of an introduction or primer on the abilities of Snort.

[Frank Tursi](https://unomaha.instructure.com/courses/43633/users/46026)

[**Frank Tursi**](https://unomaha.instructure.com/courses/43633/users/46026)

Apr 10, 2021Apr 10 at 4:23pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Frank Tursi  
CYBR 8410  
Paper Summary 3

This paper introduce a product named Snort, intended as a lightweight network intrusion detection system (NIDS). Snort was designed to address many of the shortcomings of existing NIDS such as significant system footprint, complex deployment, and high costs. Snort is a cross-platform libpcap-based packet sniffer and logger, that can be used as a lightweight NIDS. Being only 100 kilobytes in compressed source, it can quickly be compiled and deployed on different platforms. Snort maintains a list of rules that is recursively searched through for each packet that passes through. Snort also maintains logging and alerting subsystems that will display logs in a human-readable and actionable format as well as create alerts that can be sent to syslog, logged to a text file, or sent as WinPopup messages. The versatility of the log and alert output allows easy integration into multiple network environments. Snort has the advantage to other products by including real-time automatic traffic classification and real-time alerting rather than relying purely on logging alerts, reducing response time and log file sizes. Snort fulfills requirements of a fully-fledged NIDS while being lightweight and flexible enough to deployed on a number of environments at no cost.

[Khedir Qassim](https://unomaha.instructure.com/courses/43633/users/102151)

[**Khedir Qassim**](https://unomaha.instructure.com/courses/43633/users/102151)

Apr 12, 2021Apr 12 at 11:02pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Snort-Lightweight Intrusion detection for Networks

            This article is discussing the main functions and capabilities of Snort as an open-source tool licensed under GNU and as Network intrusion detection. The article was first published in 1999 and it discusses the background of Snort and its rule-based traffic collection engine, as well as new and different applications which can be very useful as part of integrated network security infrastructure. According to the paper, Snort is a small tool for lightly utilized network and is useful when it is not cost efficient to deploy commercial Network-based sensors (NIDS).

Snort according to the article can be deployed almost on any node of network with minimal disruption and should be cross-platform with easy configuration by system admins. Snort is also a packet sniffer and logger which features rules-based logging to perform content pattern matching and detect variety of attacks and intrusions incidents such buffer overflows, stealth port scan and CGI attacks etc. Snort shares some commonalities with both tcpdump and Network Flight Recorder (NFR) but Snort is financially, technically and administratively easier to adapt or implement than other open sources or commercial tools. One feature that distinguish Snort from tcpdump is packet payload inspection which allows snort to detect many types of hostile activities in addition, snort is more user-friendly handling its decoded output display, however there also one powerful feature that Snort and tcpdump share which is capability of filter traffic with Berkeley Packet Filter (BPF). On the hand NFR is more flexible and complete network analysis tool. It has complete feature set than Snort, such as IP fragmentation and TCP stream decoding.

The article also laid out Snort’s structure or the three main primary subsystems that makes up Snort, packet decoder, detection engine and logging and alerting systems. The Packet decoder basically decodes packet layers presented in data-link layer and TCP/IP protocol definitions to its raw network traffic up to the application layer. While the Detection Engine is linked list data structure that has Headers and Chain options where Snort maintains its detection rules in. Finally, the logging/Alerting systems are forms of human readable formats that trigger when certain conditions are met while setting up alerts or logs command lines, according to the article there are three logging and fine alerting options.

The final parts of the article cover more technical details like writing Snort rules such as pass, log, and alert. It also illustrates some command line example rules with their options. It also, how the rules have been developed since they found and the Boyer-Moore algorithm that Snort uses for matching patterns.

I believe Snort is a great open-source tool for NIDS, Snort is now owned by Cisco and it does offer real-time traffic analysis and packet logging on IP networks. Cisco currently uses a dual license strategy for Snort source code, once for governing the use of snort and second for community rules in GNU version 2.

[Jensen Miller](https://unomaha.instructure.com/courses/43633/users/2767)

[**Jensen Miller**](https://unomaha.instructure.com/courses/43633/users/2767)

Apr 14, 2021Apr 14 at 1:59am

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

“Snort - Lightweight Intrusion Detection for Networks” is a paper about the merits of the Snort open source LIDS software. Author Martin Roesch goes on to talk about how Snort is capable of performing similar to if not as well as most commercial NIDS in it’s lightweight niche. It benefits from a simple flexible ruleset that allows for rapid rule creation following a new threat and lowers processing time preventing snort from getting bogged down. In essence, Snort is a ruleset and alert software strapped to the libpcap library which is part of the reason why it is so lightweight (300KB install package). Snort benefits heavily from it’s open source license since the community can react to new threats and create rules much quicker than a vendor is typically able to respond. Snort fills in the area where a powerful NIDS is not feasible or cost effective, and where smaller LIDS in its class are effective but still come with a pricetag.

I found this paper very interesting since I’m doing my semester project on Lightweight IDS’s and it may be giving me a hint for who I may expect to be coming out on top.

[Jeff Smolinski](https://unomaha.instructure.com/courses/43633/users/79659)

[**Jeff Smolinski**](https://unomaha.instructure.com/courses/43633/users/79659)

Apr 14, 2021Apr 14 at 7:45am

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

In this paper the author makes a strong case for using Snort to, “fill the gaps,” in an organization’s intrusion detection system.

Among the various use cases presented by the author two, in particular, stand out. First, deploying Snort to augment a commercial intrusion detection system (IDS) when a new vulnerability is discovered. Since a vendor may be slow to update their software, a network administrator could write a new rule and stand up a snort instance rather quickly. This allows an organization to monitor that threat notwithstanding that vendor’s timetable.

The second use case is referred to by the author as focused monitoring. Focused monitoring is a technique where an IDS monitors the traffic of a singular, critical service on a network. The author suggests that this technique would be especially useful in cases where a commercial IDS provides inadequate coverage for a particular service.

I submit that snort could also prove useful in instances where suspicious traffic is observed in other logs after a manual review. A network administrator could write a Snort rule corresponding to the suspicious traffic; allowing them to better monitor that traffic and then address it as they see fit.

Since this article was written in 1999 that begs the question: how would one use Snort today?

A quick search of the Snort website shows rules with threat signatures for both [Docker (Links to an external site.)](https://www.snort.org/search?query=docker&submit_search=) and [Kubernetes (Links to an external site.)](https://www.snort.org/search?query=Kuberneties&submit_search=) CVEs. Additionally, one could probably author rules to detect compromised container behavior such as: attempts to pivot between containers or attempts to break out of a container’s context. It seems, therefore, that Snort has its place in a microservice architecture even though such an architecture was not contemplated by its authors.

In conclusion, I do not think Snort will ever be the largest piece of a modern, comprehensive IDS. However, given its flexibility to monitor almost any network threat, the ease of integrating it with most network topologies, and the ability to write new rules quickly Snort will probably remain in a network administrators tool belt for years to come.

[Xavier McCaig](https://unomaha.instructure.com/courses/43633/users/17725)

[**Xavier McCaig**](https://unomaha.instructure.com/courses/43633/users/17725)

Apr 14, 2021Apr 14 at 3:02pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Xavier McCaig

CYBR8410

Paper 3

14 April 2021

Martin Roesch presents Snort as a lightweight network intrusion detection system (NIDS) that occupies an essential part of the network security ecology. Roesch suggests the tool to be especially useful for small TCP/IP networks in detecting anomalous activity or outright attacks, as well as providing relevant systems personnel with enough information to make meaningful decisions. Snort is additionally considered to be lightweight enough to make deployment inconsequential, especially compared with other NIDS systems, weighing only roughly 100kb compressed. As a libpcap-based, free and open source system, Snort also provides a larger and more open set of community resources and a publicly-verifiable security base. Roesch presents a further benefit of Snort in acting as a more customizable intrusion detection system for recognizing new attacks which vendors may be slow to release signatures for. Overall, Snort exists in the spaces where commercial systems are too resource-intensive or cost inefficient to justify their deployment, and for some organizations, may provide enough functionality to serve as a complete replacement for commercial systems.

[John Kieran](https://unomaha.instructure.com/courses/43633/users/6118)

[**John Kieran**](https://unomaha.instructure.com/courses/43633/users/6118)

Apr 14, 2021Apr 14 at 3:03pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

John Kieran  
CYBR-8410  
Paper 3

Summary

This is a product brief on the open-source Snort IDS package.  Snort can be used as a stand-alone installation or to complement a commercial grade IDS hardware solution.  Snort works on a rules-matching principle and an emphasis was on the speed of rule processing.  Rules can be customized and quickly created once an attack fingerprint is determined.  Additionally, Snort can inspect the application-level packets which aid in the creation of rules.  If possible, an attack can be obtained and executed on a sandbox environment to obtain the attack fingerprint and assist in rule creation.  Rule creation is basic but can become very detailed.  The basic structure of a rule mimics that of a firewall rule, e.g., alert/log method, protocol, source IP, source port, ->, destination IP, destination port.  Snort features both logging and alerting functionality.  Logging options are offered by Snort include: logging in human readable format to a single file, to a tcpdump-formatted file for later decoding, or no logging at all.  Alerting options include: sending to syslog, sending to a text file in two formats, or to a Samba smbclient with pop-ups.

Critique

This is very good for a product brief.  It compares Snort to existing similar products:  tcpdump, Network Flight Recorder, and SHADOW.  Snort compares well to each product with options that competitors do not feature.  Snort offers a relatively easy-to-use feature set for network monitoring and custom rule creation.  However, I disagree with their option for obtaining an attack and running it in a sandbox.  This is a fine idea, but what if there is a new novel attack from a malicious actor?  To say "just get it and run it" seems overly simplistic.  Of course, the counter to this scenario is that if an organization is suffering a tailored attacked, that organization probably is not only running Snort but a more robust IDS.

Reflection

Interesting product and with the added bonus of being freely available.  This could work in a pinch if an organization needs a quick IDS solution.  It includes some baseline rules which might cover most situations, but anything custom would of course need custom rules.  The ability to do application-level inspection makes Snort much more appealing.

[Andrew Storms](https://unomaha.instructure.com/courses/43633/users/105646)

[**Andrew Storms**](https://unomaha.instructure.com/courses/43633/users/105646)

Apr 14, 2021Apr 14 at 3:36pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Andrew Storms

CYBR 8410

Paper 3

This paper discusses the detection system called Snort, which is classified as a  network intrusion system. This system is able to detect attacks and probes for small to medium sized companies. One of the primary reasons the companies go with Snort is because it can be more cost effective and budget friendly compared to other methods, such as other NIDS sensors. Snort can also be compared to NFR, which is a higher-end, more flexible tool than Snort is. One of the major differences between the two is that the coding language used in NFR is more complex and has a wider range, while Snort is more one-dimensional and not complex. While it is a flexible structure for maintaining and monitoring systems, many other techniques have higher qualifications for this type of service, but run a much higher price. Overall, Snort technology is focused on precision and flexibility, as opposed to long-term care. Snort rules can also be quite easy to write, but have major complexity when it comes to detecting hostile behavior in a system.

The article concludes with information regarding intrusion detection and the goals the Snort developers hoped to have achieved with the creation of this system. The overall goal was to achieve a software that outpaces commercial intrusion software.

[Chris Schmitt](https://unomaha.instructure.com/courses/43633/users/36306)

[**Chris Schmitt**](https://unomaha.instructure.com/courses/43633/users/36306)

Apr 14, 2021Apr 14 at 5:58pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Chris Schmitt

CSCI 8410

Paper Summary 3

                Snort is a lightweight intrusion detection system that is designed to be easily deployed on any “node” of a network without cause much disruption to operations. It is a libpcap-based packet sniffer and logger that is designed to alert, log, or drop packets according to a base set of pre-designed or custom rules. It is designed to have a small footprint and be easily configurable so the sys admin can get it up and running in a short amount of time.

The article highlights the differences between Snort, tcpdump, and Network Flight Recorder (NFR) and compares the main differences and similarities between them. Snort is cosmetically similar to tcpdump but is more focused on packet sniffing and packet payload inspection which allows snort to detect hostile activity like buffer overflows and CGI scans. It is also able to output the decided packet information much more “user friendly” as opposed to tcpdump. Where snort and tcpdump are similar is in how they are able to filter traffic with Berkeley Packet Filter Commands (BPF) but snort has the ability to search out and recorder TCP packets with a specific TCP flag. When it comes to snort and NFR, snort is viewed as the littler brother. It shares some of the same functionality as NFR but NFR is notes as being more flexible when it comes to a complete network analysis tool. Snort does have the advantage when it comes to writing new rules in a timely manner as opposed to writing a rule in NFR.

Snort is focused on performance and has 3 primary subsystems. The packet decoder is designed around the layers of the protocol stack present in the supported data-link layer and TCP/IP. It is able to quickly decode packets by setting pointers to the packet data for later analysis and provides data decoding capabilities for Ethernet, SLIP, and raw (PPP) data link protocols. The next subsystem, the detection engine, this engine looks to match a decoded packet with a specific rule. The last subsystem is the logging/alerting subsystem. Depending on the option selected at when creating a rule, snort will either alert, log, or drop packets. It allows for sysadmins to be flexible on what they are alerted to and filter out stuff that is deemed not a threat.

The article finishes by going over the different types of rules that are able to be created in Snort. Snort gives sysadmins the ability to rapidly create new rules and implement them in the desired environment in a matter of minutes. Sysadmins are also able to  use high performance pattern matching rules based off signatures in the packets.

The article slightly compares Snort to tcpdump and NFR but does not go to much into the performance differences. They also mentioned that Snort is a lightweight tool with a small footprint and did not provide any sort of “base” hardware needed to run snort. I would have preferred for the authors to provide more detailed analysis on how resource hungry snort is. This was more or less a general overview of Snort which highlights most of the stuff found on the Snort website.

[Jesse Hays](https://unomaha.instructure.com/courses/43633/users/11487)

[**Jesse Hays**](https://unomaha.instructure.com/courses/43633/users/11487)

Apr 14, 2021Apr 14 at 8:42pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Jesse Hays

Rui Zhao

Distributed System Security

14 Apr 2021

**Reading Summary**

Snort – Lightweight Intrusion Detection for Networks

                Network Intrusion detection systems (NIDS) monitor network traffic for predefined rules. These typically are suspicious activities. These will then notify the required parties of the rules being met. However, having NIDS can cost a high amount, and have complex deployments. Snort was designed for these reasons.

Snort is referred to as a lightweight intrusion detection. The term lightweight refers to the face that it can easily be deployed to any node, as well as only having small footprints. The only downside is that Snort is meant for small and lightly used networks. Snort is essentially a step down from a high-end commercial NIDS sensor.

                Snort is similar to tcpdump but is more heavily focused on security and packet sniffing. The main feature Snort has over tcpdump is that Snort has packet payload inspection.

                In my opinion it is a good thing that there is a step down from a commercial NIDS. If there was not the network would either have to have a lot less security or overpay for a commercial solution. These are funds that could be better spent on other things for a company, so I believe the competition is good.

[Zidong Liu](https://unomaha.instructure.com/courses/43633/users/86488)

[**Zidong Liu**](https://unomaha.instructure.com/courses/43633/users/86488)

Apr 14, 2021Apr 14 at 9:58pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Zidong Liu

CYBR 8410  
Paper Summary 3 - Snort – Lightweight Intrusion Detection for Networks

The network intrusion detection system is an important part of the network security architecture. They provide a layer of defense that can monitor network traffic to detect predefined suspicious activities or patterns, and alert system administrators when potentially malicious traffic is detected. Snort is a software that solves the problem of space and cost. Snort is a packet sniffer and recorder based on libpcap [PCAP94], which can be used as a lightweight network intrusion detection system (NIDS). There are three main subsystems that make up Snort: packet decoder, detection engine, and logging and alerting subsystems. It is characterized by performing content pattern matching and detecting various attacks and detections based on log rules. This article also introduces the difference from tcpdump. Snort is similar in appearance to tcpdump [TCPD91], but focuses more on the security application of packet sniffing. The main feature that Snort has that tcpdump does not have is packet payload inspection. Snort decodes the application layer of data packets and can provide some rules for it to collect the traffic of specific data contained in its application layer. Snort is designed to meet the needs of a prototype lightweight network intrusion detection system. It has become a small, flexible and high-performance system, used on large and small networks around the world. It has reached the original design goal. It can completely replace commercial intrusion detection systems where the cost of installing a fully functional commercial system is low.

[Stevie Siy](https://unomaha.instructure.com/courses/43633/users/29318)

[**Stevie Siy**](https://unomaha.instructure.com/courses/43633/users/29318)

Apr 14, 2021Apr 14 at 11:33pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427920)

Stevie Siy

CSCI 8410

Paper 3 Summary

This paper, written by Martin Roesch, details a lightweight network intrusion detection system called Snort. The greatest strengths of Snort are that it comes in a small package, is portable, and effectively can be used as a quick patch for commercial IDS systems that may take longer periods of time to address new attack vectors. In short, Snort is a “libpcap-based packet sniffer and logger,” capable of detecting a variety of attacks over the network. Its architecture consists of three main parts: the packet decoder, the detection engine, and the logging and alerting subsystem. In essence, Snort reads incoming packets, decodes them, determines if the packet contents match a rule that has been put in place, and then alerts whoever implemented the system if necessary. Using Snort can also allow for users to set up honeypots and other passive traps to potentially catch unwanted communication on the network. In total, Roesch gives a high-level overview of the tool. He demonstrates examples of how each component of the tool can be used including specific cases where it would be useful. The paper is put together well, escalating from the basics to what’s under the hood and finally reaching different advanced implementations of Snort. I think that he does well to emphasize that the tool is not meant to totally replace the expensive commercial intrusion detection systems, but as an additional aid that can help patch the holes temporarily or be used to bait attackers into showing their hand. It is open-source, quick to implement, and powerful enough to be used in confidence.