Computer Science Department
University of Crete

# CS-455: Internet Attacks
# Spring 2022 - 2023

## Assignment 4
## Intrusion Detection

Uploaded: 11/04/2023
Deadline: 26/04/2023

## Introduction

Snort is a free open-source network intrusion detection system (IDS) and intrusion prevention system (IPS). Snort's network-based IDS/IPS can perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection.[1]

Free download and support of Snort is available at its official website[2]. Learn how to run Snort and write Snort rules by reading Chapters 1 & 3 of the Snort User's Manual.[3] You may install snort in a Kali VM to complete the assignment.

Notes

- For every question, you need to provide all the necessary commands used with adequate explanation of the command and the relevant result/output.
- **To demonstrate your work, use screenshots extensively**!
- **Review ALL the references listed as footnotes**!

[1] https://en.wikipedia.org/wiki/Snort_(software)
[2] https://www.snort.org/
[3] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

# Questions

1. **[25%] Crafting and testing snort rules**
   **Create rule for the following cases:**
   - Log all ICMP ping request messages destined to the host
   - Log all TCP FIN packets sent to a port between 7000 and 7999 (inclusive)
   - Display an alert when snort detects both the SYN and FIN flags are set at the same time
   - Log all root login to any ftp server on your LAN
   - Check SSH brute force attacks and log IPs trying to connect more than 3 times in 60 seconds

   To test the correctness of your Snort rules, use the appropriate tools (e.g., nmap, dummy ftp server, etc.) to create the above scenarios. In your report, describe how you triggered the alert and show the alert itself from the log file.

2. **[10%] Understanding snort rules**
   **Explain the following snort rules:**
   - alert icmp any any -> any any (msg:"ICMP Source Quench"; itype: 4; icode: 0;)
   - alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS EXPLOIT named overflow";flags: A+;content:"thisissometempspaceforthesockinaddrinyeahyeahiknowthisislamebutanyway whocareshorizongotitworkingsoalliscool"; reference:cve,CVE-1999-0833;)
   - alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"NETBIOS SMB ADMIN$access"; flow:to_server,established; content:"\\ADMIN$|00 41 3a 00|"; reference:arachnids,340; classtype:attempted-admin; sid:532; rev:4;)
   - alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"SHELLCODE sparc NOOP"; content:"|a61c c013 a61c c013 a61c c013 a61c c013|"; reference:arachnids,355; classtype:shellcode-detect; sid:646; rev:4;)

3. **[20%] Configuring a snort front-end**
   Snort 3rd-party tools come and go meaning that you will have to do your own research and experiment with candidate font-ends (e.g., snowl, snorby, sguil, snez). Some are considered obsolete while others are still maintained. **Splunk**

**Enterprise**[4][5] (free trial) is one of the options currently supported. These 3rd-party tool act like a **SIEM**[6] for the IDS/IPS sensors and have a nice dashboard to few events.

- Install and demonstrate a snort frontend

4. **[20%] Managing snort rules**

   **PulledPork**[7] is a tool that allows users to download new rules as soon as new vulnerabilities or exploits are discovered

   - Integrate PulledPork into your snort installation and demonstrate its use and main features

5. **[20%] Identifying WannaCry**

   WannaCry[8] is a type of ransomware that spread rapidly across the world in May 2017, infecting hundreds of thousands of computers in over 150 countries. It exploited a vulnerability in the Microsoft Windows operating system called EternalBlue.

   The EternalBlue vulnerability allowed the ransomware to spread quickly and easily between computers on the same network, even if those computers were not running an unpatched version of Windows. Once a computer was infected with WannaCry, the ransomware would encrypt the user's files and demand payment in exchange for the decryption key.

   - Create a snort rule(s) to identify WannaCry in captured traffic
   - To test your rule use wannacry.pcapng (attached) on the command line ( -r <file>, Read a single pcap)
   - Your snort rules should capture only WannaCry packets and ignore any other packets
   - Explain in detail the rationale for the rule(s) you created

6. **[5%] Using Wireshark**

   - Use Wireshark to analyze flag.pcapng (attached) and find the hidden flag (message)
   - Explain your steps

---

[4] https://www.splunk.com/en_us/products/splunk-enterprise.html?301=/en_us/software/splunk-enterprise.html
[5] https://www.snort.org/documents/snort-3-1-18-0-on-ubuntu-18-20
[6] https://en.wikipedia.org/wiki/Security_information_and_event_management
[7] https://github.com/shirkdog/pulledpork3
[8] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

## Submission

- Submit a pdf document including all the information requested above.
- Explain the results shown in the log files (e.g., /var/log/snort)
- Submissions will be done through eLearn.
- This assignment is an individual creative process and students must submit their own work. You are not allowed, under any circumstances, to copy another person's work. You must also ensure that your work won't be accessible to others.
- You are encouraged to post any questions you may have in the eLearn forum. If, however you believe that your question contains part of the solution or spoilers for the other students you can communicate directly with the course staff at hy455@csd.uoc.gr.

## Disclaimer

It is **ILLEGAL** to attempt any type of attack against a target (individual, network, public/private entity, etc.) without authorization / explicit permission. Such actions are **prohibited and punished by law and university policies**.