HPY 413 Assignment: 7

Network traffic monitoring using the Snort intrusion detection system

Deadline: 14/1/2025

The purpose of this assignment is to introduce students to intrusion detection systems (IDS) through practical experimentation with Snort, a widely used open-source IDS. Students will configure Snort, test its detection capabilities, and analyse its operation. They will also answer theoretical questions to solidify their understanding.

Instructions:

Part 1: Installation and Setup

To simplify the setup process and ensure a consistent environment for all students, a **pre-configured virtual machine (VM)** has been provided for this assignment (https://drive.google.com/file/d/13QG1LslNDUVFwiclqsogra38gR2r_oef/view?usp=sharing). The VM contains all the necessary tools and resources required to complete the tasks, including:

- **Snort**: For writing and testing intrusion detection rules.
- **Python**: With pre-installed libraries for scripting and packet analysis.
- **Wireshark**: For inspecting the structure of PCAP files.
- Files required for the assignment.

1. **Download the VM File**:
    - The VM is provided as a .ova file (Open Virtualization Appliance), which can be easily imported into VirtualBox.
2. **Log In to the VM**:
    - **Username**: student
    - **Password**: student
    - Upon logging in, you’ll find on the desktop the provided files.
3. **Complete the Assignment in the VM**:
    - Navigate to /Desktop/assignment7/ and run the run.sh file (right click on it Run as a program).
    - Store the created PCAP file in the Desktop/assignment7/snort/lab folder.
    - Put in the local.rules file the custom Snort rules that you are going to create.
    - The command to start Snort to read an analyse a PCAP file is: snort --talos -r PCAP.pcap
    - Use the provided tools and resources to complete all tasks.

Part 2: Creating Custom Network Traffic

In this task, you will craft network packets with specific characteristics and save them in a PCAP file for analysis. This exercise will help you understand how to generate and analyse network traffic while adhering to specific requirements.

1. **Create custom packets:**
    - Generate the following packets with code or with tools.
        - **1 Student's packet:**
            - Protocol: TCP
            - Source IP: *Use a random IP address*
            - Destination IP: 192.168.1.1
            - Destination Port: 54321
            - Payload: *The payload will be the student's name and ID, followed by a timestamp (YourName-YourStudentID YYYY-MM-DD HH:MM:SS)*
        - **10 Port scan packets** for the following services: HTTP, HTTPS, SSH, TELNET, FTP, DNS, RTSP, SQL, RDP, MQTT
            - Protocol: *Configure accordingly based on the service*
            - Source IP: *Use random IP addresses*
            - Destination IP: 192.168.1.2
            - Destination Port: *Configure accordingly based on the service*
            - Payload: *The payload will be the student's name and ID, followed by a timestamp (YourName-YourStudentID YYYY-MM-DD HH:MM:SS)*
        - **5 Base64 malicious packet**:
            - Protocol: TCP
            - Source IP: *Use a random IP address*
            - Destination IP: 192.168.1.3
            - Destination Port: 8080
            - Payload: *Your student id e.g.: 123457890 as a base64 encoded string, e.g., " MTMyNDU2Nzg5MA== "*
        - **1 DNS suspicious domain packet**:
            - Protocol: UDP
            - Source IP: *Use a random IP address*
            - Destination IP: *Use the DNS IP of the VM*
            - Destination Port: 53
            - Payload: *A DNS query for a suspicious domain name like "malicious.example.com"*
        - **Ping test packet**:
            - Protocol: ICMP
            - Source IP: *Use a random IP address*
            - Destination IP: 192.168.1.4
            - Payload: *A custom string like "PingTest-2024"*
2. **Save custom packets**
    - Part of the code should save the created packets in a PCAP file.

Part 3: Creating Custom Snort Rules

In this task, you will create custom Snort rules to detect the packets you generated in the previous task. You will practice how to write Snort rules that can identify specific network behaviours and payloads.

1. **Create Snort rules**
    - Write 1 Snort rule for each of the specific packets you created in part 2. Each rule should be able to detect one of the custom packets and create an alert. The rules should be added in the /home/student/Desktop/assignment7/snort/lab/local.rules file.
2. **Test Snort rules**
    - Insert your rules to Snort and then start it in a way to read and analyze the PCAP file you created in part 2.

Part 4: Detect Slammer Worm using Snort

In this task, you will analyse the slammer.pcap file, identify the packets that constitute the attack and create Snort rules to detect the malicious traffic. In this way, you will understand how to detect real-world attack traffic using Snort.

1. **Review the PCAP file:**

    - The slammer.pcap file contains traffic related to the Slammer Worm, a well-known attack that exploits vulnerabilities in Microsoft SQL Server. Analyse the file using Wireshark or another packet analyser to understand the nature of the packets in the PCAP file (protocol, source and destination IP, ports, payload).

2. **Create a Snort rule to detect Slammer Worm traffic:**

    - Write 1 Snort rule that detects the packets in the slammer.pcap file.

    - Insert your rules to Snort and then start it in a way to read and analyse the slammer.pcap file.

    - Verify that your rules successfully detect the Slammer Worm packets.

Part 5: Evaluate Snort

The goal of this task is for students to evaluate Snort’s performance while processing a large PCAP file.

1. **Evaluate Snort’s performance**
    - Find and download a public PCAP file. The size of the file should be close to 1 GB.
    - Run Snort on this large PCAP file using the default configuration.
    - Record the following:
        - The time taken to process the file.
        - CPU and memory usage during the execution (using tools like top, htop, or ps on Linux, or Task Manager on Windows).
        - Any errors or warnings in the Snort output.
2. **Suggest optimization actions to improve the performance.**

Part 6: Theoretical Questions

1. **Describe how Snort uses rules to detect malicious activity.**

2. **Mention at least 6 limitations of signature-based intrusion detection systems like Snort with a small description for each one.**

3. **Pros and cons of using Snort in a real-world scenario.**

Submission Guidelines:

After completing all tasks in the assignment, you are required to submit a report containing the following:

1. **Part 2**: The code for the creation of the packets or the commands for the tools used, and the generated PCAP file.
2. **Part 3**: A Word document that includes all the rules. There should be a small description (a paragraph) for each rule (what the rule detects) and a screenshot from the alert it creates.
3. **Part 4**: A Word document that includes the created rule. There should be a small description (2 paragraphs) of the rule and a screenshot from the alert it creates.
4. **Part 5**: A Word document that includes a link to the large PCAP file that was used, the performance metrics along with a small description, and the suggested optimization actions. The document should not be more than 1 page long.
5. **Part 6**: A Word document that includes the answers to all the questions. The document should not be more than 2 pages long.

You should place all these files in a folder named <AM>_assign7 and then compress it as a .zip file. For example, if your login is 2020123456 the folder should be named 2020123456_assign7 you should submit 2020123456_assign7.zip. GPT-generated code/report is banned, and submission with GPT-created content would be rejected.

Disclaimer and Safety Warning

This assignment involves the analysis of a PCAP file containing recorded network traffic from the Slammer worm, a historical computer worm. While PCAP files are passive and cannot execute or spread malware, it is essential to handle this file responsibly to minimize any potential risks. By participating in this assignment, you acknowledge that you have understood these guidelines and agree to handle the provided materials responsibly.

Important Guidelines:

1. **Isolated Environment**: Perform all work in an isolated environment, such as a virtual machine or lab computer, to ensure no unintended interactions with production systems or networks.
2. **No Vulnerable Software**: Ensure that no instances of Microsoft SQL Server 2000 or other potentially vulnerable systems are running on your machine or network.
3. **File Usage**: Do not modify or use the PCAP file for purposes other than this assignment. Any misuse could violate ethical and legal guidelines for working with network traffic.
4. **Wireshark Analysis Only**: The file is provided for analysis only in tools like Wireshark. Do not attempt to replay or inject this traffic into a live network.