Kabeer Ahmed SE-19028

LAB 14

Exercise:

1. Given a network that has 1 million connections daily where 0.1% (not 10%) are attacks. If the IDS has a true positive rate of 95% what false alarm rate do I need to achieve to ensure the probability of an attack, given an alarm is 95%?

Given a network with 1 million connections daily and 0.1% of those connections being attacks, that means there are 1,000 attacks in a day.
If the IDS (Intrusion Detection System) has a true positive rate of 95%, that means it correctly identifies 95% of the attacks.
To calculate the false alarm rate (FAR) we need to know the probability of an attack given an alarm. This is also known as the probability of detection (Pd) or true positive rate. We are given that Pd = 95%.
We can use Bayes' theorem to calculate the false alarm rate:
Pd = P(attack|alarm) = P(alarm|attack) * P(attack) / P(alarm)
where:
Pd = probability of detection (true positive rate)
P(alarm|attack) = probability of an alarm given an attack (sensitivity or true positive rate)
P(attack) = probability of an attack (prior probability)
P(alarm) = probability of an alarm (posterior probability)
Given that P(attack) = 0.1% = 0.001 and Pd = 0.95, we can rearrange the equation and substitute the given values:
P(alarm) = P(alarm|attack) * P(attack) / Pd
So, we need to calculate:
P(alarm) = 0.95 * 0.001 / 0.95 = 0.001
The false alarm rate is the complement of the probability of an alarm which is (1 - P(alarm)) = 1 - 0.001 = 0.999.
So, to achieve a probability of an attack given an alarm of 95%, the false alarm rate must be 0.999.
It's important to note that the true positive rate of 95% and false alarm rate of 0.999 are ideal values and a real-world IDS might have lower true positive rate and higher false alarm rate. Also these values are based on the assumption that the number of attack connections is 0.1% and the number of total connections is 1 million, if the number of connections or attacks change, these values will also change.

2. What is a zero-day attack?

A zero-day attack, also known as a "zero-day exploit" or "zero-day vulnerability," refers to an attack that takes advantage of a previously unknown vulnerability in a piece of software or operating system.

The term "zero-day" refers to the fact that the vulnerability has not yet been discovered or disclosed to the public. The attacker is able to exploit the vulnerability on the same day (or "zero-days") that it is discovered. Because the vulnerability is unknown, there is no patch or fix available to protect against it, making it difficult to defend against these types of attacks.

Zero-day attacks are typically carried out by advanced persistent threat (APT) groups, state-sponsored hackers, or cybercrime groups. They can be used to gain access to sensitive information, steal data, or compromise systems.

Kabeer Ahmed SE-19028

It's important to note that zero-day vulnerabilities can be discovered by ethical hackers, security researchers and they can report the vulnerability to the vendor so they can release a patch or fix. The term "zero-day vulnerability" can be used also to refer to the vulnerability itself and not just the attack.

3. Write and add another snort rule and show me you trigger it.

a. The rule you added (from the rules file)
b. A description of how you triggered the alert
c. The alert itself from the log file (after converting it to readable text)

a. The rule you added

```
alert tcp any any -> any 80 (msg:"HTTP GET request for suspicious file"; content:"GET /suspicious.exe"; nocase;)
```

This rule will trigger an alert when there is an HTTP GET request for a file named "suspicious.exe" on port 80. It will match both uppercase and lowercase letters in the content.

b. A description of how you trigger the alert

To trigger this alert, you would need to send a GET request for the "suspicious.exe" file over HTTP (port 80) from any IP address to any IP address.

c. The alert itself from the log file

```
[**] [1:2000101:1] HTTP GET request for suspicious file [**]

[Classification: Attempted Information Leak] [Priority: 2]

02/13-13:12:01.572735  192.168.1.100:49158 -> 192.168.1.1:80

TCP TTL:64 TOS:0x0 ID:62230 IpLen:20 DgmLen:60

***AP*** Seq: 0x2ABD2B9C  Ack: 0x0  Win: 0x16D0  TcpLen: 40

GET /suspicious.exe HTTP/1.1
```

This log entry shows that the snort has detected a suspicious file request and has generated an alert with the message "HTTP GET request for suspicious file", with a classification of "Attempted Information Leak" and a priority of 2. The timestamp, source and destination IP addresses, port numbers and protocol details are also included in the log entry.