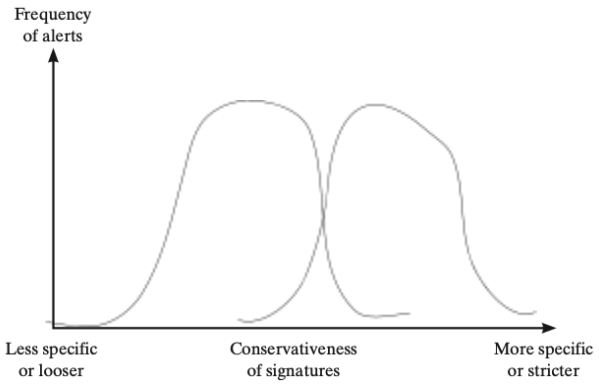
CSE 467/567 Computer and Network Security
Department of Computer Science and Engineering, Miami University
Homework-5

1. (5 points) Define a reflection attack.
    a. An attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system. When the intermediary responds, the response is sent to the target, reflecting it back off the intermediary.
2. (5 points) Define an amplification attack.
    a. An amplification attack is like a reflection attack in that they also involve sending a packet with a spoofed address to the target, but they generate multiple responses for each packet sent.
3. (5 points) What defenses are possible to prevent an organization's systems being used as intermediaries in a broadcast amplification attack?
    a. Organizations can block spoofed source addresses, they can use filters to ensure the source address is the one being used, and they can modify their TCP connections to ensure that the connections being made are valid.
4. (10 points) In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? How many per second if the attacker uses a 2-Mbps link? Or a10-Mbps link?
    a. 1 mbps = 125000 bytes / 2 = 62500 bytes / 500 = 125 packets sent to hit capacity of a 0.5Mbps link
    b. 1 mbps = 125000 bytes * 2 = 250000 bytes / 500 = 500 packets to hit capacity of a 2 mbps link
    c. 1 mbps = 125000 bytes * 10 = 1250000 bytes / 500 = 2500 packets to hit capacity of a 10mbps link
5. (10 points) Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests. Consider a server system with a table for 256 connection requests. This system will retry sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30 second intervals, before purging the request from its table. Assume that no additional countermeasures are used against this attack and that the attacker has filled this table with an initial flood of connection requests. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? Assuming that the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth does the attacker consume to continue this attack?
    a. 5 retries * 30 seconds each = 150 seconds for each connection
    b. 256 connections / 150 seconds = 1.7 original connection requests per second
    c. 256 connections * 40 bytes = 10240 bytes consumed by the attacker at any given time
6. (10 points) List and briefly describe the steps typically used by intruders when attacking a system.
    1) target acquisition and info gathering

a) explore website to gather info about corporate structure
b) gather info on target using whois, dig, host
c) map network using nmap
d) identify vulnerable services

2) initial access
   a) brute force password
   b) exploit vulnerability
   c) send phishing email
3) privilege escalation
   a) scan system applications for exploits
   b) install sniffers
   c) use known passwords
4) info gathering and system exploit
   a) scan files for info
   b) transfer documents externally
   c) use passwords to gain access to other servers
5) maintain access
   a) install remote admin tool
   b) use admin password to access network
   c) modify or disable anti-virus systems
6) cover tracks
   a) use rootkit to hide files
   b) edit logfiles to remove entry p

7. (5 points) In the context of an IDS, we define a false positive to be an alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. A false negative occurs when an IDS fails to generate an alarm when an alert-worthy condition is in effect. Using the following diagram, depict two curves that roughly indicate false positives and false negatives, respectively.



8. (10 points) One of the non-payload options in Snort is flow. This option distinguishes between clients and servers. This option can be used to specify a match only for packets flowing in one direction (client to server or vice versa) and can specify a match only on established TCP connections. Consider the following Snort rule:

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS\
     (msg: "ORACLE create database attempt:;\

flow: to_server, established; content: "create database"; nocase;\

     classtype: protocol-command-decode;)
```

a. What does this rule do?
   i. It alerts if someone attempts to create a database from an external network
b. Comment on the significance of this rule if the Snort devices is placed inside or outside of the external firewall.
   i. If it is inside the firewall, then it sees internal traffic and attacks, if it is outside the firewall, then it sees external intrusion attempts

9. (20 points) A decentralized NIDS is operating with two nodes in the network monitoring anoma- lous inflows of traffic. In addition, a central node is present, to generate an alarm signal upon receiving input signals from the two distributed nodes. The signatures of traffic inflow into the two IDS nodes follow one of four patterns: P1, P2, P3, P4. The threat levels are classified by the central node based upon the observed traffic by the two NIDS at a given time and are given by the following table:

Threat Level	Signature
Low	1 P1 + 1 P2
Medium	1 P3 + 1 P4
High	2 P4

If, at a given time instance, at least one distributed node generates an alarm signal P3, what is the probability that the observed traffic in the network will be classified at threat level 'Medium'?

This is a conditional probability. So with medium we need a P3 or a P4 probability. This can be written as P(A|B) = P(A&B)/P(B). There are 16 total combinations.

P1 + P1
P1 + P2
P1 + P3
P1 + P4
P2 + P1
P2 + P2
P2 + P3
P2 + P4
P3 + P1
P3 + P2
P3 + P3
P3 + P4
P4 + P1
P4 + P2
P4 + P3
P4 + P

Two of the possibilities contain P3 and P4. 7 of them contain P3. This gives us $\frac{\frac{2}{16}}{\frac{7}{16}} = \frac{2}{7}$ probability to get a medium threat level.

Submission Instructions:

- Upload a single PDF file to canvas assignment.
- Please prepare the response using standard word processing software such as MS Office, Google Doc, Libero Office, LaTeX.
- Please show each step of your work. **BOLD** the final answer.
- The course adheres to a strict no-late submission policy. You will get zero for a late submission.