**Student Name:**

**Network Security**

**Midterm Examination 2**

**GENERAL INSTRUCTIONS**

The midterm is out of a total of 100 points: 25 points of True/False and 75 points of short answer questions. You have one hour and 15 minutes for the entire exam plan accordingly. The questions are in no particular order of difficulty. Move on to easier ones if you find yourself stuck. You may answer questions in any order as long as they are clearly labeled. This exam is to be completed individually and is closed devices, books, and notes.

**True False questions (25 points)**

Circle only one of the choices (5 points each).

1. **True False** Stateless firewalls are able to perform Deep Packet Inspection (DPI) and detect and block attacks attempting to exploit application vulnerabilities.
2. **True False** TLS provides protection against replay attacks by including fresh random numbers in the handshake.
3. **True False** HTTPS protects against eavesdropping attacks from both a passive and active network attacker.

1. **True False** Signature based IDS are able to detect previously unknown attacks.
2. **True False** Cross-Site Request Forgery (CSRF) attacks are mitigated by the browser’s Same Origin Policy (SOP).

**Short Answer (75 points)**

1. **IDS (35 points)**
2. Wolf Security released an intrusion detection system that can detect Syn floods and SQL injection attacks. They boast a low false positive rate and high accuracy rate, rates are in the following table:

How connection is classified

|  |  |  |  |
| --- | --- | --- | --- |
| Type of connection | Syn flood | SQL Injection | Normal |
| Syn flood | 91% | 4% | 5% |
| SQL Injection | 5% | 90% | 5% |
| Normal | 5% | 0% | 95% |

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with probability 91%, misclassifies it as an SQL Injection attack with probability 4%, and misclassifies it as a normal connection with probability 5%.

For the purposes of this problem, assume that Syn floods are 1% of all connections, and that SQL Injection attacks are 4% of all connections, while 95% of traffic consists of normal connections.

Also assume that a connection cannot be both a Syn flood and an SQL injection attack at the same time.

When the IDS announces that it detected a Syn flood, what is the probability that the connection is, in fact, normal? Give your calculations. [**25 points**]

1. Describe how anomaly based IDS systems function and why this enables them to detect previously unknown attacks. [**10 points**]

Anomaly based system are built using a supervised statistical model that can differentiate between normal and anomalous behavior. Since unknown attacks might be classified as anomalous it might be able to detect them.

1. Secure Routing (40 points)
2. Describe how BGP IP address prefixing attacks are currently detected. [15 points]

Currently BGP as deployed does not have any formal security model. It is secured by ad-hoc trust between BGP routers, which results in accepting all, some, or none of the routes advertised by a peer BGP router. There are collective, such as the BGP looking glass, that share BGP route announcements that are seen by their routers. This data can be analyzed to detect anomalous routes. However, these anomalies must be manually investigated since there is a chance for false positives.

1. Describe what would be required to provide secure IP address origin authentication in BGP routing. [10 points]

The core requirement for secure IP address origin authentication would be an authoritative database of IP address prefix ownership.

1. Describe an extension to BGP routing assuming secure IP address origin authentication is deployed that could validate the authenticity and integrity of every hop of a BGP routing announcement to mitigate hop deletion attacks. [15 points]

If this authoritative database of IP address prefix ownership existed it could also include public keys for each IP address prefix owner. Then every BGP route advertisement could be signed using a secure MAC based on asemestric cryptography (i.e., RSA, DSA, Elliptical Curves) that would provide authentication and integrity. Assuming all BGP route announcements were signed, then peer BGP routers could verify the information using the public key from the database.