CS3922/CS6823 Network Security
Homework 3

True False questions (15 points)

Circle only one of the choices (3 points each)

1. A VPN which uses IPSec configured with ESP in tunnel mode provides end-to-end (i.e., between the originating host and final destination) confidentiality of the payload. **False**
2. The browser Same Origin Policy (SOP) does not protect against trackers such as Facebook and Twitter's like buttons. **True**
3. Secure BGP would protect against a data plane attack where a router that is configured to eavesdrop on messages it is processing. **False**
4. One technique for mitigating Cross Site Request Forgery (CSRF) attacks is to include a random value in forms that is validated when it is submitted. **True**
5. Signature based IDSs use statistical models to detect previously unknown attacks. **False**

Short Answer (35 points)

1. TLS (20 points)
    a. Explain how a protocol rollback against SSL 2.0 could be launched, what goal a protocol rollback achieves,. (10 points for grads and 10 points for undergrads)
    The attacker attributes the client version to 2.0, so then the sender downgrades to support communication. The downgrade now poses vulnerable to all SSL 2.0 weaknesses, such as using broken encryption algorithms that the attacker can now decrypt.
    b. Describe how TLS 1.3 mitigates protocol rollback attacks. (10 points for grads and 10 points for undergrads)
    The version is re-checked after cryptography with the public key from client to server.
2. IDS (15 points)
    a. 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	90%	5%	5%
SQL Injection	5%	90%	5%
Normal	5%	5%	90%

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with

probability 90%, misclassifies it as an SQL Injection attack with probability 5%, 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 3% of all connections, while 96% 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. [10 points for grads and 15 points for undergrads]

(0.5*0.96)/((0.5*0.96) + (0.9*0.1) + (0.5*0.3)) = 0.667 = 67% probability that a syn flood is normal