**Student Name:**

**Network Security**

**Midterm Examination 2**

**GENERAL INSTRUCTIONS**

The midterm is out of a total of 150 points: 50 points of True/False and 100 points of short answer questions. You have one and 3/4 hours 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 (50 points)**

Circle only one of the choices (10 points each).

1. **True False** Secure BGP routing would protect again attacks at the data plane level, such as dropping IP packets.
2. **True False** With properly validated, unforged certificates, HTTPS security guarantees of confidentiality, integrity, and authentication hold even if DNS has been compromised.
3. **True False** Stateless packet-filter firewalls are able to reconstruct fragmented IP packets to make filtering decisions.

1. **True False** IPSec provides source IP address authentication.
2. **True False** 802.11i provides confidentiality for the source and destination hardware MAC address of data packets.

**Short Answer (100 points)**

1. **DNSSEC (35 points)**

An interesting feature of DNS is that a 60-byte UDP query to a (recursive) DNS server can result in a 512-byte UDP response or even—in the case of the EDNS(DNSSEC) extension—a 4000-byte UDP response to the source IP address.

1. Can you think of a way to abuse this feature in order to stage denial of service attacks? **[10 points]**

The most straight forward way for an attacker to mount a DoS attack is by spoofing DNS resolution request messages for a domain that is known to reply with a larger DNSSEC resolution where the IP address is spoofed to that of the intended victim. The DNS server will then reply with with the larger DNSSEC resolution with the destination IP address of the intended victim allowing the attacker to amplify the amount for bandwidth consumed.

1. How would you redesign the DNS request-response protocol to prevent this particular attack? What are the trade-offs in terms of usability and performance of the redesign? **[15 points]**

There are several ways to redesign DNS to mitigate DoS attacks. The first would be to add an additional challenge message sent in reply to a DNS resolution request that included a cookie. The requestor would then have to reply with the correct cookie value before the actual large reply would be sent. This would add an extra round trip time to the DNS resolution process and consume additional bandwidth in the none spoofed case. The other defense might be to rate limit the number of responses sent to a single IP address. This would not completely mitigate the problem since the attacker could make uses of more DNS resolvers to compensate. It also might cause legitimate DNS resolution requests to be suppressed due to rate limiting.

1. Which of the security properties of authentication, availability, confidentiality, and integrity does DNSSEC provide for signed DNS to IP address records? [**10 points**]

DNSSEC provides authentication and integrity to DNS to IP address resolution records.

1. **Secure Network Protocols (30 points)**
2. At a high level a Public Key Infrastructure (PKI) and Certificate Authority (CA) are required to enable establishment of trust (i.e. authentication). Describe the PKI frameworks for DNSSEC and HTTPS and who the root Certificate Authorities are and what their scope of trust is (i.e. what domain names can they sign certificates for?) in DNSSEC and HTTPS? [**20 points**]

For DNSSEC the PKI is a hieratically scoped naming structure where ICANN the root CA can sign a valid DNS record for any domain name. ICANN then signs the CA keys for Top Level Domain (TLD) registrars, such as Verisign that manages the .com TLD. This CA key for Verisign is only valid for signing domains beneath .com. Verisign then will sign CA keys for the owner of a .com domain that are only valid for that domain and subdomains. In the case of HTTPS each browser includes a set of CA keys that are valid for signing certificates for any domain name. This means that any trusted CA can sign domains globally.

1. Describe one technique used by secure protocols, such as TSL and IPSec, to protect against replay attacks and one technique used to protect against man-in-the-middle attackers. [**10 points**]

In order to protect again replay attacks a protocol must include some form of freshness, such as a random nonce, sequence number, or time stamp. To protect against man-in-the middle attacks the protocol must provide some form of authentication, integrity, and optionally confidentiality if that is required for the protocol.

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 | 90% | 5% | 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 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 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**]

(.05\*.95)/((.05\*.95)+(.04\*.05)+(.01\*.90)) = 0.811965

81.2%

1. Define what a false positive and false negative is in the context of an IDS and one reason why each is costly for operators of these systems. [**10 points**]

A false positive is when an event that is benign is detected as an alert and a false negative is then malicious activity is classified as benign. The cost of false positives is the resources required to investigate alerts that are actually benign. The cost of false negatives is that an attack might occur without being detected.