**CS6823 Network Security**

**Homework 3**

This home work is worth a total of 25 points (2.5% of your total course grade). It is composed of five true/false questions each worth 1 points, two multiple part short answer with points values marked for each part and questions based on reading a research paper. It is due on 4/11 and solutions will be posted on 4/12 to assist in studying for the midterm. The midterm will follow a similar structure of true/false questions and a few multiple part short answer questions. The midterm will not include any paper summaries.

**True False questions (5 points)**

Circle only one of the choices (1 point each)

1. Secure origin authentication routing can be provided without a database of IP address prefix ownership. True False
2. Secure DNS enables DNS resolvers to verify the authenticity and integrity domain to IP address resolutions. True False
3. The resiliency of X.509 certificates against forgery attacks depends on the cryptographic strength of the hash function used in the signing process. True False
4. Application firewalls are more efficient than stateless firewalls. True False
5. IKEv2 uses cookies to protect against DoS attacks. True False

**Short Answer (15 points)**

1. Firewall (8 points)

Assume we have a stateful firewall and we would like a firewall ruleset that (1) allows outgoing HTTP and HTTPS (TCP port 80 and 443) traffic, but (2) disallows outgoing SSH and SMTP (TCP port 22 and 25) traffic, (3) blocks all other incoming or outgoing connections, and (4) also performs ingress and egress filtering. Assume that the internal network has IP addresses 60.72.\*.\*.

Using the firewall rule notation similar to the slides in class, specify a firewall ruleset that implements the policy above.

Egress interface: Action Source IP Source port Destination IP Destination Port Flags Allow 60.72.0.0/16 1024-65535 Not 60.72.0.0 /16 and not Non-routable IP address 80 Any Allow 60.72.0.0/16 1024-65535 Not 60.72.0.0 /16 and not Non-routable IP address 443 Any Deny Any Any Any Any Any Ingress interface: Action Source IP Source port Destination IP Destination Port Flags Allow Not 60.72.0.0 /16 and not Non-routable IP address 80 60.72.0.0/16 1024-65535 ACK, FIN,RST or PSH Allow Not 60.72.0.0 /16 and not Non-routable IP address 443 60.72.0.0/16 1024-65535 ACK, FIN,RST or PSH Deny Any Any Any Any Any

Egress

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Action | Source IP | Source Port | Destination IP | Destination port | Connection |
| Allow | 60.72.0.0/16 | 1024-65535 | Not 60.72.0.0 /16 and not non-routable IP address | 80 | \* |
| Allow | 60.72.0.0/16 | 1024-65535 | Not 60.72.0.0 /16 and not non-routable IP address | 443 | \* |
| Deny | \* | \* | \* | \* | \* |

Ingress

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Action | Source IP | Source Port | Destination IP | Destination port | Connection |
| Allow | Not 60.72.0.0 /16 and not non-routable IP address | 80 | 60.72.0.0 /16 | \* | established |
| Allow | Not 60.72.0.0 /16 and not non-routable IP address | 443 | 60.72.0.0 /16 | \* | established |
| Deny | \* | \* | \* | \* | \* |

1. IDS (7 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% | 5% | 90% |

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 2% of all connections, and that SQL Injection attacks are 2% 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. [5 points]

**Hint:** This problem is similar to the base rate fallacy problem: <https://en.wikipedia.org/wiki/Base_rate_fallacy>

Given that IDS detected a SYN Flood, we have to find the probability for the connection to be normal:

P(normal | syn flood) = (P(syn flood | normal) \* P(normal))/P(syn flood) = (P(Syn flood | normal) \* P(normal)) / (P(syn flood | normal) \* P(normal) + P(syn flood| syn flood) \* P(syn flood) + P(syn flood | sql injection) \* P(sql injection)) = (0.05 \* 0.96) / ((0.05 \* 0.96) + (0.91 \* 0.02) + (0.05 \* 0.02)) = 0.048/ 0.048 + 0.0182 + 0.001 = 0.7142

The probability is 71.42%

1. Explain how an anomaly based IDS can detect previously unknown attacks. [2 points]

An anomaly based IDS uses a trained model of what is normal and thought to be good on a network. Anything that deviates from this model by more than the threshold of the IDS is raises an alert as anomalous. Therefore, a previously unknown attack can be detected as anomalous if it deviates beyond the threshold of the IDS’s model.

**Research Paper and Questions (5 points)**

Read Ken Thompson’s Reflections on Trusting Trust [1]

In our day-to-day lives, we implicitly trust countless systems, institutions, people, devices, etc to be trustworthy - to not be faulty, to not be malicious, and so on. When we drink from the water fountain, we have to trust that the last person to use it didn’t spill poison into the mouthpiece, that the municipal water supply has been checked for quality by the city or county, that the pipes in the building are sufficiently new, that the pipe supplier didn’t provide faulty pipes, that the pipe supplier’s metal supplier didn’t supply faulty metal, etc. The list goes on and on. Describe two systems that you use in your daily life that you implicitly trust. For each, describe the trust relationships between that system and the systems on which it relies, the components it uses, etc. Obviously this could go on forever, so stop once you have a reasonable list (we’ll leave the definition of “reasonable” up to you, so just put in a best-faith effort). How much of a security risk do these trust relationships introduce? Describe two computer systems (software, online services, etc) that you use in your daily life that you implicitly trust. For each, describe the trust relationships between that system and the systems on which it relies, the components it uses, etc. Obviously this could go on forever, so stop once you have a reasonable list (we’ll leave the definition of “reasonable” up to you, so just put in a best-faith effort). How much of a security risk do these trust relationships introduce?

[1] Attached as part of this assignment