Denial of Service, Firewalls, Intrusion Detection

Question 1 **(8 min)**

Q1.1 TRUE or FALSE: A NIDS always provides the most insight about ongoing network traffic.

○ (A) True ● (B) False ○ (C) — ○ (D) — ○ (E) — ○ (F) —

Solution: False, a NIDS can't be used to monitor TLS traffic.

Q1.2 (3 points) An edgy hacker, xXOskiTheHackerXx, downloads a ransomware tool on GitHub and, without modifying it, tries to target the CDC. Which is the best detection strategy to detect this type of hacker?

● (G) Signature based
○ (H) Behavior based
○ (I) Anomaly based
○ (J) Specification based
○ (K) —
○ (L) —

Solution: Signature based. The tools are public (on GitHub) and xXOskiTheHackerXx won't be able to modify the program to avoid signature detection.

Q1.3 Andrew needs to decide between two burglar alarm systems - system A and system B. System A has a false positive rate of .05 percent and a false negative rate of 1 percent. System B has a false positive rate of 1 percent and a false negative rate of .05 percent. The cost of a false positive is $100, because his parents fine him for causing a ruckus, and the cost of a false negative is $10000, because the burglar steals all his stuff. Which system should Andrew pick?

○ (A) System A
○ (B) System B
● (C) Not enough information
○ (D) —
○ (E) —
○ (F) —

Solution: Not enough information — we don't know how often attacks happen.

Question 2 **(18 min)**

Q2.1 Write a stateful firewall rule that would allow all TLS traffic from an external host `161.20.2.0` into your network `16.120.20.0/24`.

○ (A) —— ○ (B) —— ○ (C) —— ○ (D) —— ○ (E) —— ○ (F) ——

Solution: `allow tcp 161.20.2.0:* -> 16.120.20.0/24:*`
Common mistakes were not including the ports, including an incorrect port, forgetting to include the CIDR notation for `16.120.20.0/24`, specifying TLS as the protocol when a firewall would not have application layer context, etc.

Q2.2 Recall that an attacker can spoof source IPs to hide themselves while executing a DoS attack. Assume the attacker securely randomly generates these IPv4 addresses. Describe a pattern in the packets that a network operator could observe to best discern whether or not their network is a victim of a DoS attack.

○ (G) —— ○ (H) —— ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Solution: Look at the distribution of the source IP addresses of the incoming packets. If they are roughly uniformly distributed across the IP address space, this is likely to be the result of a DoS attack (see backscatter analysis).
Another viable option is to see that some source IP addresses are routed to private or non-routable IP addresses. Other accepted solutions mentioned the logic for maximum or minium sized packets.

Q2.3 What intrusion detection method would be *best* fit to perform the previous analysis? Justify your answer.

○ (A) HIDS ○ (C) Logging ○ (E) ——
● (B) NIDS ○ (D) —— ○ (F) ——

Solution: NIDS allows for real-time analysis, and by looking at the IP address source fields on the IP packets, there is no need for any visibility or context from the host. A NIDS is cheap to deploy.

Q2.4 Describe a major drawback or exploit to the intrusion detection method you described above.

○ (G) —— ○ (H) —— ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Solution: The NIDS could itself be overwhelmed by the volume of traffic. Also, if the bottleneck network link is upstream, the DoS attack might overwhelm that bottleneck link, causing many packets to be dropped before they reach the NIDS, making it harder for the NIDS to have full visibility of the attack.
Also accepted due to question ambiguity: a drawback of the intrusion detection method that is irrelevant in the context of DoS detection (e.g., traffic being encrypted).

Question 3 ***Malcode*** **(12 min)**

Q3.1 (3 points) Malcode X spreads by making a copy of its own binary on another machine and executing it. Which intrusion detection technique is best for detecting this malcode?

● (A) Signature-based detection
○ (B) Anomaly-based detection
○ (C) Specification-based detection
○ (D) Behavioral detection
○ (E) ——
○ (F) ——

Solution: Because the malcode does not change each time it replicates, we can add a signature for the malcode binary to detect and block it.

Q3.2 (3 points) Malcode X connects to other machines using TLS. Which intrusion detection method is best for detecting this malcode?

Select one option, and briefly justify your answer (1 sentence) in the text box.

○ (G) NIDS ● (H) HIDS ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Solution: Because TLS is encrypted, the NIDS does not have the necessary host context in order to decrypt and inspect the traffic for the malcode. Thus, only the HIDS can defend against the malcode.

We may consider accepting NIDS if you explain that you can give the NIDS the server's private keys and let it actively intercept every connection.

Q3.3 (3 points) Malcode Y spreads by encrypting its binary, copying the encrypted binary and a decryption script to another machine, and executing the decryption script to run the malcode. The encryption key and the IV/nonce (if needed) are randomly generated each time the malcode replicates. Which encryption schemes would cause every copy of the malcode to look different? Cause every copy of the malcode to look different means that the encrypted copies of the malcode differ in at least 1 byte.

■ (A) AES-ECB
■ (B) AES-CBC
■ (C) AES-CTR
□ (D) None of the above
□ (E) ——
□ (F) ——

Solution: In all of these AES ciphers, the ciphertext looks different as long as the key is different each time.

Note that AES-ECB is deterministic with the same key, but changing the key still causes the ciphertext to look different.

Q3.4 (3 points) Malcode Z spreads the same way as Malcode Y. However, instead of randomly generating the encryption key and the IV/nonce (if needed), they are hard-coded into the binary and the decryption script. Which encryption schemes would cause every copy of the malcode to look different?

☐ (G) AES-ECB ☐ (I) AES-CTR ☐ (K) ——

☐ (H) AES-CBC ■ (J) None of the above ☐ (L) ——

Solution: A static key and IV means that the encrypted payload always remains the same.

Note that AES-CBC and AES-CTR are both deterministic if you use the same key and IV/nonce every time.