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) ——

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) ——

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) ——

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) ——

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) ——

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) ——

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

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

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) ——

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) ——

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) ——

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
☐ (H) AES-CBC
☐ (I) AES-CTR
☐ (J) None of the above
☐ (K) ——
☐ (L) ——