

Denial of Service, Firewalls, Intrusion Detection

Question 1

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 | ☐ (J) Specification based |
| ☐ (H) Behavior based | ☐ (K) — |
| ☐ (I) Anomaly based | ☐ (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 | ☐ (D) — |
| ☐ (B) System B | ☐ (E) — |
| ☐ (C) Not enough information | ☐ (F) — |

Question 2

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) —