

Q1 *Intrusion Detection Scenarios (SU21 Final Q8)*

(12 points)

For each scenario below, select the best detector or detection method for the attack.

Q1.1 (3 points) The attacker constructs a path traversal attack with URL escaping: %2e%2e%2f%2e%2e%2f.

- | | |
|--|---|
| <input type="radio"/> (A) NIDS, because of interpretation issues | <input type="radio"/> (D) HIDS, because of cost |
| <input type="radio"/> (B) NIDS, because of cost | <input type="radio"/> (E) — |
| <input type="radio"/> (C) HIDS, because of interpretation issues | <input type="radio"/> (F) — |

Q1.2 (3 points) The attacker is attacking a large network with hundreds of computers, and a detector must be installed as quickly as possible.

- | | |
|--|---|
| <input type="radio"/> (G) NIDS, because of interpretation issues | <input type="radio"/> (J) HIDS, because of cost |
| <input type="radio"/> (H) NIDS, because of cost | <input type="radio"/> (K) — |
| <input type="radio"/> (I) HIDS, because of interpretation issues | <input type="radio"/> (L) — |

Q1.3 (3 points) The attacker constructs an attack that is encrypted with HTTPS.

- | | |
|--|---|
| <input type="radio"/> (A) NIDS, because of interpretation issues | <input type="radio"/> (D) HIDS, because of cost |
| <input type="radio"/> (B) NIDS, because of cost | <input type="radio"/> (E) — |
| <input type="radio"/> (C) HIDS, because of interpretation issues | <input type="radio"/> (F) — |

Q1.4 (3 points) The attacker constructs a buffer overflow attack using shellcode they found online in a database of common attacks.

- | | |
|---|--------------------------------------|
| <input type="radio"/> (G) Signature-based | <input type="radio"/> (J) Behavioral |
| <input type="radio"/> (H) Specification-based | <input type="radio"/> (K) — |
| <input type="radio"/> (I) Anomaly-based | <input type="radio"/> (L) — |

Q2 Top-Secret Security

(14 points)

You are tasked with defending the network for Evanbot's secret server farm. All incoming network requests pass through a network-based intrusion detection system (NIDS), as well as a firewall. Outside users can only access the server with HTTPS.

Q2.1 (3 points) Which of these attacks are **always** preventable in this setup? Assume the attacker is on-path. Select all that apply.

- | | |
|---|--|
| <input type="checkbox"/> (A) RST Injection Attack | <input type="checkbox"/> (D) None of the Above |
| <input type="checkbox"/> (B) SQL Injection Attack | <input type="checkbox"/> (E) — |
| <input type="checkbox"/> (C) Reflected XSS Attack | <input type="checkbox"/> (F) — |

Q2.2 (3 points) Which of these attacks are **always** preventable in this setup? Assume the attacker is on-path. Select all that apply.

- | | |
|--|--|
| <input type="checkbox"/> (G) SYN Flooding Attack | <input type="checkbox"/> (J) None of the Above |
| <input type="checkbox"/> (H) DNS Spoofing Attack | <input type="checkbox"/> (K) — |
| <input type="checkbox"/> (I) DDoS Attack | <input type="checkbox"/> (L) — |

Q2.3 (3 points) An attacker injects malicious code on a server inside the headquarters that overwrites all text files with "Hello World". Which detection system is best suited to defend against this attacker?

- | | | |
|--------------------------------|------------------------------------|-----------------------------|
| <input type="radio"/> (A) HIDS | <input type="radio"/> (C) Firewall | <input type="radio"/> (E) — |
| <input type="radio"/> (B) NIDS | <input type="radio"/> (D) — | <input type="radio"/> (F) — |

Q2.4 (5 points) Ben, a computer scientist at the top-secret site, has a HIDS installed on his work laptop. He decides to sign into his personal email account, claiming that HTTPS will stop his employer (EvanBot) from seeing his emails. Is he correct? Justify your answer in 1–2 sentences.

- | | |
|-------------------------------|-----------------------------|
| <input type="radio"/> (G) Yes | <input type="radio"/> (J) — |
| <input type="radio"/> (H) No | <input type="radio"/> (K) — |
| <input type="radio"/> (I) — | <input type="radio"/> (L) — |