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`.

- ◯ (A) NIDS, because of interpretation issues
- ◯ (B) NIDS, because of cost
- ◯ (C) HIDS, because of interpretation issues
- ◯ (D) HIDS, because of cost
- ◯ (E) ——
- ◯ (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.

- ◯ (G) NIDS, because of interpretation issues
- ◯ (H) NIDS, because of cost
- ◯ (I) HIDS, because of interpretation issues
- ◯ (J) HIDS, because of cost
- ◯ (K) ——
- ◯ (L) ——

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

- ◯ (A) NIDS, because of interpretation issues
- ◯ (B) NIDS, because of cost
- ◯ (C) HIDS, because of interpretation issues
- ◯ (D) HIDS, because of cost
- ◯ (E) ——
- ◯ (F) ——

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

- ◯ (G) Signature-based
- ◯ (H) Specification-based
- ◯ (I) Anomaly-based
- ◯ (J) Behavioral
- ◯ (K) ——
- ◯ (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.

- ☐ (A) RST Injection Attack
- ☐ (B) SQL Injection Attack
- ☐ (C) Reflected XSS Attack
- ☐ (D) None of the Above
- ☐ (E) ——
- ☐ (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.

- ☐ (G) SYN Flooding Attack
- ☐ (H) DNS Spoofing Attack
- ☐ (I) DDoS Attack
- ☐ (J) None of the Above
- ☐ (K) ——
- ☐ (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?

- ◯ (A) HIDS
- ◯ (B) NIDS
- ◯ (C) Firewall
- ◯ (D) ——
- ◯ (E) ——
- ◯ (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.

- ◯ (G) Yes
- ◯ (H) No
- ◯ (I) ——
- ◯ (J) ——
- ◯ (K) ——
- ◯ (L) ——