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 *Election Security (SU20 Final Q8)* **(17 points)**

The 2020 elections are coming up, and the United States Government has tasked you with securing the nation's voting machines!

Assume election headquarters are in a top-secret, undisclosed site. 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 election headquarters that changes all submitted votes to one candidate. 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 protect the government from seeing his emails. Is he correct? Justify your answer in 1–2 sentences.

◯ (G) Yes

◯ (H) No

◯ (I) ——

◯ (J) ——

◯ (K) ——

◯ (L) ——

Q2.5 (3 points) You're discovered that an attacker has managed to connect to a service running inside our network from IP Address and is in the process of performing a DoS attack! Write a stateful firewall rule to block all traffic originating from the attacker. Our service is running on IP address (port 443).

Q3 *Suit of Armor Around the World (SP22 Final Q8)* **(16 points)**

You are tasked with securing The Avengers' internal network against potentially malicious protocols! For each type of firewall and set of traffic, state whether the firewall is able to achieve the desired functionality with perfect accuracy. **Assume that IP packets are never fragmented.** All connections that are not mentioned can be either allowed or denied.

If you answer Possible, briefly (in 3 sentences or less) how the firewall should operate to achieve the desired effect. If you answer False, provide a brief justification for why it isn't possible.

Q3.1 (4 points) **Desired Functionality:** Block all inbound TCP connections. Allow all outbound TCP connections.

Firewall: Stateless packet filter

○ Possible ○ Not possible

Q3.2 (4 points) **Desired Functionality:** Allow all outbound TLS connections. Block all outbound TCP connections that aren't running TLS.

Firewall: Stateful packet filter

○ Possible ○ Not possible

Q3.3 (4 points) **Desired Functionality:** Allow outbound DNS requests. Block inbound DNS responses. Assume that name servers always listen on port 53.

Firewall: Stateless packet filter

○ Possible ○ Not possible

Q3.4 (4 points) **Desired Functionality:** Block all HTTP traffic that contains the literal string **Ultron**. Allow all other HTTP traffic.

Firewall: TCP proxy

○ Possible ○ Not possible