

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 (D) HIDS, because of cost
 (B) NIDS, because of cost (E) —
 (C) HIDS, because of interpretation issues (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 (J) HIDS, because of cost
 (H) NIDS, because of cost (K) —
 (I) HIDS, because of interpretation issues (L) —

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

- (A) NIDS, because of interpretation issues (D) HIDS, because of cost
 (B) NIDS, because of cost (E) —
 (C) HIDS, because of interpretation issues (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 (J) Behavioral
 (H) Specification-based (K) —
 (I) Anomaly-based (L) —

Q2 Low-level Denial of Service

(0 points)

In this question, you will help Mallory develop new ways to conduct denial-of-service (DoS) attacks.

CHARGEN and ECHO are services provided by some UNIX servers. For every UDP packet arriving at port 19, CHARGEN sends back a packet with 0 to 512 random characters. For every UDP packet arriving at port 7, ECHO sends back a packet with the same content.

Mallory wants to perform a DoS attack on two servers. One with IP address *A* supports CHARGEN, and another with IP address *B* supports ECHO. Mallory can spoof IP addresses.

Q2.1 Is it possible to create a single UDP packet with no content which will cause both servers to consume a large amount of bandwidth?

- If yes, mark 'Possible' and fill in the fields below to create this packet.
- If no, mark 'Impossible' and explain within the provided lines.

Possible

Impossible

If possible, fill in the fields:

Source IP: _____ Destination IP: _____
Source port: _____ Destination port: _____

If impossible, why?

Q2.2 Assume now that CHARGEN and ECHO are now modified to only respond to TCP packets (post-handshake) and not UDP. Is it possible to create a single TCP SYN packet with no content which will cause both servers to consume a large amount of bandwidth? Assume Mallory is off-path from the two servers.

- If yes, mark 'Possible' and fill in the fields below to create this packet.
- If no, mark 'Impossible' and explain within the provided lines.

Possible

Impossible

If possible, fill in the fields:

Source IP: _____ Destination IP: _____
Source port: _____ Destination port: _____
Sequence #: _____ Ack #: N/A

If impossible, why?
