CS 161
Summer 2024

Introduction to Computer Security

Exam Prep 12

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) ——

Solution: This path traversal attack is masked using percent encoding in URLs. A traditional NIDS might not recognize this since it is specific to HTTP servers, so a HIDS would be the best option here in order ot avoid the interpretation issues of percent encoding.

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) ——

Solution: A major advantage of NIDS is that they can be quickly installed in order to cover an entire network. Because of the time constraints, the NIDS would be the best in order to mitigate the time cost.

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) ——

Solution: A NIDS is not able to decrypt data since it doesn't have the keys that are stored on the host. Thus, only the host can decrypt an interpret the requests, and a HIDS would be the best IDS to use here.

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) ——

Solution: This shellcode is easily obtainable and has not been modified, so a signature that matches the exact shellcode would be most effective in detecting this attack.

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: ___**B**___ Destination IP: ___**A**___
Source port: ___**7**___ Destination port: ___**19**___

If impossible, why?

____

____

Solution: Source IP: B, port: 7. Destination IP: A, port: 19. Source and destination can be flipped. Notice this will create a chain of CHARGEN and ECHO that will generate a lot of network traffic.

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?

____

____

Solution: Impossible. As seen in previous question, source/destination IP has to be B/A for the chain to work. If you send a SYN packet to A pretending to be B, A will send SYN-ACK to B, which won't respond since it never sent a SYN. The connection won't be established.