CS161 Spring 2026 — 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`.

- ○ NIDS, because of interpretation issues
- ○ NIDS, because of cost
- ● HIDS, because of interpretation issues
- ○ HIDS, because of cost

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.

- ○ NIDS, because of interpretation issues
- ● NIDS, because of cost
- ○ HIDS, because of interpretation issues
- ○ HIDS, because of cost

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.

This content is protected and may not be shared, uploaded, or distributed.

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

- ○ NIDS, because of interpretation issues
- ○ NIDS, because of cost
- ● HIDS, because of interpretation issues
- ○ HIDS, because of cost

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.

- ● Signature-based
- ○ Specification-based
- ○ Anomaly-based
- ○ Behavioral

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.

This content is protected and may not be shared, uploaded, or distributed.

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.

- ☐ RST Injection Attack
- ☐ Reflected XSS Attack
- ☐ SQL Injection Attack
- ■ None of the above

Solution:
- RST Injection Attack - HTTPS doesn't prevent RST Injection attacks, so they're still a potential vulnerability
- SQL Injection Attack - these attacks are generally application-layer (so transport-layer security and firewalls don't protect against them)
- Reflected XSS Attack - same reasoning as above. Additionally, even if NIDS were capable of detecting these over HTTP, it wouldn't be able to see any payloads under HTTPS.

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

- ■ SYN Flooding Attack
- ☐ DDoS Attack
- ☐ DNS Spoofing Attack
- ☐ None of the above

Solution:
- SYN Flooding Attack - these attacks are preventable using SYN Cookies!
- DNS Spoofing Attack - none of the defenses prevent DNS Spoofing
- DDoS Attack - not much a NIDS can do here, unfortunately

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?

- ● HIDS
- ○ NIDS
- ○ Firewall

Solution: Only a host-based system would be able to detect and/or prevent this attack from happening!

This content is protected and may not be shared, uploaded, or distributed.

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.

○ Yes ● No

Solution: Host-based intrusion detection systems are capable of reading data inbound/outbound HTTPS connections, so Ben's use of HTTPS doesn't really help him here.

We also accepted yes as an answer if it was justified by claiming he could use an email client that the HIDS didn't have access to.

This content is protected and may not be shared, uploaded, or distributed.