CS 161 Spring 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) ——

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 *Networking: A TORrible Mistake* **(7 points)**

Q2.1 (1 point) Assuming no malicious nodes collude, an n-node Tor circuit provides anonymity (i.e. no node learns who both the user and server are) when at least _____ node(s) are honest. Fill in the blank.

○ 0 ○ 1 ○ $n-1$ ○ n

For the next 3 subparts, a user is using Tor to send a message to a server. Assume that there is no collusion between any Tor nodes, and that the user choses exactly 3 nodes for their Tor circuit.

Q2.2 (1 point) Which values can a malicious **entry** node learn? Select all that apply.

☐ The IP address of the user ☐ The list of all nodes in the circuit

☐ The IP address of the server ☐ None of the above

Q2.3 (1 point) Which values can a malicious **exit** node learn? Select all that apply.

☐ The IP address of the user ☐ The list of all nodes in the circuit

☐ The IP address of the server ☐ None of the above

Q2.4 (1 point) Which values can an on-path attacker on the user's local network learn? Select all that apply.

☐ The IP address of the user ☐ The list of all nodes in the circuit

☐ The IP address of the server ☐ None of the above

When a new user first downloads Tor, they need to download a list of nodes from a trusted directory server.

A malicious, on-path attacker on the user's local network wishes to eavesdrop on the new user's Tor connection. Assume that the attacker controls 3 nodes out of 100 total Tor nodes, and can win any data race.

For the next three subparts, select the approximate probability that the attacker can learn the identity of the server.

Q2.5 (1 point) User connects to the directory via TLS, attacker is on-path.

○ Exactly 0% ○ Greater than 50%, less than 100%

○ Greater than 0%, less than 50% ○ Exactly 100%

Q2.6 (1 point) User connects to the directory via TCP, attacker is on-path.

○ Exactly 0% ○ Greater than 50%, less than 100%

○ Greater than 0%, less than 50% ○ Exactly 100%

Q2.7 (1 point) User connects to the directory via TCP, attacker is off-path.

- ○ Exactly 0%
- ○ Greater than 0%, less than 50%
- ○ Greater than 50%, less than 100%
- ○ Exactly 100%

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