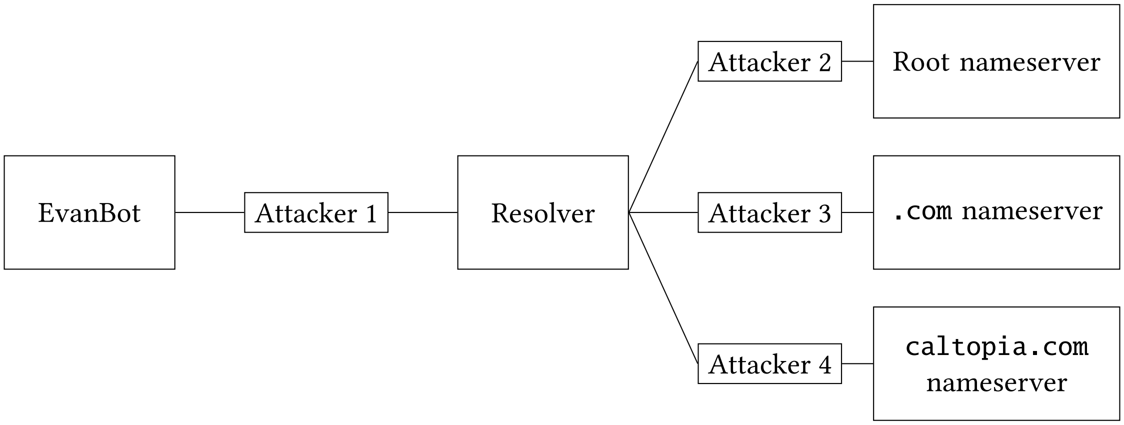
Weaver
Spring 2022

CS 161 Computer Security

Exam Prep 11

Q1 *Caltopia DNS* (21 points)

EvanBot is trying to determine the IP address of `caltopia.com` with DNS. However, some attackers on the network want to provide EvanBot with the wrong answer.



Assumptions:

- Each attacker is a man-in-the-middle (MITM) attacker between their two neighbors on the diagram above.
- No attackers can perform a Kaminsky attack.
- Standard DNS (not DNSSEC) is used unless otherwise stated.
- No private keys have been compromised unless otherwise stated.
- In each subpart, both EvanBot's cache and the local resolver's cache start empty.
- Each subpart is independent.

Clarification during exam: Assume that bailiwick checking is in use for this entire question.

In each subpart, EvanBot performs a DNS query for the address of `caltopia.com`.

Q1.1 (4 points) In this subpart only, assume the attackers only passively observe messages.

Which of the attackers would observe an `A` record with the IP address of `caltopia.com` as a result of EvanBot's query? Select all that apply.

□ (A) Attacker 1

□ (B) Attacker 2

□ (C) Attacker 3

□ (D) Attacker 4

□ (E) None of the above

□ (F) ——

Q1.2 (3 points) Which of the attackers can poison the local resolver's cached record for `cs161.org` by injecting a record into the additional section of the DNS response? Select all that apply.

Note: Attacker 1 has intentionally been left out as an answer choice.

□ (G) Attacker 2

□ (H) Attacker 3

□ (I) Attacker 4

□ (J) None of the above

□ (K) ——

□ (L) ——

Q1.3 (4 points) Assume that the resolver and the name servers all validate DNSSEC, but EvanBot does not validate DNSSEC. Which of the attackers can poison EvanBot's cached record for `caltopia.com` by modifying the DNS response? Select all that apply.

□ (A) Attacker 1

□ (B) Attacker 2

□ (C) Attacker 3

□ (D) Attacker 4

□ (E) None of the above

□ (F) ——

Q1.4 (5 points) In this subpart only, assume the attackers only passively observe messages.

Assume that everyone validates DNSSEC. Which of the following records would Attacker 3 observe as a result of EvanBot's query? Select all that apply.

□ (G) `DS` record with hash of the `.com` name server's public KSK

□ (H) `DS` record with hash of the `caltopia.com` name server's public KSK

□ (I) `A` record with the IP address of `caltopia.com`

□ (J) `A` record with the IP address of the `caltopia.com` name server

□ (K) `DNSKEY` record with the `.com` name server's public KSK

□ (L) None of the above

Q1.5 (3 points) Assume that everyone validates DNSSEC, and the `caltopia.com` name server's private KSK has been compromised (i.e. all attackers know the `caltopia.com` name server's private KSK). No other private keys have been compromised.

Can EvanBot trust that they received the correct IP address of `caltopia.com`?

○ (A) Yes, because the ZSK that signs the `A` record has not been compromised

○ (B) Yes, because the trust anchor (the root's KSK) has not been compromised

○ (C) No, because the compromised KSK can be used to sign a malicious `A` record

○ (D) No, because the compromised KSK can be used to sign a fake ZSK that is used to sign a malicious `A` record

○ (E) ——

○ (F) ——

Q1.6 (2 points) TRUE or FALSE: DNSSEC prevents Attacker 4 from learning the IP address of `caltopia.com`.

○ (G) True ○ (H) False ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Q2 *Intrusion Detection Scenarios* (12 points)

For each scenario below, select the best detector or detection method for the attack.

Q2.1 (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) ——

Q2.2 (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) ——

Q2.3 (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) ——

Q2.4 (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) ——

Q3 *Election Security* (23 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.

Q3.1 (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) ——

Q3.2 (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) ——

Q3.3 (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) ——

Q3.4 (3 points) An attacker realizes that the ballot boxes are running a vulnerable version of Linux, and uses a previously-known buffer overflow exploit. Which detection method is best suited to defend against this attacker?

○ (G) Anomaly-Based Detection

○ (H) Signature-Based Detection

○ (I) Specification-Based Detection

○ (J) Behavioral-Based Detection

○ (K) ——

○ (L) ——

Q3.5 (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.

○ (A) Yes

○ (B) No

○ (C) ——

○ (D) ——

○ (E) ——

○ (F) ——

Q3.6 (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).