CCA-AUX (5e802649)

2021-7-22 21:30:33

Exam Instructions

As shown in the example below, each test item has three parts: an optional scenario, a question (stem), and alternatives. For each test item, please answer the stem, evaluate the item, and optionally write a comment. If you believe there is a problem in the answer, report the issue using the report error button at the side. Thank you.

Question

How many centimeters in a meter?

A. 10
B. 100
C. 1000
D. 100,000
E. 1,000,000

Review

A-Accept

B-Accept w/ Minor Revisions

C-Accept w/ Major Revisions

D-Reject

Comments

Review

{{submitted_answers.text}}

{{submitted_answers.comments}}

CCA Question A3-1

When a user Mike O'Brien registered a new account for an online shopping site, he was required to provide his username, address, first and last name, and a password. Immediately after Mike submitted his request, you—as the security engineer—observe a database input error message in the logs.

Consider the following log file.

```
Time | Type| Message
-----------------------------------------------------------
11:58 INFO  GET  https://www.example.com/registerUser
11:59 INFO  GET  https://firewall.example.com/database
12:00 INFO  User Mike O'Brien at 123 Main Street with username test_user
12:01 INFO  Attempting to save test_user information
12:02 ERROR test_user could not be saved to the database.
```

Question. For the error message at 12:02 in the log file above, choose the potential vulnerability that warrants the most concern:

A. An eavesdropper may read unencrypted communications between Mike and the server.
B. Mike's input may cause the database to execute a malformed query.
C. There might be a hash collision between Mike's username and an administrator's username.
D. A misconfigured firewall might drop the database connection.
E. Someone might have already registered an account for test_user.

CCA Question C1-1

Bob's manager Alice is traveling abroad to give a sales presentation about an important new product. Bob receives an email from Alice requesting proprietary technical specifications for her presentation.

Consider the following email received by Bob:

Sender: Alice
Recipient: Bob
Subject: HELP, LOST LUGGAGE
Message:

Bob,

I just arrived and the airline lost my luggage with my laptop in it. Would you please send me the technical specifications?

Thanks,

Alice
Sales Manager - B123
ACME Corporation

Question. Choose the action Bob should take upon receiving Alice's message:

A. Initiate a mutual authentication protocol with the sender.
B. Do not reply to the message, and forward it to ACME's security officer.
C. Reply to the email attaching the technical specifications, encrypting them with Alice's public key, and signing the ciphertext with Bob's private key.
D. Create a one-time username and password to enable Alice to access the technical specifications, and text these credentials to her ACME-issued mobile device.
E. Sign into ACME's virtual private network and send the specifications to Alice through a secure tunnel.

CCA Question T4-1

You are responsible for monitoring an enterprise network that typically averages 200 Gbps of network traffic. The network comprises two segments: edge and core. The edge segment handles traffic flows from external sources; the core segment handles internal traffic, such as employee network activity. The network has two sensors each of which can inspect 15 Gbps of traffic on a single segment, leaving a gap of 170 Gbps. Each sensor is able to inspect all unencrypted traffic.

The core segment handles 10 Gbps, while the edge segment handles 190 Gbps. An external adversary is launching attacks against the edge segment.

Question. Choose the tactic that will most likely allow you to identify the adversary's traffic:

A. Direct all of the edge sensors to analyze traffic from untrusted sources.
B. Mark network traffic flows with their geographic source based on network routing to identify sources of the adversary.
C. Create a third segment with intentional vulnerabilities exposed to lure the adversary into an attack, while re-allocating some sensors to monitor this new segment.
D. Inspect random samples of network traffic to identify anomalous behavior.
E. Enhance the edge sensors with malware-detection software to identify the adversary's malicious programs; this enhancement reduces throughput to 12 Gbps.

Definitions

Gbps: Gigabits per second.

CCA Question Z3-1

A contractor asserts: "My company provides a system with a universal language in which, given specifications for any secure SCADA controller, generates a provably-secure implementation of the controller. Using our system will enhance the security of your hydroelectric dam."

Question. Choose the major fault in the contractor's assertion:

A. Formal proof systems do not handle the timing constraints required of SCADA dam controllers.
B. No language has the expressive power to implement all possible SCADA controllers.
C. It is impossible to specify any secure SCADA design.
D. A provably-secure SCADA controller cannot enhance the dam's security.
E. Proving the security of arbitrary secure SCADA controllers is undecidable.

Definitions

SCADA: Supervisory Control and Data Acquisition; a system of hardware and software that controls and monitors industrial processes.