IRAP ENTRY EXAMINATION – PRACTICE QUESTIONS

Australian Government

Department of Defence

IRAP Entry Examination – Practice Questions

The IRAP entry examination aims to assess your judgement, reasoning and ability to make recommendations for improving security. This will be based upon your knowledge of general information security principles, IRAP processes and procedures, and relevant Australian Government information security guidelines.

The IRAP entry examination comprises of both multiple choice and short answer questions. **There may be more than one correct answer to multiple choice questions**, so you must select all answers that apply in order to attain full marks for that question. In addition to this, it is acknowledged that there may be multiple correct solutions to a given short answer question, so you will be marked on your ability to adequately justify your response based on sound information security principles.

Practice Question 1 — 1 Mark

How can web services mitigate against SQL Injection?

Practice Question 2 — 1 Mark

Network segmentation and segregation can be achieved through:

A. The use of IPsec to filter ports requesting access to sensitive servers

B. Utilising jump servers for administration on the network

C. Implementing desktop virtualisation for environments allowing web browsing

D. Integrating publicly available Wi-Fi with the corporate domain

Practice Question 3 — 2 Marks

Describe how Sender Policy Framework (SPF) assists in preventing compromise of a system.

Practice Question 4 — 3 Marks

Outline the requirements of a cyber security incident register.

Practice Question 5

A government agency is investigating their options as to how to implement application whitelisting across their corporate network; currently they have no solution in place. You have been consulted to provide advice.

Part A — 2 Marks

Provide a recommendation as to how this agency should prioritise the rollout of application whitelisting.

Part B — 2 Marks

Compare the advantages and disadvantages of whitelisting applications based on file path or file hash.

irap

IRAP Entry Examination – Sample Answers

Please note that these sample answers provide only a rough indication of the types of responses that would be marked correct. It is acknowledged that multiple answers may exist, and will be marked accordingly provided appropriate justification is provided.

These answers should not provide an indication as to the depth or length of responses. Applicants are encouraged to provide as much detail as they see necessary in order to adequately express their desired answer.

Practice Question 1 – Sample Answer — 1 Mark

How can web services mitigate against SQL Injection?

By implementing prepared statements (or parameterised queries).

Practice Question 2 – Sample Answer — 1 Mark

Network segmentation and segregation can be achieved through:

A. The use of IPsec to filter ports requesting access to sensitive servers

B. Utilising jump servers for administration on the network

C. Implementing desktop virtualisation for environments allowing web browsing

D. Integrating publicly available Wi-Fi with the corporate domain

Solutions A, B and C are correct.

Practice Question 3 – Sample Answer — 2 Marks

Describe how Sender Policy Framework (SPF) assists in preventing compromise of a system.

SPF verifies that an email message originates from an email server that is authorised to send emails from that domain. SPF assists in blocking spam emails that use spoofed email addresses. Preventing these from reaching the end user reduces the potential for phishing attacks that could result in compromise of a system through the execution of malware.

Practice Question 4 – Sample Answer — 3 Marks

Outline the requirements of a cyber security incident register.

At a minimum, a cyber security incident register should include:

- *Date of incident discovery*
- *Date of incident occurrence*
- *Description of the incident*
- *Description of personnel and locations involved*
- *What actions were taken*
- *To whom the incident was reported*
- *A file reference*

Practice Question 5 – Sample Answer

A government agency is investigating their options as to how to implement application whitelisting across their corporate network; currently they have no solution in place. You have been consulted to provide advice.

Part A – Sample Answer **2 Marks**

Provide a recommendation as to how this agency should prioritise the rollout of application whitelisting.

It is advisable to deploy application whitelisting in stages. A good place to start after thorough testing may be on workstations used by senior executives and their assistants.

Agencies should prioritise application whitelisting on Most Likely Targets and on systems that pose the greatest risk, such as workstations with Internet connectivity.

Part B – Sample Answer **2 Marks**

Compare the advantages and disadvantages of whitelisting applications based on file path or file hash.

File path

- *A: Enables a more blanket coverage of apps that users may require access to*
- *D: Malware may trivially masquerade as legitimate software by executing from a whitelisted directory location*

File hash

- *A: Provides a greater degree of assurance that only authorised applications will run*
- *D: More restrictive; updates to applications will require updating of whitelisting rules*